kaspersky

# Kaspersky Security Center 15.3 Linux

© 2025 AO Kaspersky Lab

# 目次


Kaspersky Security Center Linux のヘルプ
新機能
Kaspersky Security Center Linux について
- 配布キット
- システム要件
  - 管理サーバーの要件
  - Web コンソールの要件
  - ネットワークエージェントの要件
- 互換性のあるカスペルスキーのアプリケーションとソリューション
- Kaspersky Security Center Linux のコンポーネントの互換性について
- Kaspersky Security Center の比較：Windows ベースと Linux ベース
- Kaspersky Security Center Cloud コンソールの概要

アーキテクチャと基本概念
- アーキテクチャ
- Kaspersky Security Center Linux 管理サーバーと Kaspersky Security Center Web コンソールの導入図
- Kaspersky Security Center Linux で使用するポート
- Kaspersky Security Center Web コンソールで使用されるポート
- 基本概念
  - 管理サーバー
  - 管理サーバーの階層構造
  - 仮想管理サーバー
  - Web サーバー
  - Kaspersky Security Center Linux Web サーバー
  - ネットワークエージェント
  - 管理グループ
  - 管理対象デバイス
  - 未割り当てデバイス
  - 管理コンピューター
  - Web 管理プラグイン
  - ポリシー
  - ポリシーのプロファイル
  - タスク
  - タスク範囲
  - ローカルアプリケーション設定とポリシーの関連付け
  - ディストリビューションポイント
  - 接続ゲートウェイ
  - 仮想管理サーバー

データトラフィックの流れと使用ポートの図解
- LAN 内に管理サーバーと管理対象デバイスがある構成
- プライマリ管理サーバーが LAN 内にありセカンダリ管理サーバーが 2 台ある構成
- 管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（リバースプロキシを使用）
- 管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（接続ゲートウェイを使用）
- 管理サーバーが DMZ 内にありインターネット経由で管理対象デバイスに接続している構成

Kaspersky Security Center Linux コンポーネントとセキュリティ製品の対話：詳細
対話スキームで使用される表記規則
管理サーバーと DBMS
管理サーバーとクライアントデバイス：セキュリティ製品の管理
クライアントデバイスにあるソフトウェアをディストリビューションポイント経由でアップグレードする
管理サーバーの階層構造：プライマリ管理サーバーとセカンダリ管理サーバー
DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造
ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス
DMZ に管理サーバーと 2 台のデバイス（接続ゲートウェイとクライアントデバイス）
管理サーバーと Kaspersky Security Center Web コンソール
使用の開始
ハードニングガイド
管理サーバーの導入
接続の安全性
アカウントおよび認証
管理サーバーの保護管理
クライアントデバイスの保護管理
管理対象アプリケーションの保護構成
管理サーバーのメンテナンス
サードパーティシステムへのイベント転送
サードパーティの情報システムに関するセキュリティ推奨事項
カスペルスキーセキュリティ製品の使用に関する推奨事項
シナリオ：MySQL サーバーの認証
シナリオ：PostgreSQL サーバーの認証
導入準備
Kaspersky Security Center Linux の設定の選択
標準設定：単一のオフィス
標準設定：各オフィスの管理者によって運用されている少数の大規模なオフィス
標準設定：複数の小規模なリモートオフィス
企業を保護する仕組みを選択する
保護システム導入の一般的なスキーム
DBMS の選択
管理サーバーへのインターネットアクセス
インターネットアクセス：ローカルネットワーク上の管理サーバー
インターネットアクセス：DMZ 内の管理サーバー
インストール
Kaspersky Security Center Linux と動作する MariaDB x64 サーバーの設定
Kaspersky Security Center Linux と動作する PostgreSQL または Postgres Pro サーバーの設定
Kaspersky Security Center Linux と動作する MySQL x64 サーバーの設定
Kaspersky Security Center Linux のインストール
Kaspersky Security Center Linux をサイレントモードでインストールする
閉鎖ソフトウェア環境モードでの Astra Linux への Kaspersky Security Center Linux のインストール
Kaspersky Security Center Web コンソールのインストール
Kaspersky Security Center Web コンソールのインストールパラメータ
閉鎖ソフトウェア環境モードでの Astra Linux への Kaspersky Security Center Web コンソールのインストール
Kaspersky Security Center Linux のフェールオーバークラスタの導入
シナリオ：Kaspersky Security Center Linux のフェールオーバークラスタの導入

Kaspersky Security Center Linux のフェールオーバークラスタについて
Kaspersky Security Center Linux のフェールオーバークラスタ用のファイルサーバーの準備
Kaspersky Security Center Linux のフェールオーバークラスタ用のノードの準備
Kaspersky Security Center Linux のフェールオーバークラスタノードへの Kaspersky Security Center Linux のインストール
Kaspersky Security Center Linux のフェールオーバークラスターノードにインストールされた管理サーバーに接続された Kaspersky Security Center Web コンソールのインストール
手動でのクラスターノードの開始と終了
DBMS に使用するアカウント
MySQL および MariaDB を使用するための DBMS アカウントの設定
PostgreSQL および Postgres Pro を使用するための DBMS アカウントの設定
MySQL または MariaDB DBMS で、共有テーブルスペースからテーブルごとのファイルテーブルスペースへデータを移動する
Kaspersky Security Center Linux を使用するための証明書
Kaspersky Security Center の証明書について
Kaspersky Security Center Linux で使用されるカスタム証明書の要件
Kaspersky Security Center Web コンソールの証明書の再発行
Kaspersky Security Center Web コンソールの証明書の置き換え
PFX 証明書を PEM 形式に変換する
シナリオ：管理サーバーのカスタム証明書の指定
klsetsrvcert ユーティリティを使用した管理サーバー証明書の置換
klmover ユーティリティを使用したネットワークエージェントの管理サーバーへの接続
Web サーバー証明書の再発行
共有フォルダーの定義
Kaspersky Security Center Web コンソールへのサインインとサインアウト
Kaspersky Security Center Web コンソールインターフェイス
Kaspersky Security Center Web コンソールインターフェースの言語の変更
Kaspersky Security Center Web コンソールのホームページの変更
ブックマークの追加と削除
クイックスタートウィザード
ステップ 1：インターネット接続設定の指定
ステップ 2：必要なアップデートのダウンロード
ステップ 3：保護する資産の選択
ステップ 4：ソリューションでの暗号化の選択
ステップ 5：管理対象製品のプラグインのインストールの設定
ステップ 6：配布パッケージのダウンロードとインストールパッケージの作成
ステップ 7：Kaspersky Security Network の設定
ステップ 8：アプリケーションのアクティベート方法の選択
ステップ 9：ステップ 9：サードパーティ製品のアップデート管理設定の指定
ステップ 10：基本的なネットワーク保護の設定情報の作成
ステップ 11：メール通知の設定
ステップ 12：クイックスタートウィザードの終了
製品導入ウィザード
ステップ 1：製品導入ウィザードの開始
ステップ 2：インストールパッケージの選択
ステップ 3：ライセンス情報ファイルまたはアクティベーションコードの配信方法の選択
ステップ 4：ネットワークエージェントのバージョンの選択

ステップ 5：デバイスの選択
ステップ 6：リモートインストールタスクの設定
ステップ 7：再起動の設定
ステップ 8：インストール前に競合アプリケーションを削除する
ステップ 9：管理対象デバイスへのデバイスの移動
ステップ 10：デバイスにアクセスするアカウントの選択
ステップ 11：インストールの開始
Kaspersky Security Center Linux のアップグレード
インストールファイルを使用した Kaspersky Security Center Linux のアップグレード
バックアップによる Kaspersky Security Center Linux のアップグレード
Kaspersky Security Center Linux のフェールオーバークラスタノードの Kaspersky Security Center Linux のアップグレード
Kaspersky Security Center Web コンソールのアップグレード
閉鎖ソフトウェア環境モードでの Astra Linux での Kaspersky Security Center Web コンソールのアップグレード
Kaspersky Security Center Linux への移行
管理サーバーのデータバックアップを使用した Kaspersky Security Center Linux への移行
移行ウィザードを使用した Kaspersky Security Center Linux への移行
Kaspersky Security Center Windows からのグループオブジェクトのエクスポート
エクスポートファイルを Kaspersky Security Center Linux にインポート
管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える
管理サーバーの設定
Kaspersky Security Center Web コンソールから管理サーバーへの接続の設定
管理サーバーへの暗号化された接続
Kaspersky Security Center Linux に接続するための IP アドレスの許可リストの設定
管理サーバーのインターネットアクセスを設定します
管理サーバーの階層構造
管理サーバーの階層の作成：セカンダリ管理サーバーの追加
セカンダリ管理サーバーのリストの表示
仮想管理サーバーの管理
仮想管理サーバーの作成
仮想管理サーバーの有効化および無効化
仮想管理サーバーへの管理者の割り当て
クライアントデバイスの管理サーバーの変更
仮想管理サーバーの削除
管理サーバーの接続イベントのログ記録の構成
イベントのリポジトリに保管できるイベントの最大数の設定
管理サーバーの別のデバイスへの移動
DBMS 資格情報の変更
管理サーバーデータのバックアップと復元
管理サーバーのデータバックアップタスクの作成
klbackup ユーティリティを使用したデータのバックアップとリカバリ
klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える
MySQL または MariaDB を使用する場合の管理サーバーデータのバックアップと復元
管理サーバーのメンテナンス
管理サーバーの階層の削除
パブリック DNS サーバーへのアクセス
インターフェイスの設定
管理サーバー接続用アドレスの設定

TLS による通信の暗号化
外部サービスとの相互対話のためのネットワーク設定
サブネットのグローバルリスト
klscmodchk および integrity_checker ユーティリティを使用してモジュールの整合性をチェックします
ネットワーク接続されたデバイスの検出
ネットワーク接続されたデバイスの検出シナリオ
Windows ネットワークのポーリング
IP アドレス範囲のポーリング
IP アドレス範囲の追加と変更
Zeroconf ポーリング
ドメインコントローラーのポーリング
認証とドメインコントローラーへの接続
Samba ドメインコントローラーの設定
機器のインベントリ
新しいデバイスに関する情報の追加
企業用デバイスの定義に使用する基準の設定
VDI 向け動的モードのクライアントデバイスでの使用
ネットワークエージェントインストールパッケージのプロパティでの VDI 向け動的モードの有効化
VDI から管理グループへのデバイスの移動
クライアントデバイスの管理
管理対象デバイスの設定
クライアントデバイスと管理サーバー間の接続の手動確認：Klnagchk ユーティリティ
デバイス移動ルール
デバイス移動ルールの作成
デバイス移動ルールのコピー
デバイス移動ルールの条件
デバイスを管理グループへ手動で追加
デバイスまたはクラスターを手動で管理グループに移動する
クラスターとサーバーアレイについて
クラスタまたはサーバーアレイのプロパティ
ディストリビューションポイントと接続ゲートウェイの調整
ディストリビューションポイントの概要
ディストリビューションポイントの標準設定：単一のオフィス
ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス
ディストリビューションポイントの数の計算と設定
ディストリビューションポイントの自動的な割り当て
ディストリビューションポイントの手動での割り当て
管理グループに割り当てられたディストリビューションポイントのリストの編集
プッシュサーバーの有効化
klnagent サービスのファイル記述子の上限を引き上げる
デバイスのステータスの概要
デバイスのステータスの切り替えの設定
デバイスの抽出
デバイスの抽出からデバイスリストを表示
デバイスの抽出の作成
デバイスの抽出の設定
デバイスの抽出からデバイスリストをエクスポート

抽出で管理グループからデバイスを削除
デバイスのタグ
デバイスタグの作成
デバイスタグの名前変更
デバイスタグの削除
タグを割り当てられているデバイスの表示
デバイスに割り当てられているタグの表示
デバイスへの手動でのタグ付け
デバイスに割り当てたタグの削除
デバイスの自動タグルールの表示
デバイスの自動タグルールの編集
デバイスの自動タグルールの作成
デバイスの自動タグルールの実行
デバイスの自動タグルールの削除
klscflag ユーティリティを使用したデバイスタグの管理
データ暗号化と保護機能
暗号化されたドライブのリストの表示
暗号化イベントのリストの表示
暗号化レポートの作成と表示
暗号化されたドライブへのオフラインモードでのアクセス権の付与
クライアントデバイスの管理サーバーの変更
複数の管理サーバー間での競合の回避
管理サーバーに接続されたデバイスを接続ゲートウェイ経由で別の管理サーバーに移動する
デバイスが不可視の時の処理の表示と設定
デバイスのユーザーへのメッセージの送信
クライアントデバイスのリモートでの起動、停止、再起動
管理対象デバイスへのリモートアクセス
Kaspersky Security Center Web コンソールを搭載した Linux ベースのデバイスから Linux ベースの管理対象デバイスへのリモートアクセス
Kaspersky Security Center Web コンソールを搭載した Linux ベースのデバイスから Windows ベースの管理対象デバイスへのリモートアクセス
Kaspersky Security Center Web コンソールを搭載した Windows ベースのデバイスから Linux ベースの管理対象デバイスへのリモートアクセス
Kaspersky Security Center Web コンソールを搭載した Windows ベースのデバイスから Windows ベースの管理対象デバイスへのリモートアクセス
モバイルデバイスの管理
Firebase Cloud Messaging の使用
公開鍵基盤との統合
管理グループの管理
管理グループの作成
管理グループ内のデバイスでのアプリケーションの自動インストール
管理グループの移動
管理グループの削除
カスペルスキー製品の導入
シナリオ：カスペルスキー製品の導入
カスペルスキー製品向けの管理プラグインの追加
インストールパッケージ
カスペルスキー製品のインストールパッケージのダウンロードおよび作成

ファイルからのインストールパッケージの作成
スタンドアロンインストールパッケージの作成
ネットワークエージェントのインストールパッケージ設定
Kaspersky Security Center Linux で作成された実行中のスタンドアロンパッケージ
スタンドアロンパッケージを使用したアプリケーションのインストール
セキュリティ製品のインストールパッケージで定義データベースをアップデートする
カスタムインストールパッケージのデータサイズの上限の変更
セカンダリ管理サーバーへのインストールパッケージの配布
スタンドアロンインストールパッケージのリストの表示
Linux 用のネットワークエージェントのインストール
Linux デバイスの準備と Linux デバイスへのネットワークエージェントのリモートインストール
ネットワークエージェントをインストールする SUSE Linux Enterprise Server 15 デバイスの準備
ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備します
OpenSSH バージョン 6.4 以前を使用するデバイスをネットワークエージェントのインストーラー用に準備する
Linux 用ネットワークエージェントのサイレントモードでのインストール（応答ファイルを使用）
対話モードでの Linux 用ネットワークエージェントのインストール
ネットワークエージェントをインストールしたデバイスでのファイルシステムロールバックのサポート
Windows 用のネットワークエージェントのインストール
Windows 用ネットワークエージェントをインタラクティブモードでインストールする
Windows 用ネットワークエージェントをサイレントモードでインストールする
デバイスのイメージの取得とコピーを使用した導入
ネットワークエージェントのディスククローンモード
ネットワークエージェントのインストールパラメータ
リモートインストールタスクを使用したアプリケーションのインストール
Kaspersky Security Center Linux でのリモートインストールタスクの概要
アプリケーションのリモートインストール
セカンダリ管理サーバーへのアプリケーションのインストール
ネットワークエージェントがインストールされたデバイスへのアプリケーションのリモートインストール
macOS デバイスへのアプリケーションのリモートインストール
リモートインストールタスクに含まれるデバイス再起動を管理する
Kaspersky Security Center Linux のリモートインストールタスクを使用した強制的な導入
サイレントモードでアプリケーションをインストールする
ネットワークエージェントのリモートインストール用の macOS デバイスの準備
仮想インフラストラクチャ
仮想マシンの負荷を軽減するヒント
動的仮想マシンのサポート
仮想マシンのコピーのサポート
Unix デバイスのリモートインストールを設定する
製品導入を監視する
カスペルスキー製品の起動および停止
サードパーティのセキュリティ製品からの移行とアンインストールの実施
アプリケーションまたはソフトウェアのアップデートのリモートでの削除
リモートインストールのための Windows デバイスの準備
スクリプトをリモートで実行タスクの作成
マニフェストファイルに基づいてインストールパッケージを作成する
スクリプトをリモートで実行タスク用のアーカイブを準備する

スクリプトをリモートで実行タスクを使用して、デバイスにアプリケーションをリモートでインストールする
スクリプトをリモートで実行するタスクの通知と監視を設定する
ライセンス管理
Kaspersky Security Center Linux のライセンス
使用許諾契約書について
ライセンスについて
ライセンス証書について
ライセンス情報について
プライバシーポリシーの表示
Kaspersky Security Center のライセンスオプション
ライセンス情報ファイルについて
データ提供について
定額制サービスについて
Kaspersky Security Center Linux のアクティベーション
管理されたカスペルスキー製品のライセンス
管理対象アプリケーションのライセンスの管理
ライセンスの管理サーバーリポジトリへの追加
ライセンスのクライアントデバイスへの配信
ライセンスの自動配信
使用中のライセンスに関する情報の表示
ライセンス制限超過のイベント
リポジトリからのライセンスの削除
使用許諾契約書による同意の取り消し
カスペルスキー製品のライセンスの更新
マーケットプレイスを使用してカスペルスキーの法人向けソリューションを選択する
カスペルスキー製品の設定
シナリオ：ネットワーク保護の設定
デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要
ポリシーの設定と継承先への反映：デバイスベースの管理
ポリシーの設定と継承先への反映：ユーザーベースの管理
ポリシーとポリシーのプロファイル
ポリシーとポリシープロファイルについて
「ロック」属性とロックされた設定の概要
ポリシーとポリシーのプロファイルの継承
ポリシーの階層
ポリシーの階層内のポリシープロファイル
管理対象デバイスに設定が実装される方法
ポリシーの管理
ポリシーのリストの表示
ポリシーの作成
ポリシーの全般的な設定
ポリシーの変更
ポリシー継承オプションの有効化と無効化
ポリシーのコピー
ポリシーの移動
ポリシーのエクスポート
ポリシーのインポート

強制同期
ポリシー導入ステータス図の表示
「ウイルスアウトブレイク」イベント発生時におけるポリシーの自動アクティブ化
ポリシーの削除
ポリシーのプロファイルの管理
ポリシーのプロファイルの表示
ポリシーのプロファイルの優先順位の変更
ポリシーのプロファイルの作成
ポリシーのプロファイルのコピー
ポリシーのプロファイルの有効化ルールの作成
ポリシーのプロファイルの削除
ネットワークエージェントのポリシー設定
Windows 用、Linux 用、macOS 用ネットワークエージェントの用途：比較
ネットワークエージェントの設定のオペレーティングシステム別の比較
ネットワークエージェントの低リソース消費モードの有効化と無効化
Kaspersky Endpoint Security ポリシーの手動セットアップ
Kaspersky Security Network の設定
ファイアウォールで保護されているネットワークのリストの確認
ネットワークドライブのスキャンをオフ
管理サーバーのメモリからのソフトウェアの詳細情報の除外
ワークステーションの Kaspersky Endpoint Security for Windows インターフェイスへのアクセスの設定
管理サーバー定義データベースへのポリシーイベントの登録の設定
Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ
Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ
Kaspersky Security Network（KSN）
KSN について
KSN へのアクセスの設定
KSN の使用の有効化と無効化
同意した KSN に関する声明の表示
更新された KSN に関する声明の同意
ディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかの確認
KSN プロキシサーバーの統計を表示
タスクの管理
タスクの概要
タスクの対象範囲
タスクの作成
タスクの手動での開始
選択したデバイスでのタスクの開始
タスクリストの表示
タスクの全般的な設定
タスクのエクスポート
タスクのインポート
タスクのパスワード変更ウィザードの起動
ステップ 1：資格情報の指定
ステップ 2：実行する処理の選択
ステップ 3：結果の表示
管理サーバーに保存されているタスク実行結果の確認

アプリケーションタグ
アプリケーションタグ
アプリケーションタグの作成
アプリケーションタグの名前変更
アプリケーションへのタグの割り当て
アプリケーションに割り当てたタグの削除
アプリケーションタグの削除
デバイスコントロールでブロックされた外部デバイスへのオフラインモードでのアクセス権の付与
klscflag を使用したポート 13291 の開放
Kaspersky Industrial CyberSecurity for Networks アプリケーションの Kaspersky Security Center Web コンソールでの登録
ユーザーとユーザーロールの管理
ユーザーアカウントについて
ユーザーロールの概要
製品機能のアクセス権の設定：ロールベースのアクセス制御
製品機能のアクセス権
事前定義のユーザーロール
特定のオブジェクトへのアクセス権の割り当て
ユーザーとセキュリティグループへのアクセス権の割り当て
内部ユーザーのアカウントの追加
セキュリティグループの作成
内部ユーザーのアカウントの編集
セキュリティグループの編集
ユーザーまたはセキュリティグループへのロールの割り当て
内部セキュリティグループへのユーザーアカウントの追加
デバイスの所有者ユーザーの指定
ネットワークエージェントのインストール中にユーザーをデバイスの所有者として割り当てる
ネットワークエージェントのインストール後にユーザーを Linux デバイスの所有者として割り当てる
デバイスの所有者ユーザーの削除
不正な変更からのユーザーアカウントの保護を有効にする
二段階認証
シナリオ：すべてのユーザーに対して二段階認証を設定する
アカウントの二段階認証について
自分のアカウントの二段階認証を有効にする
全ユーザーに対して二段階認証の有効化
ユーザーアカウントの二段階認証を無効にする
全ユーザーに対して二段階認証の無効化
二段階認証からアカウントを除外する
自分のアカウントの二段階認証を設定します
新規ユーザーが自分で二段階認証を設定することを禁止します
新しい秘密鍵の作成
セキュリティコードの発行元の名前を変更する
許可されるパスワード入力試行回数の変更
ユーザーとセキュリティグループの削除
ユーザーアカウントのパスワードを変更する
ユーザーロールの作成
ユーザーロールの編集
各ユーザーロールの対象範囲の編集

ユーザーロールの削除
ポリシーのプロファイルとロールの関連付け
セカンダリ管理サーバーにユーザーロールを反映させるには
アカウントパスワードの変更
ローカル管理者権限の取り消し
定義データベースとカスペルスキー製品のアップデート
シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート
定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要
「管理サーバーのリポジトリへのアップデートのダウンロード」タスクの作成
ダウンロードされたアップデートの検証
「ディストリビューションポイントのリポジトリにアップデートをダウンロード」タスクの作成
「管理サーバーのリポジトリへのアップデートのダウンロード」タスクに対するアップデート元の追加
ソフトウェアアップデートの拒否と承認
Kaspersky Endpoint Security for Windows のアップデートの自動インストール
カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用
差分ファイルのダウンロード機能の有効化
ディストリビューションポイントによるアップデートのダウンロード
オフラインデバイスの定義データベースとソフトウェアモジュールのアップデート
Web プラグインのバックアップと復元
監視、レポート、監査
シナリオ：監視とレポート
監視機能とレポート機能の種別の概要
スマートトレーニングモードでのルールの適用条件
アダプティブアノマリーコントロールルールを使用して実行された検知の表示と確認
アダプティブアノマリーコントロールルールから除外に追加
ダッシュボードとウィジェット
ダッシュボードの使用
ダッシュボードへのウィジェットの追加
ダッシュボードでウィジェットを非表示にする操作
ダッシュボードでのウィジェットの移動
ウィジェットのサイズと表示形式の変更
ウィジェットの設定の変更
ダッシュボードのみモードについて
ダッシュボードのみモードの設定
レポート
レポートの使用
レポートテンプレートの作成
レポートテンプレートのプロパティの表示と編集
レポートのファイルへのエクスポート
レポートの生成と表示
レポート配信タスクの作成
レポートテンプレートの削除
イベントとイベントの抽出
Kaspersky Security Center Linux のイベントについて
Kaspersky Security Center Linux のコンポーネントでのイベント
イベント種別のデータ構造の説明
管理サーバーのイベント

管理サーバーの緊急イベント
管理サーバーの機能エラーイベント
管理サーバーの警告イベント
管理サーバーの情報イベント
ネットワークエージェントのイベント
ネットワークエージェントの機能エラーイベント
ネットワークエージェントの警告イベント
ネットワークエージェントの情報イベント
イベントの抽出の使用
イベントの抽出の作成
イベントの抽出の編集
イベントの抽出のリストの表示
イベントの抽出のエクスポート
イベントの抽出のインポート
イベントの詳細の表示
イベントのファイルへのエクスポート
イベントに含まれるオブジェクトの履歴の表示
イベントの削除
イベントの抽出の削除
イベントの保管期間の設定
頻出イベントのブロック
頻出イベントのブロックについて
頻出イベントのブロックの管理
頻出イベントのブロックの解除
管理サーバーでのイベントの処理と保管
通知とデバイスのステータス
通知機能の使用
画面表示による通知の確認
デバイスのステータスの概要
デバイスのステータスの切り替えの設定
通知の設定
テストの通知
実行ファイルの起動により表示されるイベント通知
カスペルスキーからの通知
カスペルスキーからの通知について
カスペルスキーからの通知を設定する
カスペルスキーからの通知を無効にする
脅威の検知に関する情報の表示
Cloud Discovery
ウィジェットを使用して Cloud Discovery を有効にする
Cloud Discovery ウィジェットをダッシュボードに追加する
クラウドサービスの使用情報を確認する
クラウドサービスのリスクレベル
不要なクラウドサービスへのアクセスをブロックする
SIEM システムへのイベントのエクスポート
SIEM システムへのイベントのエクスポートの設定
事前準備

イベントのエクスポートについて
SIEM システムでのイベントのエクスポートの設定について
Syslog 形式で SIEM システムにエクスポートするイベントのマーキング
Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング
Syslog 形式でエクスポートする一般的なイベントのマーキング
Syslog 形式を使用したイベントのエクスポートについて
イベントを SIEM システムにエクスポートするための Kaspersky Security Center Linux の設定
データベースからのイベントの直接エクスポート
klsql2 ユーティリティを使用した SQL クエリの作成
klsql2 ユーティリティでの SQL クエリの例
Kaspersky Security Center Linux データベース名の表示
エクスポート結果の表示
オブジェクトリビジョンの管理
ポリシーレビジョンの表示と保存
以前のリビジョンへのオブジェクトのロールバック
オブジェクトの削除
隔離とバックアップからのファイルのダウンロードと削除
隔離とバックアップからのファイルのダウンロード
隔離、バックアップ、またはアクティブな脅威リポジトリからのオブジェクトの削除について
Kaspersky Security Center Web コンソールとその他のカスペルスキー製品の連携
バックグラウンド接続の確立
クライアントデバイスのリモート診断
リモート診断ウィンドウを開く
アプリケーションのトレースの有効化と無効化
アプリケーションのトレースファイルのダウンロード
トレースファイルの削除
アプリケーション設定のダウンロード
クライアントデバイスからシステム情報のダウンロード
イベントログのダウンロード
アプリケーションの起動、停止、再起動
Kaspersky Security Center Linux ネットワークエージェントのリモート診断を実行し、結果をダウンロードする
クライアントデバイスでのアプリケーションの実行
Linux ベースのクライアントデバイスでのリモート診断の実行
クライアントデバイス上のサードパーティ製品と実行ファイルの管理
アプリケーションコントロールを使用して実行ファイルを管理する
クライアントデバイス上の実行ファイルのリストの取得と表示
コンテンツが手動で追加されるアプリケーションカテゴリの作成
選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成
選択したフォルダーの実行ファイルを含むアプリケーションカテゴリの作成
アプリケーションカテゴリのリストの表示
イベントに関連する実行ファイルのアプリケーションカテゴリへの追加
Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定
クライアントデバイスにインストールされているアプリケーションのリストの取得と表示
サードパーティ製品について
サードパーティ製ソフトウェアのアップデートのインストール
シナリオ：サードパーティ製ソフトウェアのアップデート
サードパーティのソフトウェアアップデートのインストールオプション

脆弱性とアプリケーションのアップデートの検索タスクの設定
「脆弱性とアプリケーションのアップデートの検索」タスクの作成
サードパーティ製品の使用可能なアップデートに関する情報の表示
使用可能なソフトウェアアップデートのリストのファイルへのエクスポート
サードパーティ製ソフトウェアのアップデートの拒否と承認
「アップデートのインストールと脆弱性の修正」タスクの作成
アップデートインストールのルールの追加
タスク作成後に指定された、アップデートのインストールと脆弱性の修正タスクの設定
サードパーティ製品の自動アップデート
サードパーティ製ソフトウェアの脆弱性の修正
ソフトウェアの脆弱性の検知と修正
シナリオ：サードパーティ製ソフトウェアの脆弱性の検知と修正
サードパーティ製ソフトウェアの脆弱性の修正
脆弱性の修正タスクの作成
サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択
管理対象デバイスで検知されたすべてのソフトウェア脆弱性に関する情報の表示
指定した管理対象デバイスで検知されたソフトウェア脆弱性に関する情報の表示
管理対象デバイス上の脆弱性に関する統計情報の表示
ソフトウェア脆弱性のリストのファイルへのエクスポート
検知されたソフトウェアの脆弱性への非対応の判断
定義データベースからのサードパーティ製品のインストールパッケージの作成
定義データベースからのサードパーティ製品のインストールパッケージの設定に関する表示と変更
定義データベースからのサードパーティ製品のインストールパッケージの設定
隔離されたネットワークでの脆弱性の修正
シナリオ：分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正
分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正について
分離されたネットワークで脆弱性を修正するためのインターネットにアクセス可能な管理サーバーの構成
分離されたネットワークの脆弱性を修正するための分離された管理サーバーの設定
分離されたネットワークでのパッチの送信とアップデートのインストール
分離されたネットワークでのパッチの送信とアップデートのインストールを無効にする
API リファレンスガイド
導入と設定に関する推奨事項
Kaspersky Security Center Linux の導入を計画する
管理サーバーへのインターネットアクセス
Kaspersky Security Center Linux の標準設定
ディストリビューションポイントの概要
管理サーバーの階層構造
仮想管理サーバー
導入と初期セットアップ
管理サーバーのインストールに関する推奨事項
フェールオーバークラスターに管理サーバーサービス用のアカウントを作成する
DBMS の選択
管理サーバーのアドレスの指定
ネットワークエージェントとセキュリティ製品の導入
クライアント組織のネットワークでの保護の設定
Kaspersky Endpoint Security ポリシーの手動セットアップ
「先進の脅威対策」セクションでのポリシーの設定

「脅威対策」セクションでのポリシーの設定
「全般設定」セクションでのポリシーの設定
「イベントの設定」セクションでのポリシーの設定
Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ
Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ
「脆弱性とアプリケーションのアップデートの検索」タスクのスケジュール設定
アップデートのインストールと脆弱性の修正用グループタスクの手動セットアップ
管理グループの構造の構築とディストリビューションポイントの割り当て
MSP クライアントの標準設定：単一のオフィス
MSP クライアントの標準設定：複数の小規模なリモートオフィス
ポリシーのプロファイルを使用した、ポリシーの階層
ポリシーの階層
ポリシーのプロファイル
タスク
デバイス移動ルール
ソフトウェアのカテゴリ分け
管理サーバーの設定のバックアップと復元
管理サーバーがインストールされているデバイスを操作できない
管理サーバーまたはデータベースの設定が破損している
モバイルユーザー用の接続プロファイルの概要
管理対象デバイスへのリモートアクセス
「管理サーバーから切断しない」オプションを使用して、管理対象デバイスと管理サーバー間の継続的な接続を提供する
デバイスと管理サーバー間の接続時間の確認について
強制同期について
サイジングガイド
このガイドの概要
管理サーバーの計算
管理サーバーのハードウェアリソースの計算
DBMS および管理サーバーのハードウェア要件
データベースの容量の計算
ディスク容量の計算
管理サーバーの数と構成の算出
動的仮想マシンを Kaspersky Security Center に接続する際の推奨事項
ディストリビューションポイントと接続ゲートウェイの計算
ディストリビューションポイントの要件
ディストリビューションポイントの数の計算と設定
接続ゲートウェイの数の計算
タスクおよびポリシーのイベントに関する情報の記録
多数のデバイスを管理する管理サーバーのベストプラクティス
タスクごとの考慮事項と最適な設定
デバイスの検索の頻度
管理サーバーデータのバックアップタスクとデータベースのメンテナンスタスク
Kaspersky Endpoint Security をアップデートするグループタスク
インベントリタスク
管理サーバーと保護されるデバイスとの間のネットワーク負荷に関する詳細情報
様々なシナリオでのトラフィック

24 時間あたりの平均トラフィック
既知の問題
テクニカルサポートへの問い合わせ
テクニカルサポートのご利用方法
カスペルスキーカンパニーアカウントによるテクニカルサポート
管理サーバーのダンプファイルの取得
製品の情報源
用語解説
Cloud Discovery
HTTPS
iOS MDM サーバー
iOS MDM デバイス
JavaScript
Kaspersky Private Security Network（KPSN）
Kaspersky Security Center Linux Web サーバー
Kaspersky Security Center Linux 管理者
Kaspersky Security Center オペレーター
Kaspersky Security Center システム正常性検証ツール（SHV）
Network Location Awareness（NLA）
SSL
アップデート
アプリケーションの一元管理
アプリケーションの直接管理
アプリストア
アンチウイルスサービスプロバイダー
イベントの重要度
イベントリポジトリ
インストールパッケージ
ウイルスアウトブレイク
カスペルスキーのアップデートサーバー
仮想管理サーバー
管理グループ
管理コンソール
管理コンピューター
管理サーバー
管理サーバークライアント（クライアントデバイス）
管理サーバー証明書
管理サーバーデータのバックアップ
管理サーバーデータの復元
管理者権限
管理対象デバイス
共有証明書
クライアント管理者
グループタスク
軽量ナジェント（LWNGT）
現在のライセンス
互換性がないアプリケーション

サービスプロバイダーの管理者
手動インストール
脆弱性
接続ゲートウェイ
設定プロファイル
タスク
タスク設定
追加（または予備）ライセンス
定義データベース
ディストリビューションポイント
適用可能なアップデート
デバイスの所有者
特定のデバイスに対するタスク
内部ユーザー
認証エージェント
ネットワークエージェント
ネットワークのアンチウイルスによる保護
ネットワーク保護ステータス
バックアップフォルダー
パッチの重要度
非武装地帯（DMZ）
復元
ブロードキャストドメイン
プログラム設定
プロビジョニングプロファイル
プロファイル
ホーム管理サーバー
保護ステータス
ポリシー
ライセンス情報ファイル
ライセンスの有効期間
リモートインストール
ローカルインストール
ローカルタスク
ロールグループ
サードパーティ製のコードに関する情報
商標に関する通知

# Kaspersky Security Center Linux のヘルプ

## 新機能

- 新機能

## システム要件

- 管理サーバーの要件
- Web コンソールの要件
- ネットワークエージェントの要件

## はじめに

- インストール
- クイックスタートウィザード
- 製品導入ウィザード

## ライセンス管理とアクティベーション

- Kaspersky Security Center Linux のアクティベーション
- 管理対象アプリケーションのライセンスの管理

## 導入と設定

- ネットワーク接続されたデバイスの検出
- ディストリビューションポイントと接続ゲートウェイの調整
- サードパーティのセキュリティ製品からの移行とアンインストールの実施
- カスペルスキー製品：一元管理による導入

- ネットワーク保護の設定
- カスペルスキー製品：定義データベースとソフトウェアモジュールのアップデート
- 管理サーバー接続用アドレスの設定
- Kaspersky Security Center Linux への移行
- Kaspersky Security Center Linux のアップグレードについて

## 監視

- 監視とレポート
- Cloud Discovery

## クライアントデバイスの管理

- 管理対象デバイスへのリモートアクセス

## 脆弱性とパッチ管理

- サードパーティ製ソフトウェアの脆弱性の検知と修正

## 追加機能

- SIEM システムへのイベントのエクスポート
- KSN プロキシサーバーの統計を表示
- サイジングガイド（オンラインヘルプのみ）

# 新機能

## Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux にはいくつかの新機能と機能強化が追加されています：

- klcsngtgui ユーティリティは、Kaspersky Security Center Linux 配布キットから削除されました。klcsngtgui ユーティリティの代わりに klnagchk ユーティリティを使用することを推奨します。
- ネットワークエージェントは、次の新しいオペレーティングシステムバージョンでの動作をサポートするようになりました：
  - Windows Server 2025
  - Fedora Linux サーバー 41
  - Fedora Linux ワークステーション 41
- Kaspersky Security Center Linux が、次の DBMS の使用をサポートするようになりました：
  - PostgreSQL 17
  - Postgres Pro 17
- Kaspersky Update Utility を使用して、カスペルスキーのセキュリティ製品の定義データベースとソフトウェアモジュールの必要なアップデートのみをダウンロードできるようになりました。［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスクのプロパティウィンドウで［**アップデートリクエストファイルを自動でダウンロードする**］オプションを有効にして、Kaspersky Security Center Linux がダウンロードするアップデートに関する情報を含むアップデートリクエストファイルを作成するパスを指定します。
- KSN プロキシサーバーの使用統計を表示できるようになりました。
- klbackup ユーティリティを使用して Kaspersky Security Center Windows 管理サーバーのデータを Kaspersky Security Center Linux に移行する方法がアップデートされました。これで、Microsoft SQL Server データベースに保存されている管理サーバーデータを PostgreSQL または Postgres Pro に移行できるようになりました。
- 管理サーバーの接続アドレスを構成できるようになりました。管理サーバーの接続アドレスは、ネットワークエージェントのインストールパッケージを作成する時の既定のトアドレスとして使用され、管理対象デバイスを KSN に接続する時の KSN プロキシサーバーアドレスとして使用されます。
- 管理対象デバイスを集中的に再起動できるようになりました。
- Linux 管理対象デバイスに現在ログインしているユーザーに関する情報が、デバイスプロパティウィンドウの［**全般**］→［**セッション**］セクションに表示されるようになりました。
- これらのデバイスにインストールされたネットワークエージェントを通じて、Linux および Windows 管理対象デバイスへのリモートアクセスを取得できるようになりました。接続は、RDP、VNC、または WDS を使用して確立されます。デバイスとの接続を確立すると、管理者はそのデバイスに保存されている情報へのフルアクセス権を取得できます。そのため、そのデバイスにインストールされているアプリケーションを管理することが可能です。

- 管理対象デバイスで診断用のアプリケーション（またはスクリプト）をアップロードして実行します。実行ファイルを含むディレクトリまたはアーカイブ、あるいは実行ファイル自体をアップロードできるようになりました。アプリケーションが正常に実行されたら、実行結果をダウンロードできます。

- 新しい［**クイックリンク**］セクションを含む、ユーザーエクスペリエンスの改善。このセクションにはメインメニューマップが表示され、Kaspersky Security Center Web コンソールのすべてのセクションにすばやくアクセスできます。既定では、［**クイックリンク**］がホームページとして設定されています。

## Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux にはいくつかの新機能と機能強化が追加されています：

- 内部ユーザーアカウントのパスワードを管理するための新機能：

  - 初回または次回 Kaspersky Security Center Web コンソールにサインインしようとした時に、内部ユーザーにパスワードの変更を強制することができるようになりました。

  - 内部ユーザーアカウントのパスワードの有効期限を設定する新しいオプションが利用できるようになりました。

- klbackup ユーティリティを使用することで、Kaspersky Security Center Windows 管理サーバーのデータをバックアップして Kaspersky Security Center Linux に復元できるようになりました。同じ種類の DBMS 間、または Microsoft SQL Server から MySQL または MariaDB 間で、データを損失することなく移行できます。

- Kaspersky Security Center Linux が、次の DBMS の使用をサポートするようになりました：

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux は、一部の種類の PostgreSQL および Postgres Pro クラスタをサポートするようになりました。

- OS MES（Moscow Electronic School）、MosTech、MosTech Server の新しいバージョンを含む、新しいオペレーティングシステムと新しいオペレーティングシステムのバージョンをサポートしています。

- 以下を含むユーザーエクスペリエンスの向上：

  - ポリシー設定ウィンドウに新しいボタン［**保存**］が追加されました。ポリシー設定ウィンドウを閉じずに変更を保存する場合は、このボタンを使用します。

- Kaspersky Mobile Devices Protection and Management プラグインの新しい［アプリとファイル］セクションで、Android デバイスへのファイル送信を管理したり、以前に送信したファイルを削除したり、設定を構成できるようになりました。

- 接続ゲートウェイ上の新しい Web サーバーサービスを使用して、管理サーバーに直接接続しなくても、アプリのインストールパッケージとデバイス管理プロファイルをモバイルデバイスに転送できるようになりました。

## Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux にはいくつかの新機能と機能強化が追加されています：

- Kaspersky Security Center Web コンソールは、Kaspersky Mobile Devices Protection および Management プラグインを介してモバイルデバイス管理をサポートするようになりました。
- iOS MDM サーバーをインストールして構成できるようになりました iOS MDM サーバー設定プラグインを介して iOS MDM デバイスを管理します。
- モバイルデバイスの証明書を管理できるようになりました。
- Kaspersky Endpoint Security for Android がサポートされるようになりました。
- Kaspersky Security for iOS がサポートされるようになりました。
- Kaspersky Endpoint Security for Aurora がサポートされるようになりました。
- Windows ベースの管理対象デバイスの脆弱性とパッチ管理。Windows ベースの管理対象デバイスにインストールされているサードパーティ製ソフトウェアのアップデートを管理し、必要なアップデートをインストールしてソフトウェアの脆弱性の修正ができます。
- Kaspersky Security Center Linux は、ドメインコントローラー全体を一度にポーリングするのではなく、ページごとにドメインコントローラーをポーリングするようになりました。これにより、多数のエントリを含むドメインコントローラーをポーリングできるようになります。
- アダプティブアノマリーコントロール。これは、一連のルールを使用してクライアントデバイス上の異常な動作を追跡し、異常なアクションをブロックできる Kaspersky Endpoint Security for Windows の機能です。
- Windows デバイスおよび Linux 用ネットワークエージェントにインストールされた管理対象カスペルスキー製品をシームレスにアップデートします。インストールする必要があるアップデートプログラムを承認し、インストールしてはならないアップデートプログラムを拒否することで、アップデートプログラムのインストールプロセスを管理できます。
- 拡張ポリシー監査。ポリシーリビジョンの内容を表示し、ポリシーリビジョンをファイルに保存できるようになりました。現在、これらの機能は管理サーバーポリシーとネットワークエージェントポリシーでのみ使用できます。
- Cloud Discovery。この機能を使用すると、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と判断されるクラウドサービスへのアクセスをブロックできます。
- メインメニューの［**監視とレポート**］セクションにある新しい［**アラート**］サブセクション。［**アラート**］サブセクションには、エンドポイントデバイスで検知された脅威に関する情報が表示されます。脅威はカスペルスキーセキュリティ製品によって検知されます。
- Kaspersky Security Center Linux は、Kaspersky Managed Detection and Response ソリューションの一部として機能できるようになりました。
- Support for Kaspersky Security for Virtualization Light Agent。
- macOS デバイスのハードウェアインベントリを拡張しました。macOS デバイス上のネットワークエージェントは、MAC アドレスとデバイスのシリアル番号を管理サーバーに送信します。
- カスタムスクリプトを使用して管理対象デバイスにソフトウェアをインストールする時に、リモートインストールに関するレポートを受信できるようになりました。

- 管理対象デバイス上で複数のカスタムスクリプトを実行する場合、各スクリプトの優先順位を設定して実行順序を定義できます。スクリプトは、優先度が最も高いものから最も低いものの順に実行されます。

- Kaspersky Endpoint Security for Linux および Linux 用ネットワークエージェントによって消費される RAM の量を削減するには、Linux 用ネットワークエージェントの特別な動作モードを有効にします。このモードでは、Network Agent for Linux に必要な RAM は少なくなりますが、機能は制限されます。

- *アプリケーションのリモートアンインストールタスク*を使用して、管理対象デバイスから互換性のないソフトウェアをアンインストールできます。

- ネットワーク攻撃のレポート、攻撃デバイスの MAC アドレスとポートが含まれるようになりました。

- 内部ユーザーのパスワードの最大長が 256 文字に引き上げられました。

- 以下を含むユーザーエクスペリエンスの向上：

  - Kaspersky Security Center Web コンソールの各セクションをブックマークに追加し、［**ブックマーク**］セクションから素早くアクセスできるようにすることで、メインメニューをパーソナライズできます。

  - テーブルでの作業を最適化しました。各テーブルの既定のビューには、最も頻繁に使用される列が含まれるようになりました。また、現在のページまたはテーブル全体のすべての項目を選択したり、テーブル全体の項目を並べ替えたりできるようになりました。

  - レポート配信の設定が改善されました。レポートを送信する最大 20 個のメールアドレスとレポート配信スケジュールを指定できるようになりました。

- 幅広いオペレーティングシステムと新しいオペレーティングシステムバージョンがサポートされました。

- 新しいサイジングガイドが開発され、オンラインヘルプに公開されました。

- ユーザーインターフェイスのレビューの結果、管理サーバーのプロパティウィンドウに［**リモート診断**］セクションが表示される問題が解決されました。

- クライアントデバイス上でインストールパッケージを実行し、アプリケーションをリモートでインストールするための*スクリプトをリモートで実行*タスクを作成できます。

- Linux 上のクライアントデバイスにネットワークエージェントをインストールする際、またはインストール後に、ユーザーをデバイスの所有者として割り当てることができます。

- デバイスの所有者、セキュリティグループでのデバイスの所有者のメンバーシップ、およびデバイスの所有者のロールに基づいてデバイスの抽出を設定したり、デバイス移動ルールを作成したりできます。

- アカウントからローカル管理者権限を取り消すことができます。これにより、ユーザーアカウントをさらに細かく制御できるようになります。たとえば、1回限りの割り当ての完了後、ローカル管理者の権限を取り消すことができます。

- たとえば、ユーザーがローカルアカウントのパスワードを忘れた場合や、定期的なパスワードの変更を実行する場合に、ローカルアカウントのパスワードを変更できます。

- ［**ユーザー証明書の管理**］サブセクションでは、インストールするルート証明書を指定できます。これらの証明書は、たとえば、Web サイトまたは Web サーバーの信頼性を検証するために使用できます。

# Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux にはいくつかの新機能と機能強化が追加されています：

- ドメインコントローラーポーリングを使用すると、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーをポーリングできます。管理サーバーまたはディストリビューションポイントを使用して、Microsoft Active Directory をポーリングできます。Samba ドメインコントローラーは、Linux ベースのディストリビューションポイントを介してのみポーリングできます。ドメインコントローラーをポーリングすると、管理サーバーまたはディストリビューションポイントは、ドメイン構造、ユーザーアカウント、セキュリティ グループ、およびドメインに含まれるデバイスの DNS 名に関する情報を取得します。

- Kaspersky Security Center Linux が、次の DBMS の使用をサポートするようになりました：

  - PostgreSQL 15.x

  - Postgres Pro 15.x

- PostgreSQL または Postgres Pro を DBMS として使用する場合、Kaspersky Security Center Linux は最大 50,000 台の管理対象デバイスをサポートします。

- Kaspersky Security Center Windows から Kaspersky Security Center Linux への移行。ウィザードを実行して、タスク、ポリシー、管理グループ構造などの Kaspersky Security Center オブジェクトを移行できます。その後、インポートした管理対象デバイスを Kaspersky Security Center Linux の管理下に移動できます。

- Kaspersky Security Center Linux が、次のカスペルスキー製品の使用をサポートするようになりました：

  - Kaspersky Security for Virtualization Light Agent

  - Kaspersky Embedded Systems Security for Windows

  - Kaspersky Embedded Systems Security for Linux

  - Kaspersky Industrial CyberSecurity for Nodes

  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security for Mac

  - Kaspersky Endpoint Agent

  - Kaspersky Security for Virtualization Light Agent

- Windows ベースおよび Linux ベースの管理対象デバイスのリモート診断。

- アプリケーションコントロールコンポーネントが改善されました。選択したフォルダーの実行ファイルのリストに基づいて、またはカスペルスキー製品カテゴリに基づいて製品カテゴリを作成できるようになりました。その後、組織内で作成したカテゴリのアプリケーションを許可するかブロックするかを指定できます。

- イベントの抽出のエクスポートとインポート。ユーザー定義のイベントの抽出とその設定を KLO ファイルにエクスポートし、保存されたイベントの抽出を Kaspersky Security Center Windows または Kaspersky Security Center Linux にインポートできます。

- ［脅威レポート］で、［**アラートの表示**］リンクをクリックして脅威の活動連鎖を開くことができるようになりました。

- Kaspersky Security Center Linux がクラスタ技術をサポートするようになりました。管理グループにクラスタまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］ページには 2 つのタブが表示されます。1 つは個々のデバイス用で、もう 1 つはクラスタおよびサーバーアレイ用です。管理対象デバイスがクラスタノードとして検出されると、クラスタは個別のオブジェクトとして［**クラスターとサーバーアレイ**］タブに追加されます。クラスタノードは、他の管理対象デバイスとともに［**デバイス**］タブに一覧表示されます。

- Kaspersky Security Center Linux による一部のプラットフォームのサポートは、ベンダーによるサポートが終了したため終了しました。

## Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux にはいくつかの新機能と機能強化が追加されています：

- 管理サーバー階層では、Linux ベースの管理サーバーがプライマリサーバーとして機能し、セカンダリサーバーとして機能する Linux ベースまたは Windows ベースのサーバーを管理できるようになりました。

- Kaspersky Security Center Linux が、 Kaspersky Security Network（KSN）、 KSN プロキシサービス、および Kaspersky Private Security Network（KPSN）をサポートするようになりました。

- Kaspersky Security Center Linux が、管理対象アプリケーションとして Kaspersky Endpoint Security for Windows をサポートするようになりました。

  クライアントデバイスでの Windows 用ネットワークエージェントのリモートインストールは、Windows ベースのディストリビューションポイントを通じてオペレーティングシステムツールを使用することによってのみ可能です。

- Windows ベースの管理対象デバイス上のデータを暗号化して、ノート PC やハードドライブが盗難または紛失した場合に機密データや企業データが意図せず漏洩するリスクを軽減できるようになりました。この機能は、Kaspersky Endpoint Security for Windows を使用して実装されます。

- Kaspersky Security Center Linux では、Kaspersky Security Center Linux のユーザーインターフェイス内で、カスペルスキー製品の配布パッケージと Web 管理プラグインの両方をダウンロードしてアップデートできます。

- 既定では、Linux ベースおよび Windows ベースの管理対象デバイスにインストールされたアプリケーションに関する情報が管理サーバーに送信されます。

- カスペルスキーのサーバーへのアクセスが自動的に検証されるようになりました。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS を使用します。

- プライマリ管理サーバー、セカンダリ管理サーバー、およびネットワークエージェントの間で転送される機密データが AES 暗号化アルゴリズムで保護されるようになりました。

- 仮想管理サーバーのユーザー権限を、プライマリ管理サーバーから独立していつでも設定できます。また、プライマリサーバーユーザーに仮想サーバーを管理する権限を割り当てることもできます。

- Kaspersky Security Center Linux が、次の DBMS の使用をサポートするようになりました：

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（すべてのエディション）
  - Postgres Pro 14.x（すべてのエディション）

- Kaspersky Security Center Web コンソールを使用してファイルにポリシーとタスクをエクスポートしてから、ポリシーとタスクを Kaspersky Security Center Windows または Kaspersky Security Center Linux にインポートできます。

- ［**プロキシサーバーを使用しない**］が次のタスクから削除されました：

  - *管理サーバーのリポジトリへのアップデートのダウンロード*

  - *ディストリビューションポイントのリポジトリにアップデートをダウンロード*

## Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux にはいくつかの新機能と機能強化が追加されています：

- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクに加え、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを使用することでもカスペルスキーのセキュリティ製品の定義データベースをダウンロードできるようになりました。

- 管理対象デバイスの定義データベースと製品モジュールは、管理サーバーまたはディストリビューションポイントから反映およびアップデートが可能です。組織に最適なアップデートスキームを選択することで、管理サーバーの負荷を軽減して企業ネットワークのデータトラフィックを最適化することができます。

- カスペルスキーのセキュリティ製品からアップデートの要求があったときのみ、Kaspersky Security Center Linux はカスペルスキーのアップデートサーバーからダウンロードします。これによりダウンロードされるデータのサイズを抑えることができます。

- 定義データベースおよびソフトウェアモジュールのダウンロードに差分ファイルのダウンロード機能を使用することができるようになりました。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を軽減できます。

- *アップデートの検証*タスクが追加されました。このタスクを使用すると、管理対象デバイスにアップデートを実際にインストールする前に、ダウンロードされたアップデートの操作性やエラーを自動的に検証することができます。

- Kaspersky Security Center Linux が Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 を管理対象アプリケーションとしてサポートするようになりました。

# Kaspersky Security Center Linux について

このセクションでは、Kaspersky Security Center Linux の目的、主な機能と構成要素、および Kaspersky Security Center Linux の購入方法について説明します。

Kaspersky Security Center Linux（「Kaspersky Security Center」とも表記）を使用して、Linux ベースの管理サーバーを使用したクライアントデバイスの保護機能を導入および管理できます。

Kaspersky Security Center Linux を使用して、カスペルスキーのセキュリティ製品を企業ネットワーク内にあるデバイスにインストールして、リモートからスキャンやアップデートタスクを実行したり、管理対象デバイスのセキュリティポリシーを管理したりできます。管理者として、企業デバイスのステータスのスナップショット、詳細なレポート、保護ポリシーの詳細な設定などを表示するダッシュボードを使用できます。

Windows® ベースの管理サーバーを持つ Kaspersky Security Center と、Kaspersky Security Center Linux とは機能セットが異なります。

Kaspersky Security Center Linux は、組織内でデバイスの保護を担当する企業ネットワーク管理者および従業員を対象としています。

Kaspersky Security Center を使用して、次のことが実現できます：

- 管理サーバーの階層を作成して、組織内、リモートオフィス内、クライアント組織内のネットワークを管理する。

  *クライアント組織*とは、サービスプロバイダーからアンチウイルスによる保護の提供を受ける組織です。

- 管理グループの階層を作成して、いくつかのクライアントデバイスを1つの単位として管理する。
- カスペルスキー製品をベースに構築されたアンチウイルスによる保護システムを管理する。
- カスペルスキーまたはその他のソフトウェアベンダーの製品のリモートインストールを実行する。
- カスペルスキー製品のライセンスをクライアントデバイスへ一元的に配信し、使用状況を監視したり、ライセンスを更新したりする。
- アプリケーションやデバイスの動作に関する統計情報とレポートを受信する。
- カスペルスキー製品の動作中に発生した緊急イベントに関する通知を受信する。
- Windows ベースのデバイスのハードディスクとリムーバブルドライブに保存されている情報の暗号化を管理します。
- Windows ベースのデバイス上の暗号化されたデータへのユーザーアクセスを管理します。
- 組織のネットワークに接続されたハードウェアのインベントリを作成する。
- セキュリティ製品により隔離またはバックアップに移動されたファイルや、セキュリティ製品による処理が延期されたファイルを一元管理する。

Kaspersky Security Center Linux は、カスペルスキー（例：https://www.kaspersky.co.jp）またはパートナー会社を通じて購入することができます。

カスペルスキーから Kaspersky Security Center Linux を購入した場合は、当社のウェブサイトからアプリケーションをコピーすることができます。アプリケーションのアクティベーションに必要な情報は、支払い手続き完了後にメールで送信されます。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

# 配布キット

製品は、販売代理店（http://www.kaspersky.co.jp）から購入できます。

パートナーにお問い合わせいただくか、本件の販売を支援するパートナーをお調べください。アクティベーションに必要な情報は、購入時に入手可能です。

# システム要件

- 管理サーバーの要件
- Web コンソールの要件
- ネットワークエージェントの要件

## 管理サーバーの要件

ハードウェアの最小要件：

- CPU：動作周波数が 2.5 GHz以上、2 コア
- メモリ：6 GB
- 使用可能なディスク容量：管理サーバーのデータが保存されるフォルダー（/var/opt/kaspersky/klnagent_srv）に 10 GB 必要

次のオペレーティングシステムがサポートされています：

- Debian GNU/Linux 11.x（Bullseye）64 ビット
- Debian GNU/Linux 12（Bookworm）64 ビット
- Ubuntu Server 22.04 LTS（Jammy Jellyfish）64 ビット
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 ビット
- CentOS ストリーム 9 64 ビット

- Red Hat Enterprise Linux Server 7.x 64 ビット
- Red Hat Enterprise Linux Server 8.x 64 ビット
- Red Hat Enterprise Linux Server 9.x 64 ビット
- SUSE Linux Enterprise Server 12（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.6）64 ビット
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）64 ビット
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.8）64 ビット
- Astra Linux Special Edition RUSB.10015-16（リリース 1、運用アップデート 1.6）64 ビット
- Astra Linux Special Edition RUSB.10015-17（運用アップデート 1.7.3）64 ビット
- Astra Linux Special Edition RUSB.10015-03（運用アップデート 7.6）64 ビット
- Astra Linux Special Edition RUSB.10015-37（運用アップデート 7.7）64 ビット
- Astra Linux Common Edition（運用アップデート 2.12）64 ビット
- ALT SP Server 10 64 ビット
- ALT 8 SP Server（LKNV.11100-01）64 ビット
- ALT 8 SP Server（LKNV.11100-02）64 ビット
- ALT 8 SP Server（LKNV.11100-03）64 ビット
- ALT SP Workstation 10 64 ビット
- Oracle Linux 7 64 ビット
- Oracle Linux 8 64 ビット
- Oracle Linux 9 64 ビット
- Platform V SberLinux OS Server (SLO) 8.9.2 64 ビット
- RED OS 7.3 Server 64 ビット
- RED OS 7.3 Certified Edition 64 ビット
- RED OS 8 64 ビット
- ROSA COBALT 7.9 64 ビット
- M OS (Moscow Electronic School) 12 Server 64-bit

- Mostech Server 64 ビット
- MosOS 15.4 Arbat 64 ビット

EXT4 ファイルシステムを既定の設定で使用することを推奨します。

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7.0
- VMware vSphere 7.0.3
- Microsoft Hyper-V Server 2019 64 ビット
- Microsoft Hyper-V Server 2022 64 ビット
- Citrix XenServer 7.x
- Citrix XenServer 8.2
- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- カーネルベースの仮想マシン（管理サーバーでサポートされているすべての Linux オペレーティングシステム）

以下のデータベースサーバーがサポートされます（異なるデバイスにインストール可能）：

- MySQL 5.7 Community 32 ビット / 64 ビット
- MySQL Standard Edition 8.0（リリース 8.0.20 以降）32 ビット / 64 ビット
- MySQL Enterprise Edition 8.0（リリース 8.0.20 以降）32 ビット / 64 ビット
- MariaDB 10.1（ビルド 10.1.30 以降）32 ビット / 64 ビット
- MariaDB 10.3（ビルド 10.3.22 以降）32 ビット / 64 ビット
- MariaDB 10.4（ビルド 10.4.20 以降）32 ビット / 64 ビット
- MariaDB 10.5（ビルド 10.5.27 以降）32 ビット / 64 ビット
- MariaDB 10.6（ビルド 10.6.20 以降）32 ビット / 64 ビット
- MariaDB 10.11（ビルド 10.11.10 以降）32 ビット / 64 ビット
- MariaDB Galera Cluster 10.3 32 ビット / 64 ビット（InnoDB ストレージエンジンを使用）
- PostgreSQL 13.x 64 ビット
- PostgreSQL 14.x 64 ビット
- PostgreSQL 15.x 64 ビット

- PostgreSQL 15.x 64 ビット（クラスタ Corosync/Pacemaker）
- PostgreSQL 16.x 64 ビット
- PostgreSQL 17 64 ビット
- Postgres Pro 13.x 64 ビット（すべてのエディション）
- Postgres Pro 14.x 64 ビット（すべてのエディション）
- Postgres Pro 15.x 64 ビット（すべてのエディション）
- Postgres Pro 15.x 64 ビット（クラスタ Corosync/Pacemaker）
- Postgres Pro 16.x 64 ビット（すべてのエディション）
- Postgres Pro 16.x Enterprise 64 ビット（クラスタ組み込みの高可用性）
- Postgres Pro 17 64 ビット（すべてのエディション）
- Postgres Pro 17 Enterprise 64 ビット（クラスタ組み込みの高可用性）
- Platform V Pangolin 5.4.0 64 ビット
- Jatoba 4 64 ビット

高可用性の PostgreSQL クラスタがサポートされています。サーバーが DBMS にアクセスするために使用する Postgres ロールには、次のビューを読み取る権限が必要です （既定で有効）：

- pg_stat_replication
- pg_stat_wal_receiver

# Web コンソールの要件

## Kaspersky Security Center Web コンソールサーバー

ハードウェアの最小要件：

- CPU：4 コア、動作周波数が 2.5 GHz
- メモリ：8 GB
- 使用可能なディスク容量：管理サーバーのデータが保存されるフォルダー（/var/opt/kaspersky）に 40 GB 必要

次のいずれかのオペレーティングシステム（64 ビット版のみ）：

- Debian GNU/Linux 11.x （Bullseye）
- Debian GNU/Linux 12（Bookworm）
- Ubuntu Server 22.04 LTS（Jammy Jellyfish）

- Ubuntu Server 24.04 LTS (Noble Numbat)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- SUSE Linux Enterprise Server 12（すべての Service Pack）
- SUSE Linux Enterprise Server 15（すべての Service Pack）
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.6）
- Astra Linux Special Edition RUSB.10015-16（リリース 1、運用アップデート 1.6）
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）
- Astra Linux Special Edition RUSB.10015-17（運用アップデート 1.7.3）
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.8）
- Astra Linux Special Edition RUSB.10015-03（運用アップデート 7.6）
- Astra Linux Special Edition RUSB.10015-37（運用アップデート 7.7）
- Astra Linux Common Edition（運用アップデート 2.12）
- ALT SP Server 10
- ALT 8 SP Server（LKNV.11100-01）
- ALT 8 SP Server（LKNV.11100-02）
- ALT 8 SP Server（LKNV.11100-03）
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.9.2
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9

- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.4 Arbat

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7.0
- VMware vSphere 7.0.3
- Citrix XenServer 7.x
- Citrix XenServer 8.2
- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- Microsoft Hyper-V Server 2019
- Microsoft Hyper-V Server 2022
- カーネルベースの仮想マシン（Kaspersky Security Center Web コンソールサーバーでサポートされるすべての Linux オペレーティングシステム）

## クライアントデバイス

クライアントデバイス側で Kaspersky Security Center Web コンソールを使用するために必要なのはブラウザーのみです。

最小画面解像度は 1366x768 ピクセルです。

デバイスのハードウェアおよびソフトウェア要件は、Kaspersky Security Center Web コンソールの操作で使用するブラウザーと同じです。

ブラウザー：

- Google Chrome 133.0.6943.53 以降
- Microsoft Edge 134.0.3124.66 以降
- macOS の Safari 17.6
- Yandex Browser 25.2.3.809 以降
- Mozilla Firefox Extended Support Release 128.8.0 以降

# ネットワークエージェントの要件

ハードウェアの最小要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：512 MB
- 使用可能なディスク容量：1 GB

Linux ベースのデバイスのソフトウェア要件：Perl 言語インタープリターのバージョン 5.10 以降をインストールする必要があります。

**ネットワークエージェント。サポートされているプラットフォーム**

| | |
|---|---|
| オペレーティングシステム：<br>Microsoft Windows ワークステーション | Microsoft Windows Embedded POSReady 2009（最新の Service Pack）32 ビット<br>Microsoft Windows Embedded 7 Standard（Service Pack 1）32 ビット / 64 ビット<br>Microsoft Windows Embedded 8.1 Industry Pro 32 ビット / 64 ビット<br>Microsoft Windows 10 Enterprise 2015 LTSB 32 ビット / 64 ビット<br>Microsoft Windows 10 Enterprise 2016 LTSB 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 ビット / 64 ビット<br>Microsoft Windows 10 Enterprise 2019 LTSC 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise バージョン 1703、1709、1803、1809、32 ビット / 64 ビット<br>Microsoft Windows 10 20H2、21H2 IoT Enterprise 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise バージョン 1909 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise LTSC 2021 32 ビット / 64 ビット<br>Microsoft Windows 10 IoT Enterprise バージョン 1607 32 ビット / 64 ビット<br>Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット<br>Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット<br>Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット<br>Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット<br>Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット<br>Microsoft Windows 10 19H1、19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット<br>Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット<br>Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット<br>Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット<br>Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット<br>Microsoft Windows 8.1 Pro/Enterprise 32 ビット / 64 ビット<br>Microsoft Windows 8 Pro/Enterprise 32 ビット / 64 ビット<br>Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium （Service Pack 1 以降）32 ビット / 64 ビット<br>Microsoft Windows XP Professional（Service Pack 2）32 ビット / 64 ビット（ネットワークエージェントのバージョン 10.5.1781 のみ対応）<br>Microsoft Windows XP Professional Service Pack 3 以降 32 ビット（ネットワークエージェントバージョン 14.0.0.20023 でサポート）<br>Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 ビット（ネットワークエージェントバージョン 14.0.0.20023 でサポート） |
| オペレーティングシステム：<br>Microsoft Windows サーバー | Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 ビット<br>Microsoft Windows Server 2003 SP1 32 ビット / 64 ビット（ネットワークエージェントバージョン 10.5.1781 でのみサポートされます。テクニカルサポートを通じてリクエストできます）<br>Microsoft Windows Server 2003 SP2 Standard/Enterprise 32 ビット / 64 ビット（ネットワークエージェントバージョン 10.5.1781 でのみサポート） |

| | |
|---|---|
| | Microsoft Windows Server 2003 R2 Standard/Enterprise（SP2 32 ビット / 64 ビット）（ネットワークエージェントバージョン 10.5.1781 でのみサポート）<br>Microsoft Windows Server 2008 Foundation Service Pack 2 32 ビット / 64 ビット<br>Microsoft Windows Server 2008 Standard/Enterprise/Datacenter （Service Pack 2）32 ビット / 64 ビット<br>Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard with Service Pack 1 以降 64 ビット<br>Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 ビット<br>Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 ビット<br>Microsoft Windows Server 2016 Datacenter/Standard/Server Core (Installation Option) (LTSB) 64 ビット<br>Microsoft Windows Server 2019 Standard/Datacenter/Core 64 ビット<br>Microsoft Windows Server 2019 RS5 Essentials/Standard 64 ビット<br>Microsoft Windows Server 2022 Standard/Datacenter/Core 64 ビット<br>Microsoft Windows Server 2025 Standard/Datacenter/Core 64 ビット<br>Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 ビット<br>Microsoft Windows Storage Server 2019 64 ビット<br>Microsoft Windows Small Business Server 2011 Standard 64 ビット<br>Microsoft Windows Small Business Server 2011 Essentials 64 ビット<br>Microsoft Windows Small Business Server 2011 Premium Add-on 64 ビット |

| | |
|---|---|
| オペレーティングシステム：<br>Linux | Debian GNU / Linux 10.x（Buster）32 ビット / 64 ビット<br>Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット<br>Debian GNU/Linux 12（Bookworm）32 ビット/64 ビット<br>Ubuntu Server 10.04 LTS（Lucid Lynx）32 ビット / 64 ビット<br>Ubuntu Server 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット<br>Ubuntu Server 18.04 LTS（Bionic Beaver）64 ビット<br>Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット<br>Ubuntu Server 22.04 LTS（Jammy Jellyfish）64 ビット<br>Ubuntu Server 22.04 LTS ARM 64 ビット<br>Ubuntu Server 24.04 LTS (Noble Numbat) 64 ビット<br>Ubuntu Desktop 10.04 LTS（Lucid Lynx）32 ビット / 64 ビット<br>Ubuntu Desktop 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット<br>CentOS 6.x 32 ビット / 64 ビット<br>CentOS 7.2 以降 64 ビット<br>CentOS ストリーム 8 64 ビット<br>CentOS ストリーム 9 64 ビット<br>CentOS ストリーム 9 ARM 64 ビット<br>Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット<br>Red Hat Enterprise Linux Server 7.2 以降 64 ビット<br>Red Hat Enterprise Linux Server 8.x 64 ビット<br>Red Hat Enterprise Linux Server 9.x 64 ビット<br>SUSE Linux Enterprise Server 12.5 以降（すべての Service Pack）64 ビット<br>SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット<br>SUSE Linux Enterprise Server 15（すべての Service Pack）ARM 64 ビット<br>openSUSE Leap 15 64 ビット<br>EulerOS 2.0 SP10 64 ビット<br>EulerOS 2.0 SP10 ARM 64 ビット<br>Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.5）64 ビット<br>Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.6）64 ビット<br>Astra Linux Special Edition RUSB.10015-16（リリース 1、運用アップデート 1.6）64 ビット<br>Astra Linux Special Edition RUSB.10015-17（運用アップデート 1.7.3）64 ビット<br>Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）64 ビット<br>Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.8）64 ビット<br>Astra Linux Special Edition RUSB.10015-03（運用アップデート 7.6）64 ビット<br>Astra Linux Special Edition RUSB.10015-37（運用アップデート 7.7）64 ビット<br>Astra Linux Special Edition RUSB.10152-02（運用アップデート 4.7）ARM 64 ビット<br>Astra Linux Common Edition（運用アップデート 2.12）64 ビット<br>ALT Workstation 10.1 64 ビット<br>ALT Server 10.1 64 ビット<br>ALT Education 10.1 64 ビット<br>ALT SP Server 10 32 ビット / 64 ビット<br>ALT SP Server 10 ARM 64 ビット<br>ALT SP Workstation 10 32 ビット / 64 ビット<br>ALT SP Workstation 10 ARM 64 ビット<br>ALT 8 SP Server（LKNV.11100-01）32 ビット / 64 ビット<br>ALT 8 SP Server（LKNV.11100-02）32 ビット / 64 ビット<br>ALT 8 SP Server（LKNV.11100-03）32 ビット / 64 ビット<br>ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット<br>ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット<br>ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット<br>Mageia 4 32 ビット<br>Oracle Linux 7 64 ビット<br>Oracle Linux 8 64 ビット<br>Oracle Linux 9 64 ビット<br>Linux Mint 20.3 以降 64 ビット<br>Linux Mint 21.1 以降 64 ビット |

| | |
|---|---|
| | Linux Mint 22.x 64 ビット<br>AlterOS 7.5 以降 64 ビット<br>GosLinux IC6/7.17 64 ビット<br>GosLinux IC6/7.2 64 ビット<br>SberOS 3.3.3 64 ビット<br>Platform V SberLinux OS Server (SLO) 8.8 64 ビット<br>Platform V SberLinux OS Server (SLO) 8.9.2 64 ビット<br>RED OS 7.3 ARM 64 ビット<br>RED OS 7.3 Server 64 ビット<br>RED OS 7.3 Certified Edition 64 ビット<br>RED OS 8 64 ビット<br>RED OS 8 ARM 64 ビット<br>ROSA Enterprise Linux Server 7.9 64 ビット<br>ROSA Enterprise Linux Desktop 7.9 64 ビット<br>ROSA COBALT 7.9 64 ビット<br>ROSA CHROME 12 64 ビット<br>AlmaLinux 8 以降 64 ビット<br>AlmaLinux 9 以降 64 ビット<br>Rocky Linux 8 以降 64 ビット<br>Rocky Linux 9 以降 64 ビット<br>Atlant、Alcyone ビルド、バージョン 2022.02 64 ビット<br>MSVSPHERE 9.2 SERVER 64 ビット<br>MSVSPHERE 9.2 ARM 64 ビット<br>MSVSPHERE 9.4 SERVER 64 ビット<br>MSVSPHERE 9.4 ARM 64 ビット<br>SynthesisM Server 8.6 64 ビット<br>SynthesisM Client 8.6 64 ビット<br>OSnova 2.* 64 ビット<br>Kylin 10 64 ビット<br>EMIAS 1.0 64 ビット<br>Amazon Linux 2 64 ビット<br>MosOS 15.4 Arbat 64 ビット<br>OS MES（Moscow Electronic School）12（コンピューターおよびラップトップ用）64 ビット<br>OS MES（Moscow Electronic School）12（インタラクティブパネル用）64 ビット<br>M OS (Moscow Electronic School) 12 Server 64-bit<br>Mostech 64 ビット<br>Mostech Server 64 ビット<br>Fedora Linux Server 41 64 ビット<br>Fedora Linux Workstation 41 64 ビット |
| オペレーティングシステム：macOS | サポートされているオペレーティングシステムのリストは、Kaspersky Endpoint Security for Mac のヘルプを参照してください。 |
| 仮想化プラットフォーム | VMware vSphere 6.7.0<br>VMware vSphere 7.0.3<br>Citrix XenServer 7.x<br>Citrix XenServer 8.2<br>Parallels Desktop 18<br>Oracle VM VirtualBox 7.0.12<br>Microsoft Hyper-V Server 2019 64 ビット<br>Microsoft Hyper-V Server 2022 64 ビット<br>カーネルベースの仮想マシン（ネットワークエージェントによってサポートされるすべての Linux オペレーティングシステム）<br>サポートされている他のプラットフォームについては、管理対象アプリケーションの要件を参照してください。 |

Windows 10 RS4 または Windows 10 RS5 を使用しているデバイスでは、大文字と小文字の区別が有効にな

っているフォルダーにおいて、一部の脆弱性を Kaspersky Security Center が検知できない可能性があります。

Windows 7、Windows Server 2008、Windows Server 2008 R2、または Windows MultiPoint Server 2011 を実行しているデバイスにネットワークエージェントをインストールする前に、Windows 用セキュリティ更新プログラム KB3063858（Windows 7 用セキュリティ更新プログラム (KB3063858)、Windows 7 for x64-Based Systems 用セキュリティ更新プログラム (KB3063858)、Windows Server 2008 用セキュリティ更新プログラム (KB3063858)、Windows Server 2008 x64 Edition 用セキュリティ更新プログラム (KB3063858)、Windows Server 2008 R2 x64 Edition 用セキュリティ更新プログラム (KB3063858)）がインストールされていることを確認してください。

Microsoft Windows XP では、ネットワークエージェントの一部の機能が正常に動作しない可能性があります。

Windows XP 向けのネットワークエージェントは、Microsoft Windows XP でのみインストールまたはアップデートが可能です。Microsoft Windows XP のサポートされているエディションとそれに対応するネットワークエージェントのバージョンは、上記のサポートされているオペレーティングシステムのリストに記載されています。このページから、Microsoft Windows XP に必要なバージョンのネットワークエージェントをダウンロードできます。

Kaspersky Security Center Linux と同じバージョンの Network Agent for Linux をインストールすることを推奨します。

Kaspersky Security Center Linux は、同じバージョンまたはそれ以降のバージョンのネットワークエージェントを完全にサポートします。

macOS 用ネットワークエージェントは、このオペレーティングシステム用のカスペルスキーのセキュリティ製品と一緒に提供されます。

# 互換性のあるカスペルスキーのアプリケーションとソリューション

Kaspersky Security Center Linux は、現在サポートされているすべてのカスペルスキー製品とソリューションの一元的な導入、管理をサポートします。アプリケーションとソリューションのバージョンを調べるには、アプリケーションのサポートライフサイクル web ページを参照してください。

サポートされているカスペルスキー製品：

- Kaspersky Endpoint Security for Windows（ファイルサーバーをサポート）
- Kaspersky Endpoint Security for Linux（ファイルサーバーをサポート）
- Kaspersky Endpoint Security for Linux ARM64 Edition

- Kaspersky Endpoint Security for Linux ARM Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent

Kaspersky Security Center Linux は次のソリューションに含まれています：

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response

製品バージョンについては、製品サポートライフサイクルの Web ページを参照してください。

### 既知の問題

Kaspersky Security Center Linux は、次の制限付きで Kaspersky Endpoint Security for Windows の管理に対応しています：Kaspersky Sandbox コンポーネントはサポートされていません。

シングルサインオン（SSO）は、Kaspersky Industrial CyberSecurity for Networks ではサポートされていません。

# Kaspersky Security Center Linux のコンポーネントの互換性について

以下の表に、Kaspersky Security Center Linux コンポーネントの互換性に関する情報が記載されています。

Kaspersky Security Center Linux のコンポーネントの互換性

| コンポーネント | 互換性あり |
| --- | --- |
| Kaspersky Security Center 15.3 Linux 管理サーバー | • Kaspersky Security Center Web コンソールの次のバージョン：15.3、15.2、15.1<br>• Kaspersky Security Center ネットワークエージェントの次のバージョン：Linux の場合は 15.3、15.2、15.1、15、14.2、14、Windows の場合は 15.1、14.2、14 |
| Kaspersky Security Center 15.3 Web コンソール | 次のバージョンの Kaspersky Security Center Linux 管理サーバー：15.3、15.2、15.1 |
| Kaspersky Security Center 15.3 Linux プライマリ管理サーバー | セカンダリ管理サーバー：<br>• 次のバージョンの Kaspersky Security Center Linux：15.3、15.2、15.1、15、14.2<br>• Kaspersky Security Center Windows の次のバージョン：15.1 、14.2 |
| Kaspersky Security Center 15.3 Linux セカンダリ管理サーバー | プライマリ管理サーバー：<br>• 次のバージョンの Kaspersky Security Center Linux：15.2、15.1、15、14.2<br>• 次のバージョンの Kaspersky Security Center Windows：15.1、14.2 |

Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの両方の最新バージョンを使用することを推奨します。そうしないと、Kaspersky Security Center の機能が制限される可能性があります。Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールは個別にインストールおよびアップグレードすることができます。この場合、インストールされている Kaspersky Security Center Web コンソールが接続先の管理サーバーのバージョンと互換性があることを確認する必要があります。

最新バージョンの Kaspersky Security Center Web コンソールと以前のバージョンの Kaspersky Security Center を使用している場合、ドメイン認証中にエラーが発生すると、エラーテキストに既定のメッセージが含まれます。

# Kaspersky Security Center の比較：Windows ベースと Linux ベース

カスペルスキーは、Windows と Linux の 2 つのプラットフォームのオンプレミスのソリューションとして Kaspersky Security Center を提供しています。Windows ベースのソリューションでは、Windows デバイスに管理サーバーをインストールし、Linux ベースのソリューションには Linux にインストールされるよう設計されたバージョンの管理サーバーをインストールします。このオンラインヘルプには、Kaspersky Security Center Linux に関する情報が含まれています。Windows ベースのソリューションの詳細については、Kaspersky Security Center Windows オンライン ヘルプを参照してください。

以下の表で Windows ベースのソリューションと Linux ベースのソリューションの Kaspersky Security Center の主要な機能を比較します。

Windows ベースのソリューションと Linux ベースのソリューションとして動作する Kaspersky Security Center の機能比較

| 機能またはプロパティ | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 15.3 Linux |
| --- | --- | --- |
| 管理サーバーの位置 | オンプレミス | オンプレミス |
| データベース管理システム（DBMS）の位置 | オンプレミス | オンプレミス |
| 管理サーバーをインストールするオペレーティングシステム | Windows | Linux |

| 機能またはプロパティ | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 15.3 Linux |
|---|---|---|
| 管理コンソールの種別 | オンプレミスおよび Web ベース | Web ベース |
| Web ベースの管理コンソールをインストールするオペレーティングシステム | Windows または Linux | Linux |
| 管理サーバーの階層構造 | ✓ | ✓ |
| 管理グループの階層 | ✓ | ✓ |
| ネットワークポーリング | ✓ | ✓ |
| 管理対象デバイスの最大数 | 100000 | 50,000 （PostgreSQL および Postgres Pro を使用） |
| Windows、macOS、Linux 管理対象デバイスの保護 | ✓ | ✓ |
| モバイルデバイスの保護 | ✓ | ✓ |
| 仮想マシンの保護 | ✓ | ✓ |
| パブリッククラウドインフラストラクチャの保護 | ✓ | — |
| UEFI 保護クライアントデバイスのサポート | ✓ | — |
| デバイスベースのセキュリティ管理 | ✓ | ✓ |
| ユーザーベースのセキュリティ管理 | ✓ | ✓ |
| 製品ポリシー | ✓ | ✓ |
| カスペルスキー製品のタスク | ✓ | ✓ |
| Kaspersky Security Network | ✓ | ✓ |
| KSN プロキシ | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ |
| カスペルスキー製品のライセンスの一元的な導入 | ✓ | ✓ |
| 定義データベースのアンチウイルスの自動アップデート | ✓ | ✓ |
| 仮想管理サーバーのサポート | ✓ | ✓ |
| サードパーティ製ソフトウェアのアップデートをインストールし、サードパーティ製ソフトウェアの脆弱性を修正します。 | ✓ | ✓ |
| 管理対象デバイスで発生したイベントに関する通知 | ✓ | ✓ |
| ユーザーアカウントの作成と管理 | ✓ | ✓ |
| ドメイン認証を使用してコンソールにログインする | ✓ | ✓<br>（シングルサインオンはサポートされていません） |
| SIEM システムとの統合 | ✓ | ✓<br>（Syslog の使用によってのみ） |
| ポリシーのステータスとタスクのステータスの監視 | ✓ | ✓ |
| Kaspersky Security Center のフェールオーバークラスタの導入 | ✓ | ✓ |
| SNMP を使用した管理サーバーの統計情報のサードパーティ製品への送信 | ✓ | — |
| クライアントデバイスのリモート診断 | ✓ | ✓ |
| クライアントデバイスのデスクトップへのリモート接続 | ✓ | ✓ |
| オブジェクトリビジョンの管理 | ✓ | ✓ |
| カスペルスキー製品の自動アップデート | ✓ | ✓ |
| クライアントデバイスへのオペレーティングシステムの導入 | ✓ | — |
| インストールパッケージおよびその他のファイルを公開するための Web サーバー | ✓ | ✓ |

| 機能またはプロパティ | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 15.3 Linux |
|---|---|---|
| Kaspersky Endpoint Detection and Response Optimum によって検知されたアラートの表示と操作 | ✓ | ✓ |
| 管理サーバーの WSUS サーバーとしての使用 | ✓ | – |
| Kaspersky Managed Detection and Response との統合 | ✓ | ✓ |
| アダプティブアノマリーコントロールのサポート | ✓ | ✓ |
| 管理グループのクラスタとサーバーアレイのサポート | ✓ | ✓ |
| サードパーティライセンスの管理 | ✓ | – |

# Kaspersky Security Center Cloud コンソールの概要

Kaspersky Security Center をオンプレミスのアプリケーションとして使用することは、管理サーバーを含む Kaspersky Security Center をローカルデバイスにインストールし、ネットワークのセキュリティシステムをマイクロソフト管理コンソールベースの管理コンソール（Kaspersky Security Center Windows でのみ使用可能）、または Kaspersky Security Center Web コンソールで管理することを意味します。

その場合でも、Kaspersky Security Center をクラウドサービスとして使用することは可能です。この場合、Kaspersky Security Center がクラウド環境にインストール、維持されており、管理サーバーへのアクセスがサービスとして提供されます。ネットワークのセキュリティシステムをクラウドベースの管理コンソール（Kaspersky Security Center Cloud コンソール）で管理します。このコンソールのインターフェイスは、Kaspersky Security Center Web コンソールと同じです。

Kaspersky Security Center Cloud コンソールのインターフェイスとヘルプは、次の言語版で提供されています：

- 英語
- フランス語
- ドイツ語
- イタリア語
- 日本語
- ポルトガル語（ブラジル）
- ロシア語
- 簡体字中国語
- スペイン語
- スペイン語（中南米）
- 繁体字中国語

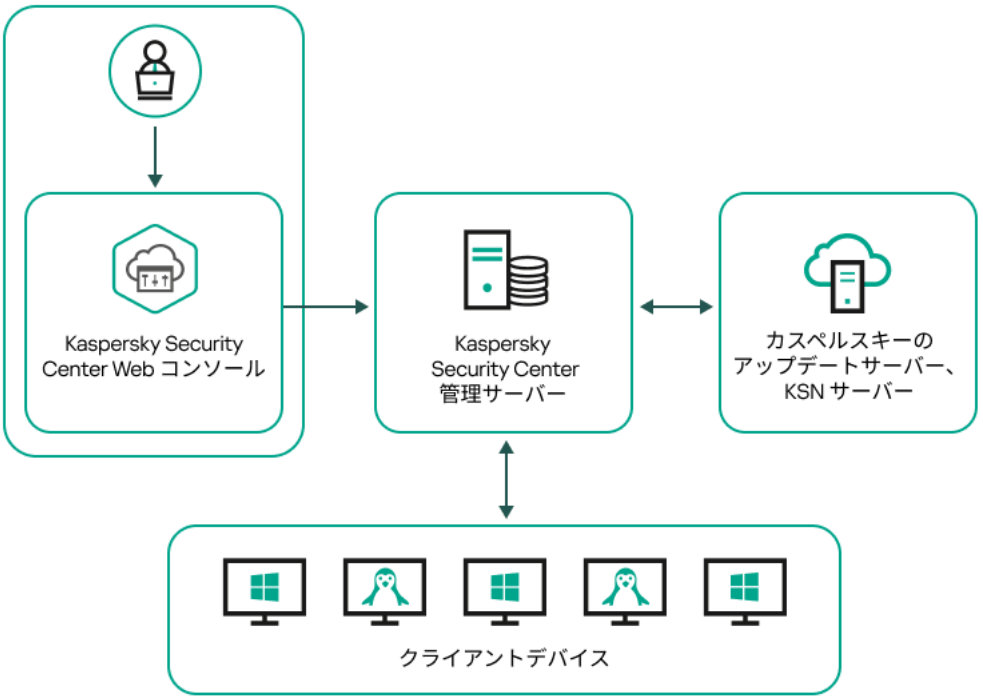
Kaspersky Security Center Cloud コンソールとその機能の詳細は、Kaspersky Security Center Cloud コンソールのヘルプ、Kaspersky Endpoint Security for Business のヘルプを参照してください。

# アーキテクチャと基本概念

このセクションでは、Kaspersky Security Center Linux の基本概念について説明します。

## アーキテクチャ

このセクションでは、Kaspersky Security Center のコンポーネントとコンポーネント間の連携について説明します。



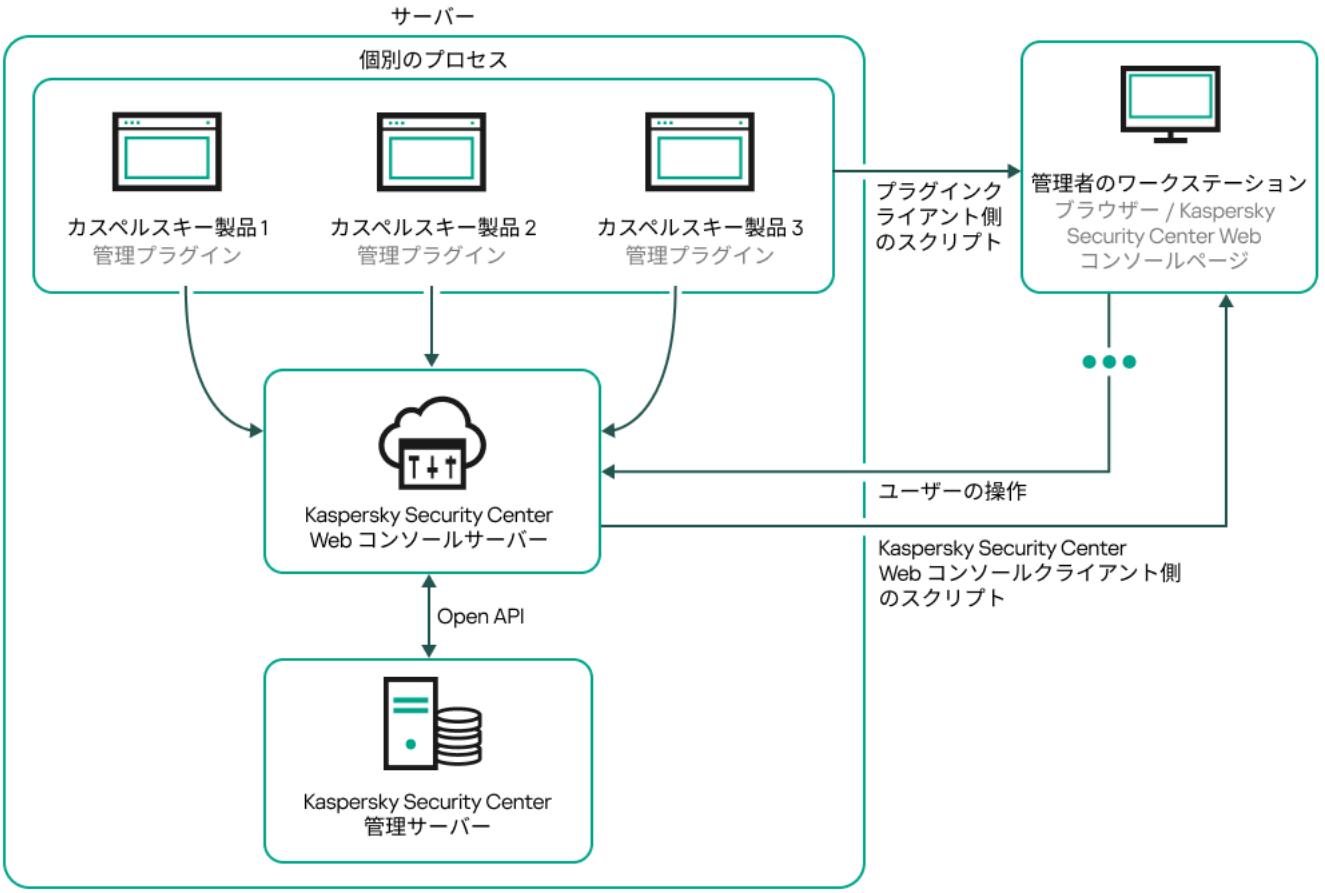

Kaspersky Security Center Linux のアーキテクチャ

Kaspersky Security Center Linux は主に次のコンポーネントで構成されています：

- **Kaspersky Security Center Web コンソール**：Kaspersky Security Center により管理されているクライアント組織のネットワークの保護システムの構築や管理が可能な Web インターフェイスです。
- **Kaspersky Security Center 管理サーバー**（以降「サーバー」とも表記）：組織のネットワークにインストールされているアプリケーションおよびその管理方法に関する情報を一元的に保管します。
- **カスペルスキーのアップデートサーバー**：カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。
- **KSN サーバー**：ファイル、Web リソース、ソフトウェアの評価情報が定期的に更新されるカスペルスキーのデータベースを格納するサーバー。Kaspersky Security Network を使用することで、カスペルスキー製品がより迅速に新しい脅威に対応します。また、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が減ります。
- **クライアントデバイス：**Kaspersky Security Center Linux によって保護されているクライアント企業のデバイス。保護する必要がある各デバイスには、カスペルスキーのセキュリティ製品のいずれかがインストールされている必要があります。

# Kaspersky Security Center Linux 管理サーバーと Kaspersky Security Center Web コンソールの導入図

Kaspersky Security Center Linux 管理サーバーと Kaspersky Security Center Web コンソールの導入図を示します。




Kaspersky Security Center Linux 管理サーバーと Kaspersky Security Center Web コンソールの導入図

保護対象デバイスにインストールされているカスペルスキー製品の管理プラグイン（1つの製品ごとに1つの管理プラグイン）は、Kaspersky Security Center Web コンソールサーバーがインストールされているサーバーに導入されます。

管理者ユーザーは、自分が使用しているワークステーションのブラウザーを使用して Kaspersky Security Center Web コンソールにアクセスします。

Kaspersky Security Center Web コンソールで個別の操作を実行すると、Kaspersky Security Center Web コンソールサーバーが OpenAPI を通して Kaspersky Security Center Linux 管理サーバーと通信を行います。Kaspersky Security Center Web コンソールサーバーは Kaspersky Security Center Linux 管理サーバーに必要な情報のリクエストを送信し、Kaspersky Security Center Web コンソールでの操作結果を表示します。

# Kaspersky Security Center Linux で使用するポート

以下の表は、管理サーバーおよびクライアントデバイスで使用される既定のポートを示しています。必要に応じて、既定のポート番号を変更できます。

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 8060 | klcsweb | TCP | 公開済みインストールパッケージをクライアントデバイスに送信する | インストールパッケージの公開<br>対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。<br>このポートの指定は任意です。セキュリティ上の理由から、8061 TCP ポートの使用を推奨します。 |
| 8061 | klcsweb | TCP (TLS) | 公開済みインストールパッケージをクライアントデバイスに送信する | インストールパッケージの公開<br>対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。 |
| 13000 | klserver | TCP (TLS) | ネットワークエージェントおよびセカンダリ管理サーバーからの接続の受信、セカンダリ管理サーバーでのプライマリ管理サーバーからの接続の受信（セカンダリ管理サーバーが DMZ にある場合など） | クライアントデバイスとセカンダリ管理サーバーの管理<br>ネットワークエージェントから接続を受信する既定のポートの番号は、Kaspersky Security Center Linux のインストール中、接続ポートを設定する時に変更できます。セカンダリ管理サーバーから接続を受信する既定のポートの番号は、管理サーバーの階層を作成する時に変更できます。 |
| 13000 | klserver | UDP | ネットワークエージェントからオフにされたデバイスに関する情報を受信する | クライアントデバイスの管理。<br>対象となる既定のポート番号はネットワークエージェントのポリシー設定で変更できます。 |
| 13291 | klserver | TCP (TLS) | klakaut ユーティリティを使用して Kaspersky Security Center Linux の操作を自動化する | klakaut ユーティリティの使用。klakaut ユーティリティとそのヘルプは、Kaspersky Security Center Linux のインストールフォルダーにあります。<br>既定でこのポートは閉じられています。klakaut ユーティリティを使用して Kaspersky Security Center Linux の操作を自動化する場合は、klscflag ユーティリティを使用して 13291 ポートを開きます。 |
| 13299 | klserver | TCP (TLS) | Identity and Access Manager（IAM）から管理サーバーへの接続の受信、OpenAPI 経由での管理サーバーへの接続の受信 | Kaspersky Security Center Web コンソールを使用して管理サーバーを管理し、OpenAPI を操作します。<br>既定のポート番号は、管理サーバーのプロパティ（［**全般**］の［**接続ポート**］サブセクション）、または管理サーバーの階層の作成時に変更することができます。 |
| 14000 | klserver | TCP | ネットワークエージェントから接続を受信する | クライアントデバイスの管理。<br>既定のポート番号は、Kaspersky Security Center Linux のインストール中の接続ポートの設定時または管理サーバーにクライアントデバイスを手動で接続する際に変更できます。<br>このポートはオプションであり、既定では閉じられています。セキュリティ上の理由から、13000 TCP ポートの使用を推奨します。 |
| 13111（KSN プロキシサービスがデバイスで実行されている場合のみ） | ksnproxy | TCP | 管理対象デバイスから KSN プロキシサーバーへの要求を受信する | KSN プロキシサーバー。<br>対象となる既定のポート番号は管理サーバーのプロパティで変更できます。 |
| 15111（KSN プロキシサービスがデバイスで実行されている場合のみ） | ksnproxy | UDP | 管理対象デバイスから KSN プロキシサーバーへの要求を受信する | KSN プロキシサーバー。<br>対象となる既定のポート番号は管理サーバーのプロパティで変更できます。 |
| 17000 | klactprx | TCP (TLS) | 管理対象デバイスから製品のアクティベーション用の接続を受信する | 管理対象デバイス用のアクティベーションプロキシサーバー。<br>既定のポート番号は、管理サーバーのプロパティウィンドウ（［**全般**］セクションの［**追加のポート**］サブセクション）で変更できます。 |

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 13292（モバイルデバイスを管理している場合のみ） | klserver | TCP (TLS) | モバイルデバイスから接続を受信する | モバイルデバイス管理。<br>管理コンソールまたはKaspersky Security Center Web コンソールにある管理サーバーのプロパティウィンドウで、既定のポート番号を変更できます。 |
| 19170 | klserver | HTTPS (TLS) | klsctunnel ユーティリティを使用した管理対象デバイスへの接続のトンネリング | Kaspersky Security Center Web コンソールを使用した管理対象デバイスへのリモート接続。<br>対象となる既定のポート番号は、管理サーバーのプロパティで変更できます（**全般→接続ポート→RDP 接続のトンネリング**）。 |
| 4444 | kliam | HTTPS | OpenID Connect プロトコルを使用した認証 | ブラウザーと Identity and Access Manager（IAM）間の認証トークンの交換。 |
| 9050 | kliam | HTTPS | IAM を使用した管理サーバーへの接続 | Kaspersky Security Center Web コンソールと IAM 間の認証トークンの交換。 |
| <DBMS ポート>（設定可能） | kliam | TCP | IAM を使用した DBMS への接続 | IAM から DBMS へのリクエストの受信。 |

管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MariaDB 用のポート 3306 など）。関連する情報については、DBMS のドキュメントを参照してください。

次のテーブルは、iOS™ MDM サーバーが使用するポートを示しています（モバイルデバイスを管理している場合のみ）。

iOS MDM サーバーで使用するポート

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 443 | kliosmdmservicesrv | TCP (TLS) | iOS モバイルデバイスから接続を受信する | モバイルデバイス管理。<br>既定のポート番号は、iOS MDM サーバーのインストール時に変更できます。 |

下記の表に、Kaspersky Security Center Web コンソールサーバーが使用するポートを示します。管理サーバーがインストールされている同じデバイスでも、別のデバイスでも問題ありません。

Kaspersky Security Center の Web コンソールサーバーで使用するポート

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 8080 | Node.js: Server-side JavaScript | TCP (TLS) | ブラウザーから Kaspersky Security Center Web コンソールへの接続を受信する | Kaspersky Security Center Web コンソール。<br>Kaspersky Security Center Web コンソールのインストール時に、既定のポート番号を変更できます。Linux ALT オペレーティングシステム上に Kaspersky Security Center Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。 |

下記の表に、ネットワークエージェントがインストールされている管理対象デバイスが使用するポートを示します。

ネットワークエージェントが使用するポート

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 15000 | klnagent | UDP | 管理サーバーまたはディストリビューションポイントからネットワークエージェントへの管理信号 | クライアントデバイスの管理。<br>対象となる既定のポート番号はネットワークエージェントのポリシー設定で変更できます。 |
| 15000 | klnagent | UDP ブロードキャスト | 同じブロードキャストドメイン内の他のネットワークエージェントに関するデータの取得（データは管理サーバーに送信されます） | アップデートおよびインストールパッケージの提供。 |
| 15001 | klnagent | UDP | ディストリビューションポイント（使用している場合）からマルチキャスト要求を受信する | ディストリビューションポイントからアップデートとインストールパッケージを受信する。<br>既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。 |
| 30522、<br>30523（ローカルホストインターフェイス上のポート） | klnagent | TCP | FileTransferBridge コンポーネントを使用して管理サーバーからカスペルスキー製品のアップデートを受信します | 定義データベースのアップデート元として指定された管理サーバーからカスペルスキー製品のアップデートを受信する管理対象デバイス。 |

klnagent プロセスは、エンドポイントオペレーティングシステムの動的ポート範囲から空きポートを要求することもできます。これらのポートは、オペレーティングシステムによって自動的に klnagent プロセスに割り当てられるため、klnagent プロセスは別のソフトウェアで使用されている一部のポートを使用できます。klnagent プロセスがそのソフトウェアの動作に影響を与える場合は、このソフトウェアのポート設定を変更するか、オペレーティングシステムの既定の動的ポート範囲を変更して、影響を受けるソフトウェアに使用されるポートを除外します。

また、Kaspersky Security Center Linux とサードパーティ製ソフトウェアとの互換性に関する推奨事項は参照のみを目的として説明されており、サードパーティ製ソフトウェアの新しいバージョンには適用できない場合があることにも注意してください。説明されているポート設定の推奨事項は、テクニカルサポートの経験とベストプラクティスに基づいています。

下記の表に、ネットワークエージェントがインストールされた管理対象デバイスがディストリビューションポイントとして使用するポートを示します。ネットワークエージェントで使用するポートに加えて、リストにあるポートをディストリビューションポイントデバイスで使用します（上記の表を参照）。

ディストリビューションポイントとして動作するネットワークエージェントが使用するポート

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 13000 | klnagent | TCP (TLS) | ネットワークエージェントおよび接続ゲートウェイからの接続の受信 | クライアントデバイスの管理、アップデートおよびインストールパッケージの提供。<br>既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。 |
| 13111（KSN プロキシサービスがデバイスで実行されている場合のみ） | ksnproxy | TCP | 管理対象デバイスから KSN プロキシサーバーへの要求を受信する | KSN プロキシサーバー。<br>既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。 |
| 15111（KSN プロキシサービスがデバイスで実行されている場合のみ） | ksnproxy | UDP | 管理対象デバイスから KSN プロキシサーバーへの要求を受信する | KSN プロキシサーバー。<br>既定のポート番号は、ディストリビューションポイントのプロパティで変更できます。 |
| 13295（ディストリビューションポイントをプッシュサーバーとして使用する場合のみ） | klnagent | TCP (TLS) | クライアントデバイスからの接続の受信 | プッシュサーバー：<br>既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。 |

| ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 8060 | klcsweb | TCP | 公開済みインストールパッケージをクライアントデバイスに送信する | インストールパッケージの公開<br>対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。 |
| 8061 | klcsweb | TCP (TLS) | 公開済みインストールパッケージをクライアントデバイスに送信する | インストールパッケージの公開<br>対象となる既定のポート番号は、管理サーバーのプロパティの［**Web サーバー**］セクションで変更できます。 |

下記の表に、ドメインコントローラーデバイスで使用されるポートを示します。

ドメインコントローラーデバイスで使用されるポート

| ポート番号 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|
| 389 | LDAP over TCP または UDP | LDAP サーバーへの接続 | ドメインコントローラーのポーリング |
| 636 | LDAP over TLS | LDAP サーバーへの接続 | ドメインコントローラーのポーリング |

# Kaspersky Security Center Web コンソールで使用されるポート

下表には、Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）がインストールされたデバイスで開放しておく必要があるポートが一覧で表示されています。

Kaspersky Security Center Web コンソールで使用されるポート

| ポート番号 | サービス名 | プロトコル | ポートの目的 | 範囲 |
|---|---|---|---|---|
| 2001 | Kaspersky Security Center 製品プラグインサーバー | HTTPS | 管理プラグインプロセスが「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用する API ポート | 管理プラグインの node プロセスの実行 |
| 1329、2003 | Kaspersky Security Center Web コンソール管理サービス | HTTPS | 同一のデバイスで実行中の「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用される API ポート | Kaspersky Security Center Web コンソールコンポーネントのアップデート |
| 2005 | Kaspersky Security Center Web コンソール | HTTPS | 同一のデバイスで実行中の「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用される API ポート | Kaspersky Security Center Web コンソールの node プロセスの実行 |
| 8200 | — | HTTP | HashiCorp Vault を使用して証明書を生成するために使用される API ポート（詳細については、HashiCorp Vault の Web サイトを参照してください） | Kaspersky Security Center Web コンソールのインストールと Kaspersky Security Center Web コンソールコンポーネントのアップデート |

| ポート番号 | サービス名 | プロトコル | ポートの目的 | 範囲 |
| --- | --- | --- | --- | --- |
| 4150、4151、4152 | Kaspersky Security Center Web コンソールメッセージキュー | HTTPS | Kaspersky Security Center Web コンソールと管理プラグインの処理間で発生する通信に使用される NSQ ベースのメッセージブローカーの API ポート<br>NSQ ベースのメッセージブローカーは、将来のアップデートで NATS ベースのブローカーに置き換えられます。 | Kaspersky Security Center Web コンソールと管理プラグインとの対話 |
| 4222 | Kaspersky Security Center Web コンソール NATS | HTTPS | Kaspersky Security Center Web コンソールと管理プラグインの処理間で発生する通信に使用される NATS ベースのメッセージブローカーの API ポート<br>将来のアップデートでは、NSQ ベースのブローカーが NATS ベースのメッセージブローカーに置き換えられます。<br>8222 ポートは NATS を監視するために使用されます。 | Kaspersky Security Center Web コンソールと管理プラグインとの対話 |

# 基本概念

このセクションでは、Kaspersky Security Center Linux の基本概念について説明します。

## 管理サーバー

Kaspersky Security Center のコンポーネントを使用すると、クライアントデバイスにインストールされたカスペルスキー製品をリモート管理できます。

管理サーバーがインストールされたデバイスは、*管理サーバー*（「サーバー」とも表記）と呼ばれます。管理サーバーについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

管理サーバーは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名前は `kladminserver_srv`
- オペレーティングシステムの起動時に自動実行される
- `ksc` アカウントまたは管理サーバーのインストール時に選択したユーザーアカウントを使用

インストール設定の完全なリストについては、次のトピックを参照してください：Kaspersky Security Center Linux のインストール

管理サーバーは、次の機能を実行します：

- 管理グループ構造の保管
- クライアントデバイスの設定に関する情報の保管
- アプリケーション配布パッケージのリポジトリの管理
- クライアントデバイスへのアプリケーションのリモートインストールおよびアプリケーションの削除

- カスペルスキー製品の定義データベースおよびソフトウェアモジュールのアップデート
- クライアントデバイスのポリシーとタスクの管理
- クライアントデバイスで発生したイベントに関する情報の保管
- カスペルスキー製品の操作に関するレポートの生成
- クライアントデバイスへのライセンスの配信と、ライセンスに関する情報の保管
- （クライアントデバイスでのウイルスの検知など）タスクの進捗に関する通知の転送

### 製品のインターフェイスで管理サーバーに名前を付ける

Kaspersky Security Center Web コンソールの製品インターフェイスで、管理サーバーに次の名前をつけることが可能です：

- 「*device_name*」または「管理サーバー：*device_name*」などの管理サーバーデバイスの名前。
- 「*IP_address*」または「管理サーバー：*IP_address*」などの管理サーバーの IP アドレス。
- セカンダリ管理サーバーおよび仮想管理サーバーには、これらをプライマリ管理サーバーに接続する際に指定したカスタム名を使用できます。
- Linux デバイスにインストールした Kaspersky Security Center Web コンソールを使用している場合は、本製品は応答ファイルで信頼済みとして指定した管理サーバーの名前を表示します。

Kaspersky Security Center Web コンソールを使用して管理サーバーに接続できます。

## 管理サーバーの階層構造

管理サーバーは、階層に配置できます。各管理サーバーは、階層の同一ネスト上に複数のセカンダリ管理サーバー（「*セカンダリサーバー*」とも表記）を保持することも、複数のネストレベル上に複数のサーバーを保持することもできます。セカンダリ管理サーバーのネストレベルに制限はありません。プライマリ管理サーバーの管理グループには、すべてのセカンダリ管理サーバーのクライアントデバイスが含められます。このようにして、ネットワークの独立したセクションを、様々な管理サーバーを使用して管理できます。管理サーバーの管理には、プライマリ管理サーバーが使用されます。

階層で、Linux ベースの管理サーバーはプライマリサーバーとセカンダリサーバーのどちらとしても機能できます。Linux ベースのプライマリサーバーは、Linux ベースと Windows ベースのセカンダリサーバーの両方を管理できます。プライマリ Windows ベースのサーバーは、セカンダリ Linux ベースのサーバーを管理できます。

*仮想管理サーバー*はセカンダリ管理サーバーの特殊な例です。

管理サーバーの階層を使用して、次のことを実現できます：

- （ネットワーク全体で1台の管理サーバーがインストールされている場合と比較して）管理サーバーの負荷を軽減する。
- イントラネットのトラフィックを削減して、リモートオフィスとの通信を簡略化する。プライマリ管理サーバーとネットワーク上のすべてのデバイス（他の地域にあるデバイスも含む）との間で接続を確立する必要はありません。各ネットワークセグメントにセカンダリ管理サーバーをインストールし、セカンダリ管理サーバーの管理グループ内にデバイスを配置し、高速通信チャネルを使用してセカンダリ管理サーバーとプライマリ管理サーバー間の接続を確立すれば十分です。
- アンチウイルスセキュリティ管理者間で、責任区分を明確にする。企業ネットワーク内のアンチウイルスセキュリティステータスの一元管理機能と監視機能も利用できます。
- サービスプロバイダーによる Kaspersky Security Center の使用。サービスプロバイダーでインストールする必要があるのは、Kaspersky Security Center と Kaspersky Security Center Web コンソールのみです。サービスプロバイダーが様々な組織の多くのデバイスを管理するには、管理サーバーの階層にセカンダリ管理サーバー（仮想サーバーを含む）を追加します。

管理グループの階層に含まれる各デバイスは、1台の管理サーバーにしか接続できません。デバイスから管理サーバーへの接続を個別に監視する必要があります。ネットワーク属性に基づいて様々な管理サーバーの管理グループ内でデバイスを検索する機能を使用してください。

# 仮想管理サーバー

仮想管理サーバー（「*仮想サーバー*」とも表記）は、クライアント組織のネットワークの保護を管理する、Kaspersky Security Center Linux のコンポーネントです。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

さらに、仮想管理サーバーには次の制限があります：

- 仮想管理サーバーのプロパティウィンドウでは、セクション数が限られています。
- 仮想管理サーバーが管理するクライアントデバイスにカスペルスキー製品をリモートからインストールするには、仮想管理サーバーと通信するためにネットワークエージェントがインストールされたクライアントデバイスが必要です。そのデバイスは、最初に仮想管理サーバーと接続する際、自動的にディストリビューションポイントとして設定され、その他のクライアントデバイスと仮想管理サーバーを接続するゲートウェイとして機能します。
- 仮想サーバーでネットワークをポーリングするためには、ディストリビューションポイントを使用する必要があります。

- 正常に動作しない仮想サーバーが Kaspersky Security Center Linux によって再起動される場合、プライマリ管理サーバーとすべての仮想サーバーが再起動されます。
- 仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

仮想管理サーバーの管理者は、その仮想管理サーバーにおけるすべての権限を持ちます。

# Web サーバー

Kaspersky Security Center *Web* サーバー（略称として単に「*Web* サーバー」とも表記）は、管理サーバーとともにインストールされる Kaspersky Security Center のコンポーネントです。Web サーバーは、スタンドアロンインストールパッケージおよび共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

スタンドアロンインストールパッケージは作成時に、Web サーバー上に自動的に公開されます。スタンドアロンパッケージをダウンロードするリンクは、作成済みスタンドアロンインストールパッケージのリストに表示されます。必要に応じて、スタンドアロンパッケージの公開を取り消したり、Web サーバー上にスタンドアロンパッケージを再度公開したりできます。

共有フォルダーは、管理サーバーで管理されるデバイスを使用するすべてのユーザーが利用できる情報の保管領域として使用されます。共有フォルダーに直接アクセスできないユーザーには、Web サーバーを使用して、そのフォルダーから情報を提供することができます。

Web サーバーを使用して共有フォルダーからユーザーに情報を提供するには、管理者が共有フォルダー内に public という名前のサブフォルダーを作成し、情報をそのサブフォルダーに貼り付ける必要があります。

情報転送リンクの構文は次の通りです：

`https://<Web サーバー名>:<HTTPS ポート>/public/<オブジェクト>`

説明：

- `<Web Server name>` は、Kaspersky Security Center Web サーバーの名前です。
- `<HTTPS port>` は、管理者が定義した Web サーバーの HTTPS ポートです。HTTPS ポートは、管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで設定できます。既定のポート番号は 8061 です。
- `<object>` は、ユーザーがアクセス権を持っているサブフォルダーまたはファイルです。

管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーは、そのリンクを使用して、必要な情報をローカルデバイスにダウンロードできます。

# Kaspersky Security Center Linux Web サーバー

Kaspersky Security Center Linux Web サーバー（「Web サーバー」とも表記）は、Kaspersky Security Center Linux のコンポーネントです。Web サーバーは、共有フォルダーからスタンドアロンインストールパッケージやファイルを公開するために設計されています。

インストールパッケージは、Web サーバーで自動的に公開され、初回のダウンロード後に削除されます。管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーはそのリンクをクリックして、必要な情報をモバイルデバイスにダウンロードできます。

### Web サーバーの設定

Web サーバーの微調整が必要な場合は、Web サーバーのプロパティで、HTTP（8060）および HTTPS（8061）のポートを変更できます。ポートの変更に加えて、HTTPS のサーバー証明書を置き換えることや、HTTP の Web サーバーの FQDN を変更することが可能です。

### 接続ゲートウェイ上の Web サーバー設定

接続ゲートウェイモードでディストリビューションポイントに別の Web サーバーサービスが実装され、Kaspersky Security Center Linux に接続されたモバイルデバイスを操作できるようになります。このサービスは、デバイスを管理サーバーに直接接続せずに、アプリのインストールパッケージとデバイス管理プロファイルをデバイスに転送する役割を担います。サービスが接続ゲートウェイで HTTP/HTTPS ファイル要求を処理すると、ファイルが転送されます。

接続ゲートウェイ上の Web サーバーサービスは、ネットワークエージェント Linux とともにインストールされます。この機能を使用するには、Web サーバーとして使用する接続ゲートウェイモードでディストリビューションポイントとして機能するデバイスを割り当て、対応する設定を指定する必要があります。接続ゲートウェイ上の Web サーバー設定の詳細については、「Kaspersky Secure Mobility Management ヘルプ」を参照してください。

## ネットワークエージェント

管理サーバーとデバイスとの対話は、Kaspersky Security Center Linux のコンポーネントの*ネットワークエージェント*によって実行されます。ネットワークエージェントは、Kaspersky Security Center Linux を使用してカスペルスキー製品を管理するすべてのデバイスにインストールします。

ネットワークエージェントがインストールされたデバイスは「*管理対象デバイス*」または単に「*デバイス*」と呼ばれます。ネットワークエージェントのインストールパッケージは、次のソースからダウンロードできます：

- 管理サーバーの保管領域（管理サーバーをインストールしている必要があります）
- カスペルスキーの Web サイト

Linux 用のネットワークエージェントは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky ネットワークエージェント」
- オペレーティングシステムの起動時に自動実行される
- ルートアカウントを使用する

Windows 用のネットワークエージェントは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky Security Center ネットワークエージェント」
- オペレーティングシステムの起動時に自動実行される
- ローカルシステムアカウントを使用する

サービスプロセスの名前：

- Linux の場合：
  - klnagent64.service（64 ビットオペレーティングシステムの場合）
  - klnagent.service（32 ビットオペレーティングシステムの場合）
- Windows の場合：
  - klnagent

既定では、ネットワークエージェントは次の場所にインストールされます：

- Linux の場合：
  - 32 ビットシステム：/opt/kaspersky/klnagent/
  - 64 ビットシステム：/opt/kaspersky/klnagent64/
- Windows の場合：
  - 32 ビットシステム：C:\Program Files\ Kaspersky Lab\NetworkAgent
  - 64 ビットシステム：C:\Program Files (x86)\ Kaspersky Lab\NetworkAgent

Windows デバイスの場合、インストールパッケージの設定で、ネットワークエージェントのインストール用に別のフォルダーを指定できます。ただし、Linux デバイスの場合、ネットワークエージェントは既定のディレクトリにのみインストールできます。

ネットワークエージェントのインストールフォルダーには、klmover ユーティリティや klnagchk ユーティリティなど、ネットワークエージェントの動作を管理および診断するためのユーティリティも含まれています。

管理サーバーをインストールすると、ネットワークエージェントのサーバーバージョンが管理サーバーとともに自動的にインストールされます。ただし、管理サーバーデバイスを他の管理対象デバイスとして管理するには、管理サーバーデバイス上で Linux 用ネットワークエージェントをインストールします。この場合、Linux 向けネットワークエージェントは、管理サーバーと一緒にインストールしたサーバー版のネットワークエージェントとは別にインストールされ、動作します。

ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。*同期*間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

# 管理グループ

*管理グループ*（以後、*グループ*と表記）は、基準に従ってまとめられた管理対象デバイスの仮想グループで、グループ内のデバイスを Kaspersky Security Center Linux 内で1つの単位として管理することを目的としています。

管理グループ内の管理対象デバイスはすべて、次の操作を実行できるように設定されます：

- 同一のアプリケーション設定を使用する（設定はグループポリシーで定義できます）。
- 特定の設定でグループタスクを作成することにより、すべてのアプリケーションで共通の動作モードを使用する。グループタスクの例としては、共通のインストールパッケージの作成とインストール、定義データベースおよびモジュールのアップデート、デバイスのオンデマンドスキャン、リアルタイム保護の有効化などがあります。

1台の管理対象デバイスが所属できる管理グループは1つだけです。

管理サーバーとグループに対して、任意の階層レベル数で階層構造を作成できます。1つの階層レベルに、セカンダリ管理サーバーや仮想管理サーバー、グループ、および管理対象デバイスを含めることができます。デバイスの物理的な位置を動かすことなく、あるグループから別のグループへデバイスを移動できます。たとえば、従業員の配属が経理から開発に異動になった場合、この従業員のデバイスを経理部門用の管理グループから開発部門用の管理グループに移動できます。これにより、デバイスでは開発部門向けのアプリケーション設定が自動的に取得されます。

# 管理対象デバイス

*管理対象デバイス*は Linux、Windows、または macOS を実行していてネットワークエージェントをインストールしているデバイスです。これらのデバイスにインストールされたセキュリティ製品のタスクとポリシーを作成することで、これらのデバイスを管理できます。管理対象デバイスからのレポートも受信できます。

管理対象デバイスをディストリビューションポイントや接続ゲートウェイとして動作させることができます。

1台のデバイスを管理対象にできる管理サーバーは1台のみです。1つの管理サーバーによって管理できるデバイスの数は、管理サーバーをホストするデバイスの構成と DBMS の制限によって異なります。

# 未割り当てデバイス

*未割り当てデバイス*とは、ネットワークに接続されているがどの管理グループにも含まれていないデバイスです。未割り当てデバイスに対して、管理グループへ移動したり、アプリケーションをインストールしたりなどの操作を実行できます。

ネットワーク内で検出された新しいデバイスは、「**未割り当てデバイス**」管理グループに割り当てられます。検出されたデバイスが自動的に他のグループに移動されるようにルールを設定できます。

# 管理コンピューター

Kaspersky Security Center Web コンソールサーバーがインストールされているデバイスを「*管理者のワークステーション*」と呼びます。管理者は、これらのデバイスを使用して、クライアントデバイスにインストールされているすべてのカスペルスキー製品を一元的にリモート管理できます。

管理コンピューターの数に制限はありません。任意の管理コンピューターから、ネットワーク上にある複数の管理サーバーで構成される管理グループを一度に管理できます。管理コンピューターは、任意の階層レベルにある管理サーバー（物理または仮想）に接続できます。

管理コンピューターは、管理グループにクライアントデバイスとして含めることができます。

任意の管理サーバーの管理グループ内で、1台のデバイスが管理サーバーのクライアント、管理サーバー、または管理コンピューターとして機能できます。

# Web 管理プラグイン

Kaspersky Security Center Web コンソールによるカスペルスキー製品のリモート管理では、*Web 管理プラグイン*という特別なコンポーネントが使用されます。以降、Web 管理プラグインは*管理プラグイン*とも表記されます。管理プラグインは、Kaspersky Security Center Web コンソールと特定のカスペルスキー製品との間のインターフェイスです。管理プラグインを使用して、該当製品のタスクとポリシーを設定できます。

管理 Web プラグインは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

管理プラグインには次の機能があります：

- カスペルスキーのタスクを作成および編集し、各種設定を編集するインターフェイス
- カスペルスキー製品と管理対象デバイスのリモートからの一元管理に使用できるポリシーおよびポリシーのプロファイルを作成および編集するインターフェイス
- カスペルスキー製品で生成されたイベントの転送
- Kaspersky Security Center Web コンソールでは、転送されたカスペルスキー製品の動作データ、イベント、および統計情報を表示できます

# ポリシー

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに1つのポリシーを提供します。ポリシーは次のいずれかのステータスを持ちます：

| ステータス | 説明 |
|---|---|
| アクティブ | 現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは1つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。 |
| 非アクティブ | 現在デバイスに適用されていないポリシー。 |
| モバイルユーザー | このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。 |

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

# ポリシーのプロファイル

別々の管理グループに対応して単一のポリシーから枝分かれした複数のポリシーの作成が必要になる場合があります。また、これらの枝分かれ後のポリシーについても、一元的に設定の変更を行えると便利です。枝分かれ後のポリシー同士では、1つか2つの設定値が異なるだけという場合もあります。たとえば、経理部門の従業員には単一のポリシーが適用されるが、部門内の管理職にはフラッシュドライブの使用が許可され、その他のメンバーには許可されないという点が異なる場合などです。こうした状況では、管理グループの階層のみを使用して適切なポリシーを適用することはそれほど簡単ではありません。

単一のポリシーから枝分かれした複数のポリシーを個別に作成しなくても、Kaspersky Security Center Linuxでは*ポリシーのプロファイル*を作成して対応できます。ポリシーのプロファイルは、同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合に必要です。

ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。プロファイルを有効にすると、元々デバイスで有効になっていた「基本」ポリシーの設定が修正されます。修正後の設定では、プロファイルで指定された値が適用されます。

# タスク

Kaspersky Security Center Linux は、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインがインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次のタスクは管理サーバーで実行されます：

- レポートの自動配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が Kaspersky Security Center Web コンソールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、管理サーバー上の Syslog ログと Kaspersky Security Center Linux のイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

# タスク範囲

*タスク範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。
- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている txt ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

  デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

# ローカルアプリケーション設定とポリシーの関連付け

ポリシーを使用して、グループ内のすべてのデバイスに同じ値のアプリケーション設定を指定できます。

ローカルアプリケーション設定を使用して、ポリシーで指定されている設定値をグループ内の個別のデバイスに再定義できます。設定値を指定できるのは、ポリシーで変更が許可されている設定（ロック解除された設定）だけです。

クライアントデバイスのアプリケーションで使用される値は、その設定がポリシー内でロックされているかどうか（🔒）に基づいて決定されます：

- 設定の変更がロックされている場合、ポリシー内で定義されている値が、すべてのクライアントデバイスで使用される。
- 設定の変更がロック解除されている場合、各クライアントデバイスのアプリケーションは、ポリシーで指定されている値ではなくローカル設定の値を使用する。設定は、ローカルアプリケーション設定で変更できます。

このため、クライアントデバイスでタスクを実行する場合、次の 2 つの方法で定義した設定が使用されます：

- タスク設定とローカルアプリケーション設定（ポリシー内の設定の変更がロックされていない場合）。
- グループポリシー（設定の変更がロックされている場合）。

ローカルアプリケーション設定は、最初にポリシー設定に基づいてポリシーが適用された後で適用されます。

# ディストリビューションポイント

*ディストリビューションポイント*（旧称：アップデートエージェント）とは、ネットワークエージェントがインストールされ、アップデートの配信やアプリケーションのリモートインストール、ネットワーク内のデバイスの情報の収集に使用されるデバイスです。

ディストリビューションポイントとして使用されるデバイスにインストールされるネットワークエージェントの機能と使用例は、オペレーティングシステムによって異なります。

ディストリビューションポイントは、次の機能を実行できます：

- 管理サーバーから受信したアップデートおよびインストールパッケージをグループ内のクライアントデバイスに配布します（UDP を使用したマルチキャストを含む）。アップデートは、管理サーバーまたはカスペルスキーのアップデートサーバーから受信可能です。後者の場合は、ディストリビューションポイントのアップデートタスクを作成する必要があります。

  ディストリビューションポイントにより、アップデートの配信が加速され、管理サーバーのリソースが解放されます。

- UDP を使用して、マルチキャストによってポリシーとグループタスクを配信します。

- 管理グループのデバイスに対して、管理サーバーとの接続のゲートウェイとして動作します。

  グループ内の管理対象デバイスと管理サーバーとの間で直接接続を確立できない場合は、このグループの管理サーバーへの接続ゲートウェイとしてディストリビューションポイントを使用できます。この場合、管理対象デバイスは接続ゲートウェイに接続され、接続ゲートウェイが管理サーバーに接続されます。

  接続ゲートウェイとして動作するディストリビューションポイントを使用することで、管理対象デバイスと管理サーバーとの間の直接接続がブロックされることはありません。接続ゲートウェイは使用できないが、管理サーバーとの直接接続が技術的に可能な場合は、管理対象デバイスは管理サーバーに直接接続されます。

- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。

- カスペルスキーおよびその他のソフトウェアベンダーによるアプリケーションのリモートインストールを実行します。これには、ネットワークエージェントを使用しないクライアントデバイスへのインストールが含まれます。

  この機能により、管理サーバーが直接アクセスできないネットワークに配置されているクライアントデバイスに、ネットワークエージェントのインストールパッケージをリモートで転送できます。

- Kaspersky Security Network（KSN）に参加したプロキシサーバーとして動作します。

  ディストリビューションポイントで KSN プロキシサーバーを有効にして、デバイスを KSN プロキシサーバーとして動作させることができます。この場合、KSN プロキシサービスはデバイス上で実行されます。

管理サーバーからディストリビューションポイントへのファイル転送は、HTTP で、または SSL 接続が有効な場合は HTTPS で実行されます。HTTP または HTTPS を使用すると、トラフィック量が削減され、SOAP と比較して速度が速くなります。

ネットワークエージェントをインストールしたデバイスは、管理者が手動で、または管理サーバーから自動で、ディストリビューションポイントに割り当てることができます。指定された管理グループのディストリビューションポイントの完全なリストは、ディストリビューションポイントのリストのレポートに表示されます。

ディストリビューションポイントの範囲は、管理者により割り当てられている管理グループ、および、埋め込みのすべてのレベルのサブグループです。複数のディストリビューションポイントが管理グループの階層に割り当てられている場合、管理対象デバイスのネットワークエージェントが、階層内の最も近いディストリビューションポイントに接続します。

管理サーバーによってディストリビューションポイントが自動的に割り当てられた場合、管理グループではなくブロードキャストドメインによって割り当てられます。これは、すべてのブロードキャストドメインが管理サーバーで認識済みである場合に発生します。ネットワークエージェントは同じサブネットに存在する他のネットワークエージェントとメッセージを交換し、得た情報を管理サーバーに送信します。管理サーバーはその情報をネットワークエージェントのブロードキャストドメインでのグループ化に利用します。管理グループ内のネットワークエージェントの 70% 以上を検索した後にブロードキャストドメインが管理サーバーに認識されます。管理サーバーはブロードキャストドメインを 2 時間ごとに検索します。ディストリビューションポイントは、ブロードキャストドメイン別に割り当てられた後、管理グループ別に再度割り当てることはできません。

管理者がディストリビューションポイントを手動で割り当てる場合、管理グループまたはネットワークロケーションに割り当てることができます。

アクティブな接続プロファイルを持つネットワークエージェントは、ブロードキャストドメインの検知の対象外となります。

Kaspersky Security Center Linux では、各ネットワークエージェントに対して、他のどのアドレスとも異なる一意の IP マルチキャストアドレスを割り当てます。これにより、IP の重複によって発生するネットワークの過負荷を回避できます。旧バージョンの製品で割り当てられた IP マルチキャストアドレスは変更されません。

2 つ以上のディストリビューションポイントを単一のネットワークエリアまたは単一の管理グループに割り当てると、それらの 1 つがアクティブなディストリビューションポイントとなり、残りがスタンバイディストリビューションポイントとなります。アクティブなディストリビューションポイントはアップデートとインストールパッケージを直接管理サーバーからダウンロードします。一方、スタンバイのディストリビューションポイントはアクティブなディストリビューションポイントからのみアップデートを受信します。この場合、ファイルは管理サーバーから一度ダウンロードされてからディストリビューションポイント間で配信されます。アクティブなディストリビューションポイントが何かの理由で利用不可能になった場合、スタンバイのディストリビューションポイントがアクティブになります。管理サーバーは自動的にディストリビューションポイントをスタンバイとして割り当てます。

ディストリビューションポイントのステータス（「*アクティブ*」または「*スタンバイ*」）とチェックボックスが、klnagchk のレポートに表示されます。

ディストリビューションポイントには、少なくとも 4 GB の空きディスク容量が必要です。ディストリビューションポイントのディスクの空き容量が 2 GB 未満の場合、Kaspersky Security Center Linux は*警告*の重要度でセキュリティ上の問題を作成します。セキュリティの問題は、デバイスのプロパティの**セキュリティ問題**セションで公開されます。

ディストリビューションポイントとして割り当てられているデバイスでリモートインストールタスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量はインストールするすべてのインストールパッケージの合計サイズを上回っていなければなりません。

ディストリビューションポイントとして割り当てられているデバイスでアップデート（パッチ適用）タスクと脆弱性の修正タスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量は、インストールするすべてのパッチの合計サイズの少なくとも 2 倍でなければなりません。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

# 接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

接続ゲートウェイが通信可能なデバイスは 10,000 台までです。

接続ゲートウェイの使用方法は次の 2 つです：

- 非武装地帯（DMZ）への接続ゲートウェイのインストールを推奨します。モバイルユーザーデバイスにインストールされた別のネットワークエージェントのために、接続ゲートウェイを介した管理サーバーへの接続を専用に設定する必要があります。

  いかなる場合でも、ネットワークエージェントから管理サーバーへ転送されるデータを接続ゲートウェイが変更または処理することはありません。また、このデータをバッファに書き込むこともありません。したがって、ネットワークエージェントからデータを受信し、それを管理サーバーへ後で転送することもありません。ネットワークエージェントが接続ゲートウェイを介して管理サーバーへの接続を試行したが接続ゲートウェイが管理サーバーへ接続できない場合、ネットワークエージェントは管理サーバーがアクセス不能であると判断します。データはすべてネットワークエージェントに残ります（接続ゲートウェイには残りません）。

  接続ゲートウェイが別の接続ゲートウェイを介して管理サーバーへ接続することはできません。これは、ネットワークエージェントが同時に接続ゲートウェイとして動作したり、接続ゲートウェイを使用して管理サーバーへ接続したりすることができないことを意味します。

  接続ゲートウェイはすべて、管理サーバーのプロパティにあるディストリビューションポイントのリストに含まれています。

- 接続ゲートウェイは、ネットワーク内で使用することも可能です。たとえば、自動的に割り当てられたディストリビューションポイントは、自身の範囲内の接続ゲートウェイにもなります。ただし、接続ゲートウェイを内部ネットワークで使用しても、大きな利点はありません。管理サーバーが受信するネットワーク接続の数は減少しますが、受信データ量は減少しません。接続ゲートウェイがない場合でも、すべてのデバイスは管理サーバーへ接続可能です。

# 仮想管理サーバー

物理管理サーバーに基づいて、複数台の仮想管理サーバーを作成できます。これは、セカンダリ管理サーバーと類似したものです。仮想管理サーバーモデルは、アクセス制御リスト（ACL）に基づいた任意のアクセスモデルと比較した場合、機能性が高く、高度の分離性を実現しています。ポリシーとタスクが存在する割り当て済みデバイスの管理グループ専用の構造に加えて、各仮想管理サーバーにも未割り当てデバイスのグループ、レポート、抽出されたデバイスとイベント、インストールパッケージ、移動ルールなどがあります。仮想管理サーバーの機能範囲は、サービスプロバイダー（xSP）が顧客の分離を最大化する用途でも、高度なワークフローと多くの管理者が存在する大規模な組織でも使用できます。

仮想管理サーバーはセカンダリ管理サーバーと非常に類似していますが、次の相違点があります：

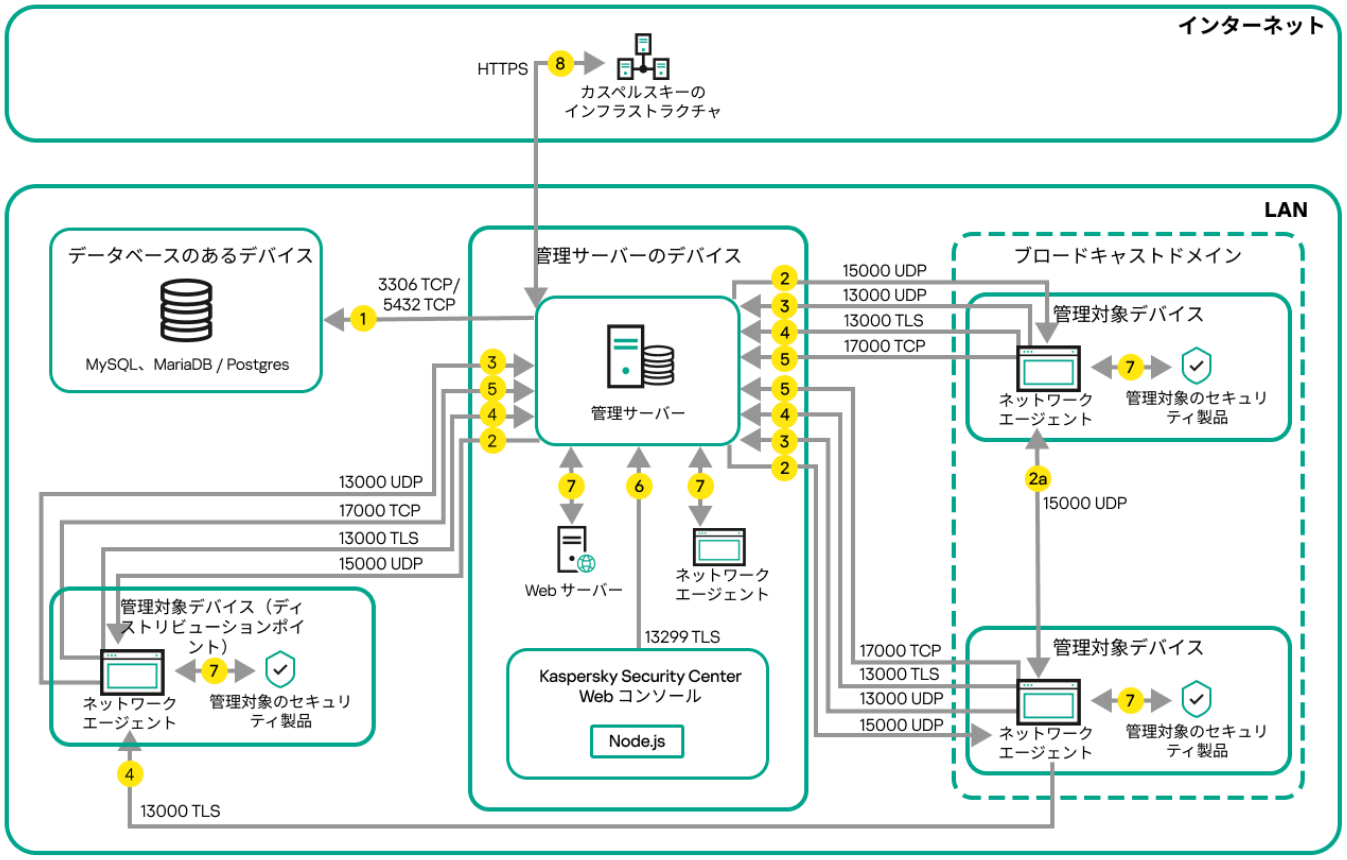
- 仮想管理サーバーには、多数のグローバル設定と独自の TCP ポートが備えられていません。
- 仮想管理サーバーには、セカンダリ管理サーバーはありません。
- 仮想管理サーバーには、他の仮想管理サーバーはありません。
- 物理管理サーバーには、すべての仮想管理サーバーの管理対象デバイスに関するデバイス、グループ、およびオブジェクトが表示されます（隔離中の項目、アプリケーションレジストリなど）。
- 仮想管理サーバーがスキャンできるのは、ディストリビューションポイントが接続されているネットワークのみです。

# データトラフィックの流れと使用ポートの図解

このセクションでは、Kaspersky Security Center Linux コンポーネント、管理されるセキュリティ製品、外部サーバーの構成に応じて、データトラフィックの流れを図解したスキーマを掲載しています。スキーマには、ローカルデバイスで使用可能になっている必要のあるポートの番号も記載されています。

## LAN 内に管理サーバーと管理対象デバイスがある構成

次の図は、Kaspersky Security Center を LAN（ローカルエリアネットワーク）内に限定して導入した場合のデータトラフィックの流れを示しています。




LAN（ローカルエリアネットワーク）内に管理サーバーと管理対象デバイスがある構成

この図には複数の管理対象デバイスが存在し、管理サーバーに直接またはディストリビューションポイントを経由して接続しています。ディストリビューションポイントを利用することで、アップデート配信時の管理サーバーの負荷を軽減し、ネットワークトラフィックを最適化できます。ただし、ディストリビューションポイントは管理対象デバイスの数が一定数以上の場合にのみ必要です。管理対象デバイスの数が少ない場合、すべての管理対象デバイスは管理サーバーから直接アップデートを取得できます。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server または MariaDB Server 用のポート 3306、または PostgreSQL サーバーと Postgres Pro サーバーの場合はポート 5432）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

   2a.モバイル以外の管理対象デバイス上のネットワークエージェントは、同じブロードキャストドメイン内の他のネットワークエージェントに関するデータを交換します（その後、データは管理サーバーに送信されます）。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

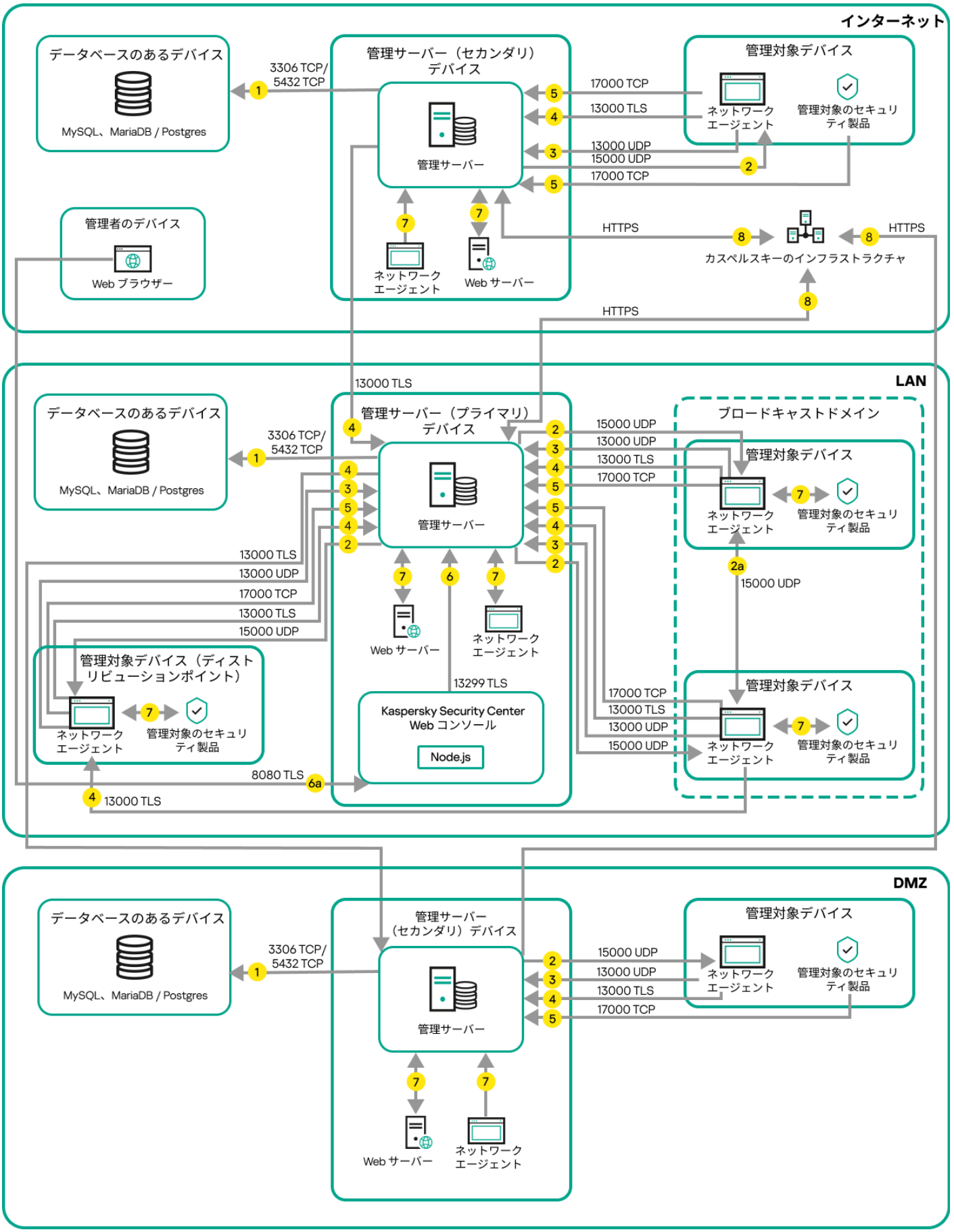
7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

# プライマリ管理サーバーが LAN 内にありセカンダリ管理サーバーが 2 台ある構成

次の図は、管理サーバーの階層構造の例を示しています。プライマリ管理サーバーがローカルエリアネットワーク（LAN）内にあります。セカンダリ管理サーバーのうち 1 台は DMZ 内にあります。もう 1 台のセカンダリ管理サーバーとはインターネット経由で接続しています。




管理サーバーの階層構造：プライマリ管理サーバーと 2 台のセカンダリ管理サーバー

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server または MariaDB Server 用のポート 3306、または PostgreSQL サーバーと Postgres Pro サーバーの場合はポート 5432）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center Linux もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   6a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

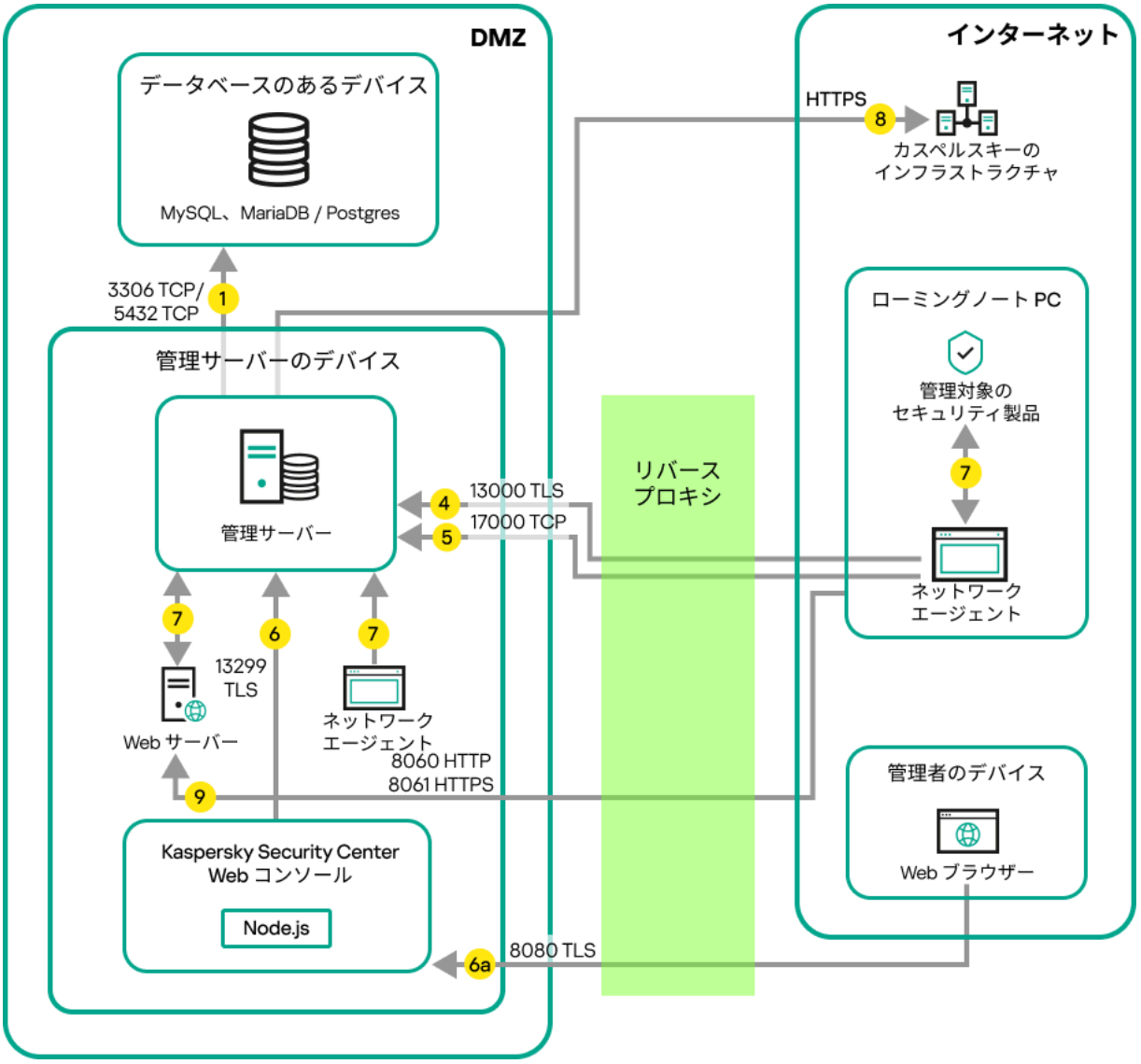
7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

# 管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（リバースプロキシを使用）

次の図は、管理サーバーがローカルエリアネットワーク（LAN）内にあり管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。この図では、任意に選択したリバースプロキシが使用されています。詳細については、製品のドキュメントを参照してください。




ローカルエリアネットワーク上の管理対象デバイスはリバースプロキシ経由で管理サーバーに接続されています

モバイルデバイスが管理サーバーに直接接続しないように構成し、なおかつ DMZ 内に接続ゲートウェイを割り当てない場合は、この構成での導入が推奨されます。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server または MariaDB Server 用のポート 3306、または PostgreSQL サーバーと Postgres Pro サーバーの場合はポート 5432）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center Linux もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   6a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. モバイルデバイスを含む管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに iOS MDM サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

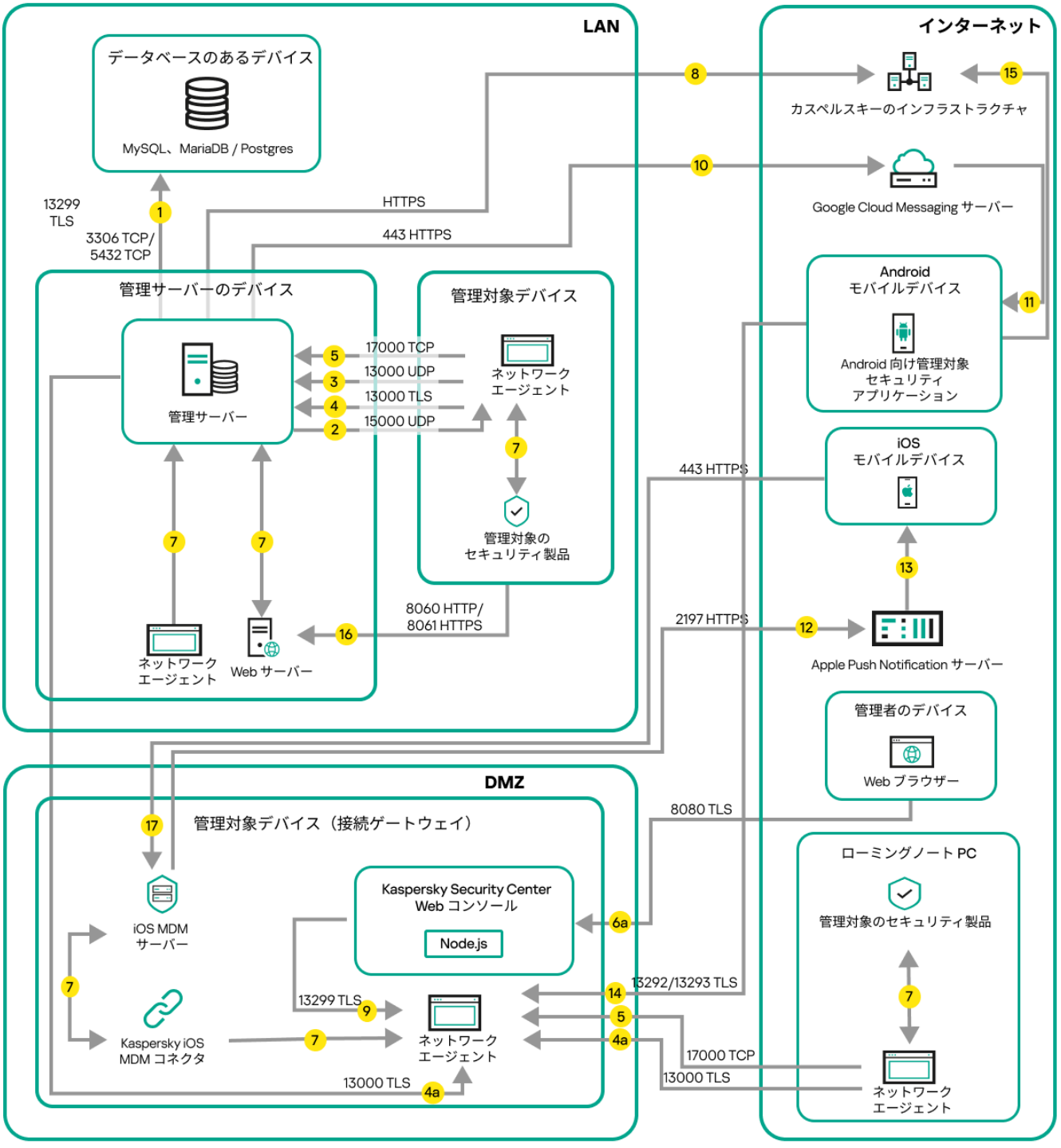
    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

16. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

# 管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（接続ゲートウェイを使用）

次の図は、管理サーバーがローカルエリアネットワーク（LAN）内にあり管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。接続ゲートウェイが使用されています。

管理対象デバイスが管理サーバーに直接接続しないように構成し、なおかつリバースプロキシまたは企業ファイアウォールを使用しない場合は、この構成での導入が推奨されます。




接続ゲートウェイを使用して管理サーバーに接続する管理対象のモバイルデバイス

この図では、管理対象デバイスは DMZ 内にある接続ゲートウェイを経由して管理サーバーに接続しています。リバースプロキシや企業ファイアウォールは使用されていません。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server または MariaDB Server 用のポート 3306、または PostgreSQL サーバーと Postgres Pro サーバーの場合はポート 5432）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center Linux もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   4a.DMZ 内の接続ゲートウェイは、TLS ポート 13000 を使用して管理サーバーからの接続も受信します。DMZ 内の接続ゲートウェイは管理サーバーのポートに到達できないため、管理サーバーは接続ゲートウェイとの永続的な信号接続を作成して維持します。信号接続はデータ転送には使用されません。これは、ネットワーク対話への招待の送信にのみ使用されます。接続ゲートウェイがサーバーに接続する必要がある場合、接続ゲートウェイはこの信号接続を介してサーバーに通知し、サーバーはデータ転送に必要な接続を作成します。

   社外のデバイスも同様に、TLS ポート 13000 を通じて接続ゲートウェイに接続します。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   6a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. モバイルデバイスを含む管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに iOS MDM サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

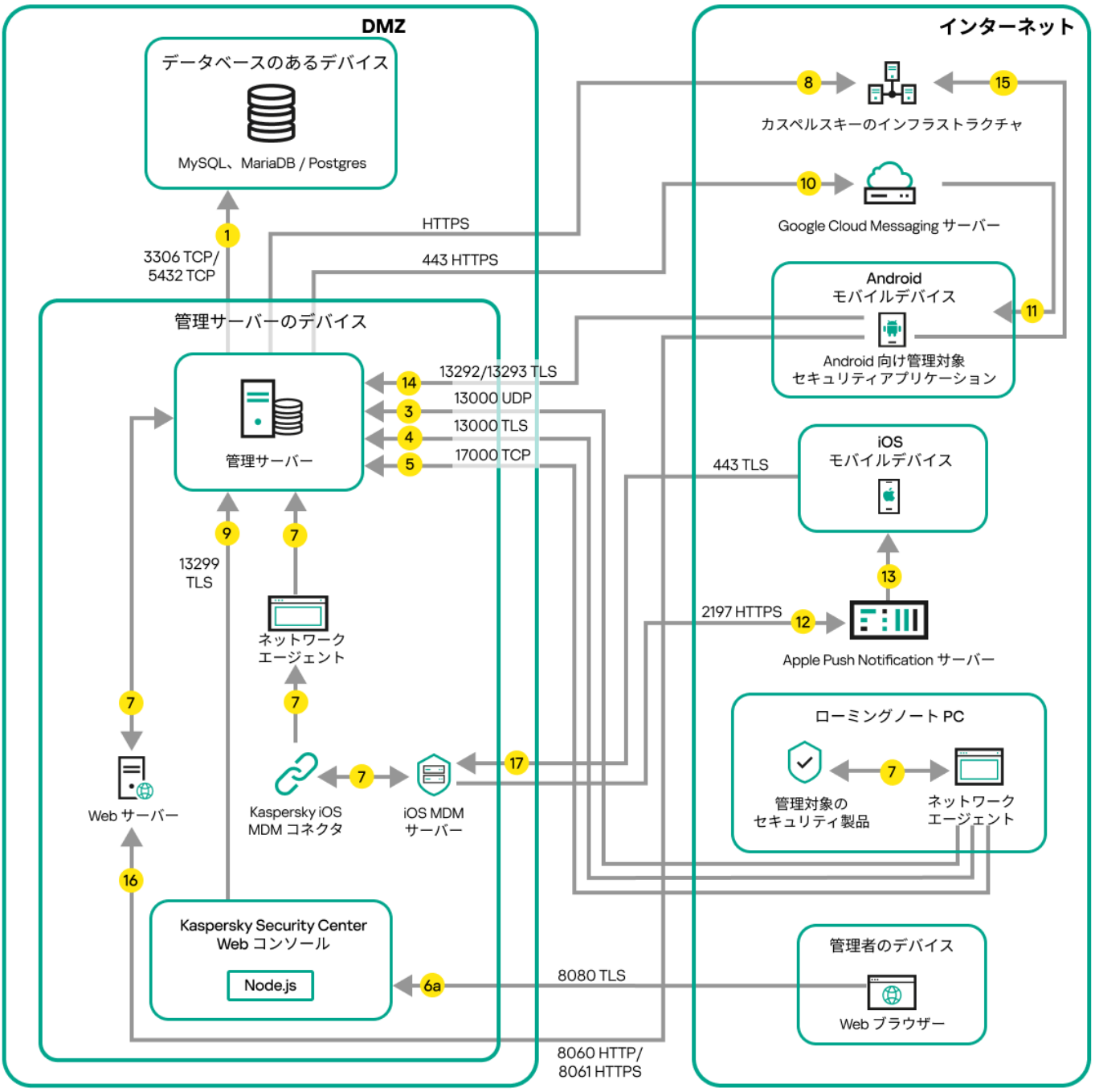
15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

16. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

# 管理サーバーが DMZ 内にありインターネット経由で管理対象デバイスに接続している構成

次の図は、管理サーバーが DMZ（非武装地帯）内にあり管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。




管理サーバーが DMZ 内にありインターネット経由で管理対象のモバイルデバイスに接続している構成

この図の構成では、接続ゲートウェイは使用されておらず、モバイルデバイスが管理サーバーに直接接続されています。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server または MariaDB Server 用のポート 3306、または PostgreSQL サーバーと Postgres Pro サーバーの場合はポート 5432）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center Linux もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   6a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. 管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。FCM サービスも 443 HTTPS ポートで実行されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに iOS MDM サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

16. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

# Kaspersky Security Center Linux コンポーネントとセキュリティ製品の対話：詳細

このセクションでは、Kaspersky Security Center Linux コンポーネントと管理アプリケーションの対話スキームについて説明します。このスキームには、使用可能にする必要があるポートの番号と、それらのポートを開くプロセスの名前が含まれます。

## 対話スキームで使用される表記規則

下の表では、対話スキームで使用される表記規則を説明します。

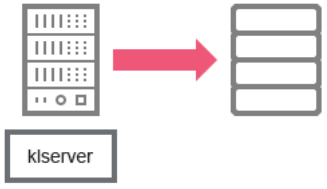
表記規則

| アイコン | 意味 |
| --- | --- |
|  | 管理サーバー |
|  | セカンダリ管理サーバー |
|  | DBMS |

| | |
|---|---|
|  | クライアントデバイス（ネットワークエージェントと Kaspersky Endpoint Security または Kaspersky Security Center Linux が管理できるセキュリティ製品がインストールされているクライアントデバイス） |
|  | 接続ゲートウェイ |
|  | ディストリビューションポイント |
|  | ユーザーのデバイスにあるブラウザー |
|  | デバイスと開いているポートで実行しているプロセス |
|  | ポートとポート番号 |
|  | TCP トラフィック（トラフィックの方向は矢印で示されます） |
|  | UDP トラフィック（トラフィックの方向は矢印で示されます） |
|  | DBMS トランスポート |
|  | DMZ の境界 |

# 管理サーバーと DBMS

管理サーバーからのデータはデータベースに入力されます。

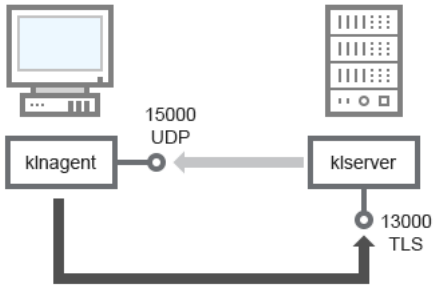



管理サーバーと DBMS

管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MariaDB 用のポート 3306 など）。関連する情報については、DBMS のドキュメントを参照してください。

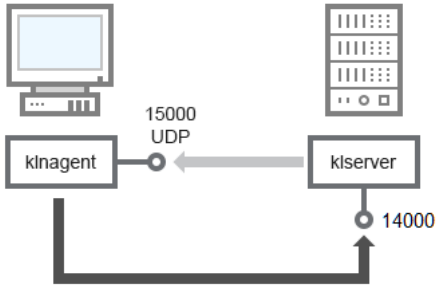
# 管理サーバーとクライアントデバイス：セキュリティ製品の管理

管理サーバーは、ネットワークエージェントからの接続を TLS ポート 13000 で受信します（次の図を参照）。




管理サーバーとクライアントデバイス：セキュリティ製品の管理、ポート 13000 を使用した接続（推奨）

Kaspersky Security Center Linux の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 SSL ポート 14000 で受信する場合があります（次の図を参照）。Kaspersky Security Center Linux もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、SSL ポート 13000 の使用が推奨されます。




管理サーバーとクライアントデバイス：セキュリティ製品の管理、ポート 14000 を使用した接続（低セキュリティ）

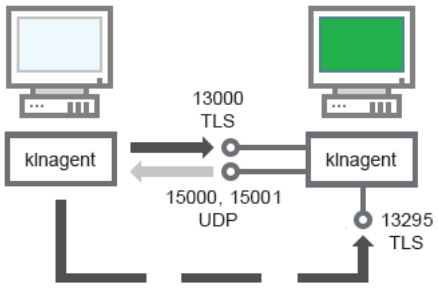
図の詳細については、次の表を参照してください。

管理サーバーとクライアントデバイス：セキュリティ製品の管理（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| ネットワークエージェント | 15000 | klnagent | UDP | ネットワークエージェント用のマルチキャスト |
| 管理サーバー | 13000 | klserver | TCP (TLS) | ネットワークエージェントから接続を受信する |
| 管理サーバー | 14000 | klserver | TCP | ネットワークエージェントから接続を受信する |

# クライアントデバイスにあるソフトウェアをディストリビューションポイント経由でアップグレードする

クライアントデバイスは、ポート 13000（ディストリビューションポイントをプッシュサーバーとして使用している場合は、13295 も）を使用して、ディストリビューションポイントへ接続します。ディストリビューションポイントは、ポート 15000 を使用してネットワークエージェントへのマルチキャストを実行します（下の図を参照）。アップデートとインストールパッケージは、ポート 15001 経由でディストリビューションポイントから受信されます。




クライアントデバイスにあるソフトウェアをディストリビューションポイント経由でアップグレードする

スキーマについては、下表を参照してください。

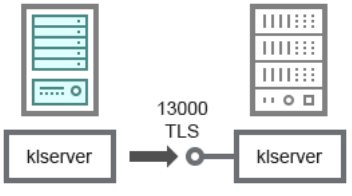
ソフトウェアをディストリビューションポイント経由でアップグレードする（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| ネットワークエージェント | 15000 | klnagent | UDP | ネットワークエージェント用のマルチキャスト |
| ネットワークエージェント | 15001 | klnagent | UDP | ディストリビューションポイントからアップデートとインストールパッケージを受信する |
| ディストリビューションポイント | 13000 | klnagent | TCP (TLS) | ネットワークエージェントから接続を受信する |
| ディストリビューションポイント | 13295 | klnagent | TCP (TLS) | クライアントデバイスからの接続の受信（サーバープッシュ） |

# 管理サーバーの階層構造：プライマリ管理サーバーとセカンダリ管理サーバー

次の図は、1 つの階層にまとめられた管理サーバーがポート 13000 を使用して通信することを示しています。

それにより、管理サーバーを組み合わせて 1 つの階層にした時、両方の管理サーバーをプライマリ管理サーバーに接続された Kaspersky Security Center Web コンソールから管理できます。したがって、プライマリ管理サーバーのポート 13299 を使用できることが唯一の前提条件です。



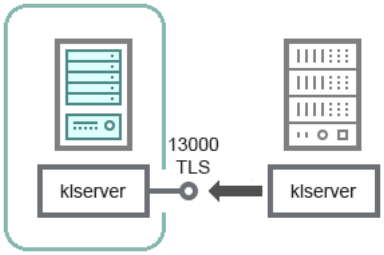

管理サーバーの階層構造：プライマリ管理サーバーとセカンダリ管理サーバー

スキーマについては、下表を参照してください。

管理サーバーの階層（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| プライマリ管理サーバー | 13000 | klserver | TCP (TLS) | セカンダリ管理サーバーから接続を受信する |

# DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造




DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造

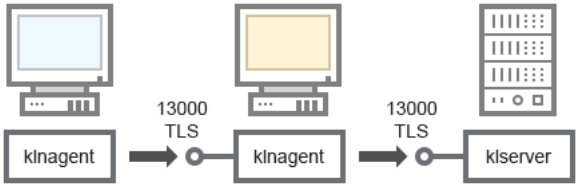
図に示す管理サーバーの階層構造では、DMZ にあるセカンダリ管理サーバーがプライマリ管理サーバーからの接続を受信します（図の詳細については次の表を参照）。2 つの管理サーバーを 1 つの階層内で組み合わせる時は、ポート 13299 が両方の管理サーバーで開放されていることを確認してください。Kaspersky Security Center Web コンソールは、ポート 13299 を介して管理サーバーに接続されます。

それにより、管理サーバーを組み合わせて 1 つの階層にした時、両方の管理サーバーをプライマリ管理サーバーに接続された Kaspersky Security Center Web コンソールから管理できます。したがって、プライマリ管理サーバーのポート 13299 を使用できることが唯一の前提条件です。

DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| セカンダリ管理サーバー | 13000 | klserver | TCP (TLS) | プライマリ管理サーバーから接続を受信する |

# ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス



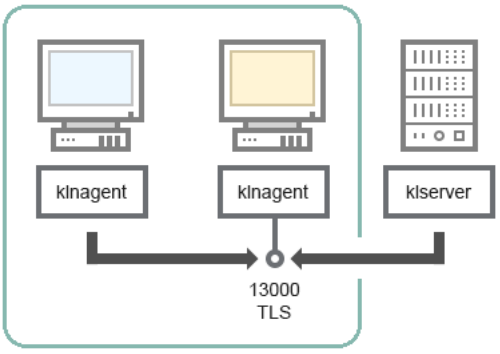

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス

スキーマについては、下表を参照してください。

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| 管理サーバー | 13000 | klserver | TCP (TLS) | ネットワークエージェントから接続を受信する |
| ネットワークエージェント | 13000 | klnagent | TCP (TLS) | ネットワークエージェントから接続を受信する |

# DMZ に管理サーバーと 2 台のデバイス（接続ゲートウェイとクライアントデバイス）



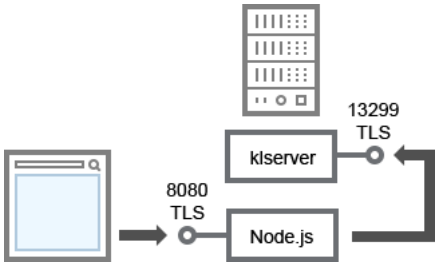

接続ゲートウェイのある管理サーバーと DMZ 内のクライアントデバイス

スキーマについては、下表を参照してください。

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| ネットワークエージェント | 13000 | klnagent | TCP (TLS) | ネットワークエージェントから接続を受信する |

# 管理サーバーと Kaspersky Security Center Web コンソール




管理サーバーと Kaspersky Security Center Web コンソール

スキーマについては、下表を参照してください。

管理サーバーと Kaspersky Security Center Web コンソール（トラフィック）

| デバイス | ポート番号 | ポートを開くプロセスの名前 | プロトコル | ポートの目的 |
|---|---|---|---|---|
| 管理サーバー | 13299 | klserver | TCP (TLS) | Kaspersky Security Center Web コンソールから OpenAPI 経由での管理サーバーへの接続を受信する |
| Kaspersky Security Center Web コンソールサーバーまたは管理サーバー | 8080 | Node.js: Server-side JavaScript | TCP (TLS) | Kaspersky Security Center Web コンソールから接続を受信する |

Kaspersky Security Center Web コンソールは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

# 使用の開始

このシナリオに従うことで、Kaspersky Security Center Linux 管理サーバーと Kaspersky Security Center Web コンソールのインストール、クイックスタートウィザードを使用した管理サーバーの初期セットアップ、および製品導入ウィザードを使用した管理対象デバイスへのカスペルスキー製品のインストールが実行できます。

## 必須条件

Kaspersky Endpoint Security for Business のライセンス（アクティベーションコード）またはカスペルスキーセキュリティ製品のライセンス（アクティベーションコード）を持っている必要があります。

Kaspersky Security Center Linux を試用版で使用する場合は、カスペルスキーの Web サイトで 30 日間有効な試用版を取得できます。

## 実行するステップ

主要なインストールシナリオは、次の手順で進みます：

1. **組織を保護する仕組みの選択**

   Kaspersky Security Center Linux コンポーネントの詳細をご確認ください。分散ネットワークを運用している場合、ネットワークの設定と通信チャネルのスループットに基づき、使用する管理サーバーの数と、使用する管理サーバーを組織内で分配すべき方法を定義します。

   管理サーバーの階層を使用するかどうかを定義します。これを定義するには、すべてのクライアントデバイスを 1 台の管理サーバーでカバーすることが可能かつ有益か、または管理サーバーの階層を構築することが必要か、いずれかを評価する必要があります。また、保護対象のネットワークが属する組織の組織構造と同一の管理サーバーの階層を構築する必要がある場合があります。

2. **カスタム証明書を使用するための準備**

   組織の公開鍵インフラストラクチャ（PKI）で、特定の認証局（CA）によって発行されたカスタム証明書を使用する必要がある場合は、それらの証明書を準備し、すべての要件を満たしていることを確認してください。

3. **DBMS（データベース管理システム）のインストール**

   Kaspersky Security Center Linux 用の DBMS（データベース管理システム）をインストールするか、既存の DBMS を使用します。

   サポート対象の DBMS のいずれかを選択します。選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

   Linux ベースのオペレーティングシステムのディストリビューションにサポートされている DBMS が含まれていない場合は、サードパーティのパッケージリポジトリから DBMS をインストールできます。サードパーティのリポジトリからのディストリビューションのインストールが禁止されている場合は、DBMS を別のデバイスにインストールできます。

   > PostgreSQL または Postgres Pro DBMS をインストールする場合は、スーパーユーザーのパスワードを指定したことを確認してください。パスワードが指定されていない場合、管理サーバーがデータベースに接続できない可能性があります。

   MariaDB、PostgreSQL、または Postgres Pro をインストールする場合は、DBMS が適切に機能するように推奨設定を使用してください。

インストール後に DBMS タイプを変更する場合は、Kaspersky Security Center Linux を再インストールする必要があります。データは部分的に手動で別のデータベースに転送できます。

4. **ポートの設定**

選択したセキュリティ構造に従ったコンポーネント間の対話に必要なすべてのポートが開いていることを確認します。

インターネットアクセスを管理サーバーに提供する必要がある場合、ネットワーク設定に応じてポートを設定し、接続設定を指定します。

5. **Kaspersky Security Center Linux のインストール**

管理サーバーとして使用する Linux デバイスを選択します。このデバイスがシステム要件を満たしていることを確認してから Kaspersky Security Center Linux をデバイスにインストールします。サーバー向けネットワークエージェントが、管理サーバーとともに自動的にインストールされます。

6. **Kaspersky Security Center Web コンソールと管理プラグインのインストール**

管理者のワークステーションとして使用する Linux デバイスを選択します。このデバイスがシステム要件を満たしていることを確認してから Kaspersky Security Center Web コンソールをデバイスにインストールします。Kaspersky Security Center Web コンソールは、管理サーバーがインストールされている同じデバイスまたは別のデバイスにインストールできます。

Kaspersky Endpoint Security for Linux 管理 Web プラグインをダウンロードしてから Kaspersky Security Center Web コンソールがインストールされているものと同じデバイスにインストールします。

7. **管理サーバーデバイスへの Kaspersky Endpoint Security for Linux およびネットワークエージェントのインストール**

既定では、管理サーバーデバイスは管理対象デバイスとして認識されません。管理サーバーをウイルスやその他の脅威から保護し、またそのデバイスをその他の管理対象デバイス同様に管理するには、Kaspersky Endpoint Security for Linux および Linux 向けネットワークエージェントを管理サーバーデバイスにインストールすることをお勧めします。この場合、Linux 向けネットワークエージェントは、管理サーバーと一緒にインストールしたサーバー版のネットワークエージェントとは別にインストールされ、動作します。

8. **初期セットアップの実行**

管理サーバーのインストールが完了すると、管理サーバーへの最初の接続時にクイックスタートウィザードが自動的に開始します。既存要件に従って、管理サーバーの初期設定を行います。初期設定段階中に、ウィザードが既定値設定を使用して、保護の導入に必要なポリシーとタスクを作成します。しかしながら、既定の設定は組織のニーズに対して十分ではない場合があります。必要に応じて、ポリシーやタスクの設定を編集できます。

9. **ネットワーク上のデバイスの検出**

デバイスを手動で検出します。Kaspersky Security Center Linux は、ネットワークで検出されたすべてのデバイスのアドレスと名前を受信します。その後、Kaspersky Security Center Linux を使用してカスペルスキー製品と他社製ソフトウェアを、検出されたデバイスにインストールできます。Kaspersky Security Center Linux はデバイスの検索を定期的に開始するため、新しいインスタンスがネットワークに現れると、それらのインスタンスは自動的に検出されます。

10. **管理グループ内へのデバイスの配置**

一部のケースでは、ネットワーク接続デバイスへ最も便利な方法で保護を導入する目的で、組織の構造を考慮してデバイスのプール全体を管理グループに分割しなければならない場合があります。グループにデバイスを配置する移動ルールを作成するか、デバイスを手動で配置することができます。管理グループへのグループタスクの割り当て、ポリシーの範囲の定義、およびディストリビューションポイントの割り当てが可能です。

すべての管理対象デバイスが適切な管理グループに正しく割り当てられ、ネットワーク上に未割り当てデバイスが存在しないことを確認します。

### ⓫ ディストリビューションポイントの割り当て

管理グループにディストリビューションポイントが自動的に割り当てられますが、必要に応じて手動で割り当てることもできます。大規模なネットワークにはディストリビューションポイントを使用することを推奨します。その理由は、低いスループットレートのチャネルを介して通信するデバイス（またはデバイスグループ）へのアクセスを管理サーバーに提供するために使用する分散構造ネットワーク上、および管理サーバーで、負荷を減らすためです。

### ⓬ ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストール

企業ネットワークへの保護の導入時には、デバイス検出中に管理サーバーによって検出されたデバイスにネットワークエージェントとセキュリティ製品をインストールする必要があります。

リモートで製品をインストールするには、製品導入ウィザードを実行します。

セキュリティ製品は、脅威をもたらすウイルスなどのプログラムからデバイスを保護します。ネットワークエージェントは、デバイスと管理サーバー間の通信が確実に行われるようにします。ネットワークエージェントは自動的に設定されるようになっています。

ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストールを開始する前に、それらのデバイスがアクセス可能である（電源が入っている）ことを確認してください。

### ⓭ ライセンスのクライアントデバイスへの導入

クライアントデバイスにライセンスを導入し、デバイス上の管理対象セキュリティ製品をアクティベートします。

### ⓮ カスペルスキー製品のポリシーの設定

異なるデバイスに異なる設定を適用するには、デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を使用できます。デバイスベースのセキュリティ管理は、ポリシーとタスクを使用することで実施できます。タスクは特定の条件を満たすデバイスに対してのみ適用できます。デバイスのフィルター処理の条件を設定するには、デバイスの抽出とタグを使用します。

### ⓯ ネットワーク保護ステータスの監視

ダッシュボードにあるウィジェットを使用したネットワーク監視、カスペルスキー製品からのレポートの生成、管理対象デバイス上のアプリケーションから受信したイベントの抽出の設定と表示、通知リストの表示ができます。

# ハードニングガイド

Kaspersky Security Center Linux は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。本製品は、管理者が組織のネットワークセキュリティレベルに関する詳細な情報にアクセスすることを可能にします。Kaspersky Security Center Linux では、カスペルスキー製品を使用することにより、構築されたすべての保護コンポーネントを設定することができます。

Kaspersky Security Center Linux 管理サーバーは、クライアントデバイスの保護管理に完全にアクセスでき、組織のセキュリティシステムを構成する最も重要なコンポーネントです。そのため、管理サーバーにはより強化された保護方法が必要です。

設定する前に、管理サーバーデータのバックアップタスクまたは klbackup ユーティリティを使用して、Kaspersky Security Center Linux 管理サーバーのバックアップコピーを作成し、安全な場所に保存してください。

ハードニングガイドでは、Kaspersky Security Center Linux とそのコンポーネントの構成に関する推奨事項と機能について説明し、セキュリティ侵害のリスクを軽減することを目的としています。

ハードニングガイドには、次の情報が含まれています：

- 管理サーバーアーキテクチャの選択
- 管理サーバーへの安全な接続の設定
- 管理サーバーにアクセスするためのアカウントの設定
- 管理サーバーの保護管理
- クライアントデバイスの保護管理
- 管理対象アプリケーションの保護構成
- 管理サーバーのメンテナンス
- サードパーティ製品への情報の転送
- サードパーティの情報システムに関するセキュリティ推奨事項

# 管理サーバーの導入

## 管理サーバーアーキテクチャ

一般に、集中管理アーキテクチャの選択は、保護対象となるデバイスの場所、隣接するネットワークからのアクセス、データベースのアップデート配信方式などによって異なります。

アーキテクチャ開発の初期段階で、Kaspersky Security Center Linux のコンポーネントとそれらの相互の対話、およびデータトラフィックとポートの使用に関する方式についてよく理解することを推奨します。

この情報をもとに、次の項目を指定するアーキテクチャを形成することができます：

- 管理サーバーの場所およびネットワーク接続
- 管理者のワークスペースの構成、および管理サーバーへの接続方法
- ネットワークエージェントと保護ソフトウェアの導入方法
- ディストリビューションポイントの使用
- 仮想管理サーバーの使用
- 管理サーバーの階層の使用
- 定義データベースのアップデート方式
- その他の情報の流れ

### 管理サーバーインストール用のデバイスの選択

組織インフラストラクチャ内の専用サーバーに管理サーバーをインストールすることを推奨します。サーバーに他のサードパーティ製ソフトウェアがインストールされていない場合は、サードパーティ製ソフトウェアの要件に依存せずに、Kaspersky Security Center Linux の要件に基づいてセキュリティ設定を構成することができます。

管理サーバーは、物理サーバーまたは仮想サーバーに導入することができます。選択されたデバイスがハードウェアおよびソフトウェアの要件を満たしていることをご確認ください。

### 管理サーバーをドメインコントローラー、ターミナルサーバー、またはユーザーデバイスに導入する際の制限

管理サーバーをドメインコントローラー、ターミナルサーバー、またはユーザーデバイスにインストールしないことを強く推奨します。

ネットワークキーノードの機能を分離することを推奨します。この方法により、ノードに障害が発生したり侵害されたりした場合でも、異なるシステムの運用性を維持することができます。同時に、ノードごとに異なるセキュリティポリシーを作成することができます。

### 管理サーバーをインストールして実行するためのアカウント

管理サーバーの展開中に、2 つの特権のないアカウントを作成する必要があります。管理サーバーに含まれるサービスは、これらの特権のないアカウントで動作します。アカウントに権限とアクセス許可を付与する時は、最小特権の原則に従います。［kladmins］グループに不要なアカウントを含めないでください。

内部 DBMS アカウントも作成する必要があります。管理サーバーは、この内部 DBMS アカウントを使用して、選択された DBMS にアクセスします。

必要なアカウントとそのアカウントの権限は、選択した DBMS の種類、管理サーバーデータベースの作成方法によって異なります。

## 接続の安全性

### TLS の使用

管理サーバーへのセキュアでない接続を禁止することを推奨します。たとえば、管理サーバーの設定で HTTP を使用する接続を禁止することができます。

既定では、管理サーバーの HTTP ポートが閉じられていることに注意してください。残りのポートは、管理サーバーのウェブサーバー（8060）に使用されます。このポートは、管理サーバーデバイスのファイアウォール設定によって制限される場合があります。

### 厳密な TLS 設定

バージョン 1.2 以降の TLS プロトコルを使用し、セキュアでない暗号化アルゴリズムを制限または禁止することを推奨します。

管理サーバーが使用する暗号化プロトコル（TLS）を設定できます。管理サーバーのバージョンがリリースされた時点では、既定では暗号化プロトコルの設定がセキュアなデータ転送を保証するように設定されていることに注意してください。

## 管理サーバーデータベースへのアクセスを制限する

管理サーバーデータベースへのアクセスを制限することを推奨します。たとえば、管理サーバーデバイスからのみアクセスを許可します。これにより、既知の脆弱性が原因で管理サーバーデータベースが危険にさらされる可能性が低くなります。

使用するデータベースの操作説明書に従ってパラメータを構成したり、ファイアウォールで閉じたポートを提供したりすることができます。

## 外部 DBMS とのセキュリティ対話

管理サーバー（外部 DBMS）のインストール中に DBMS が別のデバイスにインストールされる場合は、この DBMS とのセキュアな対話と認証のためのパラメータを設定することを推奨します。SSL 認証の設定の詳細については、「PostgreSQL サーバーの認証」および「シナリオ：MySQL サーバーの認証」を参照してください。

## 管理サーバーに接続するための IP アドレスの許可リストの設定

既定では、Kaspersky Security Linux ユーザーは、Kaspersky Security Center Web コンソールまたは OpenAPI アプリケーションがインストールされている任意のデバイスから Kaspersky Security Center Linux にログインできます。管理サーバーを設定することで、ユーザーが許可された IP アドレスを持つデバイスからのみ管理サーバーに接続できるように設定できます。たとえば、侵入者が許可リストに含まれていないデバイスにインストールされた Kaspersky Security Center Web コンソールサーバーを介して Kaspersky Security Center Linux に接続しようとしても、Kaspersky Security Center Linux にログインすることはできません。

## Kaspersky Security Center Web コンソールに接続するための IP アドレスの許可リストの設定

既定では、Kaspersky Security Center Linux ユーザーはどのデバイスからでも Kaspersky Security Center Web コンソールに接続できます。Kaspersky Security Center Web コンソールがインストールされているデバイスでは、ユーザーが許可された IP アドレスからのみ Kaspersky Security Center Web コンソールに接続できるように、ファイアウォール（オペレーティングシステムに組み込まれているものまたはサードパーティ製のもの）を設定する必要があります。

## ポーリング中のドメインコントローラーへの接続のセキュリティ

ドメインコントローラーをポーリングするために、管理サーバーまたは Linux ディストリビューションポイントは LDAPS 経由でこのドメインに接続しようとします。既定では、接続時に証明書の検証は必要ありません。証明書の検証を強制するには、`KLNAG_LDAP_TLS_REQCERT` フラグを 1 に設定します。また、`KLNAG_LDAP_SSL_CACERT` フラグを使用して、証明書チェーンにアクセスするための証明機関（CA）へのカスタムパスを指定することもできます。

# アカウントおよび認証

以下の手順を実行する前に、管理サーバーデータのバックアップまたは klbackup ユーティリティを使用して Kaspersky Security Center Linux 管理サーバーのバックアップコピーを作成し、安全な場所に保存します。

## 管理サーバーでの二段階認証の使用

**Kaspersky Security Center Linux は、RFC 6238 標準（TOTP：Time-Based One-Time Password アルゴリズム）に基づいて、Kaspersky Security Center Web コンソールのユーザーに二段階認証を提供します。**

自分のアカウントに二段階認証が適用されると、Kaspersky Security Center Web コンソールにログインするたびに、ユーザー名、パスワードおよび追加で一回のみ使用するセキュリティコードを入力するようになります。1度だけ使用するセキュリティコードを受け取るには、ご使用のコンピューターまたはモバイルデバイスなどに認証アプリがインストールされている必要があります。

RFC 6238 標準に対応したソフトウェアとハードウェアの両方の認証機能（トークン）があります。たとえば、ソフトウェア認証には、Google Authenticator、Microsoft Authenticator、FreeOTP などがあります。

管理サーバーへの接続が確立されているデバイスと同じデバイスに認証アプリをインストールすることは強く推奨しません。モバイルデバイスに認証アプリをインストールすることができます。

### 新規ユーザーによる二段階認証の設定の制限

Kaspersky Security Center Web コンソールのアクセスセキュリティをさらに向上させるために、新しいユーザーが自分自身に二段階認証を設定することを禁止できます。

このオプションをオンにする場合、二段階認証が無効になっているユーザー（例：新しいドメイン管理者など）は、自分自身に二段階認証を設定できません。したがって、そのようなユーザーは管理サーバーで認証できず、既に二段階認証を有効にしている別の Kaspersky Security Center Linux 管理者の承認がなければ Kaspersky Security Center Web コンソールにサインインできません。

## オペレーティングシステムの二要素認証の使用

管理サーバーデバイスでの認証には、トークン、スマートカード、またはその他の方法（可能な場合）を使用した多要素認証（MFA）を使用することを推奨します。

## 管理者パスワード保存の制限

Kaspersky Security Center Web コンソールを使用する場合、ユーザーのデバイスにインストールされているブラウザーに管理者パスワードを保存することは推奨しません。

## 内部ユーザーアカウントの認証

既定では、管理サーバーの内部ユーザーアカウントのパスワードは次の規則に従う必要があります：

- パスワードは、8 文字以上 256 文字以下にしてください。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

既定では、許可されるパスワードの入力試行回数の上限は 10 回です。パスワード入力の試行回数を変更することができます。

Kaspersky Security Center Linux のユーザーが無効なパスワードを入力できる回数には上限があります。入力回数が上限に達すると、ユーザーアカウントが 1 時間ブロックされます。

## 内部ユーザーアカウントのパスワードを変更するためのオプションの設定

内部ユーザーアカウントのパスワードを変更するには、次のオプションを設定することを推奨します：

- パスワードローテーション期間
- パスワードを変更する必要があることを事前に警告する時間
- ［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］の値

## 不正な改変からのアカウント保護

管理サーバーの内部ユーザーアカウントを不正な変更から保護するために、追加オプションをオンにすることを推奨します。この保護は、内部ユーザーごとに個別に設定する必要があります。

## 管理サーバー専用の管理グループ

管理サーバー専用の管理グループを作成することを推奨します。このグループには特別なアクセス権限を付与し、特別なセキュリティポリシーを作成します。

管理サーバーのセキュリティレベルを意図的に下げることを避けるために、専用の管理グループを管理できるアカウントのリストを制限することを推奨します。

## メイン管理者ロールの割り当ての制限

kladduser ユーティリティによって作成されたユーザーには、管理サーバーまたは仮想管理サーバーのアクセス制御リスト（ACL）でメイン管理者ロールが割り当てられます。メイン管理者ロールを多数のユーザーに割り当てることは避けることを推奨します。

## アプリケーション機能へのアクセス権の設定

ユーザーまたはユーザーグループごとに、Kaspersky Security Center Linux の機能へのアクセス権を柔軟に設定することを推奨します。

ロールベースのアクセス制御により、事前定義された一連の権利を持つ標準ユーザーロールを作成し、職務の範囲に応じてこれらのロールをユーザーに割り当てることができます。

ロールベースのアクセス制御モデルの主な利点：

- 管理の容易さ
- ロール階層
- 最小特権方法
- 職務の分離

職位に基づいて特定の従業員に組み込みのロールを割り当てたり、まったく新しいロールを作成したりすることができます。

ロールを構成する際は、管理サーバーデバイスの保護状態の変更とサードパーティ製ソフトウェアのリモートインストールに関連する権限に注意してください：

- 管理グループの管理。
- 管理サーバー上での操作。
- リモートインストール。
- イベントを保存して通知を送信するためのパラメータの変更。

  この権限により、イベントの発生時に管理サーバーデバイスでスクリプトまたは実行可能モジュールを実行する通知を設定できます。

## アプリケーションのリモートインストール用の個別のアカウント

アクセス権の基本的な差別化に加えて、すべてのアカウントに対してアプリケーションのリモートインストールを制限することを推奨します（メイン管理者または別の特殊なアカウントを除く）。

アプリケーションのリモートインストールには別のアカウントを使用することを推奨します。別のアカウントにロールまたは権限を割り当てることができます。

### すべてのユーザーとユーザーの行動の定期的な監査

管理サーバーデバイス上のすべてのユーザーを定期的に監査することを推奨します。これにより、デバイスが危険にさらされる可能性に関連する特定の種類のセキュリティ脅威に対応することができます。

また、管理サーバーへの接続や切断、管理サーバーへのエラーのある接続、オブジェクトの変更（リビジョン管理をサポートするオブジェクトの場合）などのユーザーのアクションを追跡することもできます。

## 管理サーバーの保護管理

### 管理サーバー保護ソフトウェアの選択

管理サーバーの導入種類と一般的な保護戦略に応じて、管理サーバーデバイスを保護するためのアプリケーションを選択します。

専用デバイスに管理サーバーを導入する場合は、Kaspersky Endpoint Security アプリケーションを選択して管理サーバーデバイスを保護することを推奨します。これにより、ふるまい分析モジュールなど、管理サーバーデバイスを保護するために使用可能なすべての技術を適用することができます。

インフラストラクチャに存在し、以前に他のタスクに使用されていたデバイスに管理サーバーがインストールされている場合は、次の保護ソフトウェアを検討することを推奨します：

- Kaspersky Industrial CyberSecurity for Nodes。産業用ネットワークに含まれるデバイスにこのアプリケーションをインストールすることを推奨します。Kaspersky Industrial CyberSecurity for Nodes は、産業用ソフトウェアの様々なメーカーとの互換性のある証明書を持つ製品です。

- 推奨するセキュリティ製品。管理サーバーが他のソフトウェアと一緒にデバイスにインストールされている場合、セキュリティ製品の互換性に関するそのソフトウェアベンダーの推奨事項を考慮することを推奨します（セキュリティソリューションを選択するための推奨事項が既に存在する場合があり、信頼ゾーンを構成する必要がある場合があります）。

### 保護アプリケーション用に別のセキュリティポリシーを作成

管理サーバーデバイスを保護するアプリケーション用に別のセキュリティポリシーを作成することを推奨します。このポリシーは、クライアントデバイスのセキュリティポリシーとは異なるものである必要があります。これにより、他のデバイスの保護レベルに影響を与えることなく、管理サーバーに最適なセキュリティ設定を指定することができます。

デバイスをグループに分けてから、特別なセキュリティポリシーを作成できる別のグループに管理サーバーデバイスを配置することを推奨します。

### 保護モジュール

管理サーバーと同じデバイスにインストールされているサードパーティ製ソフトウェアのベンダーから特別な推奨事項がない場合は、使用可能なすべての保護モジュールを有効化して構成することを推奨します（これらの保護モジュールの動作を一定時間チェックした後）。

### 管理サーバーデバイスのファイアウォールの構成

管理サーバーデバイスでは、ファイアウォールを設定して、管理者が Kaspersky Security Center Web コンソールを介して管理サーバーに接続できるデバイスの数を制限することを推奨します。

既定で、管理サーバーはポート 13299 を使用して Kaspersky Security Center Web コンソールからの接続を受信します。このポートを使用して管理サーバーを管理できるデバイスの数を制限することを推奨します。

# クライアントデバイスの保護管理

## インストールパッケージへのライセンスの追加制限

インストールパッケージは、管理サーバーの共有フォルダーのパッケージサブフォルダーに保存されます。インストールパッケージにライセンスを追加すると、このフォルダーに対する読み取り権限を持つすべてのユーザーがライセンスに（直接、または管理サーバーに組み込まれた Web サーバー経由で）アクセスできるようになります。

ライセンスへの侵害を避けるため、ライセンスをインストールパッケージに追加することは推奨しません。

管理対象デバイスへのライセンスの自動配布、管理対象アプリケーションのライセンスの追加タスクによる導入、アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加することを推奨します。

## 管理グループ間でデバイスを移動するための自動ルール

管理グループ間でデバイスを移動するための自動ルールの使用を制限することを推奨します。

デバイスを移動するための自動ルールを使用すると、移動したデバイスに移動前のデバイスよりも多くの特権を与えるポリシーが伝搬する可能性があります。

また、クライアントデバイスを別の管理グループに移動すると、ポリシー設定が伝播される可能性があります。このポリシー設定は、ゲストデバイスや信頼できないデバイスへの配布には望ましくない場合があります。

この推奨事項は、管理グループへのデバイスの 1 回限りの初期割り当てには適用されません。

## ディストリビューションポイントと接続ゲートウェイのセキュリティ要件

ネットワークエージェントがインストールされたデバイスは、ディストリビューションポイントとして機能し、次の機能を実行することができます：

- 管理サーバーから受信したアップデートとインストールパッケージをグループ内のクライアントデバイスに配布します。
- クライアントデバイスでサードパーティ製ソフトウェアとカスペルスキー製品のリモートインストールを実行します。
- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは、管理サーバーと同じデバイス検出方法を使用することができます。

次の目的で使用される組織のネットワークにディストリビューションポイントを配置します：

- 管理サーバーの負荷の低減
- トラフィックの最適化
- ネットワーク内の届きにくい場所にあるデバイスへの管理サーバーアクセスの提供

使用可能な機能を考慮して、ディストリビューションポイントとして機能するデバイスをあらゆる種類の不正アクセス（物理的アクセスなど）から保護することを推奨します。

## ディストリビューションポイントの自動割り当ての制限

管理を簡素化し、ネットワークの操作性を維持するために、ディストリビューションポイントの自動割り当てを使用することを推奨します。ただし、産業用ネットワークや小規模なネットワークでは、たとえば、リモートインストールのプッシュタスクに使用するアカウントの個人情報が OS によってディストリビューションポイントに転送される可能性があるため、ディストリビューションポイントの自動割り当ては避けることを推奨します。

産業用ネットワークおよび小規模ネットワークの場合、ディストリビューションポイントとして機能するデバイスを手動で割り当てることができます。

また、『ディストリビューションポイントのアクティビティレポート』を表示することもできます。

## Kaspersky Security Center Linux ユーザーのデバイスのセキュリティ要件

Kaspersky Security Center Linux ユーザーのデバイスには特別なセキュリティ要件を適用する必要があります。これらのデバイスをあらゆる種類の不正アクセス（物理的なアクセスも含む）から保護することを推奨します。

Kaspersky Security Center Linux ユーザーデバイスには次のものが含まれます：

- Kaspersky Security Center Linux ユーザーがブラウザーを使用して Kaspersky Security Center Web コンソールに接続するデバイス。
- OpenAPI 経由で管理サーバーと対話するアプリケーションが Kaspersky Security Center Linux に接続されるデバイス。

## Kaspersky Security Center Web コンソールがインストールされているデバイスのセキュリティ要件

Kaspersky Security Center Web コンソールがインストールされたデバイスは Kaspersky Security Center Linux の管理に使用されるため、これらのデバイスのセキュリティには特別な要件を適用する必要があります。これらのデバイスをあらゆる種類の不正アクセス（物理的なアクセスも含む）から保護することを推奨します。

# 管理対象アプリケーションの保護構成

## 管理対象アプリケーションポリシー

使用するアプリケーションと Kaspersky Security Center Linux のコンポーネント（ネットワークエージェント、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Agent など）の種別ごとにポリシーを作成することを推奨します。このポリシーは、すべての管理対象デバイス（ルート管理グループ）に適用するか、構成済みの移動ルールに従って新しい管理対象デバイスを自動的に移動させる別のグループに適用する必要があります。

## 保護を無効にしてアプリケーションをアンインストールするためのパスワードを指定

**侵入者によるカスペルスキーのセキュリティ製品の無効化やアンインストールを防ぐために、パスワード保護を有効にすることを強く推奨します。**パスワード保護がサポートされているプラットフォームでは、たとえば、Kaspersky Endpoint Security、ネットワークエージェント、その他のカスペルスキー製品のパスワードを設定できます。パスワードによる保護を有効にした後、「ロック」を閉じて対応する設定をロックすることを推奨します。

## クライアントデバイスを管理サーバーに手動で接続するためのパスワードの指定（klmover ユーティリティ）

klmover ユーティリティを使用すると、クライアントデバイスを管理サーバーに手動で接続できます。Klmover ユーティリティはネットワークエージェントのインストールフォルダーにあります。

侵入者がデバイスを管理サーバーの制御外に移動するのを防ぐために、klmover ユーティリティを実行する際のパスワード保護を有効にすることを強く推奨します。パスワード保護を有効にするには、ネットワークエージェントポリシー設定で［**アンインストール用パスワードを使用する**］をオンにします。

klmover ユーティリティにはローカル管理者権限が必要です。

Kaspersky Security Center Linux の管理下になくなったデバイスにインストールされた、パスワードで保護されたネットワークエージェントのパスワードを紛失または忘れた場合、klmover ユーティリティ、またはコマンドラインを使用してネットワークエージェントを削除することはできません。この場合、パスワードで保護されたネットワークエージェントがインストールされているデバイスにオペレーティングシステムを再インストールする必要があります。

Windows デバイスで**アンインストール用パスワードを使用する**オプションを有効にすると、クリーナーツール（cleaner.exe）のパスワード保護も有効になります。

## Kaspersky Security Network の使用

管理対象アプリケーションのすべてのポリシーと管理サーバーのプロパティで、Kaspersky Security Network（KSN）の使用を有効にし、KSN 声明を受け入れることを推奨します。管理サーバーをアップデートまたはアップグレードすると、更新された KSN 声明を受け入れることができます。法律などによりクラウドサービスの使用が禁止されている場合は、KSN を無効にすることができます。

### 管理対象デバイスの定期スキャン

すべてのデバイスグループに対して、デバイスのフルスキャンを定期的に実行するタスクを作成することを推奨します。

### 新しいデバイスの検出

デバイスの検索を適切に設定することを推奨します：ドメインコントローラーとの統合の設定、新規デバイスを検索するIPアドレス範囲の指定。

セキュリティ上の理由から、すべての新しいデバイスを含む既定の管理グループと、このグループに影響する既定のポリシーを使用することができます。

## 管理サーバーのメンテナンス

### 管理サーバーデータのバックアップコピー

データのバックアップにより、データを失うことなく管理サーバーのデータを復元することができます。

既定では、管理サーバーのインストール後にデータバックアップタスクが自動的に作成され、定期的に実行され、適切なディレクトリにバックアップが保存されます。
データバックアップタスクの設定は、次のように変更することができます：

- バックアップ頻度が上がります
- コピーを保存するための特別なディレクトリが指定されています
- バックアップコピーのパスワードが変更されます

既定のディレクトリとは異なる特別なディレクトリにバックアップコピーを保存する場合は、このディレクトリのアクセス制御リスト（ACL）を制限することを推奨します。管理サーバーアカウントと管理サーバーデータベースのアカウントには、このディレクトリへの書き込みアクセス権が必要です。

### 管理サーバーのメンテナンス

［管理サーバーのメンテナンス］により、データベースのボリュームを削減し、アプリケーションのパフォーマンスと操作の信頼性を向上させることができます。管理サーバーのメンテナンスは、少なくとも週に1回で実施することを推奨します。

管理サーバーのメンテナンスは、専用のタスクで実施されます。管理サーバーのメンテナンス時、次の処理が実行されます：

- データベースインデックスを再編成する
- データベースの統計情報をアップデート
- データベースを縮小する（必要に応じて）

### オペレーティングシステムのアップデートとサードパーティ製ソフトウェアのアップデートをインストール

オペレーティングシステムとサードパーティ製ソフトウェアのアップデートを管理サーバーデバイスに定期的にインストールすることを強く推奨します。

クライアントデバイスは管理サーバーへの継続的な接続を必要としないため、アップデートをインストール後に管理サーバーデバイスを再起動しても安全です。管理サーバーのダウンタイム中にクライアントデバイスに登録されたすべてのイベントは、接続が復元された後に管理サーバーに送信されます。

## サードパーティシステムへのイベント転送

### 監視とレポート

セキュリティ問題にタイムリーに対応するために、監視とレポート機能を設定することを推奨します。

### SIEM システムへのイベントのエクスポート

重大な損害が発生する前にセキュリティ問題を迅速に検知するには、SIEM システムでイベントエクスポートを使用することを推奨します。

### 監査イベントのメール通知

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。緊急事態にタイムリーに対応するために、公開する監査イベント、重要イベント、障害イベント、および警告に関する通知を送信するように管理サーバーを設定することを推奨します。

これらのイベントはシステム内のイベントであるため、少数のイベントが予想され、メーリングに非常に適しています。

## サードパーティの情報システムに関するセキュリティ推奨事項

### CIS ベンチマークからのセキュリティ推奨事項

管理サーバーおよびネットワークエージェントでサポートされているオペレーティングシステム、仮想化プラットフォーム、または定義データベースサーバーのバージョンを使用する場合は、Center for Internet Security（CIS）のベストインフォメーションセキュリティプラクティスを適用して（存在する場合）、これらの情報システムを微調整することを推奨します。

Center for Internect Security（CIS）は、情報技術分野におけるセキュリティの向上に取り組む非営利団体です。特に、CIS は CIS コントロールや CIS ベンチマークなどの安全基準を開発し、配布しています。これらの標準は、情報システムのセキュリティを確保するための一連の推奨事項と方法です。

CIS ポータルには、管理サーバーおよびネットワークエージェントでサポートされている次の情報システムのバージョンに対する推奨事項が含まれています：

- 次のファミリーのオペレーティングシステム：
  - デスクトップ向け Windows
  - サーバー向け Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware 仮想化プラットフォーム
- データベースサーバー：
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

## Astra Linux オペレーティングシステムのセキュリティに関する推奨事項

Astra Linux オペレーティングシステムを使用する場合は、対応するバージョンの Astra Linux の Red Book に記載されているセキュリティ推奨事項に従う必要があります。

## RED OS オペレーティングシステムのセキュリティに関する推奨事項

RED OS オペレーティングシステムを使用する場合は、公式 RED OS ドキュメントに記載されている管理者ガイドのセキュリティ推奨事項に従う必要があります。

# カスペルスキーセキュリティ製品の使用に関する推奨事項

## Kaspersky Endpoint Security for Windows で KLAdmin パスワードを使用します

KLAdmin アカウントは、Kaspersky Endpoint Security for Windows への無制限のアクセス権を持つ管理者アカウントです。KLAdmin アカウントには、Kaspersky Endpoint Security for Windows でパスワードで保護されたすべての操作（本製品の削除など）を実行する権限があります。KLAdmin アカウントの権限は取り消すことができません。Kaspersky Endpoint Security for Windows ポリシーのプロパティで KLAdmin アカウントのパスワードを設定できます。Kaspersky Endpoint Security for Windows 管理者は、KLAdmin アカウントのパスワードの安全使用について全責任を負います。組織に独自のパスワードポリシーがある場合は、そのポリシーの指示に従ってください。パスワードが長くて複雑であればあるほど、信頼性が高まります。

KLAdmin パスワードの盗難から組織を保護するための推奨事項は次の通りです。

- **一般要件**

  アカウント名または名前の一部をパスワードとして使用しないでください。

- **パスワードの最小文字数要件**

  少なくとも 10 文字の長さのパスワードを作成してください。

- **複数の文字タイプを使用するための要件**

  小文字、大文字、数字、特殊文字など、さまざまなカテゴリの文字を含む複雑なパスワードを設定します。

- **パスワードの有効期限要件**

  パスワードの有効期限を最小 90 日に設定します。新しいパスワードは、過去 24 個のパスワードのいずれとも一致してはなりません。

# シナリオ：MySQL サーバーの認証

MySQL サーバーの認証には TLS 証明書を使用することを推奨します。信頼できる証明機関（CA）の証明書または自己署名証明書を使用できます。

管理サーバーは、MySQL に対して一方向および双方向の SSL 認証の両方をサポートします。

## 一方向 SSL 認証の有効化

MySQL の一方向 SSL 認証を設定するには、次の手順に従います：

1. **MySQL サーバー用の自己署名 TLS 証明書を生成する**

   次のコマンドを実行します：

   ```
   openssl genrsa 1024 > ca-key.pem

   openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem

   openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
   > server-req.pem
   ```

```
openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **サーバーフラグファイルの作成**

   klscflag ユーティリティを使用して KLSRV_MYSQL_OPT_SSL_CA サーバーフラグを作成し、その値として証明書へのパスを指定します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem へのパス> -t d
   ```

3. **定義データベースの設定**

   ファイル my.cnf で証明書を指定します。テキストエディターでファイル my.cnf を開き、次の行を［mysqld］セクションに追加します：

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

## 双方向 SSL 認証の有効化

MySQL の双方向 SSL 認証を設定するには、次の手順に従います：

1. **サーバーフラグファイルの作成**

   klscflag ユーティリティを使用してサーバーフラグを作成し、その値として証明書ファイルへのパスを指定します。

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem へのパス ca-
   cert.pem> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v < server-cert.pem> -t s へのパス

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v < server-key.pem> -t s へのパス
   ```

   klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

2. **パスフレーズを指定する（オプション）**

   server-key.pem にパスフレーズが必要な場合は、KLSRV_MARIADB_OPT_TLS_PASPHRASE フラグを作成し、その値としてパスフレーズを指定します：

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <パスフレーズ> -t s
   ```

3. **定義データベースの設定**

   ファイル my.cnf で証明書を指定します。テキストエディターでファイル my.cnf を開き、次の行を［mysqld］セクションに追加します：

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

# シナリオ：PostgreSQL サーバーの認証

PostgreSQL サーバーの認証には TLS 証明書を使用することを推奨します。信頼できる証明機関（CA）の証明書または自己署名証明書を使用できます。

管理サーバーは、PostgreSQL に対して一方向および双方向の SSL 認証の両方をサポートします。

PostgreSQL サーバーの認証は次の段階で進行します：

1. **PostgreSQL サーバーの証明書を生成する**

   次のコマンドを実行します：

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **管理サーバーの証明書を生成する**

   次のコマンドを実行します：CN 値は、管理サーバーの代わりに PostgreSQL に接続するユーザーの名前と一致する必要があります。ユーザー名は既定で postgres に設定されます。

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **クライアント証明書認証を設定する**

   pg_hba.conf を次のように変更します：

   ```
   hostssl mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   pg_hba.conf に `host` で始まるレコードが含まれていないことを確認してください。

4. **PostgreSQL の証明書を指定する**

   **一方向 SSL 認証**

   postgresql.conf を次のように変更します（.crt およびライセンス情報ファイルへの正しいパスを指定します）：

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_cert_file = '<psql.crt>'
   ```

   ```
   ssl_key_file = '<psql.key>'
   ```

   **双方向 SSL 認証**

postgresql.conf を次のように変更します（.crt およびライセンス情報ファイルへの正しいパスを指定します）：

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **PostgreSQL デーモンを再起動する**

次のコマンドを実行します：

```
systemctl restart postgresql-14.service
```

6. **管理サーバーのサーバーフラグを指定する**

**一方向 SSL 認証**

klscflag ユーティリティを使用して KLSRV_POSTGRES_OPT_SSL_CA サーバーフラグを作成し、その値として証明書へのパスを指定します。

コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

次のコマンドを実行します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt へのパス > -t s
```

**双方向 SSL 認証**

klscflag ユーティリティを使用してサーバーフラグを作成し、その値として証明書ファイルへのパスを指定します。

コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

次のコマンドを実行します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt へのパス > -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <postgres.crt へのパス> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <postgres.key へのパス> -t s
```

postgres.key にパスフレーズが必要な場合は、KLSRV_POSTGRES_OPT_TLS_PASPHRASE フラグを作成し、その値としてパスフレーズを指定します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <パスフレーズ> -t s
```

7. **管理サーバーサービスを再起動する**

# 導入準備

このセクションでは、組織のニーズに応じて、Kaspersky Security Center Linux の導入、Kaspersky Security Center Linux の設定、および DBMS のオプションをオンにする方法について説明します。

組織のネットワークに Kaspersky Security Center Linux コンポーネントを導入するには、次の基準に応じていくつかのオプションがあります：

- デバイスの合計数
- 組織的または地理的に離れている組織単位（ローカルオフィス、支社、支店）
- 狭い帯域幅で接続されている個別のネットワーク
- 管理サーバーへのインターネットアクセス

1 台の管理サーバーで最大 50,000 台のデバイスをサポートできます（DBMS として PostgreSQL または Postgres Pro を使用）。組織ネットワーク上に合計で 50,000 台を超えるデバイスが存在する場合は、ネットワークに複数の管理サーバーを導入し、階層化して一元的に管理する必要があります。

組織に大規模なリモートローカルオフィス（支社、支店）が存在し、それぞれに独自の管理者が割り当てられている場合は、各オフィスに管理サーバーを導入するのが適切な方法です。そうしない場合は、そのようなオフィスは、低スループットチャネルによって接続された個別のネットワークとみなす必要があります（「標準設定：各オフィスの管理者によって運用されている少数の大規模なオフィス」を参照）。

狭い帯域幅で接続されている個別のネットワークを使用する際にトラフィック量を軽減するには、1つまたは複数個のネットワークエージェントをディストリビューションポイントとして動作するように割り当てます（ディストリビューションポイントの数の計算表を参照してください）。この場合、個別のネットワーク上にあるすべてのデバイスは、それらのローカルアップデートセンターからアップデートを取得します。有効なディストリビューションポイントでは、管理サーバー（既定のシナリオ）とインターネット上のカスペルスキーのサーバーの両方からアップデートをダウンロードできます（「標準設定：複数の小規模なリモートオフィス」を参照）。

［Kaspersky Security Center Linux の標準設定］セクションでは、Kaspersky Security Center Linux の標準設定について詳しく説明されています。製品の導入を計画している場合は、組織の組織構造に応じて最適な標準設定を選択してください。

導入計画段階では、管理サーバーに対して特別な X.509 証明書を割り当てることを検討する必要があります。管理サーバーに対する X.509 証明書の割り当てが有効になるのは、次の場合です（部分的なリスト）：

- SSL Termination プロキシまたはリバースプロキシを使用して、セキュアソケットレイヤー（SSL）トラフィックをスキャンする場合
- 組織の公開鍵基盤（PKI）と統合する場合
- 証明書で必要な値を指定する場合
- 証明書で必要な暗号化強度を指定する場合

# Kaspersky Security Center Linux の設定の選択

このセクションでは、組織ネットワークに Kaspersky Security Center Linux コンポーネントを導入する際に使用する次の標準設定について説明します：

- 単一のオフィス
- 少数の大規模なオフィス。地理的に離れており、各管理者が運用
- 複数の小規模なオフィス。地理的に離れている

## 標準設定：単一のオフィス

組織ネットワークには、1台または複数台の管理サーバーを導入できます。管理サーバーの数は、使用可能なハードウェアまたは管理対象デバイスの合計数に基づき選択可能です。

1台の管理サーバーで最大 50,000 台のデバイスをサポートできます（DBMS として PostgreSQL または Postgres Pro を使用）。導入後に管理対象デバイスを増やす可能性がある場合は、1台の管理サーバーに接続するデバイスの数を少なくしておきます。

管理サーバーに対するインターネットアクセスが必要かどうかに応じて、管理サーバーを内部ネットワーク上または DMZ 内に導入することができます。

複数台のサーバーを使用する場合は、1つの階層に統合してください。管理サーバーの階層を使用することによりポリシーとタスクが重複するのを防ぎ、管理対象デバイスの全セットを1台の管理サーバーで管理している場合と同様に処理できます。つまり、デバイスの検索、デバイス選択の構築、レポートの作成などの処理を、1台の管理サーバーで管理している場合と同様に実行できます。

## 標準設定：各オフィスの管理者によって運用されている少数の大規模なオフィス

組織が地理的に離れている少数の大規模なオフィスによって構成されている場合は、各オフィスに管理サーバーを導入する構成を検討する必要があります。クライアントデバイスの数と使用可能なハードウェアに応じて、各オフィスに1台または複数の管理サーバーを導入できます。この場合、個別のオフィスは「標準設定：単一のオフィス」として表示できます。管理を簡単にするために、すべての管理サーバーを管理サーバーの階層にまとめることを推奨します（場合によっては、3 層以上の階層にする必要があります）。

一部の従業員がデバイス（ノート PC）を持ってオフィス間を移動する場合は、ネットワークエージェントポリシーでネットワークエージェント接続プロファイルを作成します。ネットワークエージェント接続プロファイルは、Windows および macOS ホストでのみサポートされていることに注意してください。

## 標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィスと本社からなるネットワーク向けの設定です。各リモートオフィスのネットワークは、ネットワークアドレス変換（NAT）を介するように NAT の内側に構成することができます。その場合、2 つのリモートオフィスは分離されているため、それらのリモートオフィス間の接続は確立できません。

本社に 1 台の管理サーバーを導入すると同時に、その他のすべてのオフィスに対して 1 つまたは複数個のディストリビューションポイントを割り当てる必要があります。オフィス間がインターネットを経由して接続されている場合は、ディストリビューションポイントでディストリビューションポイントのリポジトリにアップデートを*ダウンロードタスクを作成して*おくことが有用な場合があります。これにより、管理サーバーからではなくカスペルスキーのサーバー、ローカルまたはネットワークフォルダーから直接アップデートをダウンロードできるようになります。

リモートオフィスにあるデバイスが管理サーバーに直接にはアクセスできない場合（たとえば、管理サーバーへはインターネットを介してアクセスできるが、インターネットアクセスを備えていないデバイスがある場合）は、ディストリビューションポイントを接続ゲートウェイモードに切り替える必要があります。この場合、リモートオフィスにあるデバイスのネットワークエージェントは、直接にではなくゲートウェイを介して管理サーバーに接続され、緊密に同期します。

たいていの場合、管理サーバーはリモートオフィスのネットワークをポーリングできないため、ディストリビューションポイントに対してこの機能をオンにしておくと便利です。

管理サーバーは、リモートオフィスにある NAT よりも内側にある管理対象デバイスに対して、ポート 15000 UDP に通知を送信することはできません。この問題を解決するために、ディストリビューションポイントとして動作しているデバイスのプロパティで、管理サーバーへの常時接続モードを有効にしておくことができます（[**管理サーバーから切断しない**]）。このモードは、ディストリビューションポイントの合計数が 300 を超えていない場合に使用可能です。プッシュサーバーを使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。詳細については、以下のトピックを参照してください：プッシュサーバーの有効化。

# 企業を保護する仕組みを選択する

企業組織を保護する仕組みは、次の要因に基づいて選択します：

- 組織のネットワークトポロジー
- 組織の構造
- ネットワーク保護対策の担当者数および担当者の役割
- 保護管理コンポーネントに割り当てることができるハードウェア資源
- 組織のネットワークで保護コンポーネントのメンテナンスに割り当てることができる通信チャネルの処理能力
- 組織のネットワークで重要な管理作業を実行する際の制限時間。重要な管理作業には、定義データベースの配信やクライアントデバイスについてのポリシーの変更などが含まれます

保護の仕組みを選択する際は、まず、一元的な保護システムの運用に使用できるネットワーク資源およびハードウェア資源を評価してください。

ネットワークおよびハードウェアインフラストラクチャを分析するには、以下のプロセスに従ってください：

1. 保護を導入するネットワークについて、次の設定を定義します：
   - ネットワークセグメントの数
   - 個々のネットワークセグメント間の通信チャネルの速度
   - 各ネットワークセグメントでの管理対象デバイスの数
   - 保護の運用を維持するために割り当てることができる各通信チャネルの処理能力
2. 管理対象のすべてのデバイスに対して重要な管理作業を実施する時の最大許容時間を決めます。
3. ステップ1および2からの情報、および管理システムの負荷試験のデータを分析します。分析に基づき、次の問いに回答します。
   - 1台の管理サーバーですべてのクライアントを管理することが可能か。または、管理サーバーの階層が必要か。
   - ステップ2に指定された制限時間内にすべてのクライアントを処理するには、管理サーバーのどのハードウェア構成が必要か。
   - 通信チャネルの負荷を減らすためにディストリビューションポイントを使用する必要があるか。

上記ステップ3の問いに対する回答を得たら、組織の保護の仕組みをまとめることができます。

組織のネットワークでは、次の標準的な保護の仕組みのいずれかを使用できます。

- 管理サーバー1台：すべてのクライアントデバイスを1台の管理サーバーに接続します。管理サーバーは、ディストリビューションポイントとして機能します。
- 1台の管理サーバーといくつかのディストリビューションポイント：すべてのクライアントデバイスを1台の管理サーバーに接続します。ネットワークに接続されたクライアントデバイスの一部がディストリビューションポイントとして機能します。
- 管理サーバーの階層：ネットワークセグメントごとに1台の管理サーバーを割り当て、管理サーバーの階層の一部にします。プライマリ管理サーバーがディストリビューションポイントとして機能します。
- 管理サーバーの階層といくつかのディストリビューションポイント：ネットワークセグメントごとに1台の管理サーバーを割り当て、管理サーバーの階層の一部にします。ネットワークに接続されたクライアントデバイスの一部がディストリビューションポイントとして機能します。

# 保護システム導入の一般的なスキーム

このセクションでは、Kaspersky Security Centerを使用して企業ネットワークに保護システムを導入する際の基本的なスキームについて説明します。

システムは、あらゆる不正アクセスから保護される必要があります。本製品をデバイスにインストールする前に、オペレーティングシステムで利用可能なすべてのセキュリティアップデートをインストールするとともに、管理サーバーとディストリビューションポイントが物理的な不正アクセスを受けないような保護対策を実施してください。

Kaspersky Security Center で以下の導入スキームを使用して、企業ネットワークに保護システムを導入できます：

- Kaspersky Security Center Web コンソールを通じて保護システムを導入します。

  カスペルスキー製品は、自動でクライアントデバイスにインストールされ、Kaspersky Security Center を使用することによって自動的に管理サーバーに接続されます。

- Kaspersky Security Center によって生成されたスタンドアロンインストールパッケージを使用して、手動で保護システムを導入します。

  クライアントデバイスと管理コンピューターにカスペルスキー製品を手動でインストールし、ネットワークエージェントのインストール時にクライアントデバイスと管理サーバーの接続を設定します。

  この導入方法は、リモートインストールが実行できない場合に使用してください。

Kaspersky Security Center は、 Microsoft Active Directory® グループポリシーを使用した導入をサポートしていません。

# DBMS の選択

次の表に、有効な DBMS オプションとその使用上の推奨事項と制限事項を示します。

DBMS に関する推奨事項と制限事項

| DBMS | 推奨事項と制限事項 |
| --- | --- |
| MySQL（サポートされているバージョンを参照） | 20,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |
| MariaDB（サポートされているバージョンを参照） | 20,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |
| PostgreSQL、Postgres Pro（サポートされているバージョンを参照） | 50,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |

選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。

PostgreSQL または Postgres Pro DBMS をインストールする場合は、スーパーユーザーのパスワードを指定したことを確認してください。パスワードが指定されていない場合、管理サーバーがデータベースに接続できない可能性があります。

MySQL、MariaDB、PostgreSQL、または Postgres Pro をインストールする場合は、DBMS が適切に機能するように推奨設定を使用してください。

PostgreSQL、MariaDB、または MySQL DBMS を使用する場合、［**イベント**］タブには、選択したクライアントデバイスのイベントの不完全なリストが表示されることがあります。これは、DBMS が非常に大量のイベントを保存する場合に発生します。次のいずれかを実行すると、表示されるイベントの数を増やすことができます：

- 不要なイベントを削除します。
- 不要なイベントの保存期間を短縮します。

デバイスの管理サーバーに記録されたイベントの完全なリストを表示するには、レポートを使用します。

# 管理サーバーへのインターネットアクセス

以下のケースでは、管理サーバーへのインターネットアクセスが必要になります：

- 定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデート
- サードパーティ製ソフトウェアのアップデート

  既定では、管理サーバーが管理対象デバイスに Microsoft 製品のアップデートをインストールするためにインターネット接続は必要ありません。たとえば、管理対象デバイスは、Microsoft Update サーバーから直接、または組織のネットワークに展開されている Microsoft Windows Server Update Services（WSUS）を使用して WindowsServer から、Microsoft ソフトウェアのアップデートをダウンロードできます。次の場合は、管理サーバーをインターネットに接続する必要があります。

  - 管理サーバーを WSUS サーバーとして使用する
  - Microsoft ソフトウェア以外のサードパーティ製ソフトウェアのアップデートをインストールする
- サードパーティ製ソフトウェアの脆弱性の修正

  管理サーバーで次のタスクを実行する場合は、インターネット接続が必要になります。

  - Microsoft ソフトウェアの脆弱性に対して推奨される修正のリストを作成する。このリストは、カスペルスキーのスペシャリストにより作成され、定期的に更新されます。
  - Microsoft 製ソフトウェア以外のサードパーティ製ソフトウェアで脆弱性を修正する場合。
- モバイルユーザーのデバイス（ノート PC）の管理
- リモートオフィスでのデバイスの管理
- リモートオフィスのプライマリ管理サーバーまたはセカンダリ管理サーバーとの通信
- モバイルデバイスの管理

このセクションでは、インターネットを介して管理サーバーにアクセスする一般的な方法について説明します。管理サーバーにインターネット経由でアクセスすることに焦点が当てられている場合は、管理サーバーの専用証明書が必要とされます。

## インターネットアクセス：ローカルネットワーク上の管理サーバー

組織の内部ネットワーク内に管理サーバーが配置されている場合は、管理サーバーの TCP ポート 13000 でポート転送を使用して、外部からのアクセスを可能にすることを検討してください。

## インターネットアクセス：DMZ 内の管理サーバー

組織ネットワークの DMZ 内に管理サーバーが置かれている場合、組織の内部ネットワークにはアクセスできません。この場合、次の制限事項が適用されます：

- 管理サーバーは新しいデバイスを検出できません。
- 管理サーバーは、組織の内部ネットワーク上のデバイスに対して、強制インストールによるネットワークエージェントの初期導入を実行できません。

  これが適用されるのは、ネットワークエージェントの初期インストールに対してのみです。ただし、ネットワークエージェントに関する以降のアップグレードやセキュリティ製品のインストールは、管理サーバーで実行できます。

Kaspersky Security Center Linux は、Microsoft Windows のグループポリシーを使用した導入をサポートしていないことに注意してください。

組織のネットワーク上にあるディストリビューションポイントを使用できます。複数のデバイスでネットワークエージェントを使用せずに初期導入を実行するには、最初にいずれかのデバイスにネットワークエージェントをインストールしてから、そのネットワークエージェントにディストリビューションポイントステータスを割り当てます。そうすることにより、管理サーバーがこのディストリビューションポイントを使用して、その他のデバイスにネットワークエージェントを初期インストールできるようになります。

組織の内部ネットワーク内にある管理対象デバイスから UDP ポート 15000 に対して正常に通知を送信するには、ネットワーク全体がディストリビューションポイントの管理下にある必要があります。割り当てたディストリビューションポイントのプロパティで、［**管理サーバーから切断しない**］をオンにします。その結果、管理サーバーがディストリビューションポイントに常時接続できるようになると同時に、ディストリビューションポイントは組織の内部ネットワーク（IPv4 または IPv6 ネットワーク）内のデバイスの UDP ポート 15000 に対して通知を送信できるようになります。

# インストール

このセクションでは、Kaspersky Security Center Linux と Kaspersky Security Center Web コンソールのインストールについて説明しています。

# Kaspersky Security Center Linux と動作する MariaDB x64 サーバーの設定

Kaspersky Security Center と連携するように MariaDB x64 サーバーを正常に設定するには、この記事で指定されているサーバーパラメータを除き、既定のサーバーパラメータを使用する必要があります。

### my.cnf ファイルの推奨設定

DBMS の設定の詳細については、「アカウントの設定」手順も参照してください。DBMS のインストールについては、「DBMS のインストール」手順を参照してください。

*my.cnf ファイルを設定するには：*

1. テキストエディターで my.cnf ファイルを開きます。

2. ファイル my.ini の［mysqld］セクションに、次の行を入力します：

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< 値 >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` の値は、想定される KAV データベースのサイズの 80% 以上に設定する必要があります。指定されたメモリは、サーバーの起動時に割り当てられることに注意してください。データベースのサイズが指定されたバッファサイズより小さい場合、必要なメモリのみが割り当てられます。MariaDB 10.4.3 以前を使用する場合、割り当てられたメモリの実際のサイズは、指定されたバッファー サイズよりも約 10% 大きくなります。

このパラメータの値を「1」または「2」にすると MariaDB の動作速度に悪影響を及ぼす可能性があるため、パラメータには「`innodb_flush_log_at_trx_commit=0`」を使用してください。
「`innodb_file_per_table`」パラメータが「`1`」に設定されていることを確認します。

MariaDB 10.1 の場合は、［mysqld］セクションに次の行を追加で入力します：

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

MariaDB 10.6 の場合は、［mysqld］セクションに次の行を追加で入力します：

```
optimizer_prune_level=0
optimizer_search_depth=8
```

既定では、オプティマイザのアドオン「`join_cache_incremental`、「`join_cache_hashed`」、「`join_cache_bka`」は有効になっています。これらのアドオンが無効になっている場合は、有効にする必要があります。

*オプティマイザのアドオンが有効になっているかどうかを確認するには：*

1. MariaDB クライアントコンソールで、次のコマンドを実行してください：

   ```
   SELECT @@optimizer_switch;
   ```

2. 出力に次の行が含まれていることを確認します：

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   これらの行が存在して値に「on」が指定されている場合は、オプティマイザのアドオンは有効です。

   これらの行が存在しない、または値に「off」が指定されている場合は、以下を実行する必要があります：

   a. テキストエディターで my.cnf ファイルを開きます。

   b. 次の行を my.cnf ファイルに追加します：

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

アドオン「join_cache_incremental」、「join_cache_hash」および「join_cache_bka」が有効になりました。

# Kaspersky Security Center Linux と動作する PostgreSQL または Postgres Pro サーバーの設定

Kaspersky Security Center Linux と動作するように PostgreSQL または Postgres Pro サーバーを正常に設定するには、この記事で指定されているサーバーパラメータを除き、既定のサーバーパラメータを使用する必要があります。

Kaspersky Security Center Linux は、PostgreSQL および Postgres Pro DBMS をサポートしています。これらの DBMS のいずれかを使用する場合は、DBMS サーバーパラメータを設定して、Kaspersky Security Center Linux と DBMS の連携を最適化することを検討してください。

設定情報ファイルへの既定のパスは次の通りです：`/etc/postgresql/<VERSION>/main/postgresql.conf`

PostgreSQL および Postgres Pro の推奨パラメータ：

- `shared_buffers = N`

  N = DBMS がインストールされているデバイスの RAM の値の 25%。RAM が 1 GB 未満の場合は、既定値のままにします。

- `max_stack_depth` = 最大スタックサイズ（この値を KB 単位で取得するには、「`ulimit -s`」コマンドを実行します）から 1 MB の安全マージンを引いた値

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

［`standard_conforming_strings`］パラメータが既定値の［`on`］に設定されていることを確認します。postgresql.conf ファイルを更新した後、設定を再ロードするか、サーバーを再起動します。詳細は、PostgreSQL のドキュメントを参照してください。

クラスタ Postgres DBMS を使用する場合は、クラスタ構成だけでなくすべての DBMS サーバーに対して `max_connections` パラメータを指定します。

Postgres Pro 15.7 または Postgres Pro 15.7.1 を使用する場合は、`enable_compound_index_stats` パラメータを無効にします：

```
enable_compound_index_stats = off
```

PostgreSQL および Postgres Pro サーバーパラメータの詳細とパラメータの指定方法については、該当する DBMS のドキュメントを参照してください。

PostgreSQL および Postgres Pro のアカウントを作成および構成する方法の詳細は、次のトピックを参照してください：「PostgreSQL と Postgres Pro で作業するためのアカウントの設定」。

## 高可用性クラスタのサポート

高可用性の MariaDB および PostgreSQL クラスタは、次の設定でサポートされます：

レプリケーションタイプ：同期。

最小ノード数：3。

最大ノード数：15。

サーバーが DBMS にアクセスするために使用する Postgres ロールには、次のビューを読み取る権限が必要です（既定で有効）：

- pg_stat_replication
- pg_stat_wal_receiver

データベースとして Postgres Highly Available クラスター（バージョン 14 以降）を使用する場合、データベースのユーザーは `pg_read_all_stats` 権限を持つ必要があります。次のコマンドを実行してこの権限を付与できます：

```
GRANT pg_read_all_stats TO "%1";
```

ここで、「`%1`」はデータベース ユーザーの名前です。

ユーザー名は、管理サーバーのインストール時に `KLSRV_UNATT_DBMS_LOGIN` パラメータで指定されます。

# Kaspersky Security Center Linux と動作する MySQL x64 サーバーの設定

Kaspersky Security Center と連携するように MySQL x64 サーバーを正常に設定するには、この記事で指定されているサーバーパラメータを除き、既定のサーバーパラメータを使用する必要があります。

Kaspersky Security Center に MySQL サーバーを使用する場合、InnoDB および MEMORY ストレージおよび UTF-8 と UCS-2 のエンコーディングのサポートを有効にします。

## my.cnf ファイルの推奨設定

DBMS の設定の詳細については、「アカウントの設定」手順も参照してください。DBMS のインストールについては、「DBMS のインストール」手順を参照してください。

*my.cnf ファイルを設定するには：*

1. テキストエディターで my.cnf ファイルを開きます。
2. ファイル my.cnf の `[mysqld]` セクションに、次の行を追加します：

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<実際の値は想定される KAV データベースのサイズの 80% 以上に設定する必要があります>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0（多くの場合、サーバーは少ないトランザクションを使用します）
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

`innodb_buffer_pool_size` 値で指定されたメモリは、サーバーの起動時に割り当てられることに注意してください。データベースのサイズが指定されたバッファサイズより小さい場合、必要なメモリのみが割り当てられます。割り当てられたメモリの実際のサイズは、指定されたバッファサイズよりも約 10% 大きくなります。詳細は、MySQL のドキュメントを参照してください。

このパラメータの値を「1」または「2」にすると MySQL の動作速度に悪影響を及ぼす可能性があるため、パラメータには「`innodb_flush_log_at_trx_commit = 0`」を使用してください。
「`innodb_file_per_table`」パラメータが「`1`」に設定されていることを確認します。

# Kaspersky Security Center Linux のインストール

Kaspersky Security Center Linux をインストールする方法について説明します。

インストールする前に、次を実行する必要があります。

- DBMS をインストールします。
- Kaspersky Security Center Linux をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。

  > オペレーティングシステム RED OS 7.3.4 以降または MSVSPHERE 9.2 以降を使用している場合は、管理サーバーを正しく機能させるために libxcrypt-compat パッケージをインストールしてください。

- DNS サーバーがネットワーク上で利用可能であることを確認してください。

デバイスにインストールされている Linux ディストリビューションに応じて、「ksc64_<バージョン番号>_amd64.deb」または「ksc64-<バージョン番号>.x86_64.rpm」のいずれかのインストールファイルを使用してください。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

> Kaspersky Security Center Linux をインストールするには、root 権限を持つアカウントで以下のコマンドを実行する必要があります。

*Kaspersky Security Center Linux をインストールするには：*

1. グループ「kladmins」と特権のないアカウント「ksc」を作成します。このアカウントは「kladmins」グループに属するメンバーである必要があります。このためには、次のコマンドを順に実行します：

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

2. 必要に応じて、管理サーバーサービスの機能に使用されるアカウントに対して開くことができるファイル（ファイル記述子）の既定の制限を増やします。これを行うには、/etc/security/limits.conf ファイルを開き、次のようにファイル記述子のソフト制限とハード制限を指定します。

   ```
   ksc      ソフト   ファイルなし      <開かれたファイルの最大数>
   ksc      ハード   ファイルなし      <開かれたファイルの最大数>
   ```

   既定では、ファイル記述子の制限はインストール時に指定されます。ソフトファイル制限は 32,768 ファイル、ハードファイル制限は 131,072 ファイルです。

3. Kaspersky Security Center Linux のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

   - `# apt install /<path>/ksc64_<バージョン番号>_amd64.deb`
   - `# yum install /<path>/ksc64-<バージョン番号>.x86_64.rpm -y`

4. Kaspersky Security Center Linux の設定を実行します：

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、プライバシーポリシーの内容に同意する必要があります。

6. 確認が表示されてから次の設定を入力します：

   a. 管理サーバーの DNS 名または静的 IP アドレスを入力します。そのアドレスは、他のデバイスが管理サーバーに接続するために使用されます。

   b. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

   c. 管理するデバイスの概数を見積もります：

      - 管理対象デバイスの数が 1 ～ 100 の場合は、「1」を入力します。
      - 管理対象デバイスの数が 101 ～ 1000 の場合は、「2」を入力します。
      - 管理対象デバイスの数が 1000 以上の場合は、「3」を入力します。

      この設定は、ネットワーク負荷を最適化するために、タスクの開始を自動的にランダムに遅延させるために使用されます。以下のテーブルは、遅延が計算される間隔を示しています：

| 管理対象デバイス数が 1 ～ 100 の場合、値は 1 | 管理対象デバイス数が 101 ～ 1000 の場合、値は 2 | 管理対象デバイスが 1000 台超の場合、値は 3 |
|---|---|---|
| 遅延は使用されません | 5 分 | 10 分 |

   a. サービス用のセキュリティグループ名を入力します。既定では、 `kladmins` グループが使用されます。

   b. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では `ksc` アカウントが使用されます。

   c. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では `ksc` アカウントが使用されます。

   d. Kaspersky Security Center Linux と連携するためにインストールした DBMS を選択します：

      - MySQL または MariaDB をインストールした場合は、1 を入力します。
      - PostgreSQL または Postgres Pro をインストールした場合は、2 を入力します。

   e. データベースがインストールされるデバイスの DNS 名または IP アドレスを入力します。`127.0.0.1`（ローカル DBMS インストール時の既定値）。

   f. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、次のポートが使用されます：

- ポート 3306（MySQL または MariaDB）
- ポート 5432（PostgreSQL または Postgres Pro）

g. データベースの名前を入力します。

h. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

i. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。
サービスが追加され自動的に開始されるまで待ちます。

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

j. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。
パスワードは次のルールに従う必要があります：

- ユーザーパスワードは 8 文字以上 256 文字以下である必要があります。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

この手順を省略した場合は、後で次のコマンドを使用して新しいユーザーを作成できます：/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>

ユーザーが追加され、Kaspersky Security Center Linux がインストールされます。

## ネットワークエージェントのインストール

管理サーバーデバイスを他の管理対象デバイスとして管理するには、管理サーバーデバイス上で Linux 用ネットワークエージェントをインストールします。この場合、Linux 向けネットワークエージェントは、管理サーバーと一緒にインストールしたサーバー版のネットワークエージェントとは別にインストールされ、動作します。

### サービスの検証

サービスが実行されているかどうかを確認するには、次のコマンドを実行します：

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

## Kaspersky Security Center Linux をサイレントモードでインストールする

Kaspersky Security Center Linux を Linux デバイスにインストールするには、応答ファイルを使用してサイレントモードで、つまりユーザーの参加なしでインストールを実行します。応答ファイルには、インストールパラメータのカスタムセット（変数とそれぞれの値）が含まれています。

インストールする前に：

- DBMS（データベース管理システム）をインストールします。
- Kaspersky Security Center Linux をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。

Kaspersky Security Center Linux をサイレントモードでインストールするには：

1. 使用許諾契約書をお読みください。次の手順は、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。
2. デバイスが Astra Linux 1.8 以降で実行されている場合は、この手順で説明されている操作を実行してください。デバイスが別の OS で実行されている場合は、次の手順に進みます。
   a. ディレクトリ /etc/systemd/system/kladminserver_srv.service.d を作成し、次の内容を含むファイル override.conf を作成します。
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```
   b. ディレクトリ /etc/systemd/system/klwebsrv_srv.service.d を作成し、次の内容を含むファイル override.conf を作成します。
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

3. グループ「kladmins」および非特権アカウント「ksc」を作成します。これは「kladmins」グループのメンバーである必要があります。これを行うには、ルート権限を持つアカウントで次の順番でコマンドを実行します：

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

4. 応答ファイル（TXT 形式）を作成し、変数のリストを VARIABLE_NAME=variable_value 形式で応答ファイルに追加します。1行に1つずつ追加します。応答ファイルには、次の表に示す変数を含める必要があります。

5. たとえば、次のコマンドを使用して、パスを含む応答ファイルの完全な名前を含むルートおよびユーザー環境で KLAUTOANSWERS 環境変数の値を設定します：

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Kaspersky Security Center Linux インストールをサイレントモードで実行します。Linux ディストリビューションに応じて、次のいずれかのコマンドを実行します：

   ルート環境の場合：

   - `# apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ バージョン番号 ].x86_64.rpm -y`

   ユーザー環境の場合：

   - `$ sudo -E apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`
   - `$ sudo -E yum install /<path>/ksc64-[ バージョン番号 ].x86_64.rpm -y`

7. Kaspersky Security Center Web コンソールで作業するユーザーを作成します。これを行うには、ルート権限を持つアカウントで次のコマンドを実行します：

   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <パスワード>` では、パスワードには少なくとも 8 文字が含まれている必要があります。

サイレントモードでの Kaspersky Security Center Linux インストールのパラメータとして使用される応答ファイルの変数

| 変数名 | 必須 | 説明 | 指定可能な値 |
|---|---|---|---|
| EULA_ACCEPTED | 使用する | 使用許諾契約書を理解した上で条項に同意することを確認します。 | 1 |
| PP_ACCEPTED | 使用する | プライバシーポリシーの条件を理解し、同意することを確認します。 | 1 |
| KLSRV_UNATT_SERVERADDRESS | 使用する | 管理サーバーの DNS 名または静的 IP アドレス。 | DNS 名または IP アドレス |
| KLSRV_UNATT_PORT_SRV | 使用しない | 管理サーバーのポート番号。オプショナル型の既定値は 14000 です。 | ポート番号 |
| KLSRV_UNATT_PORT_SRV_SSL | 使用しない | 管理サーバーの SSL ポート番号。オプショナル型の既定値は 13000 です。 | ポート番号 |
| KLSRV_UNATT_PORT_KLOAPI | いいえ | OpenAPI を操作するためのポート番号。このポートは、Kaspersky Security Center Web コンソールからの接続を受信するためにも使用されます。オプションで、既定値は 13299 です。 | ポート番号 |
| KLSRV_UNATT_PORT_GUI | いいえ | klakaut ユーティリティを操作するためのポート番号。オプショナル型の既定値は 13291 です。klakaut ユーティリティとそのヘルプは、Kaspersky Security Center Linux のインストールフォルダーにあります。<br>既定でこのポートは閉じられています。klakaut ユーティリティを使用して Kaspersky Security Center Linux の操作を自動化する場合は、klscflag ユーティリティを使用して13291 ポートを開きます。 | ポート番号 |
| KLSRV_UNATT_NETRANGETYPE | 使用しない | 管理するデバイスの概数。この設定はネットワーク負荷を最適化するために使用されます。オプショナル型の既定値は 1 です。 | 管理対象デバイス数が 1～100 の場合は 1。<br>管理対象デバイス数が 101～1,000 の場合は 2。<br>管理対象デバイス数が 1,000 を超える場合は 3。 |
| KLSRV_UNATT_DBMS_TYPE | 使用する | データベース管理システムのタイプ：MySQL（MariaDB）または Postgres。 | mysql<br>または<br>postgres |
| KLSRV_UNATT_DBMS_INSTANCE | 使用する | データベースサーバーの IP アドレス。 | IP アドレス |

| | | | |
|---|---|---|---|
| KLSRV_UNATT_DBMS_PORT | 使用する | データベースサーバーのポート。MySQL（MariaDB）の既定値は 3306 です。Postgres の既定値は 5432 です。 | 3306<br>または<br>5432 |
| KLSRV_UNATT_DB_NAME | 使用する | データベースの名前。 | kav |
| KLSRV_UNATT_DBMS_LOGIN | 使用する | データベースにアクセスできるユーザーのユーザー名。 | |
| KLSRV_UNATT_DBMS_PASSWORD | 使用する | データベースにアクセスできるユーザーのパスワード。 | |
| KLSRV_UNATT_KLADMINSGROUP | 使用する | サービス用のセキュリティグループ名。 | kladmins |
| KLSRV_UNATT_KLSRVUSER | 使用する | 管理サーバーサービスを開始するアカウント名。アカウントは、KLSRV_UNATT_KLADMINSGROUP 変数で指定されたセキュリティグループのメンバーである必要があります。 | ksc |
| KLSRV_UNATT_KLSVCUSER | 使用する | その他のサービスを開始するアカウント名。アカウントは、KLSRV_UNATT_KLADMINSGROUP 変数で指定されたセキュリティグループのメンバーである必要があります。 | ksc |
| 管理サーバーを Kaspersky Security Center Linux フェールオーバークラスタとして導入する場合は、応答ファイルに次の追加変数を含める必要があります： | | | |
| KLFOC_UNATT_NODE | 使用する | ノード番号（1 または 2）。 | 1<br>または<br>2 |
| KLFOC_UNATT_STATE_SHARE_MOUNT_PATH | 使用する | 状態共有のマウントポイント。 | |
| KLFOC_UNATT_DATA_SHARE_MOUNT_PATH | 使用する | データ共有のマウントポイント。 | |
| KLFOC_UNATT_CONN_MODE | 使用する | フェールオーバークラスタの接続モード。 | VirtualAdapter<br>または<br>ExternalLoadBalancer |
| KLFOC_UNATT_CONN_MODE 変数に VirtualAdapter 値がある場合、応答ファイルには次の追加変数を含める必要があります： | | | |
| KLFOC_UNATT_CONN_MODE_VA_NAME | はい | 仮想ネットワークアダプター名。 | |
| KLFOC_UNATT_CONN_MODE_VA_IPV4 | これらの変数のいずれかが必要です | 仮想ネットワークアダプターの IP アドレス。 | IP アドレス |
| KLFOC_UNATT_CONN_MODE_VA_IPV6 | | 仮想ネットワークアダプターの IPv6 アドレス。 | IPv6 アドレス |

# 閉鎖ソフトウェア環境モードでの Astra Linux への Kaspersky Security Center Linux のインストール

このセクションでは、Astra Linux Special Edition オペレーティングシステムに Kaspersky Security Center Linux をインストールする方法について説明します。

インストールする前に：

- DBMS をインストールします。
- kaspersky_astra_pub_key.gpg 製品のライセンスをダウンロードします。

インストールファイル ksc64_[バージョン番号]_amd64.deb を使用します。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

ルート権限を持つアカウントで、この手順で提供されているコマンドを高い整合性とゼロの機密性で実行します。

*Kaspersky Security Center Linux を Astra Linux Special Edition（運用アップデート 1.7.2）および Astra Linux Special Edition（運用アップデート 1.6）オペレーティングシステムにインストールするには、次の手順に従います：*

1. ファイル `/etc/digsig/digsig_initramfs.conf` を開き、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. コマンドラインで次のコマンドを実行して、適合パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 製品のライセンスにディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 前の手順で作成したディレクトリに製品のライセンスを配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. システムのすべてのカーネルの初期 RAM ファイルシステムイメージを更新します。

   ```
   update-initramfs -u -k all
   ```

   システムを再起動します。

6. グループ「kladmins」と特権のないアカウント「ksc」を作成します。このアカウントは「kladmins」グループに属するメンバーである必要があります。このためには、次のコマンドを順に実行します：

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

7. Kaspersky Security Center Linux のインストールを実行します：

   ```
   # apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb
   ```

8. Kaspersky Security Center Linux の設定を実行します：

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、プライバシーポリシーの内容に同意する必要があります。

10. 確認が表示されてから次の設定を入力します：

    a. 管理サーバーの DNS 名または静的 IP アドレスを入力します。

    b. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。

    c. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

    d. 管理するデバイスの概数を見積もります：

    - 管理対象デバイスの数が 1 ～ 100 の場合は、「1」を入力します。
    - 管理対象デバイスの数が 101 ～ 1000 の場合は、「2」を入力します。
    - 管理対象デバイスの数が 1000 以上の場合は、「3」を入力します。

    この設定は、ネットワーク負荷を最適化するために、タスクの開始を自動的にランダムに遅延させるために使用されます。以下のテーブルは、遅延が計算される間隔を示しています：

| 管理対象デバイス数が 1 ～ 100 の場合、値は 1 | 管理対象デバイス数が 101 ～ 1000 の場合、値は 2 | 管理対象デバイスが 1000 台超の場合、値は 3 |
|---|---|---|
| 遅延は使用されません | 5 分 | 10 分 |

    a. サービス用のセキュリティグループ名を入力します。既定では、「kladmins」グループが使用されます。

    b. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

    c. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

    d. データベースがインストールされるデバイスの IP アドレスを入力します。

    e. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、ポート 3306 が使用されます。

    f. データベースの名前を入力します。

    g. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

    h. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。

サービスが追加され自動的に開始されるまで待ちます。

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

i. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。
パスワードは次のルールに従う必要があります：

- ユーザーパスワードは、最小 8 文字、最大 256 文字である必要があります。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

Kaspersky Security Center Linux がインストールされ、ユーザーが追加されます。

### サービスの検証

サービスが実行されているかどうかを確認するには、次のコマンドを実行します：

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

## Kaspersky Security Center Web コンソールのインストール

このセクションでは、Linux オペレーティングシステムを使用しているデバイスに Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）をインストールする方法について説明しています。インストールの前に、DBMS と Kaspersky Security Center Linux 管理サーバーをインストールする必要があります。

Kaspersky Security Center Web コンソールを Astra Linux に閉鎖ソフトウェア環境モードでインストールする場合は、Astra Linux に固有の手順に従ってください。

デバイスにインストールされている Linux ディストリビューションに応じて、次のインストールファイルのいずれかを使用します：

- Debian の場合：ksc-web-console-<ビルド番号>.x86_64.deb
- RPM ベースのオペレーティングシステムの場合：ksc-web-console-<ビルド番号>.x86_64.rpm
- ALT 8 SP の場合：ksc-web-console-<ビルド番号>-alt8p.x86_64.rpm

インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

*Kaspersky Security Center Web コンソールをインストールするには：*

1. Kaspersky Security Center Web コンソールをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. 使用許諾契約書（EULA）をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイトからファイルをダウンロードできます。使用許諾契約書の条項に同意しない場合は、製品をインストールすることはできません。

3. Kaspersky Security Center Web コンソールを管理サーバーに接続するためのパラメータを入力した応答ファイルを作成します。ファイル名を「ksc-web-console-setup.json」とし、フォルダーに次のように配置します：/etc/ksc-web-console-setup.json

   最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "trusted":
"192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true
}
```

   1024 以上のポート番号を指定することを推奨します。Kaspersky Security Center Web コンソールを 1024 未満のポートで動作させたい場合は、インストール後に次のコマンドを実行する必要があります：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

   setcap ユーティリティがない場合は、インストールできます。**コマンドを表示するには、このリンクをクリックします**。

   Debian および Ubuntu オペレーティングシステムの場合は、次のコマンドのいずれかを実行します：

   - `sudo apt-get install libcap2-bin`
   - `sudo apt install libcap2-bin`

   SUSE Linux Enterprise Server の場合は、次のコマンドを実行します：

   - `sudo zypper install libcap-progs`

   Red Hat Enterprise Linux の場合は、次のコマンドを実行します：

   - `sudo zypper install libcap-progs`

   Linux ALT オペレーティングシステム上に Kaspersky Security Center Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

   同じ rpm インストールファイルを使用して Kaspersky Security Center Web コンソールをアップデートすることはできません。応答ファイルの設定を変更し、変更後の応答ファイルを使用して Web コンソールの再インストールを行いたい場合、Web コンソールをまずアンインストールしてから変更後の応答ファイルを使用して再インストールを行います。

4. root 権限のあるアカウントでコマンドラインを使用し、Linux ディストリビューションに応じて拡張子が「.deb」または「.rpm」のセットアップファイルを実行します。

   - deb ファイルから Kaspersky Security Center Web コンソールをインストールまたはアップグレードするには、次のコマンドを使用します：
     ```
     $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
     ```
   - 「.rpm」ファイルから Kaspersky Security Center Web コンソールを実行するには、次のコマンドのいずれかを使用します：
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-<ビルド番号>.x86_64.rpm
     ```
     または
     ```
     $ sudo alien -i ksc-web-console-<ビルド番号>.x86_64.rpm
     ```
   - Kaspersky Security Center Web コンソールを以前のバージョンからアップグレードするには、次のコマンドのいずれかを実行します：
     - RPM ベースのオペレーティングシステムのデバイスの場合：
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-<ビルド番号>.x86_64.rpm
       ```
     - Debian ベースのオペレーティングシステムのデバイスの場合：
       ```
       $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
       ```

   これにより、セットアップファイルの展開が始まります。インストールが完了するまで待機します。Kaspersky Security Center Web コンソールが「/var/opt/kaspersky/ksc-web-console」ディレクトリにインストールされます。

5. 次のコマンドを実行してすべての Kaspersky Security Center Web コンソールサービスを再起動します：
   ```
   $ sudo systemctl restart KSC*
   ```

   インストールが完了したら、ブラウザーを使用して Kaspersky Security Center Web コンソールを開き、Web コンソールにログインします。

## Kaspersky Security Center Web コンソールのインストールパラメータ

Linux で動作するデバイスに Kaspersky Security Center Web コンソールサーバーをインストールする場合、応答ファイルとして Kaspersky Security Center Web コンソールと管理サーバーの接続用のパラメータを含む「.json」ファイルを作成する必要があります。

最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "trusted":
"192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
  "acceptEula": true
}
```

以下は、拡張されたパラメータセットと既定のアドレスとポートを含む応答ファイルの例です：

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "defaultLangId": 1049,
```

```
  "enableLog": false,
  "trusted":
"192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server
1||ksc2.example.com|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server 2",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/ksc-web-console/web-server.crt",
  "keyPath": "/var/opt/kaspersky/ksc-web-console/web-server.key",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5",
  "natsMessageQueueAccount": "Group1:User6"
}
```

`webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount`、`messageQueueAccount` および `natsMessageQueueAccount` パラメータは互いに別々に使用しないでください。すべてのパラメータの値を指定するか、いずれのパラメータにも値を指定しないでください。

カスタム証明書を使用する場合は、`certPath` と `keyPath` パラメータの両方を指定します。パラメータを指定しない、または1つだけ指定した場合、Web ブラウザーは接続がプライベートではないことを通知し続けます。

1024 以上のポート番号を指定することを推奨します。Kaspersky Security Center Web コンソールを 1024 未満のポートで動作させたい場合は、インストール後に次のコマンドを実行する必要があります：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

setcap ユーティリティがない場合は、インストールできます。**コマンドを表示するには、このリンクをクリックします**。

Debian および Ubuntu オペレーティングシステムの場合は、次のコマンドのいずれかを実行します：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

SUSE Linux Enterprise Server の場合は、次のコマンドを実行します：

- `sudo zypper install libcap-progs`

Red Hat Enterprise Linux の場合は、次のコマンドを実行します：

- `sudo zypper install libcap-progs`

Linux ALT オペレーティングシステム上に Kaspersky Security Center Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

次の表で、応答ファイルで指定できるパラメータについて説明しています。

Linux で動作するデバイスへの Kaspersky Security Center Web コンソールのインストール用のパラメータ

| パラメータ | 説明 | 設定可能な値 |
| --- | --- | --- |
| `address` | Kaspersky Security Center に接続するためのアドレス（必須）。<br>Kaspersky Security Center Web コンソールを Kaspersky Security Center サーバーにインストールする場合は、Kaspersky Security Center Linux のインストール時に指定したアドレスを使用します。<br>Kaspersky Security Center Web コンソールを外部デバイスにインストールする場合は、Web ブラウザーが Kaspersky Security Center Web コンソールサーバーに接続するために使用するデバイスの外部 IP アドレスを指定します。 | 文字列値<br>例：`"ksc.example.com"` |
| `port` | Kaspersky Security Center Web コンソールが Web ブラウザーからの接続を受信するために使用するポート（必須）。 | 数値<br>推奨値は 8080 です（Linux ALT オペレーティングシステムを除く）。 |
| `defaultLangId` | ユーザーインターフェイスの言語設定（既定では `1033`）<br>必要に応じて、Kaspersky Security Center Web コンソールインターフェイスの言語を変更できます。 | 対象言語を示す数字コード<br>• ドイツ語：`1031`<br>• 英語：`1033`<br>• スペイン語：`3082`<br>• スペイン語（メキシコ）：`2058`<br>• フランス語：`1036`<br>• 日本語：`1041`<br>• カザフ語：`1087`<br>• ポーランド語：`1045`<br>• ポルトガル語（ブラジル）：`1046`<br>• ロシア語：`1049`<br>• トルコ語：`1055`<br>• 簡体字中国語：`4`<br>• 繁体字中国語：`31748`<br>値を指定しなかった場合は、言語設定で英語（en-US）が使用されます。 |
| `enableLog` | Kaspersky Security Center Web コンソールの動作ログを有効にするかどうかの設定<br>カスペルスキーのテクニカルサポートスペシャリストから要求された場合にのみ、パラメータの既定値を変更することを推奨します。 | ブール値：<br>• `true` - ログ記録が有効になります。<br>• `false` — ログ記録が無効になります（既定で選択）。 |
| `trusted` | Kaspersky Security Center Web コンソールを Kaspersky Security Center Linux に接続するためのアドレスのリスト：<br>• Kaspersky Security Center Web コンソールサーバーを管理サーバーに接続するためのアドレス。<br>• Kaspersky Security Center Web コンソールサーバーと管理サーバーの接続に使用する OpenAPI ポート（既定では 13299）。<br>• 管理サーバーの証明書へのパス。<br>• ログインウィンドウで表示される管理サーバー名。<br>パラメータは縦線（パイプ、\|）で区切ります。複数の管理サーバーを指定する場合は、2 本の縦線（\|\|）で区切ります。<br>管理サーバー証明書は、Kaspersky Security Center Linux がインストールされているデバイスにあります。証明書ファイルの既定のパスは次のとおりです：/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer。<br>Kaspersky Security Center Web コンソールを外部デバイスにインストールする場合は、Kaspersky Security Center Linux がインストールされているデバイスから証明書ファイルを外部デバイスにコピーします。Web コンソールインストーラーの応答ファイルに証明書へのローカルパスを指定します。 | 文字列の形式は次の通りです：<br>**"< Web コンソールのサーバーアドレス >\|< ポート >\|< 証明書のパス >\|< サーバー名 >"**<br>例：<br>`"X.X.X.X\|13299\|/cert/server-1.cer\|Server 1\|\|Y.Y.Y.Y\|13299\|/cert/server-2.cer\|Server 2"` |

| パラメータ | 説明 | 設定可能な値 |
| --- | --- | --- |
| acceptEula | 使用許諾契約書（EULA）の条項に同意するかどうかの設定使用許諾契約書の内容を記載したファイルは、インストールファイルと合わせてダウンロードされます。 | ブール値：<br>• true - この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します。<br>• false - 使用許諾契約書の条項に同意しません（既定で選択）。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは EULA を表示し、EULA の条項に同意するかどうかを尋ねます。 |
| certDomain | 新しい自己署名証明書を生成する場合は、このパラメータを使用して、Web ブラウザーを Kaspersky Security Center Web コンソールに接続するための FQDN を指定します。 | 文字列値 |
| certPath | パラメータを使用して、インフラストラクチャで信頼され、カスタム証明書の要件を満たす Kaspersky Security Center Web コンソールのカスタム証明書へのパスを指定します。<br>秘密鍵（keyPath）ごとに1つの証明書または証明書チェーンを指定する必要があります。 | 文字列値<br>暗号化された証明書は、Kaspersky Security Center Web コンソールではサポートされていません。<br>Kaspersky Security Center Web コンソールをインストールするデバイスで、PEM 形式の証明書ファイルへのパスを指定します。<br>例：/var/opt/kaspersky/ksc-web-console/web-server.crt |
| keyPath | このパラメータを使用して、certPath パラメータで指定された Kaspersky Security Center Web コンソールのカスタム証明書に関連付けられた秘密鍵へのパスを指定します。 | 文字列値<br>秘密鍵を含むファイルは暗号化しないでください。<br>Kaspersky Security Center Web コンソールをインストールするデバイスで、PEM 形式のライセンス情報ファイルへのパスを指定します。<br>例： /var/opt/kaspersky/ksc-web-console/web-server.key |
| webConsoleAccount | Kaspersky Security Center Web コンソールサービスが実行されるアカウントの名前。 | 文字列の形式は次の通りです："< グループ名 >:< ユーザー名 >"。<br>例："Group1:User1"。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「user_management_%uid%」で新しいアカウントを作成します。 |
| managementServiceAccount | Kaspersky Security Center Web コンソール管理サービスが実行される特権アカウントの名前。 | 文字列の形式は次の通りです："< グループ名 >:< ユーザー名 >"。<br>例："Group1:User1"。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「user_nodejs_%uid%」で新しいアカウントを作成します。 |
| serviceWebConsoleAccount | Kaspersky Security Center Web コンソールサービスが実行されるアカウントの名前。 | 文字列の形式は次の通りです："< グループ名 >:< ユーザー名 >"。<br>例："Group1:User1"。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「user_svc_nodejs_%uid%」で新しいアカウントを作成します。 |

| パラメータ | 説明 | 設定可能な値 |
| --- | --- | --- |
| `pluginAccount` | Kaspersky Security Center 製品プラグインサービスが実行されるアカウントの名前。 | 文字列の形式は次の通りです：**"< グループ名 >:< ユーザー名 >"**。<br>例：`"Group1:User1"`。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「`user_web_plugin_%uid%`」で新しいアカウントを作成します。 |
| `messageQueueAccount` | Kaspersky Security Center Web コンソールメッセージキューサービスが実行されるアカウントの名前。 | 文字列の形式は次の通りです：**"< グループ名 >:< ユーザー名 >"**。<br>例：`"Group1:User1"`。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「`user_message_queue_%uid%`」で新しいアカウントを作成します。 |
| `natsMessageQueueAccount` | Kaspersky Security Center Web コンソール NATS サービスが実行されるアカウントの名前。 | 文字列の形式は次の通りです：**"< グループ名 >:< ユーザー名 >"**。<br>例：`"Group1:User1"`。<br>値が指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは、既定の名前「`user_message_queue_%uid%`」で新しいアカウントを作成します。 |

セキュリティ上の理由から、`webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount`、`messageQueueAccount` および `natsMessageQueueAccount` パラメータの指定は推奨しません。

これらのパラメータを指定する場合は、カスタムユーザーアカウントが同じセキュリティグループに属していることを確認してください。パラメータが指定されていない場合、Kaspersky Security Center Web コンソールのインストーラーは既定のセキュリティグループを作成してから、このグループ内に既定の名前でユーザーアカウントを作成します。

# 閉鎖ソフトウェア環境モードでの Astra Linux への Kaspersky Security Center Web コンソールのインストール

ここでは、Kaspersky Security Center Web コンソールサーバー（Kaspersky Security Center Web コンソール）を Astra Linux Special Edition にインストールする方法について説明します。インストールの前に、DBMS と Kaspersky Security Center Linux 管理サーバーをインストールする必要があります。

*Kaspersky Security Center Web コンソールをインストールするには：*

1. Kaspersky Security Center Web コンソールをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。

2. 使用許諾契約書（EULA）をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイトからファイルをダウンロードできます。使用許諾契約書の条項に同意しない場合は、製品をインストールすることはできません。

3. Kaspersky Security Center Web コンソールを管理サーバーに接続するためのパラメータを入力した応答ファイルを作成します。ファイル名を「ksc-web-console-setup.json」とし、フォルダーに次のように配置します：/etc/ksc-web-console-setup.json

   最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

   ```
   {
     "address": "ksc.example.com",
     "port": 8080,
     "trusted":
   "192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": true
   }
   ```

4. ファイル `/etc/digsig/digsig_initramfs.conf` を開き、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. コマンドラインで次のコマンドを実行して、適合パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

6. 製品のライセンスにディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. 前の手順で作成したディレクトリに製品のライセンス `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` を配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Kaspersky Security Center Linux 配布キットに kaspersky_astra_pub_key.gpg ライセンスが含まれていない場合は、以下のリンクをクリックしてダウンロードできます：
   > https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

8. RAM ディスクをアップデートします：

   ```
   update-initramfs -u -k all
   ```

   システムを再起動します。

9. root 権限を持つアカウントで、コマンドラインを使用してセットアップファイルを実行します。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

   - Kaspersky Security Center Web コンソールをインストールまたはアップグレードするには、次のコマンドを実行します：

     ```
     $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
     ```

   - Kaspersky Security Center Web コンソールを以前のバージョンからアップグレードするには、次のコマンドを実行します：

     ```
     $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
     ```

   これにより、セットアップファイルの展開が始まります。インストールが完了するまで待機します。Kaspersky Security Center Web コンソールがディレクトリ `/var/opt/kaspersky/ksc-web-console` にインストールされます。

10. 次のコマンドを実行してすべての Kaspersky Security Center Web コンソールサービスを再起動します：

    ```
    $ sudo systemctl restart KSC*
    ```

インストールが完了したら、ブラウザーを使用して Kaspersky Security Center Web コンソールを開き、Web コンソールにログインします。

# Kaspersky Security Center Linux のフェールオーバークラスタの導入

このセクションでは、Kaspersky Security Center Linux のフェールオーバークラスタに関する全般的な情報と、ネットワークに Kaspersky Security Center Linux のフェールオーバークラスタを導入するための準備と導入に関する手順の両方を説明します。

## シナリオ：Kaspersky Security Center Linux のフェールオーバークラスタの導入

Kaspersky Security Center Linux のフェールオーバークラスタは Kaspersky Security Center Linux の高可用性を実現し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスタは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center Linux のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

### 必須条件

フェールオーバークラスターの要件を満たすハードウェアを持っている。

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **ファイルサーバーの準備**

   Kaspersky Security Center Linux のフェールオーバークラスタのコンポーネントとして動作するファイルサーバーを準備します。ファイルサーバーがシステム要件を満たしていることを確認して、Kaspersky Security Center Linux のデータ用に 2 つの共有フォルダーを作成し、それらの共有フォルダーのアクセス権を設定します。

   実行手順の説明：Kaspersky Security Center Linux のフェールオーバークラスター用のファイルサーバーの準備

2. **アクティブおよびパッシブノードの準備**

   アクティブおよびパッシブノードとして動作する同一のハードウェアおよびソフトウェアを持つ 2 台のデバイスを準備します。

   実行手順の説明：Kaspersky Security Center Linux のフェールオーバークラスタ用のノードの準備

3. **Kaspersky Security Center Linux サービス用のアカウントの作成**

   アクティブノード、パッシブノード、およびファイルサーバーで次の手順を実行します：

   1. 「kladmins」という名前のグループを作成し、3 つのグループすべてに同じ GID を割り当てます。
   2. 「ksc」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。作成したアカウントのプライマリグループを「kladmins」に設定します。

3. 「rightless」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。作成したアカウントのプライマリグループを「kladmins」に設定します。

4. **DBMS（データベース管理システム）のインストール**

   次の 2 つがあります：

   - MariaDB Galera Cluster を使用する場合は、DBMS 専用のデバイスは必要ありません。MariaDB Galera Cluster を各ノードにインストールします。
   - その他のサポート対象の DBMS を使用する場合は、選択した DBMS を専用のデバイスにインストールします。

5. **Kaspersky Security Center Linux のインストール**

   両方のノードのフェールオーバークラスターモードで Kaspersky Security Center Linux をインストールします。最初にアクティブノードに Kaspersky Security Center Linux インストールしてからパッシブノードにもインストールします。

   さらに、クラスターノードではない別のデバイスに Kaspersky Security Center Web コンソールをインストールできます。

6. **フェールオーバークラスターのテスト**

   フェールオーバークラスターが正しく設定され、問題なく動作していることを確認してください。たとえば、アクティブノードの Kaspersky Security Center Linux のサービス（kladminserver、klnagent、ksnproxy、klactprx または klwebsrv）のうち 1 つを停止します。サービスが停止された後、保護管理は自動的にパッシブノードに切り替わります。

### 結果

Kaspersky Security Center Linux のフェールオーバークラスターが導入されています。アクティブおよびパッシブノードの切り替えが発生するイベントについてはしっかりと把握するようにしてください。

## Kaspersky Security Center Linux のフェールオーバークラスタについて

Kaspersky Security Center Linux のフェールオーバークラスタは Kaspersky Security Center Linux の高可用性を実現し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスタは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center Linux のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

Kaspersky Security Center Linux のフェールオーバークラスタでは、すべての Kaspersky Security Center Linux サービスは自動で管理されます。手動でサービスを再起動しないでください。

トラブルシューティングには syslog 機能を使用します。

## システム要件

Kaspersky Security Center Linux のフェールオーバークラスタを導入するには、次のハードウェアを準備する必要があります：

- 同一のハードウェアおよびソフトウェアを持つ 2 台のデバイス。これらのデバイスはアクティブおよびパッシブノードとして動作します。

  デバイスの構成はアクティブおよびパッシブノードとして動作します。

| ハードウェア | 値 |
| --- | --- |
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、300 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 1 Gbps |

- EXT4 ファイルシステムの Linux を実行しているファイルサーバー。ファイルサーバーとして動作する専用のデバイスを準備する必要があります。

  ファイルサーバーの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、500 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 10 Gbps |

  ファイルサーバーとアクティブおよびパッシブノードには高帯域幅ネットワークを使用していることを確認してください。

- サポートされているデータベース管理システム（DBMS）または DBMS クラスタを持つデバイス。高可用性クラスタ DBMS を使用する場合、この目的専用のデバイスは必要ありません。

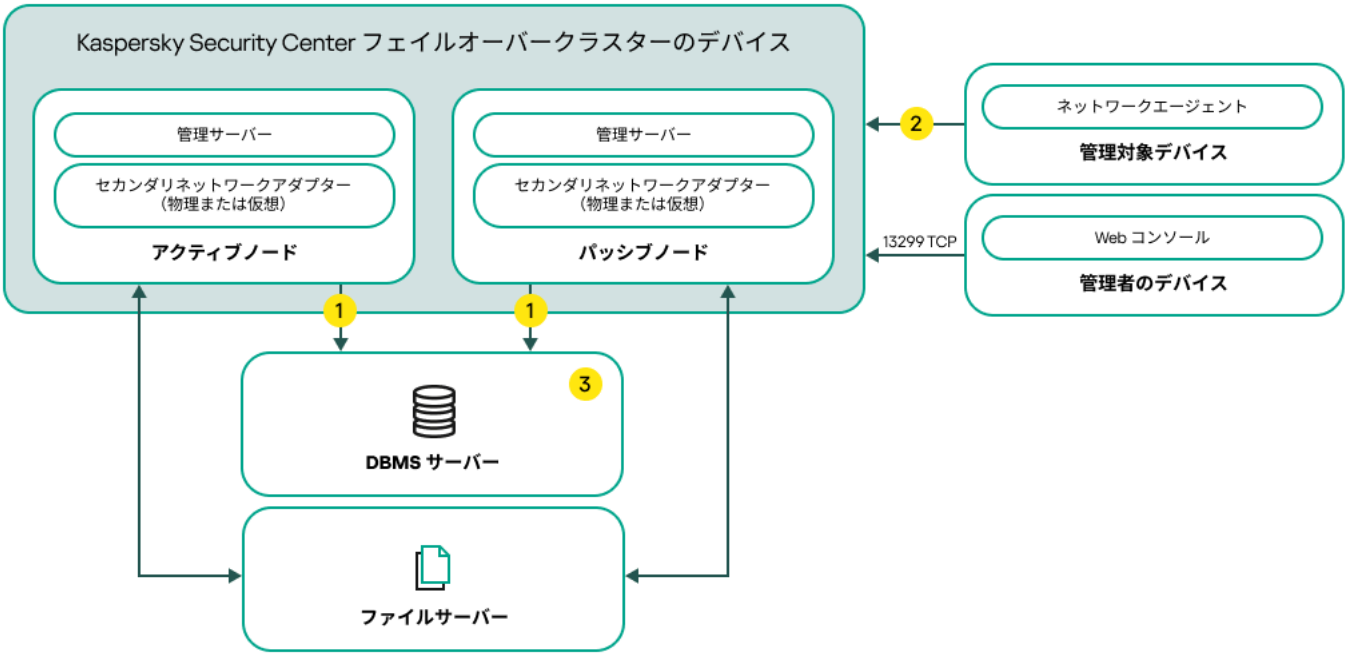
arping パッケージと iputils-arping パッケージの両方、または arping パッケージのみがインストールされている場合、フェールオーバークラスタの導入は失敗します。フェールオーバークラスターを展開する前に、両方のノードに iputils-arping パッケージのみがインストールされていることを確認してください。

## 導入スキーム

Kaspersky Security Center Linux のフェールオーバークラスタを導入するには、次のいずれかのスキームを選択できます。

- 専用デバイスにインストールされたセカンダリネットワークアダプターと DBMS を使用するスキーム。
- セカンダリネットワークアダプターと MariaDB Galera Cluster を DBMS として使用するスキーム。
- サードパーティのロードバランサーと専用デバイスにインストールされた DBMS を使用するスキーム。
- サードパーティのロードバランサーと MariaDB Galera Cluster を DBMS として使用するスキーム。

# 専用デバイスにインストールされたセカンダリネットワークアダプターと DBMS を使用するスキーム




専用デバイスにインストールされたセカンダリネットワークアダプターと DBMS を使用するスキーム

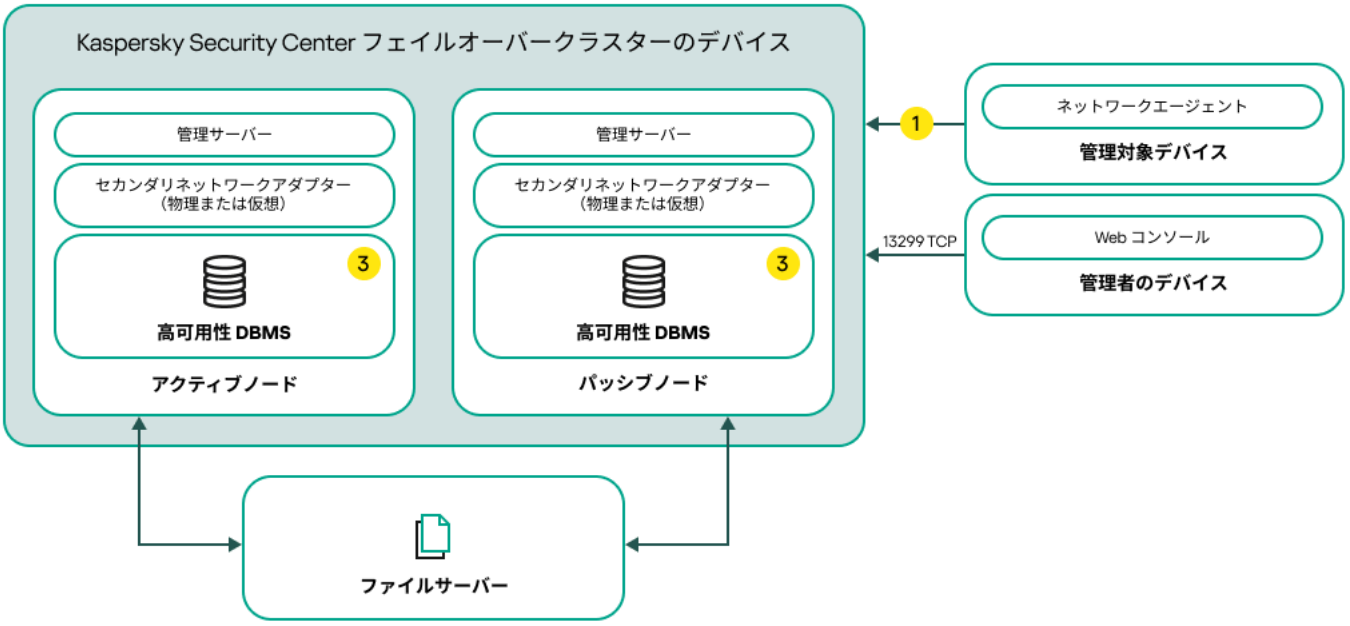
スキームの凡例：

1 管理サーバーがデータベースにデータを送信します。定義データベースが配置されているデバイスで必要なポートを開きます。たとえば、MySQL サーバーの場合はポート 3306、PostgreSQL または Postgres Pro の場合はポート 5432。関連する情報については、DBMS のドキュメントを参照してください。

2 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。

3 DBMS（データベース管理システム）がインストールされたデバイス。MariaDB Galeria Cluster を DBMS として使用している場合は、DBMS 専用のデバイスは必要ありません。MariaDB Galera Cluster を各ノードにインストールします。

セカンダリネットワークアダプターと MariaDB Galera Cluster を DBMS として使用するスキーム



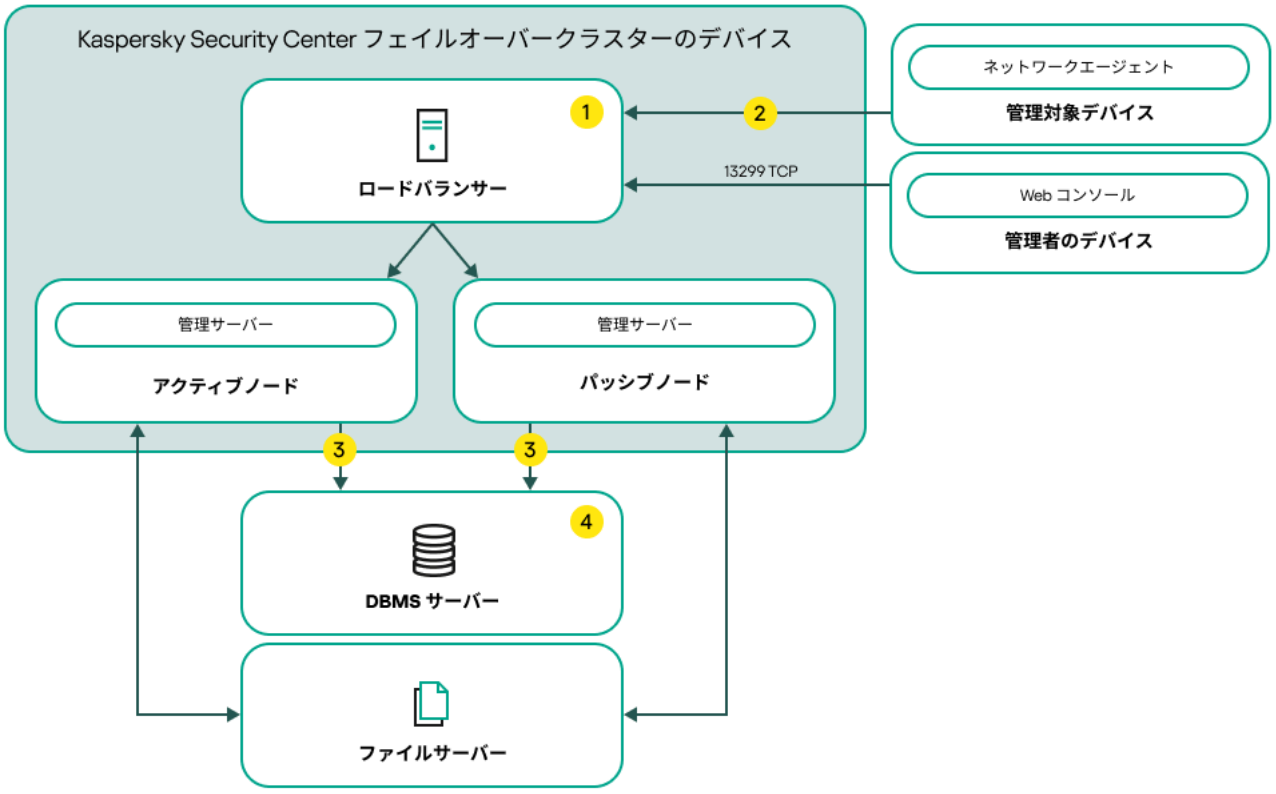

セカンダリネットワークアダプターと MariaDB Galera Cluster を DBMS として使用するスキーム

スキームの凡例：

1 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。

2 高可用性 DBMS（データベース管理システム）（例：MariaDB Galera Cluster）。各ノードに高可用性 DBMS をインストールします。

# サードパーティのロードバランサーと専用デバイスにインストールされた DBMS を使用するスキーム




サードパーティのロードバランサーと専用デバイスにインストールされた DBMS を使用するスキーム

スキームの凡例：

1 ロードバランサーデバイスで、管理サーバーのポートをすべて開きます：TCP 13000、UDP 13000、TCP 13299 および TCP 17000。

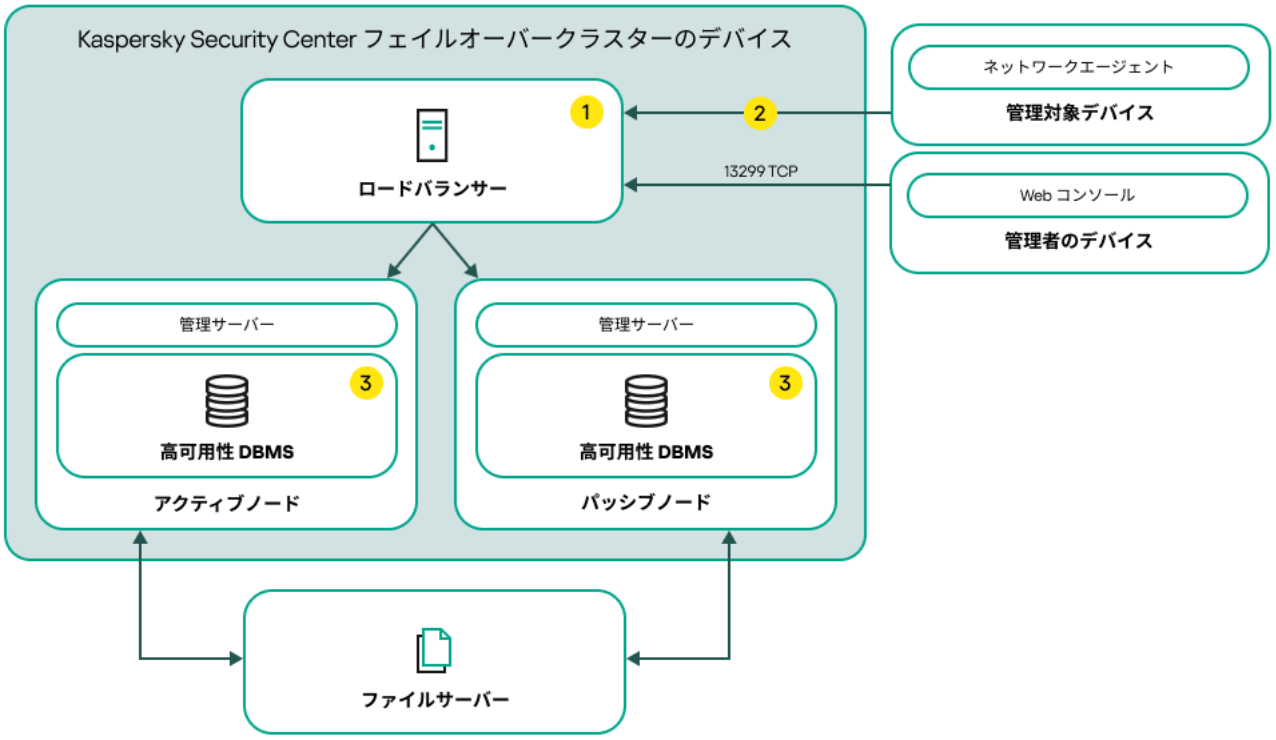
> 自動化のために klakaut ユーティリティを使用する場合は、TCP 13291 ポートも開く必要があります。

2 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。

3 管理サーバーがデータベースにデータを送信します。定義データベースが配置されているデバイスで必要なポートを開きます。たとえば、MySQL サーバーの場合はポート 3306、PostgreSQL または Postgres Pro の場合はポート 5432。関連する情報については、DBMS のドキュメントを参照してください。

4 DBMS（データベース管理システム）がインストールされたデバイス。MariaDB Galeria Cluster を DBMS として使用している場合は、DBMS 専用のデバイスは必要ありません。MariaDB Galera Cluster を各ノードにインストールします。

## サードパーティのロードバランサーと MariaDB Galera Cluster を DBMS として使用するスキーム




サードパーティのロードバランサーと MariaDB Galera Cluster を DBMS として使用するスキーム

スキームの凡例：

1 ロードバランサーデバイスで、管理サーバーのポートをすべて開きます：TCP 13000、UDP 13000、TCP 13299 および TCP 17000。

> 自動化のために klakaut ユーティリティを使用する場合は、TCP 13291 ポートも開く必要があります。

2 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。

3 高可用性 DBMS（データベース管理システム）（例：MariaDB Galera Cluster）。各ノードに高可用性 DBMS をインストールします。

## 切り替えの条件

アクティブノードに次のイベントが発生した場合、フェールオーバークラスタはクライアントデバイスの保護の管理をアクティブノードからパッシブノードに切り替えます：

- ソフトウェアまたはハードウェアの障害によりアクティブノードが破損した。
- メンテナンス操作のためアクティブノードが一時的に停止した。
- Kaspersky Security Center Linux のサービスまたはプロセスで障害が発生したかユーザーにより意図的に中断された。Kaspersky Security Center Linux のサービスは次の通りです：kladminserver、klnagent、klactprx および klwebsrv。
- アクティブノードとファイルサーバー上の保管領域のネットワーク接続が中断または切断された。

# Kaspersky Security Center Linux のフェールオーバークラスタ用のファイルサーバーの準備

Kaspersky Security Center Linux のフェールオーバークラスタの必須コンポーネントとして動作するファイルサーバーです。

*ファイルサーバーを準備するには：*

1. ファイルサーバーがシステム要件を満たしていることを確認してください。
2. NFS サーバーをインストールして設定します：
   - NFS サーバー設定で、両方のノードに対してファイルサーバーへのアクセスが有効になっている必要があります。
   - NFS プロトコルのバージョンは 4.0 または 4.1 である必要があります。
   - Linux カーネルの最小要件：
     - 3.19.0-25（NFS4.0 を使用する場合）
     - 4.4.0-176（NFS 4.1 を使用する場合）

   Linux ディストリビューションに応じて、対応するコマンドを実行して nfs-utils パッケージまたは nfs-kernel-server パッケージのいずれかをインストールします：

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. ファイルサーバーで、2 つのフォルダーを作成して NFS を使用して共有します。2 つのうち 1 つは、フェールオーバークラスタの状態に関する情報を保持するために使用されます。別の 1 つは Kaspersky Security Center Linux のデータおよび設定を保存するために使用されます。Kaspersky Security Center Linux のインストールの設定時に共有フォルダーのパスを指定することになります。

   次のフォルダーが存在していないことを確認します：

   - /mnt/KlFocStateShare
   - /mnt/KlFocDataShare_klfoc

   これらのフォルダーのいずれかが存在する場合は、再帰的に削除します。

   次のコマンドを実行します：

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

   次のコマンドを実行して自動実行を有効にします：

   ```
   sudo systemctl enable rpcbind
   ```

   カスタムのフォルダーを指定することもできますが、オンラインヘルプを使用する際の利便性を考慮し、推奨するフォルダー名の使用を推奨します。

4. ファイルサーバーを再起動します。

ファイルサーバーの準備ができました。Kaspersky Security Center Linux のフェールオーバークラスタを導入するには、シナリオの手順に従ってください。

## Kaspersky Security Center Linux のフェールオーバークラスタ用のノードの準備

続行する前に、「シナリオ： カスペルスキーフェールオーバークラスタの導入」の前の手順を完了していることを確認してください。

Kaspersky Security Center Linux のフェールオーバークラスタのアクティブノードとパッシブノードとして動作する 2 台のデバイスを準備します。

## 共通フォルダーの設定

1. Linux ディストリビューションに応じて、対応するコマンドを実行して各ノードに nfs-utils パッケージまたは nfs-kernel-server パッケージをインストールします：
   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

2. 次のコマンドを実行してマウントポイントを作成します：
   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

3. マウントポイントと共有フォルダーをマッチさせます。

   `sudo sh -c "echo {`**ファイルサーバー**`}:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo {`**ファイルサーバー**`}:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   ここで、`{ file server }` は、共有フォルダーがあるファイルサーバーの FQDN です。

4. 次のコマンドを実行して共有フォルダーをマウントします：
   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

5. 共有フォルダーにアクセスする権限が ksc:kladmins に属していることを確認してください。

   次のコマンドを実行します：

   ```
   sudo ls -la /mnt/
   ```

## ネットワークアダプターの設定

セカンダリネットワークアダプターは、物理的または仮想的に使用することができます。セカンダリネットワークアダプターを使用する導入スキーマを選択した場合は、両方のノードで対応する手順を実行します。

- 物理ネットワークアダプターに基づく仮想セカンダリネットワークアダプターを使用します（MACVLAN技術）：

  1. iputils-arping パッケージをインストールします。Linux ディストリビューションに応じて、次のコマンドのいずれかを実行します：

     - `sudo yum install iputils`

     または

     - `apt install iputils-arping`

  2. 次のコマンドを使用して、物理アダプターの管理に NetworkManager が使用されていることを確認します：

     `nmcli device status`

     コマンド出力で、物理ネットワークアダプターが管理されていないと表示される場合は、物理ネットワークアダプターを管理するように NetworkManager を設定します。具体的な設定手順は、Linux ディストリビューションに応じて異なります。

  3. 次のコマンドを使用して、インターフェイスを識別します：

     `ip a`

  4. 次のコマンドを実行して、設定プロファイルを作成します：

     `nmcli connection add type macvlan dev <physical interface> mode bridge ifname <virtual interface> ipv4.addresses <address mask> ipv4.method manual autoconnect no`

- 物理セカンダリネットワークアダプターを使用するか、ハイパーバイザを使用して仮想 TAP デバイスを作成します。このシナリオでは、ソフトウェア NetworkManage を無効にします。

  1. セカンダリネットワークアダプターをノードに接続します。

  2. iputils-arping パッケージをインストールします。Linux ディストリビューションに応じて、次のコマンドのいずれかを実行します：

     - `sudo yum install iputils`

     または

     - `apt install iputils-arping`

  3. 対象のインターフェイスの NetworkManager 接続を削除するには、次のコマンドを実行します：

     `nmcli con del <connection name>`

     対象のインターフェイスへの接続をチェックするには、次のコマンドを使用します：

     `nmcli con show`

  4. ファイル NetworkManager.conf を編集します。keyfile セクションを見つけて、対象のインターフェイスを `unmanaged-devices` パラメータに割り当てます。

```
[keyfile]
unmanaged-devices=interface-name:<interface name>
```

5. NetworkManager を再起動します：

   ```
   systemctl reload NetworkManager
   ```

   次のコマンドを使用して、対象のインターフェイスが管理対象外であることを確認します：

   ```
   nmcli dev status
   ```

### ロードバランサーの設定

ロードバランサーを含む導入スキーマを選択した場合は、次の手順を実行します：

1. nginx または別のロードバランサーがインストールされた専用の Linux ベースのデバイスを準備します。
2. ロードバランシングの設定をします。アクティブノードをメインサーバー、パッシブノードをバックアップサーバーとして設定します。
3. nginx サーバーで、次の記事の指示に従って管理サーバーのポートをすべて開きます：Kaspersky Security Center Linux で使用されるポート。

Kaspersky Security Center Linux のフェールオーバークラスタを導入するには、シナリオの手順に従ってください。

> フェールオーバークラスタノードの可用性を決定するのは、管理サーバーへの主要接続ポートの可用性です。パッシブノードは、切り替えが発生するまで外部接続を受け入れません。

## Kaspersky Security Center Linux のフェールオーバークラスタノードへの Kaspersky Security Center Linux のインストール

続行する前に、「シナリオ： カスペルスキーフェールオーバークラスタの導入」の前の手順を完了していることを確認してください。

ここでは、Kaspersky Security Center Linux のフェールオーバークラスタのノードに Kaspersky Security Center Linux をインストールする方法について説明します。Kaspersky Security Center Linux は Kaspersky Security Center Linux のフェールオーバークラスタの両方のノードに個別にインストールされます。まず最初にアクティブなノードに製品をインストールしてから、パッシブなノードにインストールします。インストール中に、どのノードがアクティブでどのノードがパッシブになるかを選択します。

デバイスにインストールされている Linux ディストリビューションに応じて、「ksc64_[バージョン番号]_amd64.deb」または「ksc64-[バージョン番号].x86_64.rpm」のいずれかのインストールファイルを使用してください。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

RED OS バージョン 7.3.4 以降、または MSVSPHERE バージョン 9.2 以降を使用している場合は、両方のノードに libxcrypt-compat パッケージをインストールしてください。

## プライマリ（アクティブ）ノードへのインストール

*プライマリノードに Kaspersky Security Center Linux をインストールするには：*

1. Kaspersky Security Center Linux をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。

2. セカンダリネットワークアダプターを使用する場合は、プロンプトが表示されたらその名前を入力する必要があります。すべてのネットワークインターフェイスを表示するには、次のコマンドを入力します：

   ```
   ip addr
   ```

3. コマンドラインで、この手順で提供されているコマンドを実行します。

4. Kaspersky Security Center Linux のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

   - `sudo apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ バージョン番号 ].x86_64.rpm -y`

5. Kaspersky Security Center Linux の設定を実行します：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、プライバシーポリシーの内容に同意する必要があります。

7. 管理サーバーのインストールモードとして**プライマリクラスタノード**を選択します

8. 確認が表示されてから次の設定を入力します：

a. State share のマウントポイントにローカルパスを入力します：`/mnt/KlFocStateShare`

b. Data share のマウントポイントにローカルパスを入力します：`/mnt/KlFocDataShare_klfoc`

c. フェールオーバークラスタの接続モードを選択します：セカンダリネットワークアダプターまたは外部のロードバランサー。

d. セカンダリネットワークアダプターを使用する場合は、名前を入力します。

e. 管理サーバーの DNS 名または静的 IP アドレスを入力するよう要求された場合は、セカンダリネットワークアダプターまたは外部ロードバランサーの IP アドレスを入力します。

f. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

g. 管理するデバイスの概数を見積もります：

- 管理対象デバイスの数が 1 ～ 100 の場合は、「1」を入力します。
- 管理対象デバイスの数が 101 ～ 1000 の場合は、「2」を入力します。
- 管理対象デバイスの数が 1000 以上の場合は、「3」を入力します。

この設定は、ネットワーク負荷を最適化するために、タスクの開始を自動的にランダムに遅延させるために使用されます。以下のリストは、遅延が計算される間隔を示しています：

- 管理対象デバイス数が 1 ～ 100 の場合、値は 1。遅延は使用されません。
- 管理対象デバイス数が 101 ～ 1000 の場合、値は 2。遅延時間は 5 分です。
- 管理対象デバイスが 1000 台超の場合、値は 3。遅延時間は 10 分です。

h. サービス用のセキュリティグループ名を入力します。既定では、「kladmins」グループが使用されます。

i. 管理サーバーサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

j. その他のサービスを開始するアカウント名を入力します。アカウントは入力したセキュリティグループのメンバーである必要があります。既定では「ksc」アカウントが使用されます。

k. Kaspersky Security Center Linux と連携するためにインストールした DBMS を選択します：

- MySQL または MariaDB をインストールした場合は、1 を入力します。
- PostgreSQL または Postgres Pro をインストールした場合は、2 を入力します。

l. データベースがインストールされるデバイスの DNS 名または IP アドレスを入力します。

m. データベースのポート番号を入力します。このポートは管理サーバーとの通信に使用されます。既定では、次のポートが使用されます：

- ポート 3306（MySQL または MariaDB）
- ポート 5432（PostgreSQL または Postgres Pro）

n. データベースの名前を入力します。

o. データベースへのアクセスに使用するデータベースのルートアカウントのログイン名を入力します。

p. データベースへのアクセスに使用するデータベースのルートアカウントのパスワードを入力します。

q. Kaspersky Security Center Linux と連携するためにインストールした DBMS を選択します：

- MySQL または MariaDB をインストールした場合は、1 を入力します。
- PostgreSQL または Postgres Pro をインストールした場合は、2 を入力します。

9. サービスが追加され自動的に開始されるまで待ちます。

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc

10. 管理サーバーの管理者とするアカウントを作成します。ユーザー名とパスワードを入力します。ユーザーパスワードは 8 文字以上 256 文字以下である必要があります。

この手順を省略した場合は、次のコマンドを実行してアカウントを後で作成できます：

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
```

ユーザーが追加され、Kaspersky Security Center Linux がプライマリノードにインストールされます。

## セカンダリー（パッシブ）ノードへのインストール

*セカンダリーノードに Kaspersky Security Center Linux をインストールするには：*

1. Kaspersky Security Center Linux をインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. コマンドラインで、この手順で提供されているコマンドを実行します。
3. Kaspersky Security Center Linux のインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

- `sudo apt install /<path>/ksc64_[ バージョン番号 ]_amd64.deb`
- `sudo yum install /<path>/ksc64-[ バージョン番号 ].x86_64.rpm -y`

4. Kaspersky Security Center Linux の設定を実行します：

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. 使用許諾契約書（EULA）およびプライバシーポリシーを読みます。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。確認が表示されてから次の値を入力します：

   a. EULA の内容を確認して同意する場合は「y」を入力します。EULA の内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、EULA の内容に同意する必要があります。

   b. プライバシーポリシーの内容を確認して同意し、またデータがプライバシーポリシーに記載される方法で処理されて送信されること（第三国への送信を含む）に同意する場合は「y」を入力します。プライバシーポリシーの内容に同意しない場合は「n」を入力します。Kaspersky Security Center Linux を使用するには、プライバシーポリシーの内容に同意する必要があります。

6. 管理サーバーのインストールモードとして**セカンダリクラスタノード**を選択します

7. プロンプトが表示されたら、State share のマウントポイントにローカルパスを入力します：`/mnt/KlFocStateShare`

Kaspersky Security Center Linux がセカンダリーノードにインストールされます。

## サービスの検証

次のコマンドを使用して、フェールオーバークラスタ管理サービスが `Active: active (running)` であることを確認します：

```
systemctl status klfocsvc_klfoc
```

次のコマンドを使用して、他のフェールオーバークラスタサービスが `Active: inactive (dead)` であることを確認します：

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Kaspersky Security Center Linux のフェールオーバークラスタが正しく設定され、クラスタが正しく動作するか確認するためテストできる状態になりました。

# Kaspersky Security Center Linux のフェールオーバークラスタノードにインストールされた管理サーバーに接続された Kaspersky Security Center Web コンソールのインストール

このセクションでは、Kaspersky Security Center Linux のフェールオーバークラスターノードにインストールされた管理サーバーに接続する Kaspersky Security Center Web コンソールサーバー（以降、「Kaspersky Security Center Web コンソール」と表記）をインストールする方法について説明します。Kaspersky Security Center Web コンソールをインストールする前に、DBMS と Kaspersky Security Center Linux 管理サーバーを Kaspersky Security Center Linux のフェールオーバークラスタノードにインストールします。

Kaspersky Security Center Web コンソールはクラスタリングに対応していません。Kaspersky Security Center Web コンソールを別のサーバーにインストールすることを推奨します。

*Kaspersky Security Center Linux のフェールオーバークラスタノードにインストールされた管理サーバーに接続する Kaspersky Security Center Web コンソールをインストールするには：*

1. Kaspersky Security Center Web コンソールのインストールのステップ 1 とステップ 2 を実行します。

2. ステップ 3 で、応答ファイルの `trusted` インストールパラメータを指定して、Kaspersky Security Center Linux のフェールオーバークラスターが Kaspersky Security Center Web コンソールに接続できるようにします。このパラメータの文字列値の形式は次の通りです：
   **`"trusted": "サーバーアドレス|ポート|証明書のパス|サーバー名"`**

   `trusted` インストールパラメータのコンポーネントを指定します：

   - **管理サーバーアドレス** クラスターノードの準備時にセカンダリネットワークアダプターを作成した場合は、アダプターの IP アドレスを Kaspersky Security Center Linux のフェールオーバークラスターのアドレスとして使用します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを指定します。

   - **管理サーバーのポート** Kaspersky Security Center Web コンソールが管理サーバーへの接続に使用する OpenAPI ポート（既定値は 13299）。

   - **管理サーバー証明書** 管理サーバーの証明書は、Kaspersky Security Center Linux のフェールオーバークラスターの共有データストレージにあります。証明書ファイルの既定のパス：<共有データフォルダー>\1093\cert\klserver.cer。証明書ファイルを共有データストレージから Kaspersky Security Center Web コンソールをインストールするデバイスにコピーします。管理サーバーの証明書のローカルパスを指定します。

   - **管理サーバー名** Kaspersky Security Center Web コンソールのログインウィンドウに表示される Kaspersky Security Center Linux のフェールオーバークラスター名。

3. Kaspersky Security Center Web コンソールの標準インストールを続行します。

インストールが完了したら、デスクトップにショートカットが作成され、Kaspersky Security Center Web コンソールにログインできます。

# 手動でのクラスターノードの開始と終了

Kaspersky Security Center Linux のフェールオーバークラスタ全体を停止したり、メンテナンスでクラスタのノードの一部を一時的に分離したりする必要がある場合があります。その場合はこのセクションの手順に従ってください。別の方法でフェールオーバークラスタに関連するサービスやプロセスを開始または停止しないでください。データを損失する可能性があります。

## メンテナンス目的でのフェールオーバークラスタ全体の開始および停止

*フェールオーバークラスタ全体を開始または停止するには：*

アクティブノードで、次のいずれかのコマンドを実行します：

- クラスタを停止するには、次のコマンドを実行します：`/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- クラスタを起動するには、次のコマンドを実行します：`/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

フェールオーバークラスタは実行したコマンドに基づいて開始または停止されます。

## ノードの一部のメンテナンス

*ノードの一部をメンテナンスするには：*

1. アクティブなノードで、コマンド「`klfoc -stopcluster --stp klfoc`」を使用してフェールオーバークラスターを停止します。
2. メンテナンス対象のノードで、/opt/kaspersky/ksc64/sbin に移動します。
3. コマンドラインを開き、コマンド「`detach_node.sh`」を実行してクラスターからノードを分離します。
4. アクティブなノードで、コマンド「`klfoc -startcluster --stp klfoc`」を使用してフェールオーバークラスターを開始します。
5. メンテナンスを行います。
6. アクティブなノードで、コマンド「`klfoc -stopcluster --stp klfoc`」を使用してフェールオーバークラスターを停止します。
7. メンテナンスしたノードで、/opt/kaspersky/ksc64/sbin に移動します。
8. コマンドラインを開き、コマンド「`attach_node.sh`」を実行してクラスターにノードを接続します。

9. アクティブなノードで、コマンド「`klfoc -startcluster --stp klfoc`」を使用してフェールオーバークラスターを開始します。

10. 現在のノードがアクティブであることを確認するには、次のコマンドを実行して、サービスが実行されているかどうかをチェックします：

    `systemctl status klnagent_srv.service`

    `systemctl status kladminserver_srv.service`

    `systemctl status klactprx_srv.service`

    `systemctl status klwebsrv_srv.service`

    これらのサービスは、アクティブノードで実行され、パッシブノードでは実行されません。

ノードのメンテナンスが完了し、フェールオーバークラスタに接続されます。

# DBMS に使用するアカウント

管理サーバーをインストールして操作するには、内部 DBMS アカウントが必要です。このアカウントは、DBMS へのアクセスを許可し、特定の権限を必要とします。必要な権限のセットは、次の基準に応じて異なります：

- DBMS タイプ：
  - MySQL または MariaDB
  - PostgreSQL または Postgres Pro
- 管理サーバーデータベースの作成方法：
  - **自動**管理サーバーのインストール中に、管理サーバーのインストーラー（インストーラー）を使用して、管理サーバーデータベース（以降、サーバーデータベースとも表記）を自動的に作成できます。
  - **手動**サードパーティのアプリケーションやスクリプトを使用して、空の定義データベースを作成することができます。その後、管理サーバーのインストール時に、このデータベースをサーバーデータベースとして指定できます。

アカウントに権限とアクセス許可を付与するときは、最小特権の原則に従います。つまり、付与する権限は、必要なアクションを実行するのに必要最低限にすべきです。

以下の表は、管理サーバーをインストールして起動する前にアカウントに付与する必要がある DBMS 権限に関する情報を示しています。

## MySQL および MariaDB

DBMS として MySQL または MariaDB を選択した場合は、DBMS 内部アカウントを作成して DBMS にアクセスし、このアカウントに必要な権限を付与します。データベースの作成方法によって、権限のセットに影響はありません。必要な権限は次の通りです：

- スキーマ権限：
  - 管理サーバーデータベース：ALL（GRANT OPTION を除く）。
  - システムスキーム（mysql および sys）：SELECT、SHOW VIEW。
  - sys.table_exists ストアドプロシージャ：EXECUTE（MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません）。
- すべてのスキームに対するグローバル権限：PROCESS、SUPER。

アカウント権限を設定する方法の詳細は、「MySQL および MariaDB を使用するための DBMS アカウントの設定」を参照してください。

共有テーブルスペースからファイルごとのテーブルスペースにデータを移動する方法の詳細については、「MySQL および MariaDB DBMS で共有テーブルスペースからファイルごとのテーブルスペースにデータを移動する」を参照してください。

## 管理サーバーのデータ復旧のための権限の設定

内部 DBMS アカウントに付与した権限は、管理サーバーのデータをバックアップから復元するのに十分です。

## PostgreSQL または Postgres Pro

PostgreSQL または Postgres Pro を DBMS として選択した場合、ユーザー *Postgres*（Postgres の既定のロール）を使用するか、新しい Postgres ロール（以降、ロールとも表記）を作成して DBMS にアクセスできます。サーバーデータベースの作成方法に応じて、次の表の説明に従って必要な権限をロールに付与します。ロールの権限を設定する方法の詳細は、「PostgreSQL および Postgres Pro を使用するための DBMS アカウントの設定」を参照してください。

Postgres ロールの権限

| 自動のデータベース作成 | | 手動のデータベース作成 |
|---|---|---|
| ユーザー*Postgres* には、追加の権限は必要ありません。 | 新しいロールの権限：CREATEDB | 新しいロールの場合：<br>• 管理サーバーデータベースに対する権限：ALL<br>• パブリックスキーマ内のすべてのテーブルに対する権限：ALL<br>• パブリックスキーマ内のすべてのシーケンスに対する権限：ALL |

データベースとして Postgres Highly Available クラスター（バージョン 14 以降）を使用する場合、データベースのユーザーは `pg_read_all_stats` 権限を持つ必要があります。次のコマンドを実行してこの権限を付与できます：

```
GRANT pg_read_all_stats TO "%1";
```

ここで、「`%1`」はデータベース ユーザーの名前です。

ユーザー名は、管理サーバーのインストール時に KLSRV_UNATT_DBMS_LOGIN パラメータで指定されます。

### 管理サーバーのデータ復旧のための権限の設定

バックアップから管理サーバーのデータを復元するには、DBMS へのアクセスに使用される Postgres ロールに管理サーバーデータベースの所有者権限が必要です。

## MySQL および MariaDB を使用するための DBMS アカウントの設定

### 必須条件

DBMS アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. MySQL または MariaDB を使用するための環境をインストールします。

### 管理サーバーをインストールするための DBMS アカウントの設定

*管理サーバーのインストール用に DBMS アカウントを設定するには：*

1. DBMS のインストール時に作成した root アカウントで、MySQL または MariaDB を使用するための環境を実行します。
2. パスワード付きの内部 DBMS アカウントを作成します。管理サーバーインストーラー（以降、インストーラーとも表記）と管理サーバーサービスは、この内部 DBMS アカウントを使用して DBMS にアクセスします。

   パスワード付きの DBMS アカウントを作成するには、次のコマンドを実行します：

   ```
   /* KSCAdmin という名前のユーザーを作成し、KSCAdmin のパスワードを指定します */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<パスワード>';
   ```

   MySQL 8.0 以前を DBMS として使用する場合、これらのバージョンでは「caching_sha2_password」認証がサポートされていないことに注意してください。既定の認証を「Caching SHA2 password」から「MySQL native password」に変更します：

   - 「mysql_native_password」認証を使用する DBMS アカウントを作成するには、次のコマンドを実行します：

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
     ```

   - 既存の DBMS アカウントの認証を変更するには、次のコマンドを実行します：

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
     ```

3. 作成した DBMS アカウントに次の権限を付与します：

   - スキーマ権限：
     - 管理サーバーデータベース：ALL（GRANT OPTION を除く）
     - システムスキーム（mysql および sys）：SELECT、SHOW VIEW
     - sys.table_exists ストアドプロシージャ：EXECUTE
   - すべてのスキームに対するグローバル権限：PROCESS、SUPER

   作成した DBMS アカウントに必要な権限を付与するには、次のスクリプトを実行します：

   ```
   /* KSCAdmin に権限を付与します */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

   MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません。この場合、次のコマンドをスクリプトから除外します：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`。

4. DBMS アカウントに付与された権限のリストを表示するには、次のコマンドを実行します：

   ```
   SHOW grants for 'KSCAdmin';
   ```

5. 管理サーバーデータベースを手動で作成するには、次のスクリプトを実行します（このスクリプトでは、管理サーバーデータベース名は *kav* です）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   DBMS アカウントを作成するスクリプトで指定したものと同じデータベース名を使用します。

6. 管理サーバーをインストールします。

インストールが完了すると、管理サーバーデータベースが作成され、管理サーバーを使用できるようになります。

# PostgreSQL および Postgres Pro を使用するための DBMS アカウントの設定

## 必須条件

DBMS アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. PostgreSQL および Postgres Pro を使用するための環境をインストールします。
3. PostgreSQL または Postgres Pro サーバーを Kaspersky Security Center Linux と動作するように設定します。

## 管理サーバーをインストールするための DBMS アカウントの設定

*管理サーバーのインストール用に DBMS アカウントを設定するには：*

1. Postgres を使用するための環境を実行します。
2. *Postgres* データベースで *Postgres* ユーザーとしてログインします。
3. 新しい Postgres ロールを作成します（この例では、ロールは*KSCAdmin*です）：

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<パスワード>';
   ```

4. 管理サーバー定義データベースを作成します（この例では、管理サーバーデータベース名は *KAV* です）：

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   「新しいエンコーディング（UTF8）はテンプレートデータベースのエンコーディングと互換性がありません」というエラーが発生した場合は、次のコマンドを使用してデータベースを作成します：
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   の代わりに：
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";` を使用します。

5. 次に、このロールに管理サーバー定義データベースに対するすべての権限を付与します：

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   ロールに、管理サーバー定義データベースに対する既定の CONNECT および TEMPORARY 権限があることを確認します。

6. 作成した Postgres ロールに次の権限を付与します：

   - パブリックスキーマ内のすべてのテーブルに対する権限：ALL
   - パブリックスキーマ内のすべてのシーケンスに対する権限：ALL

   これを行うには、サーバー定義データベースにユーザー *Postgres* でログインし、次のスクリプトを実行します（このスクリプトでは、ロールは *KSCAdmin* です）：

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. 管理サーバーをインストールします。

インストールが完了すると、管理サーバーは作成されたデータベースを管理サーバーデータの保存に使用するようになります。管理サーバーが使用できるようになります。

# MySQL または MariaDB DBMS で、共有テーブルスペースからテーブルごとのファイルテーブルスペースへデータを移動する

MySQL および MariaDB DBMS の場合、次の方法でデータを保存できます：

- 共有テーブルスペースとして、すべてのユーザー定義データベースのデータが 1 つのファイル（通常は `ibdata1` ファイル）に保存される場合。
- ファイルごとのテーブルスペースとして、テーブルごとに個別のデータスペースが個別のファイルとして作成される場合。

共有テーブルスペースを使用すると、テーブルスペースの断片化のリスクが高まります。`SHRINK` 操作を実行できないため、共有テーブルスペース内のファイルがディスク領域の約 90% を占める可能性があります。これにより、ディスクサブシステムのパフォーマンスに悪影響が生じます。したがって、ファイルごとのテーブルスペースを選択すると便利です。

この記事では、共有テーブルスペースからファイルごとのテーブルスペースにデータを移動する方法について説明します。MySQL または MariaDB DBMS が他のアプリケーションでも使用されている場合は、これらのアプリケーションのデータベースをファイルごとのテーブルスペースに移動する必要があります。

> 管理サーバーに MySQL または MariaDB DBMS を使用している場合のみ、この手順を実行することを推奨します。
> 共有テーブルスペースからファイル単位テーブルスペースへのデータ移行は、ディスクサブシステムへの負荷を増加させる可能性があります。

## 必須条件

始める前に、次の点を確認してください：

- データバックアップタスクまたは klbackup ユーティリティのいずれかを実行して、管理サーバーデータのバックアップコピーが作成されていること。
- データベースが MySQL または MariaDB DBMS（存在する場合）によって管理されている他のアプリケーションのバックアップコピーが作成されていること。
- DBMS がインストールされているデバイスの、データベースがあるパーティションにディスクの空き容量があること。

必要なディスク容量は、現在の定義データベースの合計サイズ（`ibdata1` ファイルの現在のサイズ）の 150% です。

プロセス

*共有テーブルスペースからファイルごとの表領域にデータを移動するには：*

1. この手順を実行する対象の DBMS インスタンスを使用している Kaspersky Security Center 管理サーバーサービスおよびその他のアプリケーションを停止します。

2. DBMS のバージョンに応じて、スーパーユーザーとして DBMS にログインし、任意のアプリケーションでスクリプト `fix_tablespace.sql` を実行します。

   このリンクをクリックすると、スクリプト `fix_tablespace.sql` を表示できます：

   **MySQL 5.7 および MariaDB 10.1+ のスクリプトを表示**

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

MySQL 8.0+ のスクリプトを表示

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

スクリプトの実行を停止しないでください。
DBMS エラーが発生していない状態でスクリプトの実行を終了した場合は、スクリプトを再度実行するか、この手順の実行を中止して DBMS サービスを再起動した後、バックアップから管理サーバーのデータを復元してください。

3. my.cnf ファイルの［`[mysqld]`］セクションで、`innodb_file_per_table` パラメータを `1` に設定してください。
4. MySQL または MariaDB サービスを再起動します。
5. Kaspersky Security Center 管理サーバーサービスを開始します。

データは共有テーブルスペースからファイルごとのテーブルスペースに移動されます。

# Kaspersky Security Center Linux を使用するための証明書

このセクションでは、Kaspersky Security Center Linux の証明書に関する情報と、Kaspersky Security Center Web コンソール向けの証明書を発行および置き換える方法、サーバーが Kaspersky Security Center Web コンソールと連携している場合に管理サーバー向けの証明書を更新する方法について説明します。

# Kaspersky Security Center の証明書について

Kaspersky Security Center では、次の種類の証明書を使用することで、製品コンポーネント間の安全な対話を可能にしています。

- 管理サーバー証明書
- モバイル証明書
- Web サーバーの証明書
- Kaspersky Security Center Web コンソールの証明書

既定では、Kaspersky Security Center は自己署名証明書（つまり、Kaspersky Security Center 自体によって発行された証明書）を使用しますが、組織のネットワークの要件をより適切に満たし、セキュリティ標準に準拠するために、それらをカスタム証明書に置換することができます。カスタム証明書が該当するすべての要件を満たしているかどうかを管理サーバーが検証し、その後、この証明書は自己署名証明書と同じ機能範囲があると判断されます。唯一の違いは、カスタム証明書は期限切れ時に自動的に再発行されないことです。証明書のタイプに応じて、klsetsrvcert ユーティリティを使用するか、Kaspersky Security Center Web コンソールの［管理サーバーのプロパティ］セクションを介して、証明書をカスタム証明書に置換します。Klsetsrvcert ユーティリティを使用している際には、次の値のいずれかを使用して証明書を指定する必要があります：

- C：（ポート 13000 と 13291 に共通の証明書）
- CR：（ポート 13000 と 13291 に共通の予備の証明書）
- M：（ポート 13292 のモバイル証明書）
- MR：（ポート 13292 のモバイル予備証明書）
- MCA：（自動生成されたユーザー証明書のモバイル認証局）

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

## 管理サーバー証明書

管理サーバー証明書は、次の目的のために必要です：

- Kaspersky Security Center Web コンソールが管理サーバーに接続する際の認証
- 管理対象デバイスでの管理サーバーとネットワークエージェントとの安全な連携
- プライマリ管理サーバーがセカンダリ管理サーバーに接続されている場合の認証

管理サーバー証明書は、管理サーバーのインストール中に自動的に作成され、フォルダー「/var/opt/kaspersky/klnagent_srv/1093/cert/」に格納されます。Kaspersky Security Center Web コンソールをインストールするための応答ファイルを作成する際に管理サーバーの証明書を指定しています。この証明書は共通（「C」）と呼ばれます。

管理サーバーの証明書は 397 日間有効です。Kaspersky Security Center は、共通証明書の有効期限が切れる 90 日前に予備の共通証明書（「CR」）を自動的に生成します。その後、共通予備証明書を使用して、管理サーバー証明書はシームレスに置換されます。共通証明書の有効期限が近づくと、共通予備証明書を使用して、管理対象デバイスにインストールされているネットワークエージェントインスタンスとの接続が維持されます。この目的で、共通予備証明書は、古い共通証明書の有効期限が切れる 24 時間前に自動的に新しい共通証明書になります。

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

必要に応じて、カスタム証明書を管理サーバーに割り当てることができます。たとえば、企業の既存の PKI とのより容易な統合や、証明書フィールドの設定のカスタマイズなどの理由で、こうした操作が必要になる場合があります。証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。このエラーを解消するには、証明書の置換後に接続を復元する必要があります。

管理サーバー証明書を紛失した場合、その証明書を復元するには、管理サーバーを再インストールしてデータを復元する必要があります。

データを失うことなく管理サーバーをあるデバイスから別のデバイスに移動するために、他の管理サーバー設定とは別に管理サーバー証明書をバックアップすることもできます。

別のブラウザーで Kaspersky Security Center Web コンソールを開いて、管理サーバーの証明書ファイルを管理サーバーのプロパティウィンドウでダウンロードすると、ダウンロードされたファイルに異なる名前が付与されます。

## モバイル証明書

モバイルデバイスでの管理サーバーの認証には、モバイル証明書（「M」）が必要です。モバイル証明書は管理サーバーのプロパティで指定します。

また、モバイル予備（「MR」）証明書も存在します。これは、モバイル証明書のシームレスな置換に使用されます。Kaspersky Security Center は、共通証明書の有効期限が切れる 60 日前にこの証明書を自動的に生成します。モバイル証明書の有効期限が近づくと、モバイル予備証明書を使用して、管理対象のモバイルデバイスにインストールされているネットワークエージェントインスタンスとの接続が維持されます。この目的で、モバイル予備証明書は、古い証明書の有効期限が切れる 24 時間前に自動的に新しい証明書になります。

接続シナリオで、モバイルデバイスでクライアント証明書を使用する必要がある場合（双方向 SSL 認証を含む接続）、自動生成されたクライアント証明書（「MCA」）の認証局を使用してそれらの証明書を生成できます。また、管理サーバープロパティで、別の認証局によって発行されたカスタムクライアント証明書を指定できます。一方、組織のドメイン公開鍵インフラストラクチャ（PKI）と統合すると、ドメイン認証局を使用してクライアント証明書を発行できます。

また、iOS オペレーティングシステムを実行しているモバイルデバイス上での管理サーバーの認証には、iOS MDM サーバー証明書が必要です。詳細については、「iOS MDM サーバー証明書の設定」を参照してください。

### Web サーバーの証明書

Kaspersky Security Center 管理サーバーのコンポーネントである Web サーバーは、特殊な種別の証明書を使用します。この証明書は、後で管理対象デバイスにダウンロードするネットワークエージェントインストールパッケージの公開や、Kaspersky Security for Mobile インストールパッケージの公開に必要です。この目的のために、Web サーバーは様々な証明書を使用できます。

モバイルデバイスのサポートが無効になっている場合、Web サーバーは優先度の高い順に次の証明書のいずれかを使用します：

1. 管理コンソールを使用して手動で指定したカスタム Web サーバー証明書
2. 共通管理サーバー証明書（「C」）

モバイルデバイスのサポートが有効になっている場合、Web サーバーは優先度の高い順に次の証明書のいずれかを使用します：

1. 管理コンソールを使用して手動で指定したカスタム Web サーバー証明書
2. カスタムモバイル証明書
3. 自己署名モバイル証明書（「M」）
4. 共通管理サーバー証明書（「C」）

### Kaspersky Security Center Web コンソールの証明書

Kaspersky Security Center Web コンソール（以降「Web コンソール」と表記）のサーバーには、独自の証明書があります。Web サイトを開く際に、ブラウザは接続が信頼できるかどうかを確認します。Web コンソール証明書を使用して、Web コンソールを認証できます。この証明書は、ブラウザーと Web コンソールの間のトラフィックの暗号化にも使用されます。

Web コンソールを開くと、ブラウザーから Web コンソールとの接続がプライベートでなく Web コンソールの証明書が無効であると通知される場合があります。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち1つを実行します：

- カスタム証明書と Web コンソールの証明書を置き換える（推奨）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- ブラウザーの信頼済み証明書のリストに Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

## Kaspersky Security Center Linux で使用されるカスタム証明書の要件

次の表は、Kaspersky Security Center Linux の様々なコンポーネントに指定されているカスタム証明書の要件を示しています。

| 証明書の種別 | 要件 | コメント |
| --- | --- | --- |
| 共通証明書、予備の共通証明書（「C」「CR」） | 最短鍵長：2048<br>Basic Constraints（基本制約）：<br>• Path Length Constraint（パス長制約）：None<br>Key Usage（鍵用途）：<br>• デジタル署名<br>• 証明書の署名の検証<br>• 鍵の暗号化<br>• 証明書失効リスト（CRL）の署名の検証<br>Extended Key Usage（拡張鍵用途）（任意）：サーバー認証、クライアント認証。 | Extended Key Usage パラメータは任意です。<br>Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。 |
| Web サーバーの証明書 | Extended Key Usage（拡張鍵用途）：サーバー認証。<br>証明書が指定されている PKCS #12 コンテナーや PEM コンテナーには、公開鍵のチェーン全体が含まれています。<br>証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。<br>証明書は、サーバー証明書に適用された Web ブラウザーの有効な要件、および CA/Browser Forum の現在のベースライン要件を満たしています。 | — |
| Kaspersky Security Center Web コンソールの証明書 | 証明書が指定される PEM コンテナーには、公開鍵のチェーン全体が含まれます。<br>証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。<br>証明書は、サーバー証明書に対する Web ブラウザーの有効な要件、および CA /Browser Forum の現在のベースライン要件を満たしています。 | 暗号化された証明書は、Kaspersky Security Center Web コンソールではサポートされていません。 |

# Kaspersky Security Center Web コンソールの証明書の再発行

ほとんどの Web ブラウザーは、証明書の有効期間に制限があります。この制限内に収まるように、Kaspersky Security Center Web コンソール証明書の有効期間は 397 日間に制限されています。新しい自己署名証明書を手動で発行することにより、証明機関（CA）から受け取った既存の証明書を置き換えることができます。または、有効期限切れの Kaspersky Security Center Web コンソール証明書を再発行することもできます。

Kaspersky Security Center Web コンソールの証明書の自動再発行はサポートされていません。期限切れの証明書は手動で再発行する必要があります。

Kaspersky Security Center Web コンソールを開くと、ブラウザーは Kaspersky Security Center Web コンソールとの接続はプライベートでなく Kaspersky Security Center Web コンソールの証明書が無効であると通知します。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center Linux によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち 1 つを実行します：

- 再発行する場合はカスタム証明書を指定する（推奨オプション）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- 証明書を再発行した後で、ブラウザーの信頼済み証明書のリストに Kaspersky Security Center Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

*有効期限切れの Kaspersky Security Center Web コンソール証明書を再発行するには：*

以下のいずれかを実行して Kaspersky Security Center Web コンソールを再インストールします：

- Kaspersky Security Center Web コンソールと同じインストールファイルを使用する場合は、Kaspersky Security Center Web コンソールを削除してから同じバージョンの Kaspersky Security Center Web コンソールをインストールします。
- アップグレードバージョンのインストールファイルを使用する場合は、アップグレードコマンドを実行します。

Kaspersky Security Center Web コンソールの証明書が再発行されます。有効期間は 397 日です。

## Kaspersky Security Center Web コンソールの証明書の置き換え

既定では、Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）をインストールすると、Web コンソールのブラウザー証明書が自動的に生成されます。必要に応じて、自動的に生成された証明書をカスタム証明書で置き換えることができます。

*Kaspersky Security Center Web コンソールの証明書をカスタム証明書で置き換えるには：*

1. Kaspersky Security Center Web コンソールのインストール時に作成した応答ファイルを開きます。

   必要であれば、新しい応答ファイルを作成することもできます。

2. ファイルで、次のパスを指定します：

   - `certPath` パラメータを使用して、Kaspersky Security Center Web コンソールのカスタム証明書ファイルへ
   - `keyPath` パラメータを使用して、Kaspersky Security Center Web コンソールのカスタム証明書に関連付けられた秘密鍵に移動します。

     両方のパスを指定する必要があります。そうしないと、Web ブラウザーは接続がプライベートではないことを通知し続けます。

3. 新しい応答ファイルを使用して Kaspersky Security Center Web コンソールを再インストールします。次のいずれかの手順を実行します：

   - Kaspersky Security Center Web コンソールと同じインストールファイルを使用する場合は、Kaspersky Security Center Web コンソールを削除してから同じバージョンの Kaspersky Security Center Web コンソールをインストールします。
   - アップグレードバージョンのインストールファイルを使用する場合は、アップグレードコマンドを実行します。

指定した証明書を使用して Kaspersky Security Center Web コンソールが動作するようになります。

## PFX 証明書を PEM 形式に変換する

Kaspersky Security Center Web コンソールで PFX 証明書を使用するには、まず、OpenSSL ベースの簡便に使用できる任意のクロスプラットフォームユーティリティを使用して PEM 形式に変換する必要があります。

*Linux オペレーティングシステムで PFX 証明書を PEM 形式に変換するには：*

1. OpenSSL ベースのクロスプラットフォームユーティリティで、次のコマンドを実行します。

   ```
   openssl pkcs12 -in <ファイル名.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <ファイル名.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 証明書ファイルと秘密鍵が、.pfx ファイルが格納されているのと同じディレクトリに生成されていることを確認してください。

3. Kaspersky Security Center Web コンソールはパスフレーズで保護された証明書はサポートしていません。そのため、OpenSSL ベースのクロスプラットフォームユーティリティで次のコマンドを実行して .pem ファイルからパスフレーズを削除します：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 入力と出力用の .pem ファイルに同じ名前を使用しないでください。

   結果、.pem ファイルが非暗号化となります。ファイルを使用する際にパスフレーズを入力する必要はありません。

.crt ファイルと .pem ファイルを使用する準備ができたので、Kaspersky Security Center Web コンソールのインストーラーでそれらを指定できるようになります。

## シナリオ：管理サーバーのカスタム証明書の指定

管理サーバーのカスタム証明書を割り当てることができます。目的の例として、企業で使用する既存の公開鍵インフラストラクチャ（PKI）との連携の改善、証明書フィールドのカスタム設定などがあります。管理サーバーのインストール直後、かつクイックウィザードの終了前に、証明書を置換することを推奨します。

> 管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

## 必須条件

以下の条件を満たす必要があります：

- 新しい証明書は、PKCS#12 形式（たとえば、組織の PKI を使用）で作成する必要があります。
- その新規の証明書は、次の表にリストされた要件を満たす必要があります。

  以下の表では、新しい証明書が信頼できる認証局（CA）によって発行される必要があることを意味する要件「CA：true」に注意してください。「CA：true」という要件の新しい証明書には、信頼の連鎖全体と秘密鍵が含まれている必要があり、その秘密鍵は拡張子が pfx または p12 のファイルに格納されている必要があります。

  管理サーバー証明書の要件

| 証明書の種別 | 要件 |
| --- | --- |
| 共通証明書、予備の共通証明書（「C」「CR」） | 最短鍵長：2048<br>Basic Constraints（基本制約）：<br>• Path Length Constraint（パス長制約）：None<br>Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。<br>Key Usage（鍵用途）：<br>• デジタル署名<br>• 証明書の署名の検証<br>• 鍵の暗号化<br>• 証明書失効リスト（CRL）の署名の検証<br>Extended Key Usage（EKU：拡張鍵用途）：サーバー認証、クライアント認証。EKU は任意ですが、証明書に含まれる場合、サーバーとクライアントの認証データは EKU で指定されている必要があります。 |
| モバイルデバイス用証明書、モバイルデバイス用の予備の証明書（「M」「MR」） | 最短鍵長：2048<br>Basic Constraints（基本制約）：<br>• CA：true<br>• Path Length Constraint（パス長制約）：None<br>Path Length Constraint の値は「None」ではない場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。<br>Key Usage（鍵用途）：<br>• デジタル署名<br>• 証明書の署名の検証<br>• 鍵の暗号化<br>• 証明書失効リスト（CRL）の署名の検証<br>Extended Key Usage（EKU：拡張鍵用途）：サーバー認証。EKU は任意ですが、証明書に含まれる場合、サーバーの認証データは EKU で指定されている必要があります。 |
| 自動生成されたユーザー証明書用の CA 証明書（「MCA」） | 最短鍵長：2048<br>Basic Constraints（基本制約）：<br>• CA：true<br>• Path Length Constraint（パス長制約）：None<br>Path Length Constraint の値は「None」ではない場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。<br>Key Usage（鍵用途）：<br>• デジタル署名<br>• 証明書の署名の検証<br>• 鍵の暗号化<br>• 証明書失効リスト（CRL）の署名の検証<br>Extended Key Usage（EKU：拡張鍵用途）：クライアント認証。EKU は任意ですが、証明書に含まれる場合、クライアントの認証データは EKU で指定されている必要があります。 |

パブリック CA によって発行された証明書には、証明書署名の許可がありません。このような証明書を使用するには、ネットワークのディストリビューションポイントまたは接続ゲートウェイに、ネットワークエージェントのバージョン 13 以降がインストールされていることを確認してください。そうしないと、署名の許可なしに証明書を使用できなくなります。

## 実行するステップ

管理サーバー証明書の指定は段階的に進行します。

1. **管理サーバー証明書の置換**

   この目的のために、コマンドラインで klsetsrvcert ユーティリティを使用します。

2. **新しい証明書を指定し、ネットワークエージェントの管理サーバーへの接続を復元**

   証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。新しい証明書を指定して接続を復元するには、コマンドラインで klmover ユーティリティを使用します。

3. **Kaspersky Security Center Web コンソールの設定で新しい証明書を指定する**

   証明書を置き換えた後、応答ファイルで証明書を指定し、このファイルを使用して Kaspersky Security Center Web コンソールをアップデートします。この操作を実行しない場合、Kaspersky Security Center Web コンソールは管理サーバーに接続できなくなります。

### 結果

このシナリオを終了すると、管理サーバー証明書が置換され、管理対象デバイスのネットワークエージェントでサーバーが認証されます。

## klsetsrvcert ユーティリティを使用した管理サーバー証明書の置換

*管理サーバーの証明書を手動で置換するには：*

コマンドラインから、次のユーティリティを実行します：

**klsetsrvcert [-t <証明書の種類> {-i <新しい証明書へのパス> [-p <パスワード>] [-o <検証パラメータ>] | -g <DNS 名>}][-f <交換時期>][-r <ルート証明書>][-l <ログファイルパス>]**

klsetsrvcert ユーティリティをダウンロードする必要はありません。Kaspersky Security Center Linux の配布キットに含まれています。Kaspersky Security Center Linux の以前のバージョンとは互換性がありません。

klsetsrvcert ユーティリティのパラメータの説明を次のテーブルに示します。

klsetsrvcert ユーティリティのパラメータ値

| パラメータ | 値 |
| --- | --- |
| **-t <証明書の種類>** | 置換する証明書の種別。**<証明書の種類>** パラメータの：<br>• C：ポート 13000 と 13291 の共通証明書を置換<br>• CR：ポート 13000 と 13291 の予備の証明書を置換 |
| **-f <交換時期>** | 証明書の変更の予定時刻。形式は「DD-MM-YYYY hh:mm」です（ポート 13000 と 13291 向け）。<br>共通証明書の有効期間の終了前に、共通証明書を共通予備証明書に置換する場合は、このパラメータを使用します。<br>管理対象デバイスが新しい証明書で管理サーバーと同期する必要がある時間を指定します。 |
| **-i <新しい証明書へのパス>** | PKCS#12 形式の証明書と秘密鍵を持つコンテナー（拡張子が .p12 または .pfx のファイル）。 |
| **-p <パスワード>** | p12 コンテナーの保護に使用されるパスワード<br>証明書と秘密鍵はコンテナに保存されているため、コンテナでファイルを復号化するにはパスワードが必要です。 |

| パラメータ | 値 |
| --- | --- |
| `-o <検証パラメータ>` | 証明書の検証パラメータ（セミコロン区切り）。<br>証明書署名の権限なしにカスタム証明書を使用するには、klsetsrvcert ユーティリティで `-o NoCA` を指定します。これは、パブリック認証局（CA）によって発行された証明書に役立ちます。<br>証明書タイプ C または CR の暗号化鍵の長さを変更するには、klsetsrvcert ユーティリティで `-o RsaKeyLen:<鍵長>` を指定します。ここで、`<鍵長>` パラメータは必要な鍵の長さの値です。それ以外の場合は、現在の証明書の鍵の長さが使用されます。 |
| `-g <DNS 名>` | 指定した DNS 名に対する新しい証明書が作成されます。 |
| `-r <ルート証明書>` | 信頼済みのルート証明機関のリスト（PEM 形式）。 |
| `-l <ログファイルパス>` | 結果出力ファイル。既定では、出力は標準出力ストリームにリダイレクトされます |

例えば、カスタム管理サーバー証明書を指定するには、次のコマンドを使用します。

```
klsetsrvcert -t C -i <新しい証明書へのパス> -p <パスワード> -o NoCA
```

証明書が置換されると、SSL を介して管理サーバーに接続されているすべてのネットワークエージェントの接続は切断されます。復元するには、コマンドライン klmoverユーティリティを使用します。

ネットワークエージェントの接続が切断されないようにするには、次のコマンドを使用します：

1. 新しい証明書をインストールするには、

   ```
   klsetsrvcert -t CR -i <新しい証明書へのパス> -p <パスワード> -o NoCA
   ```

2. 新しい証明書を適用する日付を指定するには、

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

"DD-MM-YYYY hh:mm" は、現在より 3 ～ 4 週間先の日付です。時間を変えて証明書を新しいものに変更することにより、新しい証明書をすべてのネットワークエージェントに配信できます。

## klmover ユーティリティを使用したネットワークエージェントの管理サーバーへの接続

たとえば、管理サーバーに障害が発生した後、バックアップから復元できない場合は、klmover ユーティリティを使用して、制御されていないデバイスから管理サーバーへの接続を復元することができます。

*接続を復元するには、コマンドラインから klmover ユーティリティを実行します：*

- Linux の場合：
  - 32 ビットシステムの場合：`/opt/kaspersky/klnagent/bin/klmover [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルへのパス>]`
  - 64 ビットシステムの場合：`/opt/kaspersky/klnagent64/bin/klmover [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルへのパス>]`
- Windows の場合：
  - 64 ビットシステムの場合：`<パス>\klmover.exe [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルへのパス>]`
  - 64 ビットシステムの場合：`<パス>\klmover.exe [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルへのパス>]`

ここで、**<パス>** は、ネットワークエージェントの既定のインストールパス、またはネットワークエージェントのインストールパッケージの設定で指定したインストールパスです。

侵入者がデバイスを管理サーバーの制御外に移動するのを防ぐために、klmover ユーティリティを実行する際のパスワード保護を有効にすることを強く推奨します。パスワード保護を有効にするには、ネットワークエージェントポリシー設定で［**アンインストール用パスワードを使用する**］をオンにします。

Kaspersky Security Center Linux の管理下になくなったデバイスにインストールされた、パスワードで保護されたネットワークエージェントのパスワードを紛失または忘れた場合、klmover ユーティリティ、またはコマンドラインを使用してネットワークエージェントを削除することはできません。この場合、パスワードで保護されたネットワークエージェントがインストールされているデバイスにオペレーティングシステムを再インストールする必要があります。

klmover ユーティリティにはローカル管理者権限が必要です。

Windows デバイスで**アンインストール用パスワードを使用する**オプションを有効にすると、クリーナーツール（cleaner.exe）のパスワード保護も有効になります。

接続ゲートウェイを介して管理サーバーに接続されたクライアントデバイスでは、klmover ユーティリティは使用できません。このようなデバイスの場合は、ネットワークエージェントを再構成するか、ネットワークエージェントを再インストールして接続ゲートウェイを指定する必要があります。

klsetsrvcert ユーティリティのパラメータの説明を次のテーブルに示します。

klmover ユーティリティのパラメータ値

| パラメータ | 値 |
| --- | --- |
| `-address <サーバーアドレス>` | 接続する管理サーバーのアドレス。<br>IP アドレスまたは DNS 名を指定できます。 |
| `-pn <ポート番号>` | 管理サーバーへの暗号化されていない接続が確立されるポートの番号。<br>既定のポート番号は 14000 です。 |

| パラメータ | 値 |
| --- | --- |
| `-ps <SSL ポート番号>` | SSL を使用した管理サーバーへの暗号化接続の確立に使用する SSL ポートの番号。<br>既定のポート番号は 13000 です。 |
| `-nossl` | 管理サーバーへの暗号化されていない接続を使用します。<br>このキーを使用しない場合、ネットワークエージェントは暗号化された SSL プロトコルを使用して管理サーバーに接続されます。 |
| `-cert <証明書ファイルのパス>` | 管理サーバーへのアクセス認証で使用する証明書ファイル。 |
| `-nauninstpwd <パスワード>` | このパラメータを使用して、ネットワークエージェントのアンインストールパスワードを指定します。<br>このパラメータは必須ではありません。 |

# Web サーバー証明書の再発行

Kaspersky Security Center Linux で使用される Web サーバー証明書は、後で管理対象デバイスにダウンロードするネットワークエージェントインストールパッケージの公開、および iOS MDM プロファイル、iOS アプリ、Kaspersky Endpoint Security for Mobile インストールパッケージの公開に必要です。現在のアプリケーション設定に応じて、様々な証明書を Web サーバー証明書として機能させることができます（詳細については、Kaspersky Security Center Linux 証明書についてを参照してください）。

アプリケーションのアップグレードを開始する前に、組織の特定のセキュリティ要件を満たすため、または管理対象デバイスの常時接続を維持するために、Web サーバー証明書を再発行する必要があります。Kaspersky Security Center Linux では、Web サーバー証明書の再発行には 2 つの方法が用意されています。どちらを選択するかは、モバイルプロトコルを介して（つまり、モバイル証明書を使用して）モバイルデバイスを接続および管理しているかどうかによって異なります。

管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで独自のカスタム証明書を Web サーバー証明書として指定していなければ、モバイル証明書が Web サーバー証明書として機能します。この場合、Web サーバー証明書の再発行は、モバイルプロトコル自体の再発行を通じて行われます。

*モバイルプロトコルを介して管理されているモバイルデバイスがある場合に Web サーバー証明書を再発行するには：*

1. カスタム証明書を生成し、Kaspersky Security Center Linux で使用できるように準備します。カスタム証明書が Kaspersky Security Center Linux の要件および Apple による信頼済み証明書の要件を満たしているかどうかを確認します。必要に応じて、証明書を変更します。

   kliossrvcertgen ユーティリティを使用して証明書を生成できます。

2. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

3. ［**全般**］タブで、［**Web サーバー**］セクションを選択します。

4. ［**HTTP 経由**］サブセクションで、［**ファイルから証明書をアップロードする**］オプションをオンにし、［**証明書の変更**］をクリックします。

5. ［Certificate］が表示されるので、［**証明書の形式**］で証明書のタイプを選択します。

   - ［**PKCS #12 コンテナー**］を選択した場合、［**証明書**］フィールドの横の［**参照**］をクリックして、ハードディスク上の証明書ファイルを指定します。証明書ファイルがパスワードで保護されている場合は、［**パスワード**］にパスワードを入力します。

   - ［**X.509 証明書**］を選択した場合、［**秘密鍵**］の横の［**参照**］をクリックして、ハードディスク上の秘密鍵を指定します。秘密鍵がパスワードで保護されている場合は、［**パスワード**］にパスワードを入力します。

6. ［**保存**］をクリックし、［**OK**］をクリックします。

   ウィンドウは閉まっています。

7. 必要に応じて、［**Web サーバーの HTTPS ポート**］フィールドで Web サーバーの HTTPS ポート番号を変更し、［**保存**］をクリックします。

Web サーバー証明書が再発行されます。

*モバイルプロトコルを介して管理されているモバイルデバイスがない場合に Web サーバー証明書を再発行するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**証明書**］セクションを選択します。

3. Kaspersky Security Center によって発行された証明書を引き続き使用する場合は、次の手順を実行します：

   a. ［**管理サーバーを使用して発行された証明書**］を選択し、［**参照**］をクリックします。

   b. 開いたウィンドウで、［**接続アドレス**］および［**アクティベーション期間**］の設定グループで関連するオプションを選択し、［**OK**］をクリックします。

または、独自のカスタム証明書を使用する場合は、次の手順を実行します：

a. カスタム証明書が Kaspersky Security Center Linux の要件および Apple による信頼済み証明書の要件を満たしているかどうかを確認します。必要に応じて、証明書を変更します。

b. ［**その他の証明書**］を選択し、［**証明書の管理**］をクリックし、開いたウィンドウで［**参照**］をクリックします。

c. 開いたウィンドウの［**証明書の形式**］フィールドで証明書のタイプを選択します。

   - ［**PKCS #12 コンテナー**］を選択した場合、［**証明書**］フィールドの横の［**参照**］をクリックして、ハードディスク上の証明書ファイルを指定します。証明書ファイルがパスワードで保護されている場合は、［**パスワード**］にパスワードを入力します。

   - ［**X.509 証明書**］を選択した場合、［**秘密鍵**］の横の［**参照**］をクリックし、ハードディスク上の秘密鍵を指定します。秘密鍵がパスワードで保護されている場合は、［**パスワード**］にパスワードを入力します。

d. ［**保存**］をクリックし、［**OK**］をクリックします。

モバイル証明書が再発行され、Web サーバー証明書として使用できます。

# 共有フォルダーの定義

管理サーバーのインストール後、管理サーバーのプロパティで共有フォルダーの場所を指定できます。既定では、共有フォルダーは管理サーバーがインストールされたデバイスに作成されます。ただし、特定のケース（高負荷、分離されたネットワークからのアクセスが必要な場合など）においては、共有フォルダーを専用ファイルリソースに置くのが適切な方法です。

共有フォルダーは、ネットワークエージェントの導入時に使用されることもあります。

共有フォルダーでは、大文字と小文字の区別を無効にする必要があります。

# Kaspersky Security Center Web コンソールへのサインインとサインアウト

管理サーバーと Web コンソールサーバーのインストールが完了すると、Kaspersky Security Center Web コンソールにサインインできます。インストール中に指定した管理サーバーのアドレスとポート番号の情報が必要になります（既定のポート番号は 8080 です）。ブラウザーでは、JavaScript が有効になっている必要があります。

*Kaspersky Security Center Web コンソールにサインインするには：*

1. ブラウザーで、https://<**Kaspersky Security Center Web コンソールのアドレス**>:<**ポート番号**> にアクセスします。

   サインインページが表示されます。

2. 複数台の信頼する管理サーバーを追加している場合、管理サーバーのリストから接続する管理サーバーを選択します。

   管理サーバーを 1 つだけ追加した場合、管理サーバーのリストはロックされます。

3. 次のいずれかの手順を実行します：

   - ドメインユーザーアカウントを使用して管理サーバーにサインインするには、ドメインユーザーのユーザー名とパスワードを入力します。

     ドメインユーザーのユーザー名は、次のいずれかの形式で入力できます：

     - **ユーザー名@dns.domain**
     - **NTDOMAIN\ユーザー名**

     > ドメインユーザーアカウントでサインインする前に、ドメインコントローラーをポーリングしてドメインユーザーのリストを取得します。

   - 管理者のユーザー名とパスワードを指定して管理サーバーにサインインするには、内部ユーザーのユーザー名とパスワードを入力します。
   - サーバー上に1つ以上の仮想管理サーバーが作成されており、仮想サーバーにサインインしたい場合：

     a. ［**仮想サーバーのオプションを表示する**］をクリックします。

     b. 仮想サーバーの作成時に指定した仮想管理サーバー名を入力します。

     c. 仮想管理サーバーの権限を持つ管理者のユーザー名とパスワードを入力します。

4. ［**サインイン**］をクリックします。

5. アカウントで二段階認証が有効になっている場合は、モバイルデバイスの認証アプリによって生成されたセキュリティコードを指定します。

   必要に応じて、サインインページに戻ることができます。

6. アカウントで強制パスワード変更が有効になっている場合、またはパスワードの有効期限が切れている場合は、パスワード変更ウィンドウが表示されます。Kaspersky Security Center Web コンソールにサインインするための新しいパスワードを設定します。

ログイン後、Kaspersky Security Center Web コンソールのホームページが表示され、前回使用した言語とテーマが表示されます。Kaspersky Security Center Web コンソールを操作して、Kaspersky Security Center Linux による処理を実行できます。

### サインアウト

*Kaspersky Security Center Web コンソールからサインアウトするには：*

メインメニューで、アカウント設定に移動して、［**ログアウト**］を選択します。

Kaspersky Security Center Web コンソールが終了し、サインインページが表示されます。

# Kaspersky Security Center Web コンソールインターフェイス

Kaspersky Security Center Linux は、Kaspersky Security Center Web コンソールインターフェイスを通じて管理されます。

Kaspersky Security Center Web コンソールウィンドウには、次の項目が含まれています：

- ウィンドウ左側のメインメニュー
- ウィンドウ右側の作業領域

## メインメニュー

メインメニューには次のセクションがあります：

- **管理サーバー**。現在接続している管理サーバーの名前が表示されます。設定アイコン（  ）をクリックして、管理サーバーのプロパティを開きます。
- **クイックリンク**。メインメニューマップを表示します。既定では、［**クイックリンク**］がホームページとして設定されています。この設定は変更できます。
- **監視とレポート**。インフラストラクチャの状況、保護ステータス、統計情報を提供します。
- **資産（デバイス）**。資産、タスク、カスペルスキー製品ポリシーのためのツールが含まれています。
- **ユーザーとロール**。ユーザーとロールを管理し、ユーザーにロールを割り当ててユーザー権限を構成し、ポリシープロファイルをロールに関連付けることができます。
- **操作**。アプリケーションのライセンス管理、暗号化されたドライブと暗号化イベントの表示と管理、サードパーティのアプリケーションの管理など、さまざまな操作が含まれます。これにより、アプリケーションリポジトリへのアクセスも可能になります。
- **検出と製品の導入**。ネットワークをポーリングしてクライアントデバイスを検出し、デバイスを管理グループに手動または自動で配布できます。これには、クイックスタートウィザードと製品導入ウィザードも含まれています。
- **マーケットプレイス**。カスペルスキーの法人向けソリューション全体に関する情報が含まれており、必要なソリューションを選択して、カスペルスキーの Web サイトでそれらのソリューションの購入に進むことができます。
- **設定**。Web プラグインの現在の状態をバックアップして、後から保存した状態を復元できます。インターフェイスの言語またはテーマなど、インターフェイスの表示に関連する個人設定が含まれます。
- **アカウントメニュー**：Kaspersky Security Center Linux ヘルプへのリンクが含まれています。また、Kaspersky Security Center Linux からログアウトし、Kaspersky Security Center Web コンソールのバージョンとインストールされている管理 Web プラグインのリストを表示することもできます。

## 作業領域

作業領域には、Kaspersky Security Center Web コンソールインターフェイスウィンドウの各セクションで表示を選択した情報が表示されます。また、情報の表示方法の構成に使用できるコントロール要素も含まれています。

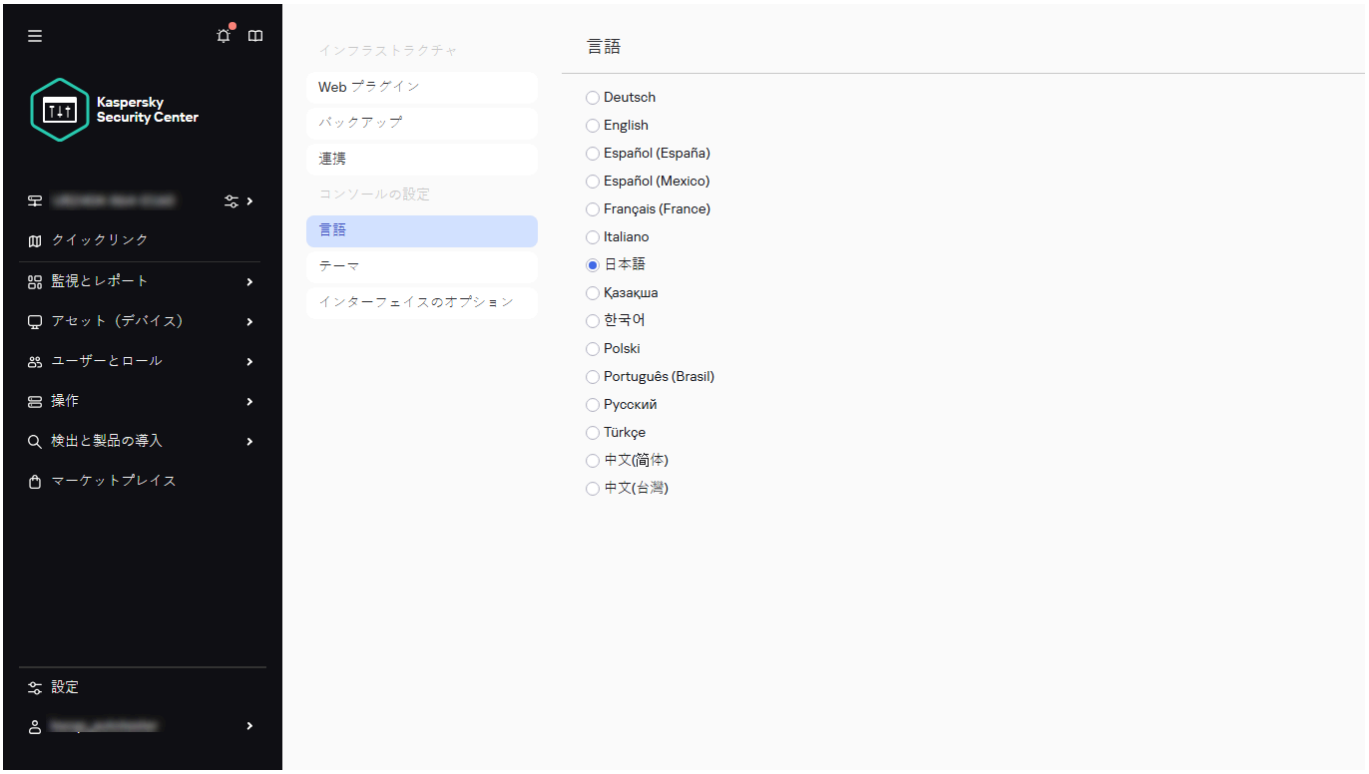
Kaspersky Security Center Web コンソールを操作するには、単一のブラウザータブを使用することを推奨します。

# Kaspersky Security Center Web コンソールインターフェイスの言語の変更

Kaspersky Security Center Web コンソールインターフェイスの言語を選択できます。

*インターフェイス言語を変更するには：*

1. メインメニューで、［**設定**］→［**言語**］の順にクリックします。
2. サポートされているローカリゼーション言語のいずれかを選択します。




Kaspersky Security Center Web コンソールインターフェイスの言語の変更

# Kaspersky Security Center Web コンソールのホームページの変更

Kaspersky Security Center Web コンソールにサインインすると、ホームページが表示されます。

既定では、［**クイックリンク**］セクションがホームページとして設定されています。必要に応じてホームページを変更することができます。

*ホームページを変更するには：*

1. ［**クイックリンク**］セクションで、ホームページとして設定する項目の上にマウスカーソルを置きます。
2. ホーム（）アイコンが表示されたら、アイコンをクリックします。

ホームページが変更され、適切なメッセージが画面に表示され、ホームページとして選択された項目にホーム（）アイコンをクリックします。

［**マーケットプレイス**］および［**設定**］セクションをホームページとして設定することはできません。

## ブックマークの追加と削除

Kaspersky Security Center Web コンソールのよく使用するセクションをブックマークに追加し、メインメニューの［**ブックマーク**］セクションからすばやくアクセスすることができます。

ブックマークに要素を追加しなかった場合、メインメニューに［**ブックマーク**］セクションは表示されません。

ページを表示するセクションのみブックマークに追加できます。たとえば、［**アセット（デバイス）**］→［**管理対象デバイス**］に移動すると、デバイスの表を含むページが開き、このセクションをブックマークに追加できるようになります。メインメニューでこのセクションを選択した後にウィンドウまたは要素が表示されない場合は、そのセクションをブックマークに追加することはできません。

*ブックマークにセクションを追加するには：*

1. メインメニューで、ピン留めするセクションの上にマウスカーソルを置きます。
2. ブックマークの後（）アイコンが表示されたら、アイコンをクリックします。

   セクションが［**ブックマーク**］セクションに表示されます。

*ブックマークからセクションを削除するには：*

1. メインメニューで、［**ブックマーク**］セクションに移動します。
2. 削除したいセクションにマウスカーソルを合わせ、ブックマーク（）アイコンをクリックします。

   セクションがブックマークから削除されます。

［**クイックリンク**］セクションのブックマークに要素を追加したり削除したりすることもできます。その場合は、マウスカーソルを要素の上に置き、ブックマーク（）アイコンをクリックします。選択された項目にはブックマーク（）アイコンが付与され、メインメニューの［**ブックマーク**］セクションに表示されます。ブックマークからアイテムを削除する場合は、ブックマーク（）アイコンをクリックします。

［**ブックマーク**］セクションはメインメニューにのみ表示されます。［**クイックリンク**］ページには表示されません。

# クイックスタートウィザード

Kaspersky Security Center Linux では、セキュリティ上の脅威から社内ネットワークを保護するための一元的な管理システムを構築する上で調整が必要な最小限の設定項目が選定されており、これらの設定を編集してセキュリティ管理システムを構築できます。この設定は、クイックスタートウィザードを使用して行います。ウィザードの実行中、次の変更をアプリケーションに対して行うことができます：

- 管理グループ内のデバイスに自動配信可能なライセンス情報ファイルを追加するか、アクティベーションコードを入力します。
- 管理サーバーおよび管理対象アプリケーションの操作中に発生するイベントの通知をメールで配信するように設定します。
- 管理対象デバイスの最上位階層で、ワークステーションとサーバーの保護ポリシー、およびマルウェアスキャンタスク、アップデートのダウンロードタスク、データバックアップタスクを作成します。

  クイックスタートウィザードでは、［**管理対象デバイス**］フォルダーにポリシーがないアプリケーションに対してのみポリシーが作成されます。管理対象デバイスの最上位階層で同じ名前のタスクが作成済みの場合、クイックスタートウィザードではタスクが作成されません。

管理サーバーのインストール後に初めて接続すると、クイックスタートウィザードを実行することを指示するメッセージが自動的に表示されます。また、クイックスタートウィザードはいつでも手動で起動できます。

*クイックスタートウィザードを手動で起動するには：*

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**全般**］セクションを選択します。




管理サーバーのプロパティウィンドウ

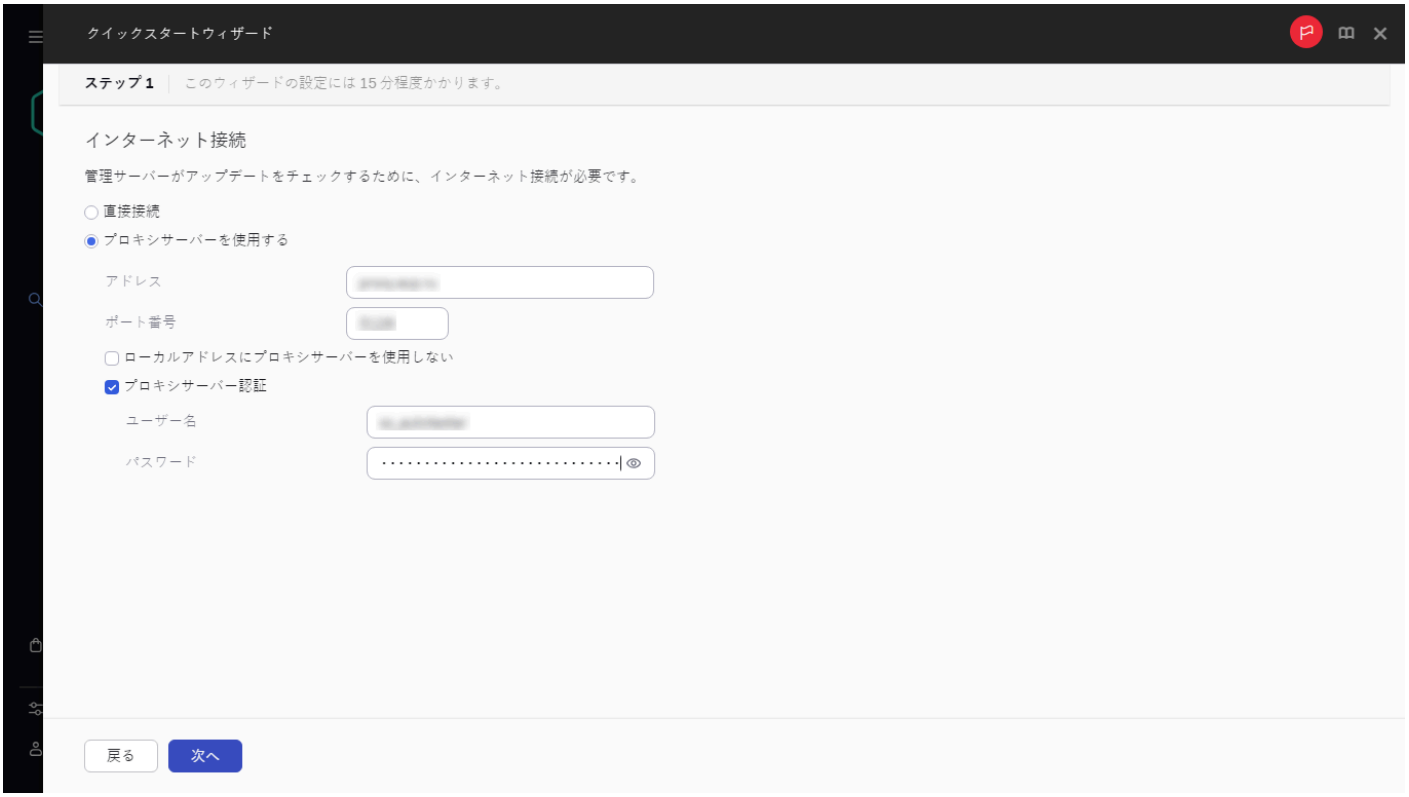
3. ［**クイックスタートウィザードを開始**］をクリックします。

管理サーバーの初期設定を実行するように指示されます。ウィザードの指示に従ってください。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

# ステップ1：インターネット接続設定の指定

管理サーバーのインターネットアクセスを設定します。Kaspersky Security Network を使用し、Kaspersky Security Center Linux 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：




インターネット接続設定

- **アドレス**

  インターネットへの Kaspersky Security Center Linux の接続に使用するプロキシサーバーのアドレス。

- **ポート番号**

  Kaspersky Security Center Linux でプロキシサーバーへの接続を確立するポートの番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
  ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（[**プロキシサーバー認証**]をオンにした場合に有効になります）。

- **パスワード**

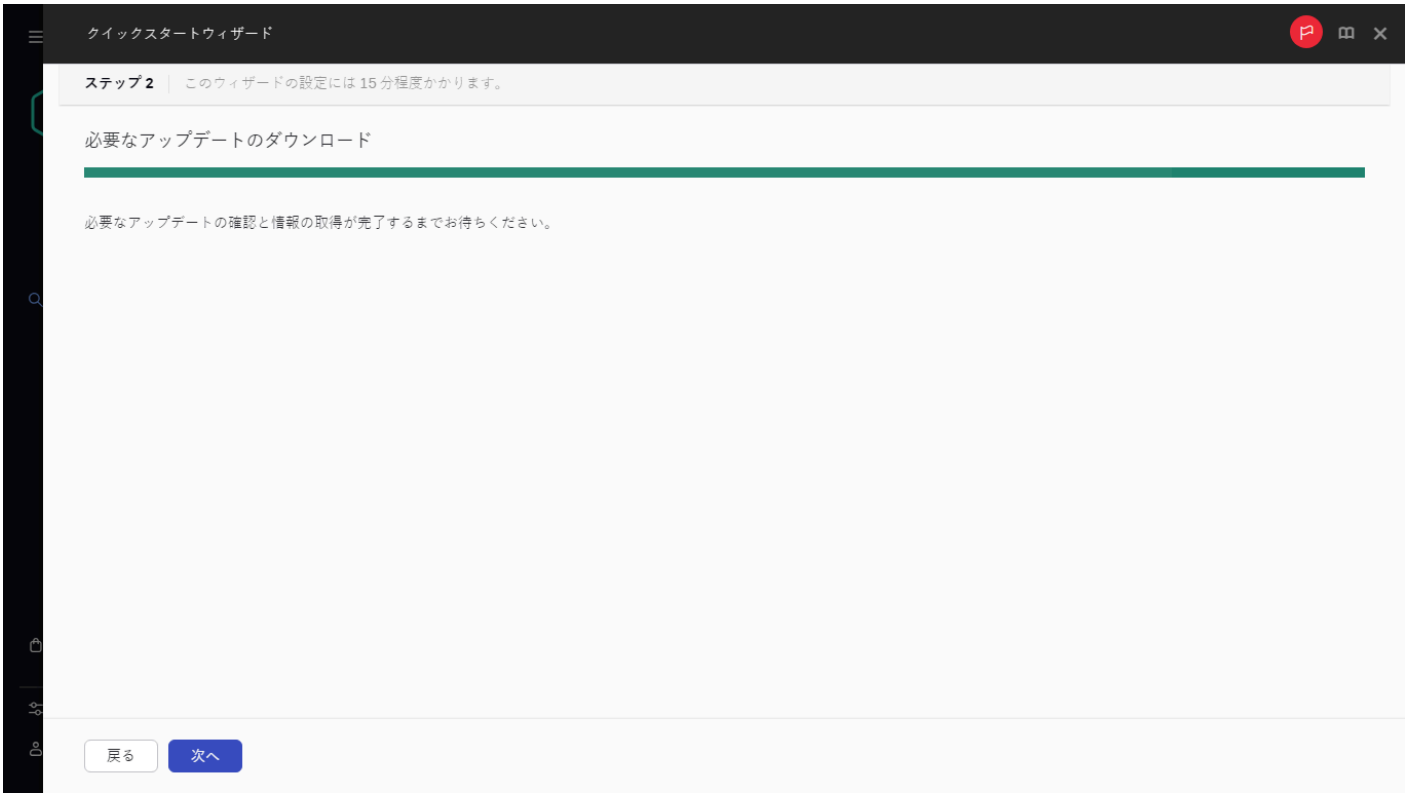
  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（[**プロキシサーバー認証**]をオンにした場合に有効になります）。

  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用せずに、後からインターネットアクセスを設定することもできます。

## ステップ 2：必要なアップデートのダウンロード

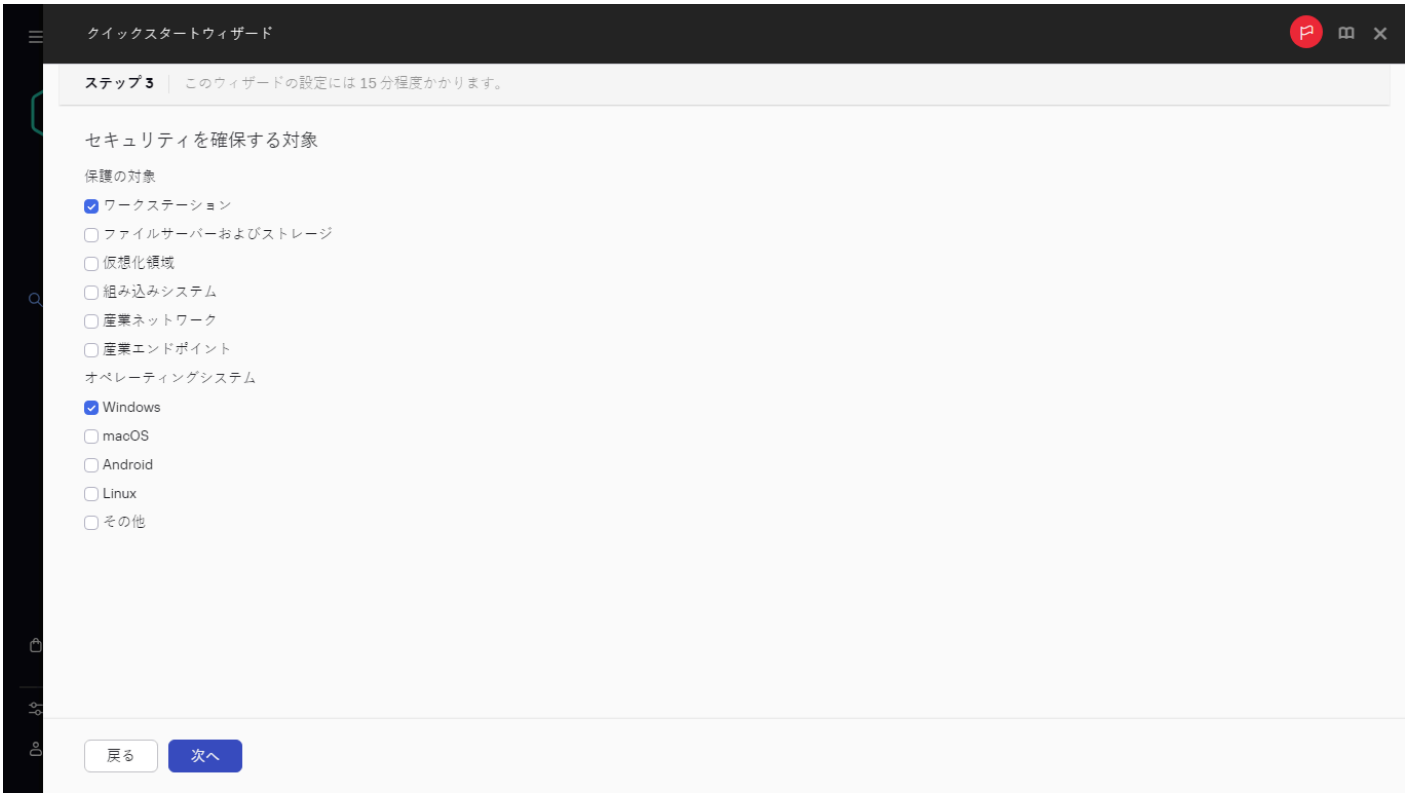
必要なアップデートはカスペルスキーのアップデートサーバーから自動的にダウンロードされます。




必要なアップデートのダウンロード

# ステップ 3：保護する資産の選択

所属組織のネットワークで保護対象範囲とオペレーティングシステムを選択します。これらの項目を選択することによって、ネットワーク内のクライアントデバイスにインストールするためにカスペルスキーのサーバーからダウンロードできる管理プラグインと配布パッケージが絞り込まれます。




保護する資産の選択

オプションを選択します：

- **保護の対象**

  次の保護対象範囲を選択できます：

  - **ワークステーション**
  - **ファイルサーバーおよびストレージ**
  - **仮想化**
  - **組み込みシステム**
  - **産業用ネットワーク**
  - **産業用エンドポイント**

- **オペレーティングシステム**

  次のプラットフォームを選択できます：

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - その他

  サポートされているオペレーティングシステムの詳細は、「Kaspersky Security Center Web コンソールのシステム要件」を参照してください。

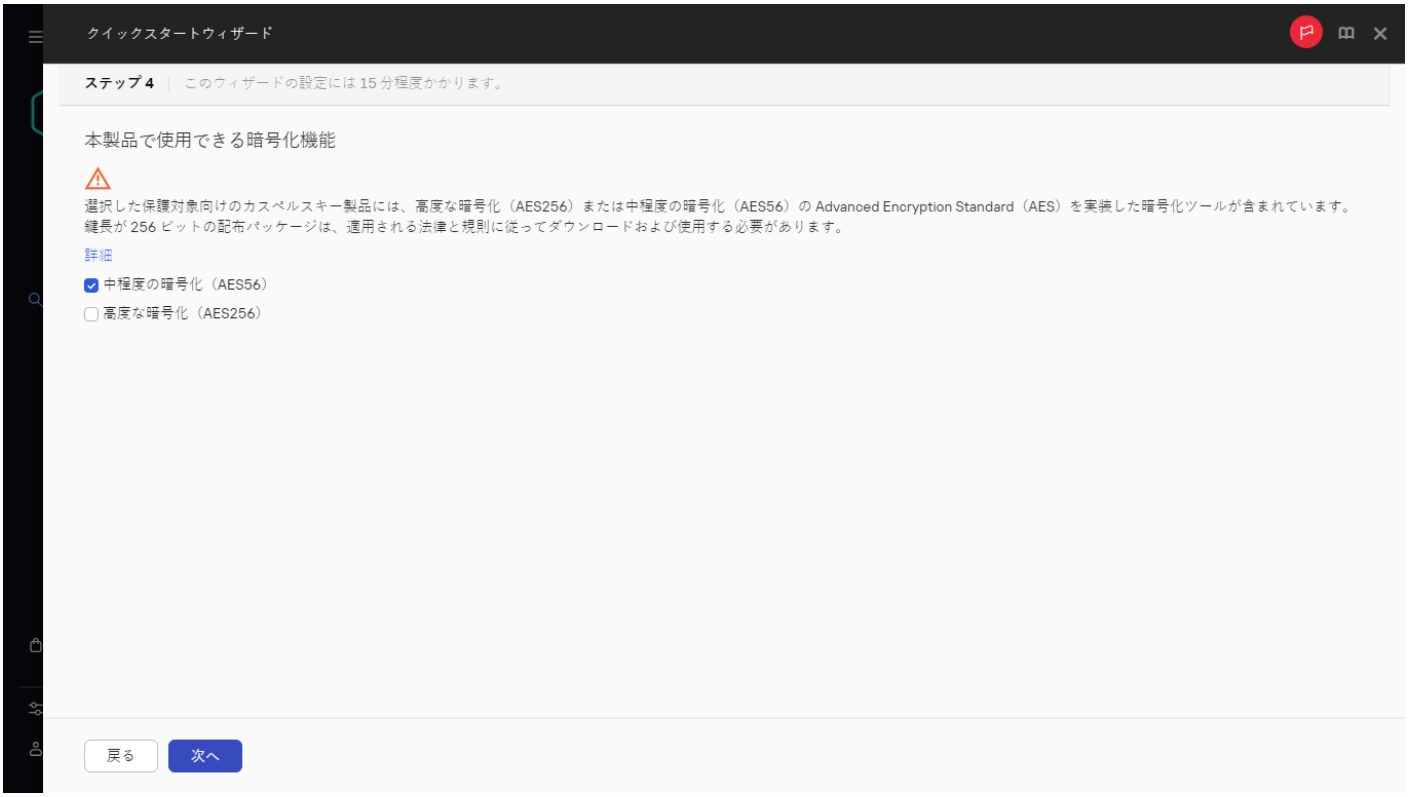
クイックスタートウィザードを使用せずに、後からカスペルスキー製品パッケージを使用可能なパッケージのリストから選択できます。必要なパッケージを検索しやすくするために、さまざまな基準に従って使用可能なパッケージのリストをフィルタリングできます。

# ステップ 4：ソリューションでの暗号化の選択

［**本製品で使用できる暗号化機能**］ウィンドウは、保護範囲として［**ワークステーション**］を選択した場合にのみ表示されます。

Kaspersky Endpoint Security for Windows は、Windows ベースのクライアントデバイスに保存されている情報を暗号化する機能を備えています。これには、256 ビットまたは 56 ビットの鍵長を実装した Advanced Encryption Standard（AES）を備えた暗号化ツールが含まれます。

256 ビットの鍵長を持つ配布パッケージのダウンロードと使用は、適用法令および規制に従って実行する必要があります。組織のニーズに合致した Kaspersky Endpoint Security for Windows の配布パッケージをダウンロードするには、組織内のクライアントデバイスの所在地における法令などを確認してください。




ソリューションでの暗号化の選択

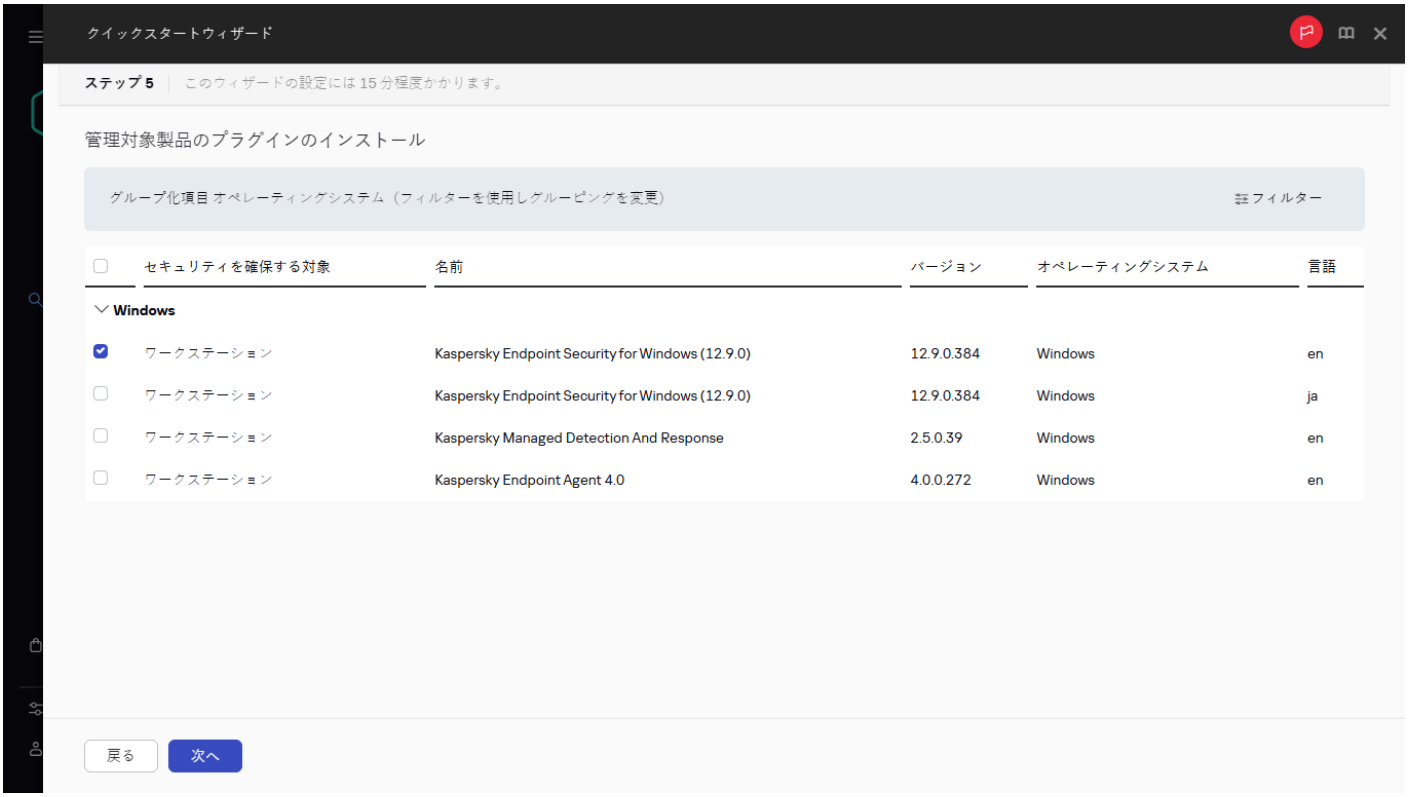
［**本製品で使用できる暗号化機能**］ウィンドウで、次のいずれかの暗号化種別を選択します：

- 中程度の暗号化。この暗号化種別では、56 ビットの鍵長が使用されます。
- 高度な暗号化。この暗号化種別では、256 ビットの鍵長が使用されます。

Kaspersky Endpoint Security for Windows の配布パッケージは、後でクイックスタートウィザードとは別に、必要な暗号化タイプで選択できます。

# ステップ 5：管理対象製品のプラグインのインストールの設定

インストールする管理対象製品のプラグインを選択します。カスペルスキーのサーバーから利用できるプラグインのリストが表示されます。リストは、ウィザードの前のステップで選択されたオプションに従ってフィルタリングされます。既定では、このリストではプラグインのすべての言語バージョンが表示されます。特定の言語バージョンのみを対象にプラグインを表示するには、フィルターを使用します。




管理対象製品のプラグインのインストール

プラグインのリストには次の列が含まれます：

- **セキュリティを確保する対象**

  保護するために選択された領域がこの列に表示されます。

- **種別**

  プラグインの種類がこの列に表示されます。

- **名前**

  前のステップで選択した保護領域とプラットフォームに応じて、対応するプラグインが選択されています。

- **バージョン**

  リストには、カスペルスキーのサーバーから利用できるすべてのバージョンのプラグインが含まれています。既定では、最新バージョンのプラグインが選択されています。

- **最新バージョン**

  この列は、プラグインのバージョンが最新かどうかを示します。**true** 値が表示されている場合、対応するプラグインは最新バージョンです。**false** 値が表示された場合、対応するプラグインのバージョンが新しいことを示しています。

- **オペレーティングシステム**

  この列には、プラグインのオペレーティングシステムが表示されます。

- **言語**

  既定では、インストール時に選択した Kaspersky Security Center Linux の言語に応じてプラグインのローカリゼーション言語も選択されます。［**管理コンソールの言語または次の言語で表示**］ドロップダウンリストで、その他の言語を指定することもできます。

プラグインを選択したら、［**次へ**］をクリックしてインストールを開始します。

クイックスタートウィザードとは別に、カスペルスキー製品の管理プラグインを手動でインストールできます。

クイックスタートウィザードは、選択したプラグインを自動的にインストールします。一部のプラグインのインストールでは使用許諾契約書に同意する必要があります。使用許諾契約書の内容を確認し、同意する場合は［**Kaspersky Security Network への参加に同意する**］をオンにして［**インストール**］をクリックします。使用許諾契約書の条項に同意しない場合、プラグインはインストールされません。

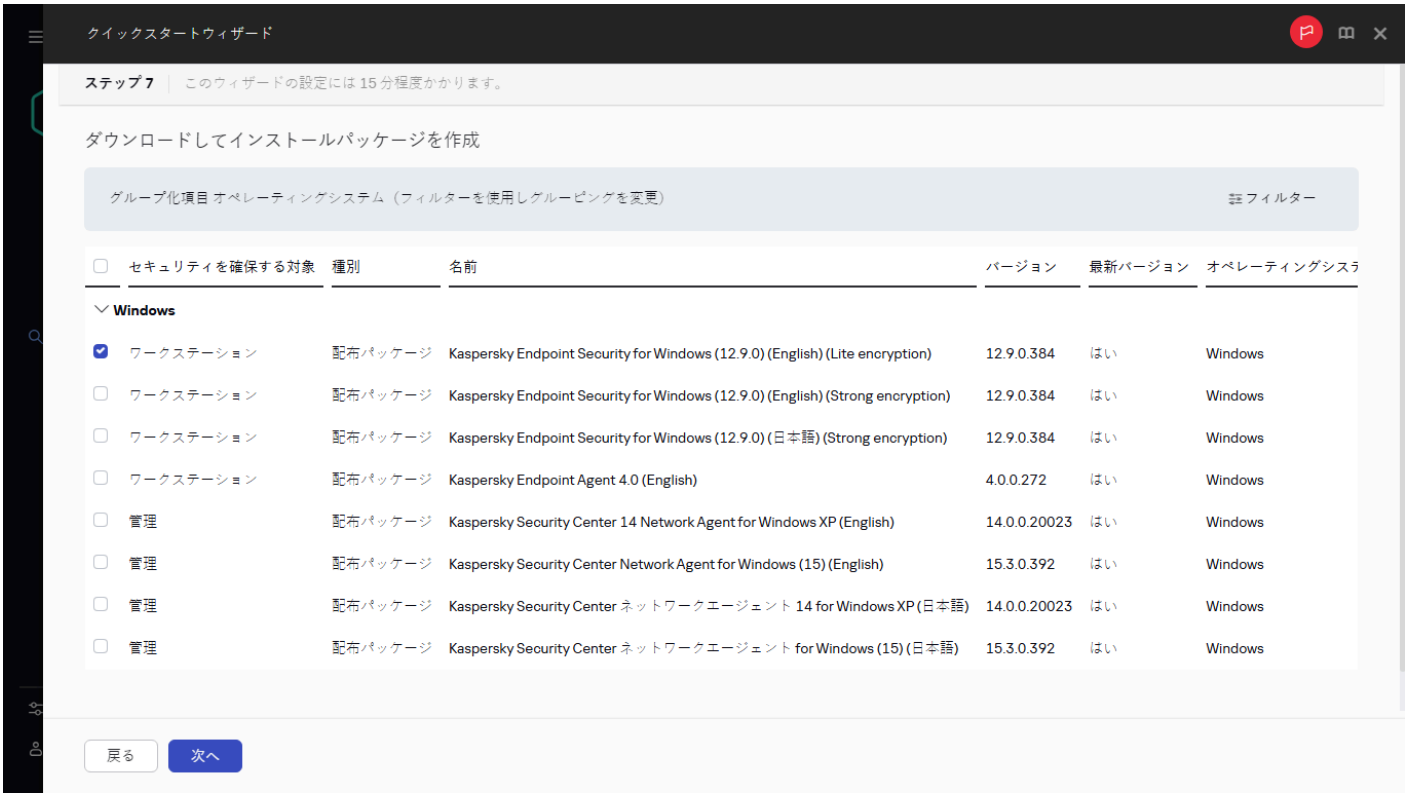
選択したすべてのプラグインがインストールされると、クイックスタートウィザードが自動的に次のステップに進みます。

# ステップ 6：配布パッケージのダウンロードとインストールパッケージの作成

ダウンロードする配布パッケージを選択します。

管理対象製品の配布パッケージには、Kaspersky Security Center Linux の特定の最小バージョンをインストールする必要がある場合があります。

Kaspersky Endpoint Security for Windows の暗号化種別を選択すると、両方の暗号化種別のバージョンの配布パッケージのリストが表示されます。選択した暗号化種別の配布パッケージがリストで選択されています。任意の暗号化種別の配布パッケージを選択できます。配布パッケージの言語には、Kaspersky Security Center Linux の言語に対応するものが選択されます。Kaspersky Security Center Linux の言語のアプリケーション配布パッケージが存在しない場合は、英語の配布パッケージが選択されます。




配布パッケージのダウンロードとインストールパッケージの作成

一部の配布パッケージのダウンロードを完了させるには、使用許諾契約書に同意する必要があります。[**同意する**]をクリックすると、使用許諾契約書の条項が表示されます。ウィザードの次のステップに進むには、使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項に同意する必要があります。パッケージのダウンロードに必要な条項に同意しない場合、パッケージのダウンロードはキャンセルされます。

使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項への同意が完了すると、配布パッケージのダウンロードが引き続き実行されます。インストールパッケージを使用して、後でカスペルスキー製品をクライアントデバイスに導入できます。

# ステップ 7：Kaspersky Security Network の設定

Kaspersky Security Center Linux の動作に関する情報を Kaspersky Security Network ナレッジベースに転送する設定を指定します。




Kaspersky Security Network の設定

次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center Linux とクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center Linux と管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

クイック スタート ウィザードとは別に、後で Kaspersky Security Network（KSN）へのアクセスを設定できます。

# ステップ 8：アプリケーションのアクティベート方法の選択

Kaspersky Security Center Linux のアクティベーションオプションのいずれかを選択します：

- **アクティベーションコードを入力**

  *アクティベーションコード*は、英数字 20 文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center Linux をアクティベートするライセンス情報を追加することができます。アクティベーションコードは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

  アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。

  このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動的に配信する**］を有効にできます。

  このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

  このオプションをオフにすると、メインメニューの［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］で、後で管理対象デバイスにライセンスを適用できます。

- **ライセンス情報ファイルを指定**

  *ライセンス情報ファイル*は、拡張子「key」のファイルであり、カスペルスキーから提供されます。ライセンス情報ファイルを製品に追加し、製品をアクティベートする目的で作成されています。

  ライセンス情報ファイルは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

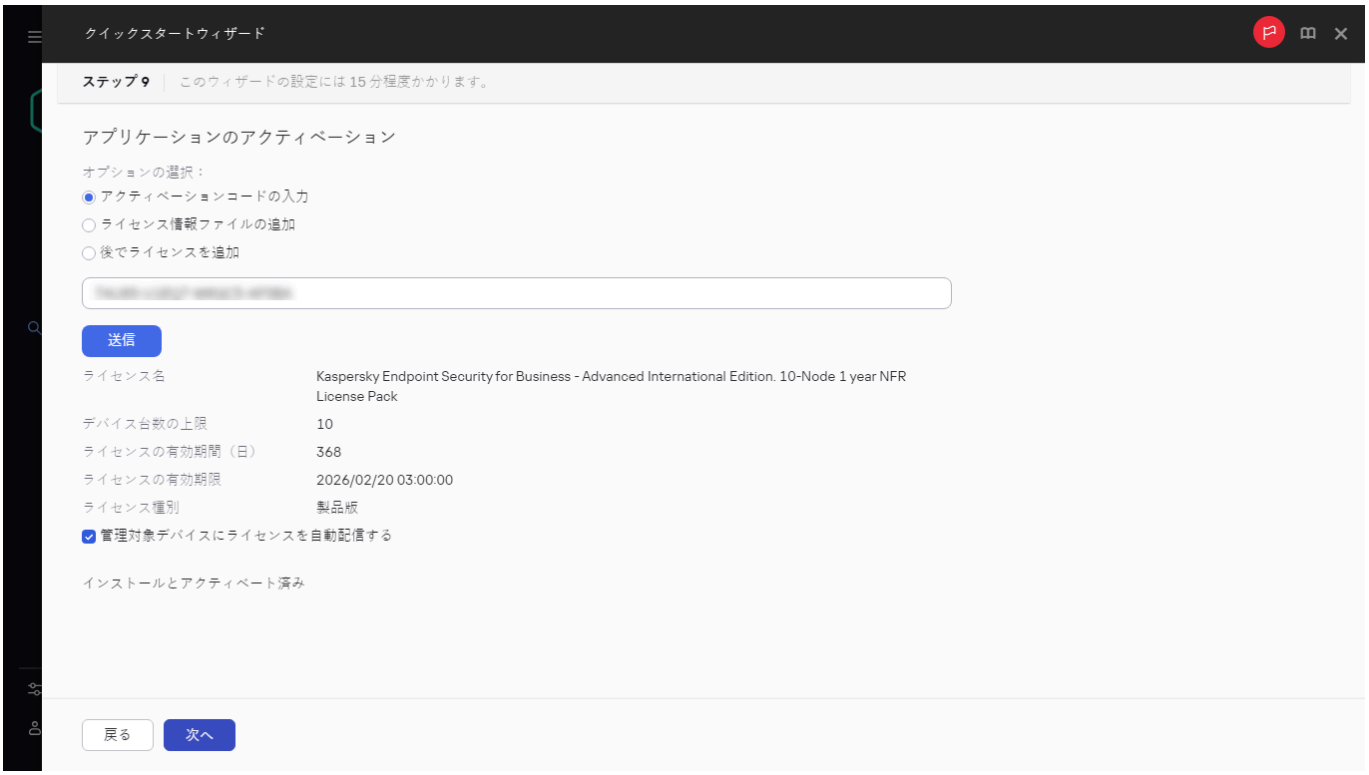
  ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

  このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動的に配信する**］を有効にできます。

  このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

  このオプションをオフにすると、メインメニューの［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］で、後で管理対象デバイスにライセンスを適用できます。

- アプリケーションのアクティベーションを後で実行




アプリケーションのアクティベート方法の選択

アプリケーションのアクティベーションを延期する場合は、メニューの［**操作**］→［**ライセンス管理**］を選択して後でいつでもライセンスを追加できます。

有料 AMI または月単位の従量課金の SKU から導入した Kaspersky Security Center で作業を行う場合は、ライセンス情報ファイルを指定したりアクティベーションコードを入力することはできません。

# ステップ 9：ステップ 9：サードパーティ製品のアップデート管理設定の指定

脆弱性とパッチ管理が使用可能なライセンスをお持ちでなく、*脆弱性とアプリケーションのアップデートの検索*タスクが既に存在している場合、クイックスタートウィザードの**アップデート管理設定**ステップは表示されません。




サードパーティ製品のアップデート管理設定

サードパーティ製ソフトウェアのアップデートの場合は、次のいずれかのオプションを選択します：

- **必要なアップデートの検索**

  *脆弱性とアプリケーションのアップデートの検索*タスクがない場合は、自動的に作成されます。

  既定ではこのオプションが選択されます。

- **必要なアップデートの検索とインストール**

  ［*脆弱性とアプリケーションのアップデートの検索*］タスクと［*アップデートのインストールと脆弱性の修正*］タスクがまだ作成されていない場合は、自動的に作成されます。

  この機能は、脆弱性とパッチ管理が使用可能なライセンスでのみ使用できます。

Windows Update の更新の場合は、［**ドメインポリシーで定義されたアップデート元を使用する**］を選択します。

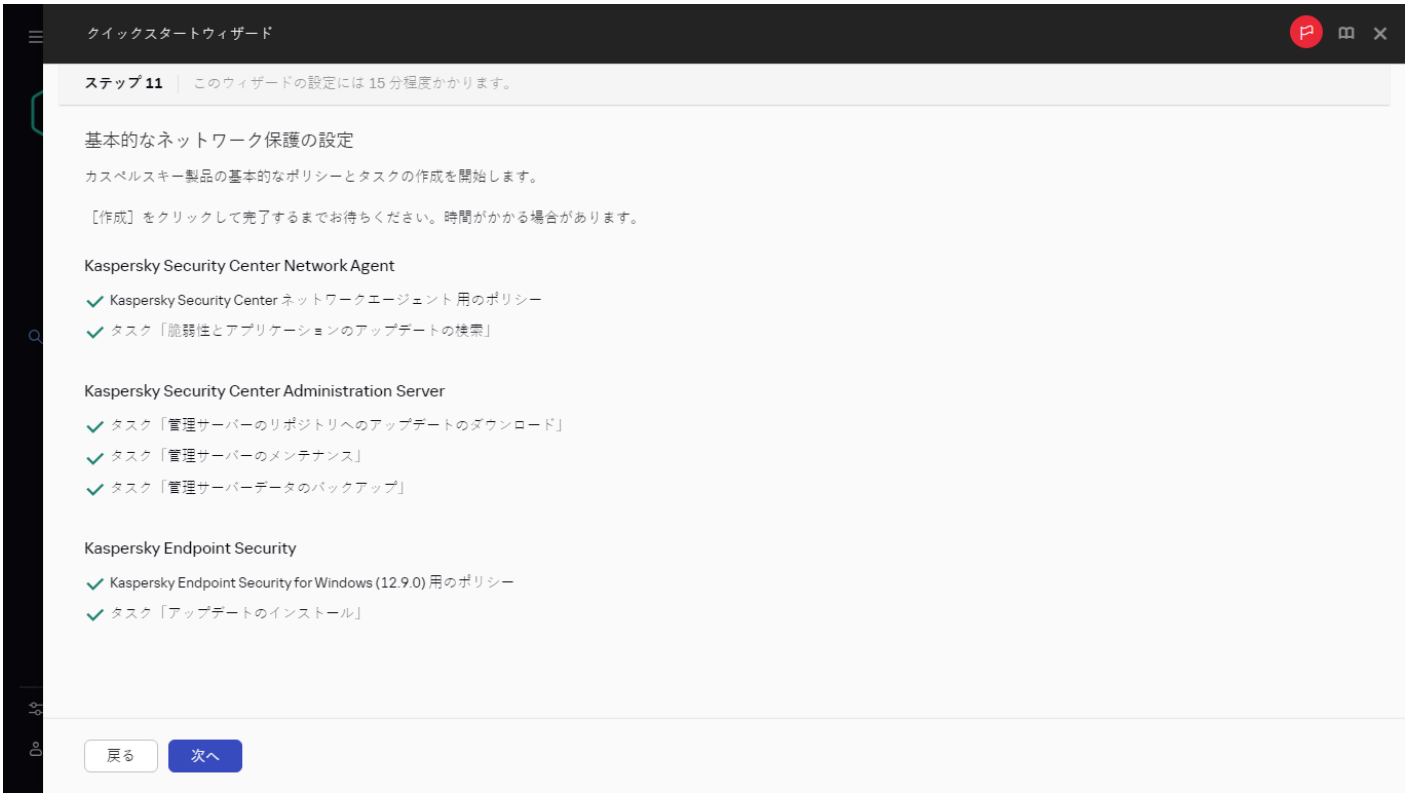
クライアントデバイスは、ドメインポリシー設定に従って Windows Update 更新プログラムをダウンロードします。ネットワークエージェントポリシーがまだ作成されていない場合は、自動的に作成されます。

クイックスタートウィザードとは別に、*脆弱性とアプリケーションのアップデートの検索*および*アップデートのインストールと脆弱性の修正*タスクを作成できます。

# ステップ 10：基本的なネットワーク保護の設定情報の作成

作成されたポリシーとタスクのリストを確認できます。

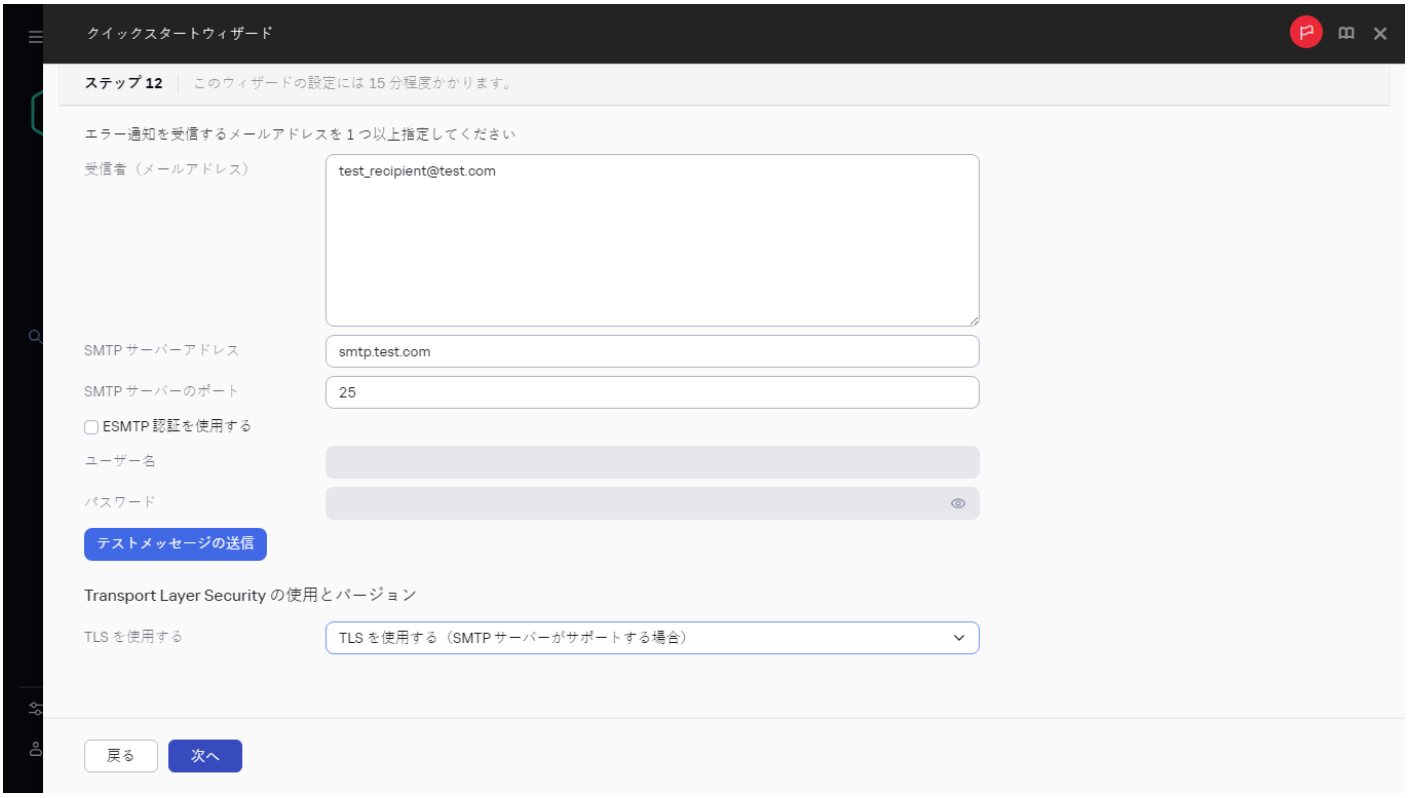
ポリシーとタスクの作成が完了してから、ウィザードの次のステップに進んでください。




基本的なネットワーク保護の設定情報の作成

# ステップ 11：メール通知の設定

クライアントデバイス上のカスペルスキー製品の実行中に登録されたイベントに関する通知の配信方法を設定します。この設定は、アプリケーションポリシーの既定の設定として使用されます。




メール通知の設定

カスペルスキー製品で発生したイベントに関する通知の配信を設定するには、次の設定を使用します：

- **受信者（メールアドレス）**

  通知が送られるユーザーのメールアドレスです。1つ以上のアドレスを入力できます。複数のアドレスを入力する場合はセミコロンで区切ってください。

- **SMTP サーバーアドレス**

  組織のメールサーバーのアドレスです。

  複数のアドレスを入力する場合はセミコロンで区切ってください。次の値を使用できます：

  - IPv4 / IPv6 アドレス
  - SMTP サーバーの DNS 名

- **SMTP サーバーのポート**

  SMTP サーバーの通信ポート番号。複数の SMTP サーバーを使用する場合、それらサーバーへの接続は指定された通信ポートを介して確立されます。既定のポート番号は 25 です。

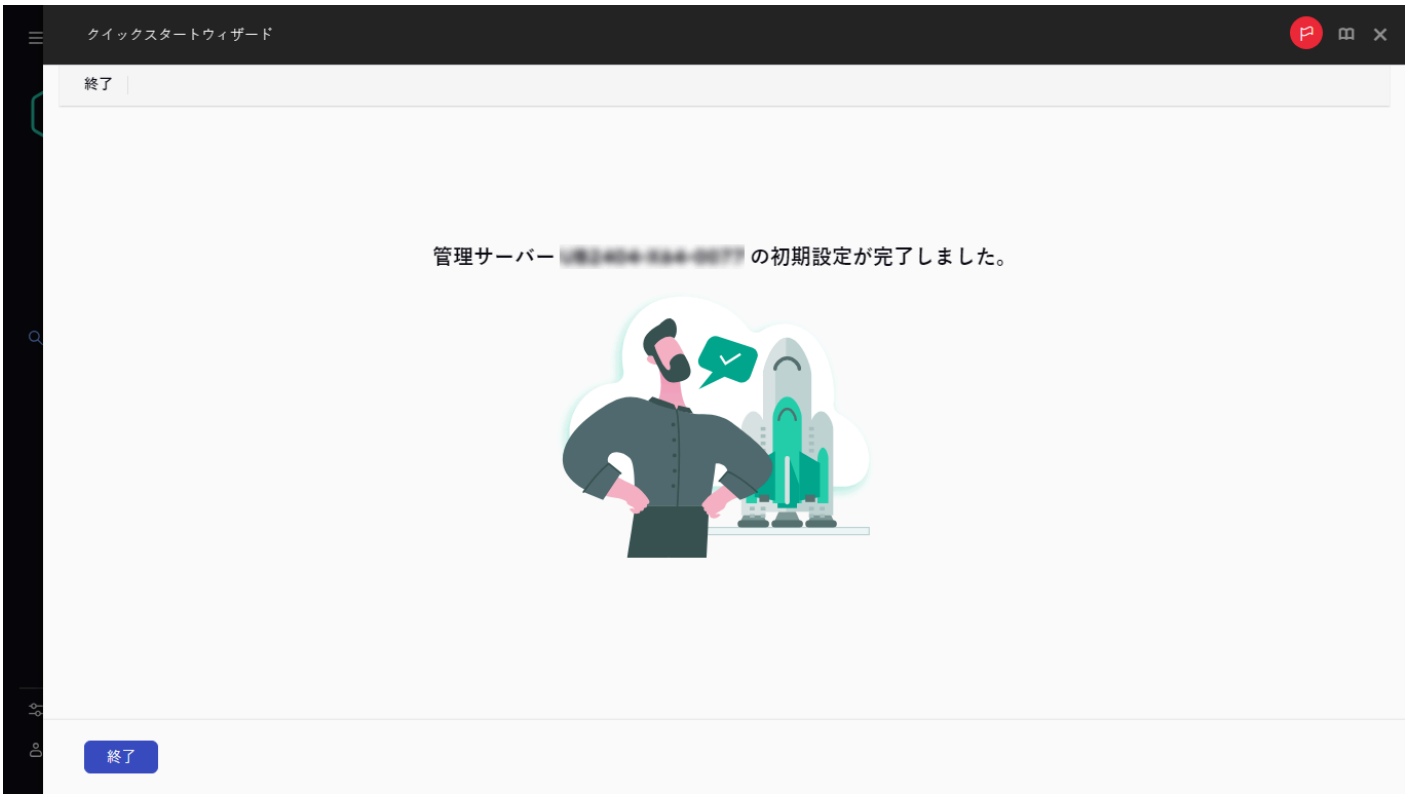
- **ESMTP 認証を使用する**

  ESMTP 認証のサポートを有効にします。チェックボックスをオンにすると、［**ユーザー名**］と［**パスワード**］で ESMTP 認証を設定できます。既定では、このチェックボックスはオフです。

［**テストメッセージの送信**］をクリックして、新しいメール通知設定をテストできます。

## ステップ 12：クイックスタートウィザードの終了

ウィザードを終了するには、［**終了**］をクリックします。




クイックスタートウィザードの最終手順

クイックスタートウィザードを終了したら、製品導入ウィザードを実行して、アンチウイルス製品またはネットワークエージェントをネットワーク上のデバイスに自動的にインストールできます。

# 製品導入ウィザード

カスペルスキー製品をインストールするには、製品導入ウィザードを使用できます。製品導入ウィザードにより、専用に作成されたインストールパッケージを使用するか、または配布パッケージから直接、アプリケーションをリモートインストールすることができます。

製品導入ウィザードにより、次の操作が実行できます：

- アプリケーションをインストールするためのインストールパッケージをダウンロードします（まだ作成されていない場合）。［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動すると、インストールパッケージにアクセスできます。今後アプリケーションをインストールする時に、このインストールパッケージを使用できます。

- 特定のデバイスまたは管理グループに対するリモートインストールタスクを作成して実行します。新しく作成されたリモートインストールタスクは、［**タスク**］セクションに保存されます。このタスクは後から手動で開始できます。タスクの種別は［**アプリケーションのリモートインストール**］になります。

SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

# ステップ 1：製品導入ウィザードの開始

また、製品導入ウィザードはいつでも手動で起動できます。

*製品導入ウィザードを手動で起動するには：*

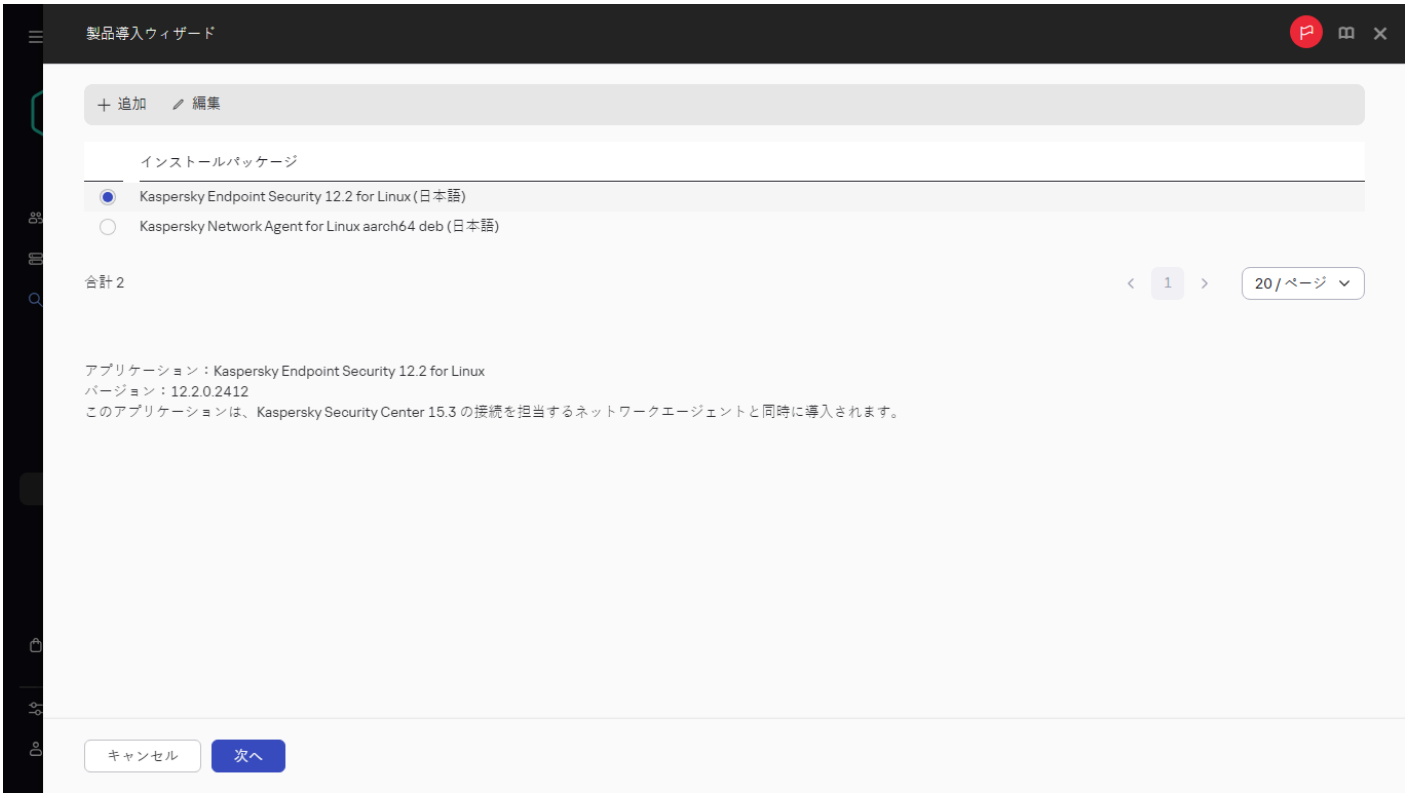
メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**製品導入ウィザード**］の順に移動します。

製品導入ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

# ステップ 2：インストールパッケージの選択

インストールする製品のインストールパッケージを選択します。

目的の製品のインストールパッケージがリストに含まれていない場合、［**追加**］をクリックしてリストから製品を選択します。




インストールパッケージの選択

# ステップ 3：ライセンス情報ファイルまたはアクティベーションコードの配信方法の選択

ライセンス情報ファイルまたはアクティベーションコードの配信方法を選択します：

- **インストールパッケージにライセンスを含めない**

  次の条件を満たす場合、ライセンスは互換性のあるすべてのデバイスへ自動的に配信されます：
  - ライセンスのプロパティで［自動配信］が有効になっている場合。
  - ［**ライセンスの追加**］タスクが作成されている場合。

- **インストールパッケージにライセンスを含める**

  ライセンスはインストールパッケージと共にデバイスへ配信されます。

  共有読み取りアクセス権がインストールパッケージのリポジトリに対して有効になっているため、この方法はできるだけ使用しないでください。

インストールパッケージに既にライセンス情報ファイルまたはアクティベーションコードが含まれる場合も、同様のウィンドウが表示されますが、ライセンスの情報のみが表示されます。

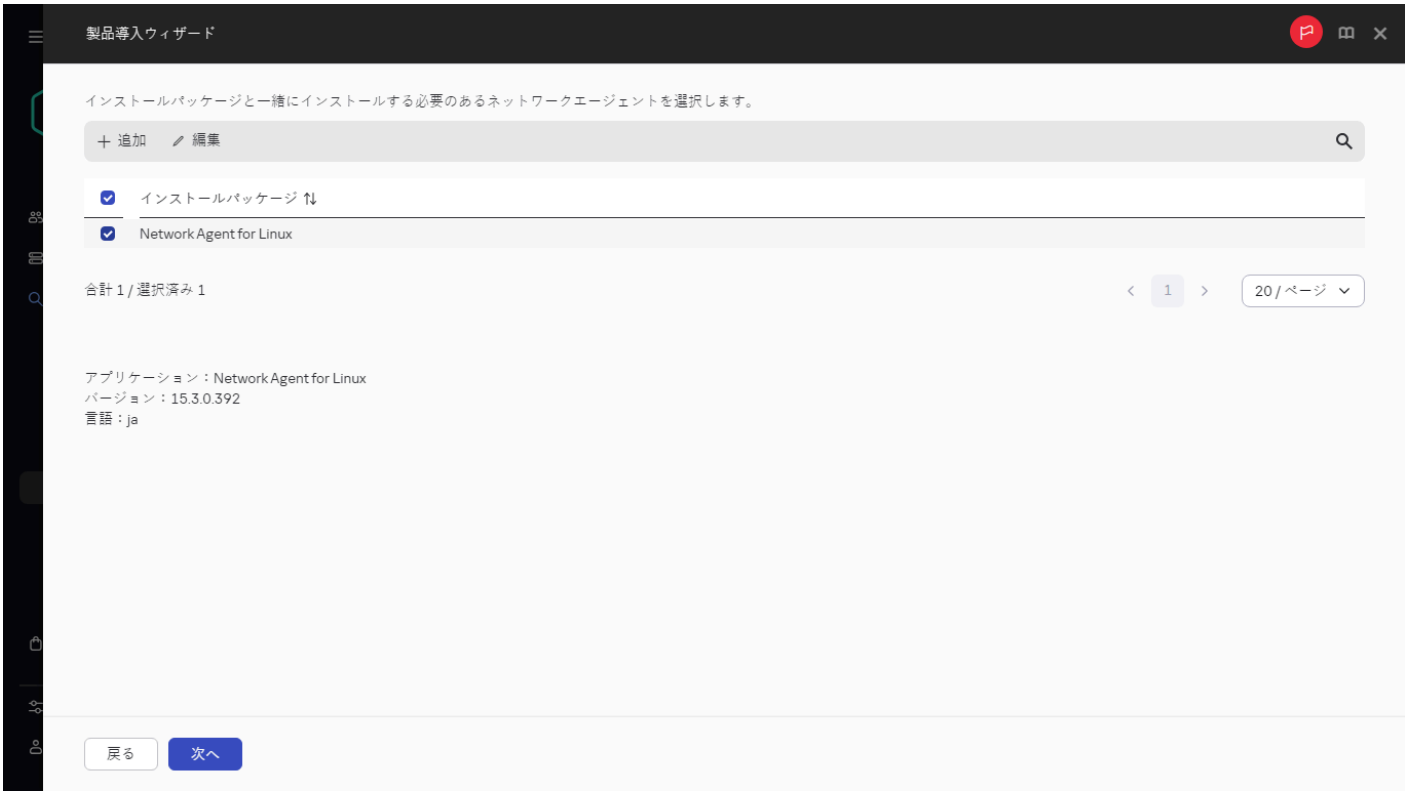



ライセンス情報ファイルまたはアクティベーションコードの配布方法の選択

# ステップ 4：ネットワークエージェントのバージョンの選択

ネットワークエージェント以外の製品のインストールパッケージを選択した場合でも、各製品と Kaspersky Security Center 管理サーバーとを接続するために、ネットワークエージェントのインストールが必要になります。

最新バージョンのネットワークエージェントを選択してください。




ネットワークエージェントのバージョンの選択

# ステップ 5：デバイスの選択

アプリケーションをインストールするデバイスを指定します。

- **管理対象デバイスにインストール**

  このオプションをオンにすると、デバイスのグループに対してリモートインストールタスクが作成されます。

- **インストールするデバイスの選択**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。




アプリケーションをインストールするデバイスのリストの指定

# ステップ 6：リモートインストールタスクの設定

［**リモートインストールタスク設定**］ウィンドウで、アプリケーションのリモートインストール設定を指定します。

［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

- **ネットワークエージェントを使用する**

  このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

  このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

  既定では、このオプションはオンです。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

  ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

  既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

  Network Agent がインストールされていないデバイスに Windows 用のアプリケーション（Windows 用ネットワークエージェントを含む）をインストールするには、Windows ベースのディストリビューションポイントを使用するのが唯一の方法です。したがって、Windows アプリケーションをインストールする場合：

  - このオプションをオンにします。
  - ターゲットのクライアントデバイスにディストリビューションポイントが割り当てられていることを確認します。
  - ディストリビューションポイントが Windows ベースであることを確認します。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションをオンにすると、管理サーバーを通じてクライアントデバイスのオペレーティングシステムツールを使用してクライアントデバイスにファイルが送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

  既定では、このオプションはオンです。

詳細設定を行います：

- **アプリケーションが既にインストールされている場合は再インストールしない**

  このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

  このオプションをオフにすると、アプリケーションは常にインストールされます。

  既定では、このオプションはオンです。

- **Active Directory のグループポリシーにパッケージのインストールを割り当てる**

  このオプションをオンにすると、Active Directory のグループポリシーを使用してインストールパッケージがインストールされます。

  このオプションは、ネットワークエージェントのインストールパッケージが選択されている場合に使用可能になります。

  既定では、このオプションはオフです。




リモートインストールタスクの設定

# ステップ 7：再起動の設定

アプリケーションの使用中、インストール中、アンインストール中にオペレーティングシステムの再起動が必要になった場合に行う動作を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは1回だけ表示されます。

  - **再起動するまでの時間（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。




オペレーティングシステムの再起動のオプションの選択

# ステップ 8：インストール前に競合アプリケーションを削除する

この手順の実施ウィンドウは、インストール対象の製品に既知の競合アプリケーションが存在する場合にのみ表示されます。

インストール対象の製品と互換性がないアプリケーションを自動的に削除するには、オプションをオンにします。

互換性がない競合アプリケーションのリストも表示されます。

このオプションをオフにした場合、インストール対象の製品は、競合アプリケーションがインストールされていないデバイスにのみインストールされます。

# ステップ 9：管理対象デバイスへのデバイスの移動

ネットワークエージェントのインストール後に、デバイスを管理グループに移動するかどうかを指定します。

- **デバイスを移動しない**

  デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

- **未割り当てデバイスをグループへ移動**

  指定した管理グループにデバイスが移動されます。

既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。




デバイスを管理グループに移動するオプションの選択

# ステップ 10：デバイスにアクセスするアカウントの選択

必要に応じて、リモートインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントまたは SSH 証明書を指定して、アプリケーションをインストールできます。

  - **ローカルアカウント**。このオプションをオンにする場合、アプリケーションのインストーラーを実行するユーザーアカウントを指定します。[**追加**] をクリックし、[**ローカルアカウント**] を選択してから、ユーザーアカウントの資格情報を指定します。

    タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

  - **SSH 証明書**。Linux ベースのクライアントデバイスにアプリケーションをインストールする場合、ユーザーアカウントの代わりに SSH 証明書を指定できます。[**追加**] をクリックし、[**SSH 証明書**] を選択してから、証明書の秘密鍵と公開鍵を指定します。

    秘密鍵を生成するには、ssh-keygen ユーティリティを使用できます。Kaspersky Security Center Linux は PEM 形式の秘密鍵をサポートしますが、ssh-keygen ユーティリティは既定で SSH 鍵を OPENSSH 形式で生成します。OPENSSH 形式は Kaspersky Security Center Linux ではサポートされていません。サポートされる PEM 形式で秘密鍵を作成するには、ssh-keygen コマンドに -m PEM オプションを追加します。例：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<ユーザーのメールアドレス>"
    ```




デバイスにアクセスするアカウントの選択

# ステップ 11：インストールの開始

このページが、このウィザードの最後のステップです。このステップを完了すると、**リモートインストールタスク**の作成と設定が完了します。

既定では、［**ウィザードの終了後にタスクを実行**］はオフになっています。このオプションをオンにすると、ウィザードの完了後すぐに**リモートインストールタスク**が開始されます。このオプションをオフにすると、**リモートインストールタスク**は開始されません。このタスクは後から手動で開始できます。

製品導入ウィザードを完了するには、［**OK**］をクリックします。

# Kaspersky Security Center Linux のアップグレード

管理サーバーのバージョン 15.3 をそれより前のバージョンの管理サーバー（バージョン 13 以降）がインストールされたデバイスにインストールすることができます。バージョン 15.3 にアップグレードすると、以前のバージョンの管理サーバーのデータと設定がすべて維持されます。

Kaspersky Security Center Linux をアップグレードする前に、管理サーバーのバージョン 15.3 でサポートされているオペレーティングシステムと DBMS のバージョンを使用していることを確認してください。必要に応じて、新しいバージョンのオペレーティング システムおよび DBMS を搭載した別のデバイスに管理サーバーを移動できます。

次のいずれかの方法を使用して、管理サーバーのバージョンをアップグレードできます：

- Kaspersky Security Center Linux インストールファイルを使用する
- 管理サーバーのデータのバックアップを作成し、管理サーバーの新しいバージョンをインストールして、バックアップから管理サーバーのデータを復元する

アップグレード中、管理サーバーと別のアプリケーションで同時に DBMS を使用することは厳重に禁じられています。

ネットワークに複数の管理サーバーが含まれている場合は、それぞれのサーバーを手動でアップグレードする必要があります。Kaspersky Security Center Linux では集中アップグレードはサポートされません。

また、Kaspersky Security Center Web コンソールを新しいバージョンにアップグレードする必要があります。

管理サーバーをバージョン 15.3 にアップグレードすると、ネットワークエージェントバージョン 15 以前の新しいインストールパッケージを作成できなくなることに注意してください。ただし、以前に作成されたインストールパッケージは利用できます。

Kaspersky Security Center Linux を旧バージョンからアップグレードすると、サポート対象のカスペルスキー製品のインストール済みプラグインはすべて残ります。管理サーバープラグインとネットワークエージェントプラグインは自動的にアップグレードされます。アップグレードを開始する前に、管理サーバーデータのバックアップコピーを作成することを推奨します。

# インストールファイルを使用した Kaspersky Security Center Linux のアップグレード

管理サーバーを旧バージョン（バージョン 13 以降）から新しいバージョン（最新版など）にアップグレードするには、Kaspersky Security Center Linux インストールファイルを使用して、旧バージョンに新しいバージョンを上書きインストールできます。

*インストールファイルを使用して旧バージョンの管理サーバーを新しいバージョンにアップグレードするには：*

1. カスペルスキーの Web サイトから、新しいバージョンの完全なパッケージを含む Kaspersky Security Center Linux インストールファイルをダウンロードします：

   - RPM ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64-<バージョン番号>.x86_64.rpm

   - Debian ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64_<バージョン番号>_amd64.deb

2. 管理サーバーで使用するパッケージマネージャーを使用して、インストールパッケージをアップグレードします。たとえば、ルート権限を持つアカウントで、コマンドラインターミナルを使用して次のコマンドを使用できます：

   - RPM ベースのオペレーティングシステムのデバイスの場合：
     `$ sudo yum install ./ksc64-<バージョン番号>.x86_64.rpm`

   - Debian ベースのオペレーティングシステムのデバイスの場合：
     `$ sudo apt-get install ./ksc64_<バージョン番号>_amd64.deb`

   コマンドが正常に実行されると、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトが作成されます。これに関するメッセージがターミナルに表示されます。

3. ルート権限を持つアカウントで、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトを実行し、アップグレードした管理サーバーを設定します。

4. コマンドラインターミナルに表示される使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーの諸条件すべてに同意する場合：

   a. 「Y」と入力して、EULA の諸条件をすべて読み、理解した上で条項に同意することを確認します。

   b. 「Y」ともう一度入力して、データの取り扱い方法を記載しているプライバシーポリシーをすべて読み、理解した上で条項に同意することを確認します。

   「Y」と 2 回入力すると、製品のデバイスへのインストールが続行されます。

5. 「1」と入力して、管理サーバーの標準インストールモードを選択します。

   下の図は、最後の 2 つの手順を示しています。

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

EULA とプライバシーポリシーの条項に同意し、コマンドラインターミナルで管理サーバーの標準インストールモードを選択する

   次に、スクリプトにより管理サーバーのアップグレードが設定され、終了します。アップグレード中は、アップグレード前に変更した管理サーバーの設定は変更することができません。

6. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

   > Network Agent for Linux を Kaspersky Security Center Linux と同じバージョンにアップグレードすることを推奨します。

   リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

   不要になった依存関係を削除するには、Linux ベースの資産で次のコマンドを実行します：

   - Debian ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - RPM ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `dnf autoremove`
     - `yum autoremove`

# バックアップによる Kaspersky Security Center Linux のアップグレード

管理サーバーを旧バージョン（バージョン 14.2 以降）からバージョン 15.3 にアップグレードする には、管理サーバーデータのバックアップを作成し、新しいバージョンの Kaspersky Security Center Linux をインストールした後でこのデータを復元します。インストール中に問題が発生した場合は、アップグレード操作の前に作成した管理サーバーデータのバックアップを使用して管理サーバーを前のバージョンに戻すことが可能です。

*バックアップを使用して旧バージョンの管理サーバーをバージョン 15.3 にアップグレードするには：*

1. アップグレードする前に、旧バージョンのアプリケーションで管理サーバーデータをバックアップします。
2. 旧バージョンの Kaspersky Security Center Linux をアンインストールします。
3. 以前の管理サーバーに Kaspersky Security Center Linux バージョン 15.3 をインストールします。
4. アップグレード前に作成したバックアップから管理サーバーデータを復元します。
5. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

   Network Agent for Linux を Kaspersky Security Center Linux と同じバージョンにアップグレードすることを推奨します。

   リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

   不要になった依存関係を削除するには、Linux ベースの資産で次のコマンドを実行します：

   - Debian ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - RPM ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `dnf autoremove`
     - `yum autoremove`

# Kaspersky Security Center Linux のフェールオーバークラスタノードの Kaspersky Security Center Linux のアップグレード

旧バージョン（バージョン 14 以降）の管理サーバーがインストールされているすべての Kaspersky Security Center Linux のフェールオーバークラスターノードに、管理サーバーバージョン 15.3 をインストールできます。バージョン 15.3 にアップグレードすると、以前のバージョンの管理サーバーのデータと設定がすべて維持されます。

以前にデバイスに Kaspersky Security Center Linux をローカルにインストールした場合は、インストールファイルまたはバックアップを使用して、これらのデバイスの Kaspersky Security Center Linux をアップグレードすることもできます。

*Kaspersky Security Center Linux のフェールオーバークラスタノードの Kaspersky Security Center Linux をアップグレードするには：*

1. カスペルスキーの Web サイトから、バージョン 15.3 の完全なパッケージを含む Kaspersky Security Center Linux インストールファイルをダウンロードします：

   - RPM ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64-<バージョン番号>-<ビルド番号>.x86_64.rpm
   - Debian ベースのオペレーティングシステムを実行しているデバイスの場合 — ksc64_<バージョン番号>-<ビルド番号>_amd64.deb

2. クラスタを停止します。

3. クラスタの共有フォルダーをアンマウントし、［Kaspersky Security Center Linux フェールオーバークラスタ用のファイルサーバーの準備］セクションで指定されたオプションを使用してマウントします。

4. ［Kaspersky Security Center Linux フェールオーバークラスタ用のノードの準備］セクションの説明に従って、クラスタノード上のマウントポイントと共有フォルダーを再照合します。

5. クラスタのアクティブノードで、管理サーバーで使用するパッケージマネージャーを使用して、インストールパッケージをアップグレードします。

   たとえば、ルート権限を持つアカウントで、コマンドラインターミナルを使用して次のコマンドを使用できます：

   - RPM ベースのオペレーティングシステムのデバイスの場合：
     ```
     $ sudo yum install ./ksc64-<バージョン番号>-<ビルド番号>.x86_64.rpm
     ```
   - Debian ベースのオペレーティングシステムのデバイスの場合：
     ```
     $ sudo apt-get install ./ksc64_<バージョン番号>-<ビルド番号>_amd64.deb
     ```

   コマンドが正常に実行されると、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトが作成されます。これに関するメッセージがターミナルに表示されます。

6. ルート権限を持つアカウントで、/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl スクリプトを実行し、アップグレードした管理サーバーを設定します。

7. コマンドラインターミナルに表示される使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーの諸条件すべてに同意する場合：

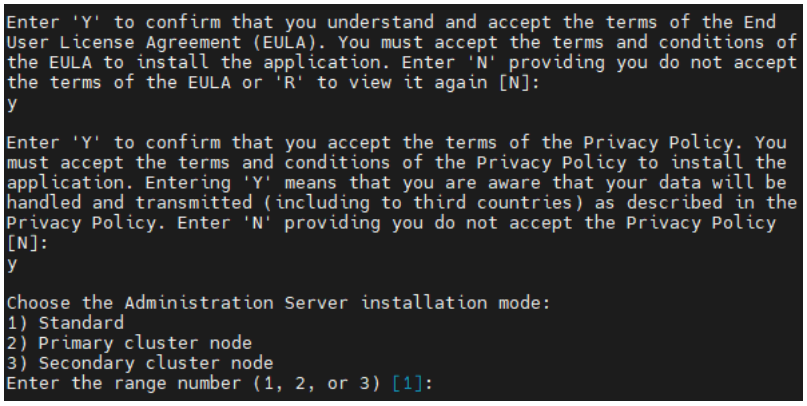
   a. 「Y」と入力して、EULA の諸条件をすべて読み、理解した上で条項に同意することを確認します。

   b. 「Y」ともう一度入力して、データの取り扱い方法を記載しているプライバシーポリシーをすべて読み、理解した上で条項に同意することを確認します。

   「Y」と 2 回入力すると、製品のデバイスへのインストールが続行されます。

8. 「2」を入力して、アップグレードするノードを選択します。

   下の図は、最後の 2 つの手順を示しています。




EULA とプライバシーポリシーの条項に同意し、コマンドラインターミナルでインストールモードを選択する

   次に、スクリプトにより管理サーバーのアップグレードが設定され、終了します。アップグレード中は、アップグレード前に変更した管理サーバーの設定は変更することができません。

9. パッシブノードで手順 3 ～ 5 を実行します。

   ステップ 6 で、「3」を入力してノードを選択します。

10. クラスタを開始します。

> クラスタは任意のノードで開始できることに注意してください。パッシブノードでクラスタを起動すると、それがアクティブノードになります。

11. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

> Network Agent for Linux を Kaspersky Security Center Linux と同じバージョンにアップグレードすることを推奨します。

   リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

   不要になった依存関係を削除するには、Linux ベースの資産で次のコマンドを実行します：

   - Debian ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - RPM ベースの資産の場合は、次のいずれかのコマンドを実行します：
     - `dnf autoremove`
     - `yum autoremove`

   この結果、Kaspersky Security Center Linux のフェールオーバークラスタのノードに最新版の管理サーバーがインストールされました。

# Kaspersky Security Center Web コンソールのアップグレード

この記事では、Linux オペレーティングシステムを使用しているデバイスで Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）をアップグレードする方法について説明しています。

Kaspersky Security Center Web コンソールを Astra Linux に閉鎖ソフトウェア環境モードでアップグレードする必要がある場合は、Astra Linux に固有の手順に従ってください。

デバイスにインストールされている Linux ディストリビューションに応じて、次のインストールファイルのいずれかを使用します：

- Debian の場合：ksc-web-console-<ビルド番号>.x86_64.deb
- RPM ベースのオペレーティングシステムの場合：ksc-web-console-<ビルド番号>.x86_64.rpm
- ALT 8 SP の場合：ksc-web-console-<ビルド番号>-alt8p.x86_64.rpm

インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

*Kaspersky Security Center Web コンソールをアップグレードするには：*

1. Kaspersky Security Center Web コンソールをアップグレードするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. 使用許諾契約書（EULA）をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイトからファイルをダウンロードできます。使用許諾契約書の条項に同意しない場合は、インストールファイルを使用して Kaspersky Security Center Web コンソールをアップグレードしないでください。

3. Kaspersky Security Center Web コンソールをインストールする前に準備したものと同じ応答ファイルを使用します。応答ファイル名は ksc-web-console-setup.json で、ファイルの場所は /etc/ksc-web-console-setup.json です。

> Kaspersky Security Center Web コンソールのインストール時に、 webConsoleAccount、managementServiceAccount、serviceWebConsoleAccount、pluginAccount、messageQueueAccount および natsMessageQueueAccount パラメータの値を指定した場合は、これらのパラメータがすべて応答ファイルに指定されていることを確認してください。

応答ファイルが存在しない場合は、Kaspersky Security Center Web コンソールを管理サーバーに接続するためのパラメータを含む新しい応答ファイルを作成します。ファイルに ksc-web-console-setup.json という名前を付け、/etc ディレクトリに配置します。

最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "trusted":
  "192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC サーバー",
  "acceptEula": true
}
```

Kaspersky Security Center Linux フェールオーバークラスターノードにインストールされた管理サーバーに接続されている Kaspersky Security Center Web コンソールをアップグレードする場合は、応答ファイルで、trusted インストールパラメータを指定して、Kaspersky Security Center Linux フェールオーバークラスターが Kaspersky Security Center Web コンソールに接続できるようにします。このパラメータの文字列値の形式は次の通りです：

`"trusted": "<Web コンソールのサーバーアドレス>|<ポート>|<証明書のパス>|<サーバー名>"`

trusted インストールパラメータのコンポーネントを指定します：

- **Kaspersky Security Center Web コンソールサーバーを管理サーバーに接続するためのアドレス**。クラスタノードの準備時にセカンダリネットワークアダプターを作成した場合は、アダプターの IP アドレスを Kaspersky Security Center Linux のフェールオーバークラスタのアドレスとして使用します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを指定します。

- **管理サーバーのポート**Kaspersky Security Center Web コンソールが管理サーバーへの接続に使用する OpenAPI ポート（既定値は 13299）。

- **管理サーバー証明書**管理サーバーの証明書は、Kaspersky Security Center Linux のフェールオーバークラスターの共有データストレージにあります。証明書ファイルの既定のパス：<共有データフォルダー>\1093\cert\klserver.cer。証明書ファイルを共有データストレージから Kaspersky Security Center Web コンソールをインストールするデバイスにコピーします。管理サーバーの証明書のローカルパスを指定します。

- **管理サーバー名**Kaspersky Security Center Web コンソールのログインウィンドウに表示される Kaspersky Security Center Linux のフェールオーバークラスター名。

> 同じ .rpm インストールファイルを使用して Kaspersky Security Center Web コンソールをアップグレードすることはできません。応答ファイルの設定を変更し、変更後の応答ファイルを使用して Web コンソールの再インストールを行いたい場合、Web コンソールをまずアンインストールしてから変更後の応答ファイルを使用して再インストールを行います。

4. root 権限のあるアカウントでコマンドラインを使用し、Linux ディストリビューションに応じて拡張子が「.deb」または「.rpm」のセットアップファイルを実行します。

   Kaspersky Security Center Web コンソールを以前のバージョンからアップグレードするには、次のコマンドのいずれかを実行します：

   - RPM ベースのオペレーティングシステムのデバイスの場合：
     ```
     $ sudo rpm -Uvh --nodeps --force ksc-web-console-<ビルド番号>.x86_64.rpm
     ```
   - Debian ベースのオペレーティングシステムのデバイスの場合：
     ```
     $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
     ```

   これにより、セットアップファイルの展開が始まります。インストールが完了するまで待機します。

5. 次のコマンドを実行してすべての Kaspersky Security Center Web コンソールサービスを再起動します：
   ```
   $ sudo systemctl restart KSC*
   ```

アップグレードが完了したら、ブラウザーを使用して Kaspersky Security Center Web コンソールを開き、Web コンソールにログインします。

# 閉鎖ソフトウェア環境モードでの Astra Linux での Kaspersky Security Center Web コンソールのアップグレード

この記事では、Kaspersky Security Center Web コンソールサーバー（Kaspersky Security Center Web コンソール）を Astra Linux Special Edition でアップグレードする方法について説明します。

*Kaspersky Security Center Web コンソールをアップグレードするには：*

1. Kaspersky Security Center Web コンソールをアップグレードするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。

2. 使用許諾契約書（EULA）をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイトからファイルをダウンロードできます。使用許諾契約書の条項に同意しない場合は、インストールファイルを使用して Kaspersky Security Center Web コンソールをアップグレードしないでください。

3. Kaspersky Security Center Web コンソールをインストールする前に準備したものと同じ応答ファイルを使用します。応答ファイル名は ksc-web-console-setup.json で、ファイルの場所は /etc/ksc-web-console-setup.json です。

   応答ファイルが存在しない場合は、Kaspersky Security Center Web コンソールを管理サーバーに接続するためのパラメータを含む新しい応答ファイルを作成します。ファイルに ksc-web-console-setup.json という名前を付け、/etc ディレクトリに配置します。

   最小限のパラメータと、既定のアドレスとポートの内容を記載した応答ファイルの作成例は次のようになります：

   ```
   {
     "address": "ksc.example.com",
     "port": 8080,
     "trusted":
   "192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC サーバー",
     "acceptEula": true
   }
   ```

4. ファイル /etc/digsig/digsig_initramfs.conf で、DIGSIG_ELF_MODE パラメータが次のように指定されていることを確認します：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. astra-digsig-oldkeys 互換パッケージがインストールされていることを確認します。

   このパッケージがインストールされていない場合は、次のコマンドを実行します。

   ```
   apt install astra-digsig-oldkeys
   ```

6. アプリケーションライセンスのディレクトリが存在しない場合は、作成します。

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. 前の手順で作成したディレクトリに製品のライセンス /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg を配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Kaspersky Security Center Linux 配布キットに kaspersky_astra_pub_key.gpg ライセンスが含まれていない場合は、以下のリンクをクリックしてダウンロードできます：
   > https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

8. RAM ディスクをアップデートします：

   ```
   update-initramfs -u -k all
   ```

   システムを再起動します。

9. root 権限を持つアカウントで、コマンドラインを使用してセットアップファイルを実行します。インストールファイルは、カスペルスキーの Web サイトからダウンロードして取得できます。

   Kaspersky Security Center Web コンソールを以前のバージョンからアップグレードするには、次のコマンドを実行します：

   ```
   $ sudo dpkg -i ksc-web-console-<ビルド番号>.x86_64.deb
   ```

   これにより、セットアップファイルの展開が始まります。インストールが完了するまで待機します。

10. 次のコマンドを実行してすべての Kaspersky Security Center Web コンソールサービスを再起動します：

    ```
    $ sudo systemctl restart KSC*
    ```

アップグレードが完了したら、ブラウザーを使用して Kaspersky Security Center Web コンソールを開き、Web コンソールにログインします。

# Kaspersky Security Center Linux への移行

Kaspersky Security Center Windows から Kaspersky Security Center Linux への移行は、管理サーバーのデータバックアップ（klbackup ユーティリティを使用）と移行ウィザードを使用して実行できます。

以下の表では、管理サーバーのデータバックアップと移行ウィザードを使用した移行の主な機能と制限事項を比較し、組織にとってどのアプローチがより適しているかを判断できます。

移行アプローチの比較

| パラメータ | 管理サーバーデータのバックアップ | 移行ウィザード |
| --- | --- | --- |
| 移行プロセス | Kaspersky Security Center Windows 管理サーバーデータの完全バックアップを作成し、Kaspersky Security Center Linux 管理サーバーに復元 | 移行する管理サーバーのデータの選択とエクスポート、エクスポートされたデータの Kaspersky Security Center Linux 管理サーバーへのインポート、および Kaspersky Security Center Linux の管理下にある管理対象デバイスの切り替え |
| 移行方法の特徴 | • すべての管理サーバーデータの移行<br>• 任意の数の管理対象デバイスの移行<br>• Kaspersky Security Center Windows 管理サーバーのデータの完全なコピーを取得し、Kaspersky Security Center Linux 管理サーバーに転送するために使用 | • 管理サーバーデータの一部移行<br>• 移行対象オブジェクトの選択が可能<br>• 移行する管理グループまたはサブグループに含めることができるデバイスは 10,000 台以下<br>• 移行範囲内のグループオブジェクトのみを含む管理サーバーデータを部分的に転送するために使用。移行範囲外のグループオブジェクトは手動で復元 |
| 移行範囲 | 管理サーバーデータの完全転送、管理対象デバイスの数は無制限 | • 管理グループ構造<br>• 管理グループに含まれる管理対象デバイス数（**10,000 以下**）<br>• 移行デバイスに割り当てられたタグ<br>• ネットワークエージェントと管理対象アプリケーションのグローバルタスク（管理サーバーを除く）<br>• ネットワークエージェントと管理対象アプリケーションのグループタスク<br>• 管理対象アプリケーションのポリシー<br>• レポートテンプレート<br>• ユーザーロール<br>• 内部ユーザーとセキュリティグループ<br>• コンテンツが手動で追加されるカスタムアプリケーションカテゴリ<br>• デバイスのカスタム抽出 |
| 移行範囲に含まれないもの | — | • 管理サーバーのグローバルタスク<br>• 管理サーバーに保存されたイベント<br>• リモートインストール用アプリケーション配布パッケージのリポジトリ<br>• 管理サーバー証明書<br>• 管理サーバーと管理対象アプリケーションで使用されるライセンスの転送<br>• 仮想管理サーバー<br>• ネットワークエージェントのポリシー設定<br>• デバイス移動ルール<br>• 自動タグ付けデバイスのルール<br>• ディストリビューションポイント<br>• 管理サーバーに保存されたカスペルスキー製品の設定 |

| | | |
|---|---|---|
| 移行をサポートする Kaspersky Security Center のバージョン | • サポートされているバージョンすべての Kaspersky Security Center Windows<br>• Kaspersky Security Center Linux バージョン 15.2 以降 | • Kaspersky Security Center Windows バージョン 14.2 以降<br>• Kaspersky Security Center Linux バージョン 15 以降 |
| 移行可能な DBMS | • Microsoft SQL Server → MySQL、MariaDB<br>• Microsoft SQL Server → PostgreSQL、Postgres Pro（パッチがインストールされたKaspersky Security Center Windows バージョン 14.2 以降から Kaspersky Security Center Linux バージョン 15.3 以降への移行のみ）<br>• MySQL → MySQL、MariaDB<br>• MariaDB → MySQL、MariaDB | サポートされている DBMS 間の制限なしの移行 |

# 管理サーバーのデータバックアップを使用した Kaspersky Security Center Linux への移行

データバックアップを使用して、Kaspersky Security Center Windows 管理サーバーのデータを Kaspersky Security Center Linux に移行することができます。移行する前に、Kaspersky Security Center Windows の必要な機能が Kaspersky Security Center Linux でサポートされていることを確認してください。

わかりやすくするために、バックアップを使用して管理サーバーのデータを Kaspersky Security Center Linux に移行する方法についてのチュートリアルビデオが用意されています。

制限事項：

- 移行は次の DBMS 間で実行できます：
  - Microsoft SQL Server → MySQL、MariaDB
  - Microsoft SQL Server → PostgreSQL、Postgres Pro
  - MySQL → MySQL、MariaDB
  - MariaDB → MySQL、MariaDB
- Microsoft SQL Server、MySQL、または MariaDB データベースに保存されている管理サーバーデータの MySQL または MariaDB への移行は、サポートされているすべてのバージョンの Kaspersky Security Center Windows から Kaspersky Security Center Linux バージョン 15.2 以降への移行がサポートされています。

- Microsoft SQL Server データベースに保存されている管理サーバーデータの PostgreSQL または Postgres Pro への移行は、Kaspersky Security Center Windows バージョン 14.2 以降から Kaspersky Security Center Linux バージョン 15.3 以降への移行でサポートされています。

  PostgreSQL またはPostgreSQL Postgres Pro への移行をサポートするには、カスペルスキーテクニカルサポートに依頼して、次のいずれかのパッチをインストールする必要があります：

  - Kaspersky Security Center 14.2 Windows の場合：14.2.0.26967-pf5
  - Kaspersky Security Center 14.2 Windows ベースの Kaspersky Secure Mobility Management の場合：14.2.0.48079-pf5
  - Kaspersky Security Center 15.1 Windows の場合：15.1.0.20748-pf2

    Kaspersky Security Center Windows をバージョン 15.1.0.22239 にアップデートすると、PostgreSQL または Postgres Pro への移行も可能になります。

- Kaspersky Security Center Windows および Kaspersky Security Center Linux の DBMS として MySQL または MariaDB を使用する場合、`lower_case_table_names` パラメータは現在の DBMS と新しい DBMS で一致する必要があります。

  データのバックアップを作成する前に、`lower_case_table_names` パラメータを確認してください。次に、Kaspersky Security Center Linux に MySQL または MariaDB をインストールする時に、このパラメータを Windows で指定した値と同じ値に設定する必要があります。

## 実行するステップ

管理サーバーのデータバックアップを使用した移行は段階的に進行します：

1. **管理サーバーにログインできる管理者の内部ユーザーアカウントがあることを確認します**

   管理者アカウントは、Kaspersky Security Center Linux 管理サーバーにログインするために使用されます。このアカウントを持たず、ローカル Windows アカウントまたはドメインアカウントでのみログインしている場合は、バックアップを復元した後に Kaspersky Security Center Linux 管理サーバーにログインできなくなります。Kaspersky Security Center Linux 管理サーバーは、ローカル Windows アカウントを使用したログインをサポートしていません。ドメインアカウントでログインすることは可能ですが、管理サーバーの追加設定が必要になる場合があります。

   管理者アカウントがない場合は、kladduser ユーティリティを使用してバックアップコピーを復元した後にこのアカウントを作成する必要があります。

2. **Kaspersky Security Center Windows 管理サーバーデータの最新のバックアップコピーを作成する**

   Kaspersky Security Center Windows および Kaspersky Security Center Linux で使用される DBMS の種類に応じて、次のいずれかを実行します：

   - MySQL または MariaDB から MySQL または MariaDB への移行の場合：管理サーバーがインストールされているデバイス上で klbackup ユーティリティまたはデータバックアップタスクを使用してバックアップコピーを作成します。
   - Microsoft SQL Server から MySQL または MariaDB への移行の場合：［**MySQL/MariaDB 形式へ移行**］がオンになった klbackup ユーティリティを使用します。
   - Microsoft SQL Server から PostgreSQL または Postgres Pro への移行の場合：

     1. PostgreSQL および Postgres Pro への移行をサポートするには、管理サーバーのパッチをインストールします。このパッチを入手するには、カスペルスキーのテクニカルサポートにお問い合わせください。

        Kaspersky Security Center 15.1 Windows の場合は、バージョン15.1.0.22239 にアップデートできます。

2. klbackup ユーティリティを使用してバックアップコピーを作成します。

   コマンドラインから klbackup を実行する場合は、`-migrate postgres` フラグを使用します。

   klbackup インターフェイスを使用する場合は、**Postgres フォーマットへの移行**をオンにします。

バックアップコピーを作成した後、Kaspersky Security Center Windows 管理サーバーをネットワークから切断します。

### 3 Kaspersky Security Center Linux をインストールするための新しいデバイスの準備

シナリオのこの段階では、次の操作を実行します：

1. 管理サーバーをインストールする新しいデバイスを選択します。このデバイスはハードウェアおよびソフトウェアの要件を満たしている必要があります。また、管理サーバーで使用されるポートが使用可能であることを確認してください。

2. 新しいデバイスに同じアドレスを割り当てます。

   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

### 4 DBMS のインストールと設定

シナリオのこの段階では、次の操作を実行します：

1. 最適なパフォーマンスを提供する DBMS タイプを選択します。ネットワークに接続されたデバイスの数、ネットワークトポロジ、ネットワーク上のワークロードを考慮してください。サポートされている任意の DBMS を選択できます。

2. バックアップ作成時に選択した DBMS タイプに従って DBMS をインストールします。選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

   > 新しい定義データベースのバージョンは、現在のバージョンよりも低くすることはできません。

3. Kaspersky Security Center Linux と動作する DBMS の設定

### 5 Kaspersky Security Center Linux のインストール

新しいデバイスに Kaspersky Security Center Linux をインストールするには：

インストール中に作成された管理者の内部ユーザーアカウント、およびバックアップから管理サーバーデータを復元する前に作成されたその他のオブジェクト (グループ、ポリシー、タスク、ユーザー) は、復元後に失われます。これらのオブジェクトは、バックアップに含まれるオブジェクトに置き換えられます。

### 6 バックアップコピーから管理サーバーのデータを復元します

シナリオのこの段階では、次の操作を実行します：

1. klbackup ユーティリティを使用して、新しいデバイスに管理サーバーのデータを復元します。

   > PostgreSQL の制限により、管理サーバーが DBMS に接続するために使用するアカウントに、一時的に PostgreSQL スーパーユーザー権限を付与する必要があります。

2. Kaspersky Security Center Windows 管理サーバーにログインした際に管理者の内部ユーザーアカウントが存在せず、ローカル Windows アカウントまたはドメインアカウントを使用した場合は、次のように

kladduser ユーティリティを使用して管理者アカウントを作成します：

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
```

<password>パラメータが以下の要件を満たす場合：

- ユーザーパスワードは 8 文字以上 256 文字以下である必要があります。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

7. **Kaspersky Security Center Web コンソールサーバーのインストールと管理サーバーの設定**

   シナリオのこの段階では、次の操作を実行します：

   1. Kaspersky Security Center Web コンソールのインストール。

      Kaspersky Security Center Web コンソールが以前にインストールされていた場合は、同じ応答ファイルを使用して再インストールしてください。

   2. 管理者の内部ユーザーアカウントで Kaspersky Security Center Web コンソールにログインします。

      データ初期化プロセスは通常、管理サーバーデータの復元後に最大 15 分かかりますが、時間はハードウェアのパフォーマンスと管理サーバーデータのサイズによって異なります。この間、Kaspersky Security Center Web コンソールが接続に失敗し、エラーが表示される場合があります。

   3. 定義データベース内のデータの初期化が完了したら、管理サーバーの主な機能の動作を確認します。管理サーバーが管理対象デバイスと同期し、管理サーバーのデータが回復されていることを確認します。

   4. ドメインコントローラーをポーリングする時、ドメイン構造、ユーザーアカウント、セキュリティグループ、およびドメインに含まれるデバイスの DNS 名に関する情報を復元します。

   5. 移行されたタスクを確認します。いずれかのパラメータに Windows ファイルパスが含まれている場合は、対応する Linux ファイルパスに置き換えます。

   6. 必要な場合、以前のデバイスから管理サーバーと定義データベースサーバーをアンインストールします。

      同じネットワーク上で、同じ接続アドレスと管理サーバー証明書を共有する複数の管理サーバーは存在できません。

管理者は、Kaspersky Security Center Linux でサポートされている機能を考慮して、Kaspersky Security Center Windows で管理されていた管理サーバーのデータと管理対象デバイスにアクセスできます。

# 移行ウィザードを使用した Kaspersky Security Center Linux への移行

このシナリオに従うと、Kaspersky Security Center Linux の管理下で Kaspersky Security Center Windows から、管理対象デバイスとその他のグループオブジェクト（ポリシー、タスク、グローバルタスク、タグ、およびデバイスの抽出）を含む管理グループ構造を転送できます。

制限事項：

- 移行は、Kaspersky Security Center Windows バージョン 14.2 以降から Kaspersky Security Center Linux バージョン 15 以降にのみ可能です。
- このシナリオは、Kaspersky Security Center Web コンソールを使用してのみ実行できます。

始める前に、Kaspersky Security Center Linux の機能と制限事項について確認してください：

- Kaspersky Security Center Windows と Kaspersky Security Center Linux の機能の違い
- Kaspersky Security Center Linux がサポートするカスペルスキー製品のリスト

## 実行するステップ

移行シナリオは段階的に進行します：

1. **移行方法を選択します**

   Kaspersky Security Center Linux への移行は、移行ウィザードを使用して行います。移行ウィザードの手順は、Kaspersky Security Center Windows および Kaspersky Security Center Linux の管理サーバーが階層に配置されているかどうかによって異なります：

   - 管理サーバーの階層を使用した移行

     Kaspersky Security Center Windows の管理サーバーが Kaspersky Security Center Linux の管理サーバーのセカンダリとして機能する場合は、このオプションをオンにします。移行プロセスの管理とサーバーの切り替えは、Kaspersky Security Center Web コンソールの単一インスタンス内で行います。このオプションを使用する場合は、管理サーバーを階層構造にまとめて、移行手順を簡素化できます。これを行うには、移行を開始する前に階層を作成します。

   - エクスポートファイル（ZIP アーカイブ）を使用した移行

     Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層化されていない場合は、このオプションをオンにします。移行プロセスの管理には、Kaspersky Security Center Web コンソールの 2 つのインスタンス（Kaspersky Security Center Windows 用のインスタンスと Kaspersky Security Center Linux 用のインスタンス）を使用します。この場合、Kaspersky Security Center Windows からのエクスポート中に作成およびダウンロードしたエクスポートファイル（ZIP アーカイブ）を使用し、このファイルを Kaspersky Security Center Linux にインポートします。

2. **Kaspersky Security Center Windows 管理サーバーの証明書と秘密鍵をバックアップします（オプションの手順）**

   管理サーバーの証明書と秘密鍵をバックアップコピーから復元して、管理対象デバイスを Kaspersky Security Center Linux の管理サーバーの管理下に置くことができます。この場合、Kaspersky Security Center Windows 管理サーバーの証明書と秘密鍵をバックアップします。次に、ステージ 6 で証明書とプライベートライセンスを復元する必要があります。

3. **Kaspersky Security Center Windows からのデータのエクスポート**

   Kaspersky Security Center Windows を開き、移行ウィザードを実行します。

4. **Kaspersky Security Center Linux へのデータのインポート**

   移行ウィザードを続行して、エクスポートされたデータを Kaspersky Security Center Linux にインポートします。サーバーが階層に配置されている場合、同じウィザード内でエクスポートが成功する時、インポートが自動的に開始されます。サーバーが階層に配置されていない場合は、Kaspersky Security Center Linux に切り替えた後、移行ウィザードを続行します。

**5 追加の操作を実行することで、Kaspersky Security Center Windows から Kaspersky Security Center Linux にオブジェクトと設定を手動で転送します（任意のステップ）**

移行ウィザードによる転送できないオブジェクトと設定も転送したい場合があります。たとえば、さらに次のことを実行できます：

- 管理サーバーと管理対象製品で使用されるライセンスの転送
- 管理サーバーのグローバルタスクの設定
- ネットワークエージェントのポリシー設定のこと
- 製品のインストールパッケージの作成
- 仮想サーバーの作成
- デバイス移動ルールの設定
- デバイスの自動タグルールの設定
- アプリケーションカテゴリの作成
- ディストリビューションポイントの割り当てと設定

  ディストリビューションポイントとして機能するデバイスを別の管理サーバーに移動した場合、ディストリビューションポイントの範囲に含まれるデバイスは自動的に移動されません。各デバイスを個別に移動する必要があります。ディストリビューションポイントがゲートウェイとして機能している場合は、ディストリビューションポイントがゲートウェイとして機能しないように、`# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` スクリプトを実行する必要があります。

**6 インポートされた管理対象デバイスを Kaspersky Security Center Linux の管理下に移動する**

移行を完了するには、インポートされた管理対象デバイスを Kaspersky Security Center Linux の管理下に移動します。次のいずれかの方法で、これを行うことができます：

- klmover ユーティリティを使用します

  klmover ユーティリティを使用して、新しい管理サーバーの接続設定を指定します。

- *管理サーバーの変更*タスクを通じて

  *管理サーバーの変更*タスクを作成し、インポートされた管理対象デバイス、新しい管理サーバー、およびその他のタスク設定を指定します。次に、管理対象デバイスを Kaspersky Security Center Linux の管理サーバーの管理下に置くタスクを実行します。

- （既にインストールされている場合は）削除し、管理対象デバイスにネットワークエージェントをさらにインストールします。

  新しいネットワークエージェントインストールパッケージを作成し、インストールパッケージのプロパティで新しい管理サーバーの接続設定を指定します。インポートされた管理対象デバイス上のネットワークエージェントを削除し、インストールパッケージを使用して、リモートインストールタスクを通じてインポートされた管理対象デバイスにネットワークエージェントをインストールします。スタンドアロンインストールパッケージを作成および使用して、ネットワークエージェントをローカルにインストールすることもできます。詳細については、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替えるを参照してください。

- バックアップコピーから管理サーバー証明書とプライベートライセンスを復元します（Kaspersky Security Center Linux 15.1 またはそれ以降への移行のみ）。

Kaspersky Security Center Linux の管理サーバーを使用するデバイスには、Kaspersky Security Center Windows の管理サーバーと同じネットワークアドレスを割り当てます。`-cert_only` パラメータを指定して klbackup ユーティリティを実行し、ステージ 2 で保存したバックアップコピーから管理サーバー証明書とプライベートライセンスを復元します。コマンドラインで、次のコマンドを実行します：`/opt/kaspersky/ksc64/sbin/klbackup -path <管理サーバー証明書のバックアップコピーへのパス> -restore -cert_only`。詳細については、「klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える」を参照してください。

7. **ネットワークエージェントを最新バージョンにアップデートします**

   Network Agent for Linux を Kaspersky Security Center と同じバージョンにアップグレードすることを推奨します。

8. **管理対象デバイスが新しい管理サーバーに表示されることを確認します**

   Kaspersky Security Center Linux 管理サーバーで、管理対象デバイスのリスト（[**アセット（デバイス）**] → [**管理対象デバイス**]）を開き、 [**可視**]、[**ネットワークエージェントがインストール済み**] および [**前回の管理サーバーへの接続**] 列の値を確認します。

### データ移行のその他の方法

移行ウィザード以外にも、現在のオブジェクトを転送する別の方法がありますが、この方法ではポリシーとタスクのみを転送できます：

- Kaspersky Security Center Windows からのタスクをエクスポートして、Kaspersky Security Center Linux にそのタスクをインポートします。
- Kaspersky Security Center Windows から特定のポリシーをエクスポートして、Kaspersky Security Center Linux にそのポリシーをインポートします。関連するポリシープロファイルは、選択したポリシーとともにエクスポートおよびインポートされます。

## Kaspersky Security Center Windows からのグループオブジェクトのエクスポート

Kaspersky Security Center Windows から Kaspersky Security Center Linux へ管理対象デバイスやその他のグループオブジェクトを含む管理グループ構造を移行するには、最初にエクスポートするデータを選択し、エクスポートファイルを作成する必要があります。エクスポートファイルには、移行するすべてのグループオブジェクトに関する情報が含まれています。このエクスポートファイルは、続けて実行する Kaspersky Security Center Linux へのインポートに使用します。

次のオブジェクトをエクスポートできます：

- 管理対象アプリケーションのタスクとポリシー
- グローバルタスク
- デバイスのカスタム抽出
- 管理グループの構造と含まれるデバイス
- 移行するデバイスに割り当てられているタグ

エクスポートを開始する前に、Kaspersky Security Center Linux への移行に関する一般情報をご確認ください。Kaspersky Security Center Windows および Kaspersky Security Center Linux の管理サーバーの階層を使用するかどうか、移行方法を選択します。

*移行ウィザードを使用して管理対象デバイスと関連グループオブジェクトをエクスポートするには：*

1. Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層構造にまとめられているかどうかに応じて、次のいずれかを実行します：

   - サーバーが階層構造にまとめられている場合は、Kaspersky Security Center Web コンソールを開き、Kaspersky Security Center Windows のサーバーに切り替えます。

   - サーバーが階層構造にまとめられていない場合は、Kaspersky Security Center Windows に接続された Kaspersky Security Center Web コンソールを開きます。

2. メインメニューで、［**操作**］→［**移行**］の順に選択します。

3. ［**Kaspersky Security Center Linux または Open Single Management Platform へ移行**］を選択してウィザードを開始し、その手順に従います。

4. エクスポートする管理グループまたはサブグループを選択します。選択した管理グループまたはサブグループに含まれるデバイスが 10,000 台以下であることを確認します。

5. タスクとポリシーをエクスポートする管理対象アプリケーションを選択します。Kaspersky Security Center Linux でサポートされているアプリケーションのみを選択してください。サポートされていないアプリケーションのオブジェクトもエクスポートされますが、操作はできなくなります。

6. 左側のリンクを使用して、エクスポートするグローバルタスク、デバイスの抽出、およびレポートを選択します。［**グループオブジェクト**］を使用すると、カスタムロール、内部ユーザーとセキュリティグループ、およびカスタムアプリケーションカテゴリをエクスポート対象から除外できます。

エクスポートファイル（ZIP アーカイブ）が作成されます。管理サーバーの階層サポートを使用して移行を実行するかどうかに応じて、エクスポートファイルは次のように保存されます：

- サーバーが階層に配置されている場合、エクスポートファイルは Kaspersky Security Center Web コンソールサーバーの一時フォルダーに保存されます。

- サーバーが階層に配置されていない場合、エクスポートファイルはデバイスにダウンロードされます。

管理サーバーの階層サポートのある移行では、エクスポートが正常に完了すると、インポートが自動的に開始されます。管理サーバーの階層サポートなしで移行する場合は、保存したエクスポートファイルを Kaspersky Security Center Linux に手動でインポートできます。

# エクスポートファイルを Kaspersky Security Center Linux にインポート

管理対象デバイス、オブジェクト、および Kaspersky Security Center Windows からエクスポートされた設定に関する情報を転送するには、Kaspersky Security Center Linux または Kaspersky Next XDR Expert にインポートする必要があります。

*移行ウィザードを使用して管理対象デバイスと関連グループオブジェクトをインポートするには：*

1. Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層構造にまとめられているかどうかに応じて、次のいずれかを実行します：

   - サーバーが階層に配置されている場合は、エクスポートの完了後に移行ウィザードの次のステップに進みます。このウィザード内でエクスポートが成功すると、インポートが自動的に開始されます（この手順のステップ 2 を参照）。

   - サーバーが階層に配置されていない場合：

     a. Kaspersky Security Center Linux または Kaspersky Next XDR Expert に接続されている Kaspersky Security Center Web コンソールを開きます。

     b. メインメニューで、［**操作**］→［**移行**］の順に選択します。

     c. Kaspersky Security Center Windows からのエクスポート中に作成およびダウンロードしたエクスポートファイル（ZIP アーカイブ）を選択します。エクスポートファイルのアップロードが開始されます。

2. エクスポートファイルが正常にアップロードされたら、インポートを続行できます。別のエクスポートファイルを指定する場合は、［**変更**］リンクをクリックし、必要なファイルを選択します。

3. Kaspersky Security Center Linux の管理グループの階層全体が表示されます。

   エクスポートされた管理グループのオブジェクト（管理対象デバイス、ポリシー、タスク、およびその他のグループオブジェクト）を復元する必要があるターゲット管理グループの横にあるチェックボックスをオンにします。

4. グループオブジェクトのインポートが開始されます。移行ウィザードを最小化して、インポート中に他の操作を同時に実行することはできません。オブジェクトのリスト内のすべてのアイテムの横にある更新アイコン（）が緑色のチェックマーク（）に変わり、インポートが完了するまで待ちます。

5. インポートが完了すると、エクスポートされた管理グループの構造（デバイスの詳細を含む）が、選択したターゲットの管理グループの下に表示されます。復元するオブジェクトの名前が既存のオブジェクトの名前と同じである場合、復元されたオブジェクトには増分サフィックスが追加されます。

> 移行されたタスクで、タスクを実行するアカウントの詳細が指定されている場合は、インポートの完了後にタスクを開いてパスワードを再度入力する必要があります。

インポートがエラーで完了した場合は、次のいずれかを実行できます：

- 管理サーバー階層サポートを使用した移行の場合は、エクスポートファイルのインポートを再度開始できます。

- 管理サーバー階層サポートを使用しない移行の場合は、移行ウィザードを開始して別のエクスポートファイルを選択し、それを再度インポートします。

エクスポート範囲に含まれるグループオブジェクトが Kaspersky Security Center Linux に正常にインポートされたかどうかを確認できます。これを行うには、［**アセット（デバイス）**］セクションに移動し、インポートされたオブジェクトが対応するサブセクションに表示されるかどうかを確認します。

インポートされた管理対象デバイスは［**管理対象デバイス**］サブセクションに表示されますが、ネットワーク内では表示されず、ネットワークエージェントがインストールされて実行されていないことに注意してください（［**可視**］、［**ネットワークエージェントがインストール済み**］、および［**ネットワークエージェントが実行中**］列の値が *NO*）。

移行を完了するには、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える必要があります。

# 管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える

管理対象デバイス、オブジェクト、およびそれらの設定に関する情報が Kaspersky Security Center Linux に正常にインポートされたら、移行を完了するには、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える必要があります。

次のいずれかの方法で、管理対象デバイスを Kaspersky Security Center Linux に移動できます：

- klmover ユーティリティを使用します。
- *管理サーバーの変更*タスクを使用します。
- バックアップコピーから管理サーバーの証明書と秘密鍵を復元します（Kaspersky Security Center Linux 15.1 またはそれ以降への移行のみ）。

  詳細については、メイン移行シナリオのステージ 6 を参照してください。
- リモートインストールタスクを通じて管理対象デバイスにネットワークエージェントをインストールします。

*ネットワークエージェントをインストールして、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替えるには：*

1. Kaspersky Security Center Linux の管理下に切り替えるインポートされた管理対象デバイス上のネットワークエージェントを削除します。
2. Kaspersky Security Center Windows の管理サーバーに切り替えます。
3. ［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動し、ネットワークエージェントの既存のインストールパッケージのプロパティを開きます。

   ネットワークエージェントのインストールパッケージがパッケージリストにない場合は、新しいパッケージをダウンロードします。

   スタンドアロンインストールパッケージを作成および使用して、ネットワークエージェントをローカルにインストールすることもできます。
4. ［**設定**］タブで［**接続**］セクションを選択します。Kaspersky Security Center Linux の管理サーバーの接続設定を指定します。

5. インポートされた管理対象デバイスのリモートインストールタスクを作成し、再構成されたネットワークエージェントインストールパッケージを指定します。

   ネットワークエージェントは、Kaspersky Security Center Windows の管理サーバーを通じて、またはディストリビューションポイントとして機能する Windows ベースのデバイスを通じてインストールできます。管理サーバーを使用する場合は、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。ディストリビューションポイントを使用する場合は、［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。

6. リモートインストールタスクを実行します。

リモートインストールタスクが正常に完了したら、Kaspersky Security Center Linux の管理サーバーに移動し、管理対象デバイスがネットワーク内に表示されていること、およびネットワークエージェントがインストールされて実行されていることを確認します（［**可視**］、［**ネットワークエージェントがインストール済み**］、［**ネットワークエージェントが実行中**］列の値が *Yes*）。

# 管理サーバーの設定

このセクションでは、Kaspersky Security Center 管理サーバーの設定手順とプロパティについて説明しています。

# Kaspersky Security Center Web コンソールから管理サーバーへの接続の設定

管理サーバーのプロパティまたは管理サーバーのポリシー設定を使用して、Kaspersky Security Center Web コンソールから管理サーバーへの接続を設定できます。

*管理サーバーのプロパティで接続ポートを設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。
3. 必要に応じて、［**Web コンソール用の SSL ポート**］を指定するか、他の管理サーバー接続ポートを指定します。

選択したサーバーの主な接続設定が指定されます。

*管理サーバーのポリシー設定を通じて接続ポートを設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 管理サーバーポリシーの名前をクリックし、［**アプリケーション設定**］タブに移動します。
3. 必要に応じて、［**Web コンソール用の SSL ポート**］を指定するか、他の管理サーバー接続ポートを指定します。

> ［**Web コンソール用にポートを開く**］をオフにし、このポリシー設定がデバイスに適用されると、Kaspersky Security Center Web コンソールを使用して管理サーバーに接続できなくなります。この場合、接続は終了します。このポリシーが適用されていない管理サーバーがある場合は、Kaspersky Security Center Web コンソールを介してこの管理サーバーに再接続できます。

選択したサーバーの主な接続設定が指定されます。

# 管理サーバーへの暗号化された接続

クライアントデバイスと管理サーバー間のデータ交換は、TLS（Transport Layer Security）プロトコルを使用して実行できます。TLS によって、交信する双方の識別、送信データの暗号化、送信データ通信中の改竄防止が可能になります。TLS プロトコルは、交信する双方の認証とデータの暗号化のために公開鍵を使用します。

クライアントデバイスが管理サーバーに初めて接続する場合、デバイスのネットワークエージェントは管理サーバー証明書のコピーをダウンロードし、それをローカルに保存します。

ネットワークエージェントをデバイスにローカルにインストールする場合は、管理サーバー証明書を手動で選択できます。

以降の接続では、管理サーバーの権限の検証にダウンロードされた証明書のコピーが使用されます。

以降のセッションでは、デバイスから管理サーバーへの接続ごとに、ネットワークエージェントが管理サーバー証明書を要求して、ローカルコピーと比較します。コピーが一致しない場合、デバイスから管理サーバーへのアクセスは許可されません。

# Kaspersky Security Center Linux に接続するための IP アドレスの許可リストの設定

既定では、Kaspersky Security Center Linux への接続はどのデバイスからでも許可されます。たとえば、要件を満たす任意のデバイスに Kaspersky Security Center Web コンソールサーバーをインストールでき、Kaspersky Security Center Web コンソールサーバーは Kaspersky Security Center Linux と通信します。ただし、指定した IP アドレスを持つデバイスからの接続のみが許可されるように管理サーバーを構成することもできます。この場合、侵入者が許可リストに含まれていないデバイスにインストールされた Kaspersky Security Center Web コンソールサーバーを介して Kaspersky Security Center Linux に接続しようとしても、Kaspersky Security Center Linux にログインすることはできません。

ユーザーが Kaspersky Security Center Linux にログインするか、Kaspersky Security Center Linux OpenAPI を介して管理サーバーと連携するアプリケーションを実行した場合に IP アドレスが検証されます。この時点で、デバイス上のアプリケーションは管理サーバーとの接続を確立しようとします。デバイスの IP アドレスが許可リストにない場合、 認証エラーが発生し、KLAUD_EV_SERVERCONNECT イベントが管理サーバーとの接続が確立されていないことを通知します。

## IP アドレスの許可リストの要件

次のアプリケーションが管理サーバーに接続しようとした際にのみ IP アドレスが検証されます：

- Kaspersky Security Center Web コンソールサーバー

  Kaspersky Security Center Web コンソールを介して Kaspersky Security Center Linux にログオンすると、オペレーティングシステムの標準の方法で、Kaspersky Security Center Web コンソールサーバーがインストールされているデバイスのファイアウォールを設定することができます。誰かがあるデバイスから Kaspersky Security Center Linux にログインしようとした場合、Kaspersky Security Center Web コンソールサーバーが別のデバイスにインストールされていると、ファイアウォールが侵入者の干渉防止に役立ちます。

- Klakaut 自動化オブジェクト経由で管理サーバーと連携しているアプリケーション

- Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization のような、OpenAPI 経由で管理サーバーと連携するアプリケーション

このため、上のリストにあるアプリケーションがインストールされているデバイスのアドレスを指定してください。

IPv4 と IPv6 アドレスを指定できます。IP アドレスの範囲を指定することはできません。

## IP アドレスの許可リストを設定する方法

事前に許可リストを設定していなかった場合は、次の手順に従ってください。

*Kaspersky Security Center Linux にログインするための IP アドレスの許可リストを設定するには：*

1. 管理サーバーデバイスで、管理者権限を持つアカウントでコマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center Linux のインストールフォルダー（通常は /opt/kaspersky/ksc64/sbin）に変更します。
3. root アカウントで次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s`

   前述の要件を満たす IP アドレスを指定します。複数の IP アドレスを指定する場合はセミコロンで区切ります。

   単一のデバイスに対して管理サーバーへの接続を許可する方法の例：

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   複数のデバイスに対して管理サーバーへの接続を許可する方法の例：

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```
4. 管理サーバーサービスを再起動します。

管理サーバーの SysLog イベントログで、IP アドレスの許可リストが正常に設定されているかどうかを確認できます：

## IP アドレスの許可リストを変更する方法

最初に許可リストを作成した方法と同じ方法で許可リストを変更できます。同じコマンドを実行して新しい許可リストの名前を指定します。

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s
```

許可リストから一部の IP アドレスを削除する場合は、書き直します。たとえば、許可リストに IP アドレス「192.0.2.0; 198.51.100.0; 203.0.113.0」が含まれているとします。IP アドレス「198.51.100.0」を削除したいとします。この場合、コマンドプロンプトで次のコマンドを入力します：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

管理サーバーサービスを忘れずに再起動してください。

### 設定済みの IP アドレスの許可リストをリセットする方法

*既に設定済みの IP アドレスの許可リストをリセットするには：*

1. root アカウントのコマンドプロンプトで次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. 管理サーバーサービスを再起動します。

その後、IP アドレスは検証されなくなります。

# 管理サーバーのインターネットアクセスを設定します

Kaspersky Security Network を使用し、Kaspersky Security Center Linux 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

*管理サーバーのインターネットアクセスを指定するには：*

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**インターネットアクセスの設定**］セクションを選択します。
3. インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

   - **アドレス**

     インターネットへの Kaspersky Security Center Linux の接続に使用するプロキシサーバーのアドレス。

   - **ポート番号**

     Kaspersky Security Center Linux でプロキシサーバーへの接続を確立するポートの番号。

   - **ローカルアドレスにプロキシサーバーを使用しない**

     ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

   - **プロキシサーバー認証**

     このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
     ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

   - **ユーザー名**

     プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

   - **パスワード**

     プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。
     入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用して、インターネットアクセスを構成することもできます。

# 管理サーバーの階層構造

MSP などの一部のクライアント企業は、複数の管理サーバーを実行している場合があります。複数台の別の管理サーバーを管理するのは不便であるため、1つの階層を適用することができます。階層で、Linux ベースの管理サーバーはプライマリサーバーとセカンダリサーバーのどちらとしても機能できます。Linux ベースのプライマリサーバーは、Linux ベースと Windows ベースのセカンダリサーバーの両方を管理できます。プライマリ Windows ベースのサーバーは、セカンダリ Linux ベースのサーバーを管理できます。

2 台の管理サーバーのプライマリおよびセカンダリ設定には、次のオプションがあります：

- セカンダリ管理サーバーは、プライマリ管理サーバーからポリシー、タスク、ユーザーロール、インストールパッケージを継承することにより、設定の重複を防ぎます。
- プライマリ管理サーバーのデバイスには、セカンダリ管理サーバーのデバイスを含めることができます。
- プライマリ管理サーバーのレポートには、セカンダリ管理サーバーのデータ（詳細情報を含む）を含めることができます。
- プライマリ管理サーバーは、セカンダリ管理サーバーのアップデート元として使用できます。

プライマリ管理サーバーは、上記のオプションの範囲内で非仮想セカンダリ管理サーバーからのみデータを受信します。この制限は、プライマリ管理サーバーと定義データベースを共有する仮想管理サーバーには適用されません。

# 管理サーバーの階層の作成：セカンダリ管理サーバーの追加

階層で、Linux ベースの管理サーバーはプライマリサーバーとセカンダリサーバーのどちらとしても機能できます。Linux ベースのプライマリサーバーは、Linux ベースと Windows ベースのセカンダリサーバーの両方を管理できます。プライマリ Windows ベースのサーバーは、セカンダリ Linux ベースのサーバーを管理できます。

## セカンダリ管理サーバーの追加（プライマリ管理サーバーとして指定する管理サーバーで実行）

管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立することができます。

*Kaspersky Security Center Web コンソールから接続できる管理サーバーをセカンダリ管理サーバーとして追加するには：*

1. プライマリ管理サーバーとして指定する管理サーバーのポート 13000 にセカンダリ管理サーバーから接続できることを確認します。
2. プライマリ管理サーバーとして指定する管理サーバーで、［設定］アイコン（  ）をクリックします。
3. 表示されたプロパティページで、［**管理サーバー**］タブをクリックします。
4. 管理サーバーを追加する管理グループの名前に隣接するチェックボックスをオンにします。

5. メニューのリストから［**セカンダリ管理サーバーの接続**］を選択します。

   セカンダリ管理サーバー追加ウィザードが起動します。［**次へ**］をオンにして、ウィザードに沿って手順を進めます。

6. 次のフィールドに値を入力します：

   - **セカンダリ管理サーバーの表示名**

     階層で表示する、セカンダリ管理サーバーの名前。必要に応じて、IP アドレスを名前として入力するか、「グループ 1 のセカンダリサーバー」などの名前を使用できます。

   - **セカンダリ管理サーバーアドレス（任意）**

     セカンダリ管理サーバーの IP アドレスまたはドメイン名を指定します。

     このパラメータは、［**DMZ のプライマリ管理サーバーをセカンダリ管理サーバーに接続**］オプションが有効になっている場合に必要です。

   - **管理サーバーの SSL ポート**

     プライマリ管理サーバー上の SSL ポート番号を指定します。既定のポート番号は 13000 です。

   - **管理サーバーの API ポート**

     OpenAPI 経由の接続を受信するためのプライマリ管理サーバー上のポート番号を指定します。既定のポート番号は 13299 です。

   - **プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**

     セカンダリ管理サーバーが非武装地帯（DMZ）にある場合は、このオプションをオンにします。

     このオプションを選択すると、プライマリ管理サーバーがセカンダリ管理サーバーへの接続を開始します。あるいは、セカンダリ管理サーバーがプライマリ管理サーバーへの接続を開始します。

   - **プロキシサーバーを使用する**

     プロキシサーバーを使用してセカンダリ管理サーバーに接続する場合は、このオプションをオンにします。

     この場合、プロキシサーバーの次の設定も指定する必要があります：

     - **プロキシサーバーアドレス**
     - **ユーザー名**
     - **パスワード**

7. 接続の設定を指定します：

- 将来のプライマリ管理サーバーのアドレスを入力します。
- 将来のセカンダリ管理サーバーがプロキシサーバーを使用する場合は、プロキシサーバーのアドレスとユーザー資格情報を入力して、プロキシサーバーに接続します。

8. 将来のセカンダリ管理サーバーへのアクセス権を持つユーザーの資格情報を入力します。

> 指定したアカウントの二段階認証が無効になっていることを確認します。このアカウントで二段階認証が有効になっている場合は、将来のセカンダリサーバーからのみ階層を作成できます（以下の手順を参照してください）。これは既知の問題です。

接続設定が正しければ、将来のセカンダリサーバーとの接続が確立され、「プライマリ / セカンダリ」階層が構築されます。接続に失敗した場合は、接続設定を確認するか、将来のセカンダリサーバーの証明書を手動で指定します。

将来のセカンダリサーバーは、Kaspersky Security Center Linux によって自動的に生成された自己署名証明書で認証されるため、接続が失敗することもあります。その結果、ブラウザーが自己署名証明書のダウンロードをブロックする可能性があります。この場合、次のいずれかの手順を実行できます：

- 将来のセカンダリサーバーに対し、企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- 将来のセカンダリサーバーの自己署名証明書を、信頼できるブラウザー証明書のリストに追加する。カスタム証明書を作成できない場合には、この方法を推奨します。信頼できる証明書のリストに証明書を追加する方法については、ブラウザーのドキュメントを参照してください。

ウィザードが完了すると、プライマリとセカンダリの階層が構築されます。プライマリとセカンダリの管理サーバー間の接続は、ポート 13000 で確立されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

## セカンダリ管理サーバーの追加（セカンダリ管理サーバーとして指定する管理サーバーで実行）

将来のセカンダリ管理サーバーに接続できなかった場合（たとえば、一時的に切断された、または使用できなくなった、またはセカンダリ管理サーバーの証明書ファイルが自己署名されているなどの理由で）、セカンダリ管理サーバーを追加することができます。

*Kaspersky Security Center Web コンソールから接続できない管理サーバーをセカンダリ管理サーバーとして追加するには：*

1. セカンダリ管理サーバーとして指定する管理サーバーがあるオフィスのシステム管理者に、プライマリ管理サーバーとして指定する管理サーバーの証明書ファイルを渡します（たとえば、フラッシュドライブなどの外部デバイスにファイルを書き込んで送付したり、メールで送信したりできます）。

   証明書ファイルは、プライマリ管理サーバーとして指定する管理サーバーの /var/opt/kaspersky/klnagent_srv/1093/cert/ にあります。

2. セカンダリ管理サーバーとして指定する管理サーバーを担当しているシステム管理者に、次の操作を依頼します：

   a. 設定アイコン（）をクリックします。

   b. 表示されるプロパティページで、［**全般**］タブの［**管理サーバーの階層**］セクションに移動します。

   c. ［**この管理サーバーをセカンダリ管理サーバーとして使用する**］を選択します。

   d. ［**プライマリ管理サーバーのアドレス**］に、プライマリ管理サーバーのネットワーク名を入力します。

   e. ［**参照**］をクリックして、プライマリ管理サーバーとして指定する管理サーバーの保存した証明書ファイルを選択します。

   f. 必要に応じて、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにします。

   g. プロキシサーバーを使用してプライマリ管理サーバーとして指定する管理サーバーに接続する場合、［**プロキシサーバーを使用する**］をオンにして接続設定を指定します。

   h. ［**保存**］をクリックします。

プライマリとセカンダリの階層が構築されます。ポート 13000 を使用して、セカンダリ管理サーバーからプライマリ管理サーバーへの接続が開始されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

# セカンダリ管理サーバーのリストの表示

*セカンダリ管理サーバー（仮想管理サーバーを含む）のリストを表示するには：*

メインメニューで、設定アイコン（）の横にある管理サーバーの名前をクリックします。

セカンダリ管理サーバー（仮想管理サーバーを含む）のドロップダウンリストが表示されます。

表示されている管理サーバーの名前をクリックすると、そのサーバーに移動できます。

管理グループも表示されますが、グレーアウトされており、このメニュー内では管理できません。

Kaspersky Security Center Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに接続できるようになります。

  1. Kaspersky Security Center Web コンソールがインストールされているデバイスで、デバイスにインストールされている Linux ディストリビューションに対応する Kaspersky Security Center Web コンソールのインストールファイルを管理者権限を持つアカウントで実行します。

     セットアップウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

  2. ［**アップグレード**］をオンにします。

  3. ［**変更の種別**］ステップで、［**接続設定の編集**］を選択します。

  4. ［**信頼済みの管理サーバー**］ステップで、必要なセカンダリ管理サーバーを追加します。

  5. 最後のステップで［**変更**］をクリックし、新しい設定を適用します。

  6. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに切り替えられるようになります。

# 仮想管理サーバーの管理

このセクションでは、仮想管理サーバーを管理する次の操作について説明します：

- 仮想管理サーバーの作成
- 仮想管理サーバーの有効化および無効化
- 仮想管理サーバーの管理者を割り当てる
- クライアントデバイスの管理サーバーの変更
- 仮想管理サーバーの削除

# 仮想管理サーバーの作成

仮想管理サーバーを作成して、管理グループに追加できます。

仮想管理サーバーを作成すると、プライマリ管理サーバーのユーザーリストとすべてのユーザー権限が継承されます。ユーザーがプライマリサーバーへのアクセス権を持っている場合、このユーザーは仮想サーバーへのアクセス権も持っています。作成後、サーバーへのアクセス権を個別に設定します。

*仮想管理サーバーを作成して追加するには：*

1. メインメニューで、管理サーバー名をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 仮想管理サーバーを追加する管理グループを選択します。
   仮想管理サーバーは選択したグループ（サブグループを含む）からデバイスを管理します。
4. メニューのリストから［**新しい仮想管理サーバー**］を選択します。
5. 表示されるウィンドウで、新しい仮想管理サーバーのプロパティを指定します。
   - **仮想管理サーバー名**
   - **管理サーバー接続用アドレス**
     管理サーバーの名前または IP アドレスを指定できます。
6. ユーザーのリストから、仮想管理サーバーの管理者を選択します。必要に応じて、既存のアカウントを管理者ロールに割り当てる前にこのアカウントを編集したり、新しいアカウントを作成したりできます。
   必要に応じて、kladduser ユーティリティを使用して、仮想管理サーバー管理者として機能する新しいアカウントを作成できます。これを行うには、次のコマンドを使用します：
   `kladduser -n <ユーザー名> -p <パスワード> -vs <仮想サーバー名>`
   ここで、**仮想サーバー名** は仮想管理サーバー名です。
7. ［**保存**］をクリックします。

新しい仮想管理サーバーが作成され、［**管理サーバー**］タブで表示されていた管理グループに追加されます。

Kaspersky Security Center Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに接続できるようになります。

  1. Kaspersky Security Center Web コンソールがインストールされているデバイスで、デバイスにインストールされている Linux ディストリビューションに対応する Kaspersky Security Center Web コンソールのインストールファイルを管理者権限を持つアカウントで実行します。

     セットアップウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

  2. ［**アップグレード**］をオンにします。

  3. ［**変更の種別**］ステップで、［**接続設定の編集**］を選択します。

  4. ［**信頼済みの管理サーバー**］ステップで、必要なセカンダリ管理サーバーを追加します。

  5. 最後のステップで［**変更**］をクリックし、新しい設定を適用します。

  6. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに切り替えられるようになります。

# 仮想管理サーバーの有効化および無効化

新しい仮想管理サーバーを作成すると、既定で有効になります。いつでも無効にしたり、再び有効にできます。仮想管理サーバーの無効化または有効化は、物理管理サーバーをオフまたはオンに切り替えることと同じです。

*仮想管理サーバーを有効または無効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。

3. 有効または無効にする仮想管理サーバーを選択します。

4. メニューヘッダーで［**仮想管理サーバーの有効化または無効化**］を選択します。

   以前の状態に応じて、仮想管理サーバーの状態が有効または無効に変更されます。管理サーバー名の横にアップデートされた状態が表示されます。

# 仮想管理サーバーへの管理者の割り当て

組織内で仮想管理サーバーを使用する場合、仮想管理サーバーごとに専任の管理者を割り当てることができます。たとえば、仮想管理サーバーを作成して組織の個別のオフィスや部門を管理する場合や、MSP プロバイダーで仮想管理サーバーを介してテナントを管理する場合に便利です。

仮想管理サーバーを作成すると、プライマリ管理サーバーのユーザーリストとすべてのユーザー権限が継承されます。ユーザーがプライマリサーバーへのアクセス権を持っている場合、このユーザーは仮想サーバーへのアクセス権も持っています。作成後、サーバーへのアクセス権を個別に設定します。仮想管理サーバーのみに管理者を割り当てる場合は、管理者がプライマリ管理サーバーへのアクセス権を持っていないことを確認してください。

仮想管理サーバーへの管理者アクセス権を付与することにより、仮想管理サーバーの管理者を割り当てます。次のいずれかの方法で、必要なアクセス権を付与できます：

- 管理者のアクセス権を手動で設定する
- 管理者に1つ以上のユーザーロールを割り当てる

Kaspersky Security Center Web コンソールにサインインするには、仮想管理サーバーの管理者が仮想管理サーバーの名前、ユーザー名、およびパスワードを指定します。Kaspersky Security Center Web コンソールは管理者を認証し、管理者がアクセス権を持つ仮想管理サーバーを開きます。管理者は、管理サーバーを切り替えることはできません。

## 必須条件

開始する前に、次の条件が満たされていることを確認してください：

- 仮想管理サーバーが作成されている。
- プライマリ管理サーバーで、仮想管理サーバーに割り当てる管理者のアカウントを作成した。
- ［**一般的な機能**］→［**ユーザーのアクセス許可**］機能領域の**オブジェクト ACL の変更**権限を持っている。

## アクセス権の手動設定

*仮想管理サーバーの管理者を割り当てるには：*

1. メインメニューで、必要な仮想管理サーバーに切り替えます：
   a. シェブロンアイコン（）が現在の管理サーバー名の右側に表示されます。
   b. 必要な管理サーバーを選択します。
2. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
3. ［**アクセス権**］タブで、［**追加**］をクリックします。
   プライマリ管理サーバーと現在の仮想管理サーバーのユーザーの統合リストが表示されます。

4. ユーザーのリストから、仮想管理サーバーに割り当てる管理者のアカウントを選択し、［**OK**］をクリックします。

   選択したユーザーが［**アクセス権**］タブのユーザーリストに追加されます。

5. 追加されたアカウントの横にあるチェックボックスをオンにし、［**アクセス権**］をクリックします。

6. 仮想管理サーバーで管理者が持つ権限を設定します。

   認証が成功するためには、管理者には少なくとも次の権限が必要です：

   - **読み取り**権限（［**一般的な機能**］→［**基本機能**］の機能領域）
   - **読み取り**権限（［**一般的な機能**］→［**仮想管理サーバー**］の機能領域）

変更されたユーザー権限が管理者アカウントに保存されます。

## ユーザーロールの割り当てによるアクセス権の設定

あるいは、ユーザーロールを介して仮想管理サーバー管理者にアクセス権を付与することもできます。たとえば、同じ仮想管理サーバーに複数の管理者を割り当てる場合に便利です。この場合、複数の管理者に同じユーザー権限を構成する代わりに、管理者のアカウントに同じ1つ以上のユーザーロールを割り当てることができます。

*ユーザーロールを割り当てて仮想管理サーバーの管理者を割り当てるには：*

1. プライマリ管理サーバーで、新しいユーザーロールを作成し、管理者が仮想管理サーバーで持つ必要があるすべてのアクセス権を指定します。たとえば、様々な機能領域へのアクセスを分離する場合は、複数のロールを作成できます。

2. メインメニューで、必要な仮想管理サーバーに切り替えます：

   a. シェブロンアイコン（  ）が現在の管理サーバー名の右側に表示されます。

   b. 必要な管理サーバーを選択します。

3. 新しいロールまたは複数のロールを管理者アカウントに割り当てます。

   ロールが管理者アカウントに割り当てられます。

## オブジェクトレベルでのアクセス権の設定

機能領域レベルでのアクセス権の割り当てに加えて、仮想管理サーバー上の特定のオブジェクト（特定の管理グループやタスクなど）へのアクセスを設定できます。これを行うには、仮想管理サーバーに切り替えてから、オブジェクトのプロパティでアクセス権を設定します。

# クライアントデバイスの管理サーバーの変更

［***管理サーバーの変更***］タスクを使用して、クライアントデバイスを管理する管理サーバーを別のサーバーに変更できます。タスクの完了後、選択したクライアントデバイスは指定した管理サーバーの管理下に置かれます。

接続ゲートウェイを介して管理サーバーに接続されたクライアントデバイスに対して、*管理サーバーの変更*タスクを使用することはできません。このようなデバイスの場合は、ネットワークエージェントを再構成するか、ネットワークエージェントを再インストールして接続ゲートウェイを指定する必要があります。

*クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの［**新規タスク設定**］ステップで、次の設定を指定します：

   a. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Security Center**］を選択します。

   b. ［**タスク種別**］フィールドで、［**管理サーバーの変更**］を選択します。

   c. ［**タスク名**］フィールドに、作成中のタスク名を指定します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

   d. タスクを割り当てるデバイスを選択します：

   - **管理グループにタスクを割り当てる**

     任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

     たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

     タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

   - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

     タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

     特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

   - **デバイスの抽出にタスクを割り当てる**

     デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

     たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

4. ウィザードの［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

5. ウィザードのこのステップで、クライアントデバイスの管理サーバーの変更条件に同意することを確認します。

6. ウィザードのこのステップで、選択したデバイスの管理に使用する管理サーバーを選択します：

- **別のプライマリ管理サーバーに変更する**

  クライアントデバイスを別のプライマリ管理サーバーに移動するには、次の管理サーバー接続設定を指定します：

  1. ［**管理サーバーアドレス**］フィールドに、新しいプライマリ管理サーバーのアドレスを指定します。
  2. ［**ポート番号**］フィールドで、管理サーバーに接続するためのポート番号を指定します。
     既定のポート番号は 14000 です。
  3. ［**SSL ポート**］フィールドで、プライマリ管理サーバーの SSL ポート番号を指定します。
     既定のポート番号は 13000 です。
  4. 必要に応じて、［**プロキシサーバーを使用する**］をオンにします。
     このオプションをオフにすると、デバイスを管理サーバーに接続するために直接接続が使用されます。
     このオプションをオンにする場合は、プロキシサーバーのパラメータを指定します：
     - **プロキシサーバーアドレス**
     - **プロキシサーバーのポート**

     プロキシサーバーで認証が必要な場合は、［**ユーザー名**］と［**パスワード**］フィールドで、プロキシサーバーへの接続を確立するアカウントの資格情報を指定します。プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。
  5. 必要に応じて、新しい管理サーバー証明書をアップロードします。

- **このプライマリサーバー上で別の仮想サーバーに変更する**

  現在のプライマリ管理サーバー上の仮想管理サーバーにクライアントデバイスを移動するには、このオプションを選択します。これを行うには、［**仮想管理サーバー名**］ドロップダウンリストで、必要な仮想管理サーバーを選択します。

7. ウィザードの［**タスクを実行するアカウントの選択**］ステップで、アカウント設定を指定します：

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

    タスクを実行するアカウント。

  - **パスワード**

    タスクが実行されるアカウントのパスワード。

8. 既定のタスク設定を変更する場合は、ウィザードの［**タスク作成の終了**］ステップで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。

   このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. 既定のタスク設定を変更する場合は、タスクプロパティウィンドウで、必要に応じてタスクの全般的な設定を指定します。

12. ［**保存**］をクリックします。

    タスクが指定した設定で作成されます。

13. 作成したタスクを実行します。

タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

# 仮想管理サーバーの削除

仮想管理サーバーを削除すると、管理サーバーで作成したすべてのオブジェクト（ポリシーとタスクを含む）も削除されます。仮想管理サーバーで管理されていた管理グループの管理対象デバイスは、管理グループから削除されます。Kaspersky Security Center Linux の管理下にあるデバイスを返却するには、ネットワークポーリングを実行してから、見つかったデバイスを[未割り当てのデバイス]グループから管理グループに移動します。

*仮想管理サーバーを削除するには：*

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 削除する仮想管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。

仮想管理サーバーが削除されます。

# 管理サーバーの接続イベントのログ記録の構成

動作中の管理サーバーへの接続と接続試行の履歴がログファイルに保存されます。ログファイル内の情報により、ネットワークインフラストラクチャ内の接続だけでなく、サーバーに対する不正アクセスの試行についても追跡できます。

*管理サーバーへの接続イベントのログを記録するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。
3. ［**管理サーバーへの接続イベントを記録する**］をオンにします。

管理サーバーの受信接続イベント、認証の結果、SSL エラーが「/var/opt/kaspersky/klnagent_srv/logs/sc.syslog」ファイルに記録されます。

# イベントのリポジトリに保管できるイベントの最大数の設定

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

アプリケーションは 10 分ごとにデータベースをチェックします。イベント数が指定された最大値に 10,000 を加えた値に達すると、アプリケーションは最も古いイベントを削除し、指定された最大数のイベントのみが残ります。

*管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報はオペレーティングシステムログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。既定では、イベントキューは 20,000 イベントに制限されます。KLEVP_MAX_POSTPONED_CNT フラグ値を編集することで、キュー制限をカスタマイズできます。*

*管理サーバーのイベントリポジトリに保存できるイベント数を制限するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**イベントリポジトリ**］セクションを選択します。データベースに記録するイベント数の上限を指定します。

3. ［**保存**］をクリックします。

加えて、次のことができます：

- 任意のタスクの設定を変更して、タスクの進行状況に関連するイベントを保存したり、タスクの実行結果のみを保存したりできます。

- 管理対象デバイスにインストールされている管理サーバー、ネットワークエージェント、およびカスペルスキー製品のイベントの保存期間を短縮または無効にします。

それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって重要なイベントが上書きされる可能性を低下させることができます。

# 管理サーバーの別のデバイスへの移動

新しいデバイスで管理サーバーを使用する必要がある場合は、次のいずれかの方法で移動できます：

- 管理サーバーおよび定義データベースサーバーを新しいデバイスに移動します（定義データベースサーバーは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます）。

- データベースサーバーを以前のデバイスに保持し、管理サーバーのみを新しいデバイスに移動する。

*管理サーバーとデータベースサーバーを新しいデバイスに移動するには：*

1. 以前のデバイスで、管理サーバーデータのバックアップを作成します。

   このためには、Kaspersky Security Center Web コンソールからデータバックアップタスクを実行するか、klbackup ユーティリティを実行します。

2. 前のデバイスで、管理サーバーをネットワークから切断します。

3. 管理サーバーをインストールする新しいデバイスを選択します。選択したデバイスのハードウェアとソフトウェアが、管理サーバー、Kaspersky Security Center Web コンソール、およびネットワークエージェントの要件を満たしていることを確認してください。また、管理サーバーで使用されるポートが使用可能であることを確認してください。

4. 新しいデバイスに同じアドレスを割り当てます。

   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

5. 必要に応じて、別のデバイスに管理サーバーが使用するデータベース管理システム（DBMS）をインストールします。

   定義データベースは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます。このデバイスがハードウェアおよびソフトウェアの要件を満たしていることを確認してください。DBMS を選択する際は、管理サーバーが対応するデバイスの数を考慮してください。

6. 新しいデバイスに管理サーバーをインストールします。

   定義データベースサーバーを別のデバイスに移動する場合は、ローカルアドレスを定義データベースがインストールされているデバイスの IP アドレスとして指定することに注意してください（Kaspersky Security Center Linux のインストール手順の「h」項目）。データベースサーバーを以前のデバイスに保持する必要がある場合は、Kaspersky Security Center Linux のインストール手順の「h」項目で以前のデバイスの IP アドレスを入力します。

7. インストールが完了したら、klbackup ユーティリティを使用して、新しいデバイスで管理サーバーのデータを復元します。

8. Kaspersky Security Center Web コンソールを開き、管理サーバーに接続します。

9. すべての管理対象デバイスが管理サーバーに接続されていることを確認します。

10. 以前のデバイスから管理サーバーとデータベースサーバーをアンインストールします。

# DBMS 資格情報の変更

たとえば、セキュリティ目的で資格情報のローテーションを実行するために、DBMS 資格情報の変更が必要になる場合があります。

*Linux 環境で klsrvconfig ユーティリティを使用して DBMS 資格情報を変更するには：*

1. Linux コマンドラインを開始します。

2. 表示されたコマンドラインウィンドウで klsrvconfig ユーティリティを指定します：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. 新しいアカウント名を指定します。DBMS に存在するアカウントの資格情報を指定する必要があります。

4. 新しいパスワードを入力します。

5. 確認のため新しいパスワードを再入力します。

DBMS 資格情報が変更されます。

# 管理サーバーデータのバックアップと復元

データバックアップにより、データを失わずに、管理サーバーをデバイス間で移動できます。バックアップを使用すると、管理サーバーのデータベースを別のデバイスに移動した時や、新しいバージョンの Kaspersky Security Center にアップグレードした時に、データを復元できます。また、データバックアップを使用して、Kaspersky Security Center Linux の管理下にある Kaspersky Security Center Windows から管理サーバーのデータを移動することもできます（Kaspersky Security Center Linux から Kaspersky Security Center Windows へのデータの移動はサポートされていません）。

インストールされている管理プラグインはバックアップされないこと留意してください。管理サーバーのデータをバックアップコピーから復元した後で、管理対象アプリケーション用のプラグインをダウンロードして再インストールする必要があります。

管理サーバーのデータをバックアップする前に、仮想管理サーバーが管理グループに追加されているかどうかを確認してください。仮想管理サーバーを追加する場合は、バックアップ前にこの仮想管理サーバーに管理者が割り当てられていることを確認してください。バックアップ後は、仮想管理サーバーへの管理者アクセス権を付与できません。管理者アカウントの資格情報が失われると、仮想管理サーバーに新しい管理者を割り当てることができなくなることに注意してください。

Kaspersky Security Center Linux フェールオーバークラスタをバックアップまたは復元するには、メンテナンスのためにクラスタ全体を停止し、バックアップまたは復元が完了したらクラスタを再起動する必要があります。

次の方法のいずれかを使用して、管理サーバーデータのバックアップコピーを作成できます。

- Kaspersky Security Center Web コンソールで、データバックアップタスクを作成して実行する。
- 管理サーバーがインストールされているデバイスで klbackup ユーティリティを実行する。このユーティリティは、Kaspersky Security Center の配布キットに含まれています。管理サーバーをインストールすると、このユーティリティは、アプリケーションのインストール時に指定したインストール先フォルダー（通常は /opt/kaspersky/ksc64/sbin/klbackup）のルートに格納されます。

次のデータが管理サーバーのバックアップコピー内に保存されます：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- リモートインストール用アプリケーション配布パッケージのリポジトリ
- 管理サーバー証明書

管理サーバーデータを復元するには、klbackup ユーティリティを使用する必要があります。

# 管理サーバーのデータバックアップタスクの作成

バックアップタスクは管理サーバーのタスクであり、クイックスタートウィザードで作成されます。クイックスタートウィザードで作成されたバックアップタスクが削除された場合、手動で作成することができます。

［*管理サーバーデータのバックアップ*］タスクは1つのみ作成できます。管理サーバーの管理サーバーデータのバックアップタスクが既に作成されている場合は、タスク種別選択ウィンドウには表示されません。

*管理サーバーのデータバックアップタスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］リストから［**Kaspersky Security Center 15.3**］を選択し、［**タスク種別**］リストから［**管理サーバーデータのバックアップ**］を選択します。
4. 対応するステップで、次の情報を指定します。
   - バックアップコピーの保管用のフォルダー
   - バックアップのパスワード（省略可能）
   - 保存するバックアップコピー数の最大値
5. ［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
6. ［**終了**］をクリックします。

タスクが作成され、タスクリストに表示されます。

# klbackup ユーティリティを使用したデータのバックアップとリカバリ

バックアップと将来の復元に備えて、Kaspersky Security Center 配布キットに含まれている klbackup ユーティリティを使用して、管理サーバーのデータをコピーできます。

復元を実行する対象の管理サーバーのインスタンスでは、同じ種別の DBMS を使用している必要があります。管理サーバーのバージョンは、同じ（同一またはそれ以降のパッチを適用）またはそれ以降にする必要があります。

以前のバージョンの MariaDB DBMS を使用して、Kaspersky Security Center Linux 15 以前に含まれていた管理サーバーのデータをバックアップし、それ以降のバージョンの MariaDB を搭載したデバイスでデータを復元すると、エラーが発生する可能性があります。詳細については、「以前の DBMS バージョンで作成されたバックアップから管理サーバーデータを復元する方法」を参照してください。

klbackup ユーティリティを使用すると、ネットワークエージェントフラグは復元されません。ネットワークエージェントフラグを手動で構成する必要があります。

*サイレントモードでバックアップコピーを作成または管理サーバーデータを復元するには：*

管理サーバーがインストールされているデバイスのコマンドラインで、必要なキーを指定して klbackup を実行します。

ユーティリティのコマンドライン構文は次の通りです：

```
klbackup -path <バックアップパス> [-linux_path < DBMS バックアップパス>-node_cert <証明書パス>] [-logfile <ログファイル> [-use_ts]|[-restore] [-password <パスワード>] [-cert_only]
```

klbackup ユーティリティのコマンドラインでパスワードを指定しないと、対話形式でパスワードを入力するように指示されます。

キーの説明：

- `-path <バックアップパス>`—バックアップフォルダーに情報を保存するか、バックアップフォルダーのデータを復元に使用します（必須パラメータ）。
- `-linux_path <DBMS バックアップのパス>`—DBMS バックアップデータが格納されているフォルダーのローカルパス。

  データベースサーバーアカウントと klbackup ユーティリティには、DBMS バックアップフォルダー内のデータを変更する権限が付与されている必要があります。
- `-node_cert <証明書パス>` – 回復後に非アクティブなフェールオーバークラスターノードを設定するためのサーバー証明書ファイル。設定されていない場合は、サーバーから自動的に取得されます。
- `-logfile <ログファイル名>` – 管理サーバーデータのバックアップと復元に関するレポートを保存します。

  データベースサーバーアカウントと klbackup ユーティリティには、バックアップフォルダー内のデータを変更する権限が付与されている必要があります。

- `-use_ts`—データを保存する際は、情報をバックアップフォルダー内のサブフォルダーにコピーします。サブフォルダー名は「`klbackup YYYY-MM-DD # HH-MM-SS`」形式で、現在の日付と UTC での操作時刻が含まれています。キーを指定しない場合は、バックアップフォルダーのルートに保存されます。

  既にバックアップコピーがあるフォルダーに情報を保存しようとすると、エラーメッセージが表示されます。情報は更新されません。

  `-use_ts` キーを使用することで、管理サーバーデータのアーカイブを保持することができます。たとえば、`-path` キーにフォルダー `/tmp/KLBackups` を指定した場合、フォルダー `klbackup 2022/6/19 # 11-30-18` には、2022 年 6 月 19 日午前 11 時 30 分 18 秒時点の管理サーバーのステータス情報が保存されます。

- `-restore`—管理サーバーデータを復元します。データ復元はバックアップフォルダーに保管された情報に基づいて実行されます。使用可能なキーがない場合、データはバックアップフォルダーにバックアップされます。

- `-password <パスワード>` — 機密データを保護するためのパスワード。

  パスワードを忘れた場合、復元できません。パスワードに条件はありません。パスワードの長さは無制限です。また、0 文字（パスワードを設定しない）も可能です。

  データを復元する時は、バックアップ時に入力したパスワードを指定します。共有フォルダーへのパスがバックアップ後に変更された場合は、復元されたデータを使用するタスクの操作（復元タスクとリモートインストールタスク）を確認します。必要に応じて、これらのタスクの設定を編集します。バックアップファイルからのデータの復元中は、共有フォルダーまたは管理サーバーにアクセスしないでください。klbackup ユーティリティを開始するアカウントは、共有フォルダーへのフルアクセスの権限を持っている必要があります。バックアップから管理サーバーのデータを復元するには、新しくインストールされた管理サーバーでユーティリティを実行することを推奨します。

- `-cert_only` – 管理サーバーの証明書と秘密鍵のみを保存または回復します。

  このフラグは、Kaspersky Security Center Windows の管理サーバーから Kaspersky Security Center Linux の管理サーバーへの移行を実行する時に役立ちます。また、管理対象デバイスを Kaspersky Security Center Linux 管理サーバー間、および Kaspersky Security Center Windows 管理サーバー間で移行することもできます。

データバックアップを使用して、Kaspersky Security Center Windows 管理サーバーのデータを Kaspersky Security Center Linux の管理下に移動できます。
Kaspersky Security Center Windows および Kaspersky Security Center Linux の DBMS として MySQL または MariaDB を使用する場合、`lower_case_table_names` パラメータは現在の DBMS と新しい DBMS で一致する必要があります。
データのバックアップを作成する前に、`lower_case_table_names` パラメータを確認してください。次に、Kaspersky Security Center Linux に MySQL または MariaDB をインストールする時に、`lower_case_table_names` パラメータを、Windows のこのパラメータに指定された値と同じ値に設定する必要があります。

# klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える

klbackup ユーティリティを使用すると、別の管理サーバーの管理下にある管理対象デバイスを切り替えることができます。移行を実行する時に、klbackup ユーティリティを使用して、Kaspersky Security Center Windows 管理サーバーを Kaspersky Security Center Linux 管理サーバーに変更できます。また、管理対象デバイスを Kaspersky Security Center Linux 管理サーバー間、および Kaspersky Security Center Windows 管理サーバー間で移行することもできます。

*klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替えるには、次の手順を実行します：*

1. 以前のデバイスで、管理サーバー証明書と秘密鍵のバックアップコピーを作成します。

   次のいずれかの方法でバックアップコピーを作成できます：

   - klbackup ユーティリティインターフェイスを使用する（Kaspersky Security Center Windows 管理サーバーのみ）

     Kaspersky Security Center インストールフォルダーにある klbackup ユーティリティを実行し、**管理サーバーの証明書のみを復元またはバックアップする**オプションを使用してバックアップを作成します。

   - コマンドプロンプトを使用する (Kaspersky Security Center Windows および Kaspersky Security Center Linux 管理サーバーバージョン 15.1 以降)

     管理サーバー証明書と秘密鍵のバックアップコピーを作成するには、コマンドラインから `-cert_only` キーを指定して klbackup ユーティリティを実行します。

     `klbackup -path <管理サーバー証明書のバックアップコピーへのパス> -cert_only`

2. 前のデバイスで、管理サーバーをネットワークから切断します。

3. 別の管理サーバーを使用してデバイスに同じアドレスを割り当てます。

   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

4. 別の管理サーバーがあるデバイスで、バックアップコピーから管理サーバー証明書と秘密鍵を復元します。

   次のいずれかの方法でバックアップコピーを復元できます：

   - klbackup ユーティリティインターフェイスを使用する（Kaspersky Security Center Windows 管理サーバーのみ）

     klbackup ユーティリティを実行し、**管理サーバーの証明書のみを復元またはバックアップする**オプションを使用してバックアップを復元します。

   - コマンドプロンプトを使用する（Kaspersky Security Center Windows および Kaspersky Security Center Linux 管理サーバーバージョン 15.1 以降）

     管理サーバー証明書と秘密鍵のバックアップコピーを復元するには、コマンドラインから `-cert_only` キーを指定して klbackup ユーティリティを実行します：

     `klbackup -path <管理サーバー証明書のバックアップコピーへのパス> -restore -cert_only`

管理対象デバイスは別の管理サーバーの管理下に置かれます。この管理サーバーにアクセスし、管理対象デバイスがネットワークで表示されていること、ネットワークエージェントがインストールされ、実行されていることを確認できます（[**可視**]、[**ネットワークエージェントがインストール済み**]、[**ネットワークエージェントが実行中**] 列の［*はい*］の値）。

# MySQL または MariaDB を使用する場合の管理サーバーデータのバックアップと復元

データバックアップを使用して、Kaspersky Security Center Linux の管理下にある Kaspersky Security Center Windows から管理サーバーのデータを移行できます。管理サーバーのデータバックアップを使用した移行は、サポートされているバージョンの Kaspersky Security Center Windows から Kaspersky Security Center Linux 15.2 以降への移行でのみサポートされます。

Kaspersky Security Center Windows および Kaspersky Security Center Linux の DBMS として MySQL または MariaDB を使用する場合、`lower_case_table_names` パラメータは現在の DBMS と新しい DBMS で一致する必要があります。そうしないと、管理サーバーのデータが正しく移行されません。

Kaspersky Security Center Windows で管理サーバーデータをバックアップする前に、`lower_case_table_names` パラメータの値を確認してください。以前の DBMS インストール時にこのパラメータを指定しなかった場合は、既定のパラメータ値が使用されます。Windows の `lower_case_table_names` パラメータの既定値は `1` です。

Kaspersky Security Center Linux に MySQL または MariaDB をインストールする場合は、MySQL Web サイトの指示に従って、 `lower_case_table_names` パラメータを Windows のこのパラメータに指定されている値と同じ値に設定します。このパラメータを指定しない場合は、既定のパラメータ値が使用されます。Linux ベースのオペレーティングシステムの場合、`lower_case_table_names` パラメータの既定値は、Windows の既定値と異なります。

MySQL 8.0 をインストールする場合、この手順に従って `lower_case_table_names` パラメータを指定しても機能しない可能性があります。この場合、まず MySQL 5.7 をインストールし、以下の命令を使用して `lower_case_table_names` パラメータを指定する必要があります。そして MySQL 5.7 を MySQL 8.0 にアップグレードします。現在の DBMS と新しい DBMS の `lower_case_table_names` パラメータが一致しない場合、管理サーバーのデータは正しく復元されません。

# 管理サーバーのメンテナンス

管理サーバーのメンテナンスにより、管理サーバーのフォルダー内のスペースを解放し、不要になったオブジェクトを削除して定義データベースのサイズを縮小できます。これにより、アプリケーションのパフォーマンスと動作の信頼性が向上します。管理サーバーのメンテナンスは、少なくとも週1回は実施してください。

管理サーバーのメンテナンスは、専用のタスクで実施されます。管理サーバーのメンテナンス時、次の処理が実行されます：

- ストレージフォルダーから不要なフォルダとファイルを削除します。
- テーブルから不要なレコード（「ダングリングポインター」とも呼ばれます）を削除します。

- キャッシュをクリアします。
- 定義データベースを管理します（DBMS として PostgreSQL を使用する場合）：
  - データベースのインデックスを再編成する
  - データベースの統計情報を更新する
  - データベースを縮小する（必要に応じて）

管理サーバーのメンテナンスタスクは、MariaDB バージョン 10.3 以降をサポートします。MariaDB バージョン 10.2 以前を使用する場合、管理者はこの DBMS を独自に維持する必要があります。

管理サーバーのメンテナンス タスクは、Kaspersky Security Center Linux をインストールすると自動的に作成されます。管理サーバーのメンテナンスタスクを削除してしまった場合は、手動で作成することができます。

*管理サーバーのメンテナンスを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの［**新規タスク設定**］ウィンドウで、タスク種別に［**管理サーバーのメンテナンス**］を選択し、［**次へ**］をクリックします。
4. 引き続きウィザードの指示に従って操作します。

作成したタスクはタスクリストに表示されます。1台の管理サーバーに対して実行できる管理サーバーのメンテナンスタスクは1つのみです。管理サーバーに対して、既に 管理サーバーのメンテナンス タスクが作成されている場合は、新たに 管理サーバーのメンテナンス タスクを作成することはできません。

# 管理サーバーの階層の削除

管理サーバーの階層構造が不要になった場合は、管理サーバーを階層構造から離脱させることができます。

*管理サーバーの階層を削除するには：*

1. メインメニューで、プライマリ管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されたページで、［**管理サーバー**］タブに移動します。
3. セカンダリ管理サーバーを削除する管理グループで、目的のセカンダリ管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。
5. 表示されるウィンドウで、［**OK**］をクリックし、セカンダリ管理サーバーを削除する処理を確定させます。

プライマリ管理サーバーとして動作していた管理サーバーと、セカンダリ理サーバーとして動作していた管理サーバーは、互いに独立して動作するようになります。これにより、階層構造が解消されます。

# パブリック DNS サーバーへのアクセス

システム DNS を使用してカスペルスキーのサーバーにアクセスできない場合、Kaspersky Security Center Linux では、以下のパブリック DNS サーバーを次の順序で使用できます：

1. Google Public DNS （8.8.8.8）
2. Cloudflare DNS（1.1.1.1）
3. Alibaba Cloud DNS（223.6.6.6）
4. Quad9 DNS（9.9.9.9）
5. CleanBrowsing（185.228.168.168）

DNS サーバーへの TCP/UDP 接続を確立するため、これらの DNS サーバーへの要求にはドメインアドレスと管理サーバーのパブリック IP アドレスが含まれる場合があります。Kaspersky Security Center Linux がパブリック DNS サーバーを使用している場合、データ処理は関連するサービスのプライバシーポリシーによって管理されます。

*klscflag ユーティリティを使ってパブリック DNS の使用を設定するには、次の手順を実行します：*

1. コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。
2. パブリック DNS の使用を無効にするには、root アカウントで次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. パブリック DNS の使用を有効にするには、root コマンドで次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

# インターフェイスの設定

Kaspersky Security Center Web コンソールのインターフェイスを設定して、使用している機能に応じてセクションとインターフェイス要素を表示または非表示にすることができます。

*現在使用している機能に基づいて Kaspersky Security Center Web コンソールのインターフェイスを設定するには：*

1. メインメニューで、［**設定**］→［**インターフェイスのオプション**］の順にクリックします。
2. 必要なオプションをオンまたはオフにします：
   - **データ暗号化と保護機能の表示**
   - **EDR アラートを表示**
3. ［**保存**］をクリックします。

必要なオプションがオンになると、コンソールのメインメニューに該当するセクションが表示されます。たとえば、［**EDR アラートを表示**］をオンにした場合、メインメニューに［**監視とレポート**］→［**アラート**］セクションが表示されます。

# 管理サーバー接続用アドレスの設定

管理サーバーの接続アドレスは、次の目的で使用されるネットワークアドレスです：

- ネットワークエージェントのインストールパッケージを作成する時の既定のアドレスとして

  ネットワークエージェントをインストールすると、管理対象デバイスはこのアドレスで管理サーバーに接続します。

- KSN のプロキシサーバーアドレスとして

  管理対象デバイスはこのアドレスを介して KSN プロキシサーバーに接続します。

*管理サーバーの接続アドレスを設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**全般**］セクションを選択します。

3. 開いたウィンドウで、［**管理サーバー接続用アドレス**］フィールドに、新しい管理サーバーの接続アドレスを指定します。

   接続アドレスの最大長は 255 文字です。

   管理サーバーの接続アドレスは、管理サーバーの NetBIOS 名、FQDN、または IP アドレスとして指定できます。

4. ［**保存**］をクリックします。

指定されたアドレスは、管理サーバーアドレスおよび KSN プロキシサーバーアドレスとして使用されます。

# TLS による通信の暗号化

社内の企業ネットワークの脆弱性を修正するために、TLS プロトコルを使用したトラフィックの暗号化を有効にすることができます。管理サーバーで TLS 暗号化プロトコルとサポートされている暗号スイートを有効にすることができます。Kaspersky Security Center Linux は、TLS プロトコルのバージョン 1.0、1.1、1.2 および 1.3 をサポートしています。必要な暗号化プロトコルと暗号化スイートを選択できます。

Kaspersky Security Center Linux は、自己署名証明書を使用します。証明書を自分で用意して使用することもできます。カスペルスキーの専門家は、信頼できる認証機関が発行した証明書を使用することを推奨します。

*管理サーバーで許可される暗号化プロトコルと暗号化スイートを設定するには、次の手順に従います：*

1. コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

2. SrvUseStrictSslSettings フラグを使用し、管理サーバーで許可される暗号化プロトコルと暗号化スイートを指定します。root アカウントのコマンドラインで次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <値> -t d
   ```

   SrvUseStrictSslSettings フラグの <値> パラメータを指定します：

   - 4—TLS 1.2 および TLS 1.3 プロトコルのみが有効になります。また、TLS_RSA_WITH_AES_256_GCM_SHA384 の暗号スイートも有効になります（この暗号スイートは、Kaspersky Security Center Linux との下位互換性のために必要です）。これは既定値です。

     TLS 1.2 プロトコルでサポートされる暗号スイート：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384（TLS_RSA_WITH_AES_256_GCM_SHA384 を使用した暗号スイート）
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 プロトコルでサポートされる暗号スイート：

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—TLS 1.2 および TLS 1.3 プロトコルのみが有効になります。TLS 1.2 および TLS 1.3 プロトコルの場合、以下にリストされている特定の暗号スイートがサポートされています。

     TLS 1.2 プロトコルでサポートされる暗号スイート：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 プロトコルでサポートされる暗号スイート：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

SrvUseStrictSslSettings フラグのパラメータ値として 0、1、2、または 3 を使用することは推奨しません。これらのパラメータ値は、セキュアでない TLS プロトコルバージョン（TLS 1.0 および TLS 1.1）およびセキュアでない暗号スイートに対応しており、以前の Kaspersky Security Center バージョンとの下位互換性のためにのみ使用されます。

3. 次の Kaspersky Security Center Linux サービスを再起動します：
   - 管理サーバー
   - Web サーバー
   - アクティベーションプロキシ

その結果、TLS プロトコルを使用したトラフィック暗号化が有効になります。

KLTR_TLS12_ENABLED フラグおよび KLTR_TLS13_ENABLED フラグを使用して、それぞれ TLS 1.2 および TLS 1.3 プロトコルのサポートを有効にすることができます。これらのフラグは既定で有効になっています。

*TLS 1.2 および TLS 1.3 プロトコルのサポートを有効または無効にするには：*

1. klscflag ユーティリティを実行します。

   コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

2. root アカウントのコマンドラインで次のコマンドのいずれかを実行します：
   - 次のコマンドを使用して、TLS 1.2 プロトコルのサポートを有効または無効にします：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <値> -t d
     ```

   - 次のコマンドを使用して、TLS 1.3 プロトコルのサポートを有効または無効にします：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <値> -t d
     ```

   フラグの <値> パラメータを指定します：
   - `1`—TLS プロトコルのサポートを有効にします。
   - `0`—TLS プロトコルのサポートを無効にします。

# 外部サービスとの相互対話のためのネットワーク設定

Kaspersky Security Center Linux は、外部サービスと対話するために次のネットワーク設定を使用します。

ネットワーク設定

| ネットワーク設定 | アドレス | 説明 |
| --- | --- | --- |
| ポート：443<br>プロトコル：HTTPS | https://activation-v2.kaspersky.com | アプリケーションのアクティベーション。 |
| ポート：443<br>プロトコル：HTTPS | https://s00.upd.kaspersky.com<br>https://s01.upd.kaspersky.com<br>https://s02.upd.kaspersky.com<br>https://s03.upd.kaspersky.com<br>https://s04.upd.kaspersky.com<br>https://s05.upd.kaspersky.com<br>https://s06.upd.kaspersky.com<br>https://s07.upd.kaspersky.com<br>https://s08.upd.kaspersky.com<br>https://s09.upd.kaspersky.com<br>https://s10.upd.kaspersky.com<br>https://s11.upd.kaspersky.com<br>https://s12.upd.kaspersky.com<br>https://s13.upd.kaspersky.com<br>https://s14.upd.kaspersky.com<br>https://s15.upd.kaspersky.com<br>https://s16.upd.kaspersky.com<br>https://s17.upd.kaspersky.com<br>https://s18.upd.kaspersky.com<br>https://s19.upd.kaspersky.com<br>https://cm.k.kaspersky-labs.com | 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。 |
| ポート：443<br>プロトコル：HTTPS | https://www.kaspersky.co.jp/downloads | • 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。<br>• カスペルスキーサーバーにアクセスできるかどうかを確認しています。Kaspersky Security Center Linux は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。 |

| ネットワーク設定 | アドレス | 説明 |
| --- | --- | --- |
| ポート：80<br>プロトコル：HTTP | http://p00.upd.kaspersky.com<br>http://p01.upd.kaspersky.com<br>http://p02.upd.kaspersky.com<br>http://p03.upd.kaspersky.com<br>http://p04.upd.kaspersky.com<br>http://p05.upd.kaspersky.com<br>http://p06.upd.kaspersky.com<br>http://p07.upd.kaspersky.com<br>http://p08.upd.kaspersky.com<br>http://p09.upd.kaspersky.com<br>http://p10.upd.kaspersky.com<br>http://p11.upd.kaspersky.com<br>http://p12.upd.kaspersky.com<br>http://p13.upd.kaspersky.com<br>http://p14.upd.kaspersky.com<br>http://p15.upd.kaspersky.com<br>http://p16.upd.kaspersky.com<br>http://p17.upd.kaspersky.com<br>http://p18.upd.kaspersky.com<br>http://p19.upd.kaspersky.com<br>http://downloads0.kaspersky-labs.com<br>http://downloads1.kaspersky-labs.com<br>http://downloads2.kaspersky-labs.com<br>http://downloads3.kaspersky-labs.com<br>http://downloads4.kaspersky-labs.com<br>http://downloads5.kaspersky-labs.com<br>http://downloads6.kaspersky-labs.com<br>http://downloads7.kaspersky-labs.com<br>http://downloads8.kaspersky-labs.com<br>http://downloads9.kaspersky-labs.com<br>http://downloads.kaspersky-labs.com<br>http://cm.k.kaspersky-labs.com | 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート |
| ポート：443<br>プロトコル：HTTPS | https://ds.kaspersky.com<br>https://dc1.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com<br>https://dc1-cert.ksn.kaspersky-labs.com<br>https://dc1-cf.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-kas.ksn.kaspersky-labs.com<br>https://dc1-ml.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com<br>https://dc1.ksn.kaspersky-labs.com | Kaspersky Security Network の使用。 |

| ネットワーク設定 | アドレス | 説明 |
| --- | --- | --- |
| ポート：<br>443、1443<br>プロトコル：<br>HTTPS | https://ksn-a-stat-geo.kaspersky-labs.com<br>https://ksn-file-geo.kaspersky-labs.com<br>https://ksn-verdict-geo.kaspersky-labs.com<br>https://ksn-url-geo.kaspersky-labs.com<br>https://ksn-a-p2p-geo.kaspersky-labs.com<br>https://ksn-info-geo.kaspersky-labs.com<br>https://ksn-cinfo-geo.kaspersky-labs.com | Kaspersky Security Network の使用。 |
| ポート：<br>443、1443<br>Protocol:<br>KSN | ksn://ksn-a-p2p-geo.kaspersky-labs.com<br>ksn://ksn-a-stat-geo.kaspersky-labs.com<br>ksn://ksn-ca-geo.kaspersky-labs.com<br>ksn://ksn-cinfo-geo.kaspersky-labs.com<br>ksn://ksn-crypto-catm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com<br>ksn://ksn-crypto-hash-geo.kaspersky-labs.com<br>ksn://ksn-crypto-ipm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com<br>ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com<br>ksn://ksn-eu-stat-kmp.kaspersky-labs.com<br>ksn://ksn-file-geo.kaspersky-labs.com<br>ksn://ksn-his-geo.kaspersky-labs.com<br>ksn://ksn-info-geo.kaspersky-labs.com<br>ksn://ksn-kas-geo.kaspersky-labs.com<br>ksn://ksn-kddi.kaspersky-labs.com<br>ksn://ksn-ml-geo.kaspersky-labs.com<br>ksn://ksn-oui-geo.kaspersky-labs.com<br>ksn://ksn-pp.kaspersky-labs.com<br>ksn://ksn-src.kaspersky-labs.com<br>ksn://ksn-stat-geo.kaspersky-labs.com<br>ksn://ksn-tcert-geo.kaspersky-labs.com<br>ksn://ksn-url-geo.kaspersky-labs.com<br>ksn://ksn-verdict-geo.kaspersky-labs.com<br>ksn://mdr.ksn.kaspersky-labs.com<br>ksn://stat-eu.ksn.kaspersky-labs.com<br>ksn://stat-hq.ksn.kaspersky-labs.com<br>ksn://stat-ru.ksn.kaspersky-labs.com<br>ksn://stat-sa.ksn.kaspersky-labs.com<br>ksn://stat-sbr.ksn.kaspersky-labs.com | Kaspersky Security Network の使用。 |
| プロトコル：<br>HTTPS | https://click.kaspersky.com<br>https://redirect.kaspersky.com | インターフェイスからリンクをたどります。 |

| ネットワーク設定 | アドレス | 説明 |
| --- | --- | --- |
| ポート：80<br>プロトコル：HTTP | http://crl.kaspersky.com<br>http://ocsp.kaspersky.com | これらのサーバーは公開鍵インフラストラクチャ (PKI) の一部であり、カスペルスキーのデジタル署名証明書の有効性ステータスを確認するために必要です。CRL は失効した証明書のリストです。OCSP を使用すると、特定の証明書のステータスをリアルタイムで要求できます。これらのサーバーは、デジタル証明書との対話のセキュリティを確保し、起こり得る攻撃から保護するのに役立ちます。 |
| ポート：443<br>プロトコル：HTTPS | https://ipm-klca.kaspersky.com | マーケティング関連告知。 |

Kaspersky Security Center Linux と外部サービスとを適切に連携させるには、次の推奨事項を考慮してください：
- 組織のネットワーク機器およびプロキシサーバーのポート 443 および 1443 で、暗号化されていないネットワークトラフィックを許可する必要があります。
- 管理サーバーがカスペルスキーのアップデートサーバーおよび Kaspersky Security Network サーバーと通信する場合、証明書の置換によるネットワークトラフィックのハイジャック（MITM 攻撃）を回避する必要があります。

*klscflag ユーティリティを使用して、HTTP または HTTPS プロトコル経由でアップデートをダウンロードするには、次の手順を実行します：*

1. コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

2. HTTP プロトコル経由でアップデートをダウンロードする場合は、root アカウントで次のコマンドのいずれかを実行します：

   - 管理サーバーがインストールされたデバイスで：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - ディストリビューションポイントについて：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   HTTPS プロトコル経由でアップデートをダウンロードする場合は、root アカウントで次のコマンドのいずれかを実行します：

   - 管理サーバーがインストールされたデバイスで：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - ディストリビューションポイントについて：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

# サブネットのグローバルリスト

使用する管理サーバーごとに、サブネットのグローバルリストを設定して、ネットワークのサブネットに関する情報を保存できます。リストは、IP アドレスとマスクのペアと支社などの物理的な単位を対応させる上で役立ちます。ネットワークのルールと設定でこのリストにあるサブネットを使用できます。

*サブネットのグローバルリストにサブネットを追加するには*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**グローバルサブネット**］セクションを選択します。
3. ［**追加**］をクリックします。
   ［**新規サブネット**］ウィンドウが表示されます。
4. 次のフィールドに値を入力します：
   - **名前**
   - **サブネットアドレス**
   - **サブネットマスク**
   - **説明**
5. ［**保存**］をクリックします。

   ウィンドウが閉じられ、サブネットがサブネットのリストに表示されます。

必要に応じて、グローバルサブネットのリストで次の操作を実行できます：

- 必要なサブネットを選択し、［**削除**］をクリックして、リストからサブネットを削除します。
- 必要なサブネットの名前のリンクをクリックし、手順 4 ～ 5 で説明されているアクションを実行して、サブネットのプロパティを変更します。

# klscmodchk および integrity_checker ユーティリティを使用してモジュールの整合性をチェックします

Kaspersky Security Center Linux には、動的にリンクされたライブラリ、実行ファイル、設定ファイル、およびインターフェイスファイルの形式で複数のバイナリモジュールが含まれています。侵入者は、1つ以上の実行可能モジュールまたはアプリケーションファイルを、悪意のあるコードを含む他のファイルに置き換えることができます。モジュールとファイルの置換を防ぐために、Kaspersky Security Center Linux は、klscmodchk および integrity_checker ユーティリティを使用してコンポーネントの整合性チェックを提供します。これらのユーティリティは、モジュールとファイルに不正な変更や破損がないかチェックします。モジュールまたはアプリケーションファイルのチェックサムが正しくない場合は、破損していると判断されます。

klscmodchk ユーティリティは、次の Kaspersky Security Center Linux コンポーネントの整合性チェックを実行します：

- 管理サーバー
- ネットワークエージェント

integrity_checker ユーティリティは、次の Kaspersky Security Center Linux コンポーネントの整合性チェックを実行します：

- 管理サーバー
- ネットワークエージェント
- Kaspersky Security Center Web コンソール

どちらのユーティリティも、Kaspersky Security Center Linux ビルドの一部であり、インストールフォルダーにある kl_file_integrity_manifest.xml マニフェストファイルに基づいてモジュールの整合性をチェックします。コンポーネントマニフェストファイルには、Kaspersky Security Center Linux コンポーネントの正しい動作に整合性が重要なファイルが含まれています。マニフェストファイル自体の整合性もチェックされます。

kl_file_integrity_manifest.xml マニフェストファイルを変更することは、デジタル署名が無効になり、整合性チェックが失敗するため、強くお勧めしません。

Kaspersky Security Center Linux コンポーネントの整合性をチェックするには、次のいずれかのコマンドを実行します：

- **`$ klscmodchk [ パラメータ ]`**

  klscmodchk ユーティリティは、`--verbose` パラメータを使用して integrity_checker ユーティリティを起動し、モジュールの整合性をチェックします。

  klscmodchk ユーティリティのパラメータ：

  - `-logfile <log_file_path>` —ログ記録用のディスク上のファイルへのパスを指定します。既定では、情報はコンソールに出力されます。
  - `-verbose` —整合性チェック中に拡張情報を出力します。

- **`$ integrity_checker [ パラメータ ] <マニフェストファイルパス>`**

  integrity_checker ユーティリティのパラメータ：

  - `--help` — integrity_checker ユーティリティのヘルプを表示します。
  - `--version` — integrity_checker ユーティリティのバージョンを表示します。
  - `--verbose` —ユーティリティの操作に関する情報を表示します。整合性チェックを実行する場合は、コマンドでこのパラメータを使用するだけで十分です。

各マニフェストファイルのチェック結果は、マニフェストファイル名の横に次の形式で表示されます：

- 成功 - ファイルの整合性が確認されました (戻りコード 0)。
- 失敗 - ファイルの整合性が確認されませんでした（ゼロ以外の戻りコード）。

アプリケーションの起動時に整合性チェックが自動的に開始されるように設定することもできます。既定では、自動的な整合性チェックは無効になっています。

*自動的な整合性チェックを有効にするには：*

1. 管理サーバーがインストールされているデバイスの Windows コマンドプロンプトで、次のコマンドを入力します：

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. デバイスを再起動します。

   自動的な整合性チェックが有効になります。

Kaspersky Security Centerの次回実行時に、klscmodchk ユーティリティが管理サーバーと一緒に実行され、モジュールの整合性チェックが開始されます。整合性チェックの結果は、Kaspersky イベントログに書き込まれます。

# ネットワーク接続されたデバイスの検出

このセクションでは、ネットワーク接続されたデバイスを検出するプロセスについて説明します。

Kaspersky Security Center Linux では、条件を指定してデバイスを検索できます。検索結果をテキストファイルに保存できます。

デバイスの検出機能により、次のデバイスを見つけることができます：

- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーの管理グループに属する管理対象デバイス
- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーで管理される未割り当てデバイス

# ネットワーク接続されたデバイスの検出シナリオ

セキュリティ製品のインストール前にデバイスの検索を実行する必要があります。ネットワーク接続されたデバイスがすべて検出されると、これらのデバイスに関する情報を取得しポリシーを通してデバイスを管理できます。ネットワーク内に新しいデバイスが存在するか、また過去に検出されたデバイスが現在もネットワーク内に存在するかを確認するには、定期的なネットワークポーリングが必要です。

ネットワーク上のデバイスの検出は、以下の手順で進みます：

1. **最初のデバイス検出**

   クイックスタートウィザードを完了したら、デバイスの検索を手動で実行してください。

2. **ポーリングのスケジュール設定**

   IP アドレス範囲のポーリングがオンになっていることと、ポーリングのスケジュール設定が社内で要求される条件を満たしていることを確認します。ポーリングのスケジュールを設定する際には、ネットワークポーリングの頻度に関する推奨事項を参照してください。

   ネットワークに Ipv6 デバイスが含まれている場合は Zeroconf ポーリングを有効にすることができます。

   ネットワークに接続されたデバイスがドメインに含まれている場合は、ドメインコントローラーのポーリングを使用することを推奨します。

3. **検出されたデバイスを管理グループに追加するルールの設定（任意）**

   ネットワーク内に新しいデバイスが追加された場合、これらのデバイスは定期的なポーリング中に検出され、［**未割り当てデバイス**］グループに含まれます。必要に応じて、［**管理対象デバイス**］にこれらのデバイスを自動的に移動するルールを設定できます。また、保持ルールを確立することもできます。

   このルール設定のステップを省略した場合、新しく検出されたデバイスはすべて［**未割り当てデバイス**］グループに割り当てられ、そこから移動しません。必要に応じて、これらのデバイスを［**管理対象デバイス**］グループに手動で移動できます。デバイスを［**管理対象デバイス**］グループに手動で移動する場合、各デバイスの情報を分析し、管理グループに移動するかどうかやどの管理グループに移動するかを決定できます。

### 結果

これらのステップがすべて完了すると、次の状態を実現できます：

- Kaspersky Security Center Linux 管理サーバーがネットワーク内のデバイスを検出し、その情報を利用できるようになります。
- ポーリングのスケジュールが設定され、指定したスケジュールに従ってポーリングが実行されます。

新しく検出されたデバイスは、設定されたルールに従って配置されます（または、ルールが設定されていない場合、デバイスは［**未割り当てデバイス**］グループに割り当てられたままになります）。

# Windows ネットワークのポーリング

## Windows ネットワークのポーリングの概要

Kaspersky Security Center Linux 管理サーバーは、Windows ネットワークポーリングをサポートしていません。Windows ベースのディストリビューションポイントを使用して、Windows ネットワークをポーリングします。

簡易ポーリングの間、ディストリビューションポイントは、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して次の情報が要求されます：

- オペレーティングシステムの名前
- IP アドレス
- DNS 名
- NetBIOS 名

簡易ポーリングと完全ポーリングの両方で次の要件を満たす必要があります：

- UDP 137/138、TCP 139、UDP 445、TCP 445 ポートをネットワーク内で利用できる必要があります。
- SMB プロトコルが有効になっています。
- Microsoft のコンピューターブラウザーサービスを使用し、管理サーバー上でプライマリブラウザーコンピューターが有効である必要があります。
- Microsoft のコンピューターブラウザーサービスを必ず使用し、クライアントデバイス上でプライマリブラウザーコンピューターが有効であり、かつ次の条件を満たす必要があります：
  - ネットワークデバイスが 32 台以内の場合、1 台以上のデバイスで実行する
  - ネットワークデバイス 32 台につき、1 台以上のデバイスで

完全ポーリングは簡易ポーリングを 1 回以上実行している場合にのみ実行できます。

## Windows ネットワークのポーリング設定の表示と変更

*Windows ネットワークのポーリングのプロパティを変更するには：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**Windows ドメイン**］の順に移動します。
2. ［**プロパティ**］をクリックします。

   Windows ドメインのプロパティウィンドウが開きます。
3. ［**Windows ネットワークのポーリングを有効にする**］を使用して、Windows ネットワークのポーリングをオンまたはオフにします。
4. ポーリングスケジュールを設定します。既定では、簡易ポーリングが 15 分ごとに、完全ポーリングが 60 分ごとに実行されます。

   ポーリングスケジュールのオプション：

   - **N 日ごと**

     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。

     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。
   - **N 分ごと**

     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
   - **曜日ごと**

     指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
   - **毎月、選択した週の指定日**

     毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
   - **未実行のタスクを実行する**

     ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

     このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

     このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

     既定では、このオプションはオフです。
5. ［**保存**］をクリックします。

プロパティが保存され、検出されたすべての Windows ドメインおよびワークグループに適用されます。

### 手動でのポーリングの実行

*手動でポーリングを実行するには：*

［**簡易ポーリングの開始**］または［**完全ポーリングの開始**］をクリックします。

ポーリングの完了後、［**Windows ドメイン**］ページでドメイン名に隣接するチェックボックスをオンにして［**デバイス**］をクリックすると、検出されたデバイスのリストを表示できます。

# IP アドレス範囲のポーリング

Kaspersky Security Center Linux は、通常の DNS 要求を使用して、指定された範囲のすべての IPv4 アドレスに対して、IP アドレスを DNS 名へ解決する逆引きの名前解決を試行します。この処理が成功すると、取得した名前に対してサーバーは「`ICMP ECHO REQUEST`（Ping コマンドと同一）」を送信します。これに対してデバイスが応答した場合、デバイスの情報が Kaspersky Security Center Linux のデータベースに追加されます。逆引きの名前解決は、IP アドレスを付与されているがコンピューターではないネットワークデバイス（ネットワークプリンターやルーターなど）を除外するために必要です。

このポーリング方法は、ローカル DNS サービスが適切に構成されているかどうかに依存します。ローカル DNS サービスで、逆引きの検索ゾーンが設定されている必要があります。逆引きの検索ゾーンが設定されていない場合、IP アドレス範囲のポーリングを実行しても、ポーリング結果は得られません。

Kaspersky Security Center Linux は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center Linux がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center Linux は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center Linux は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。

IP アドレス範囲のポーリングのみが有効になっている場合、Kaspersky Security Center Linux は Ipv4 アドレスを持つデバイスのみを検出します。ネットワークに Ipv6 デバイスが含まれる場合は、デバイスの Zeroconf ポーリングをオンにします。

Microsoft Active Directory または Samba ドメインコントローラ内のすべての Linux ベースのホストに対して、`/etc/samba/smb.conf` ファイルで `netbios name` と `workgroup` パラメータを指定します。そうしないと、ポーリング結果に重複したホストが含まれる可能性があります。

# IP アドレス範囲のポーリング設定の表示と変更

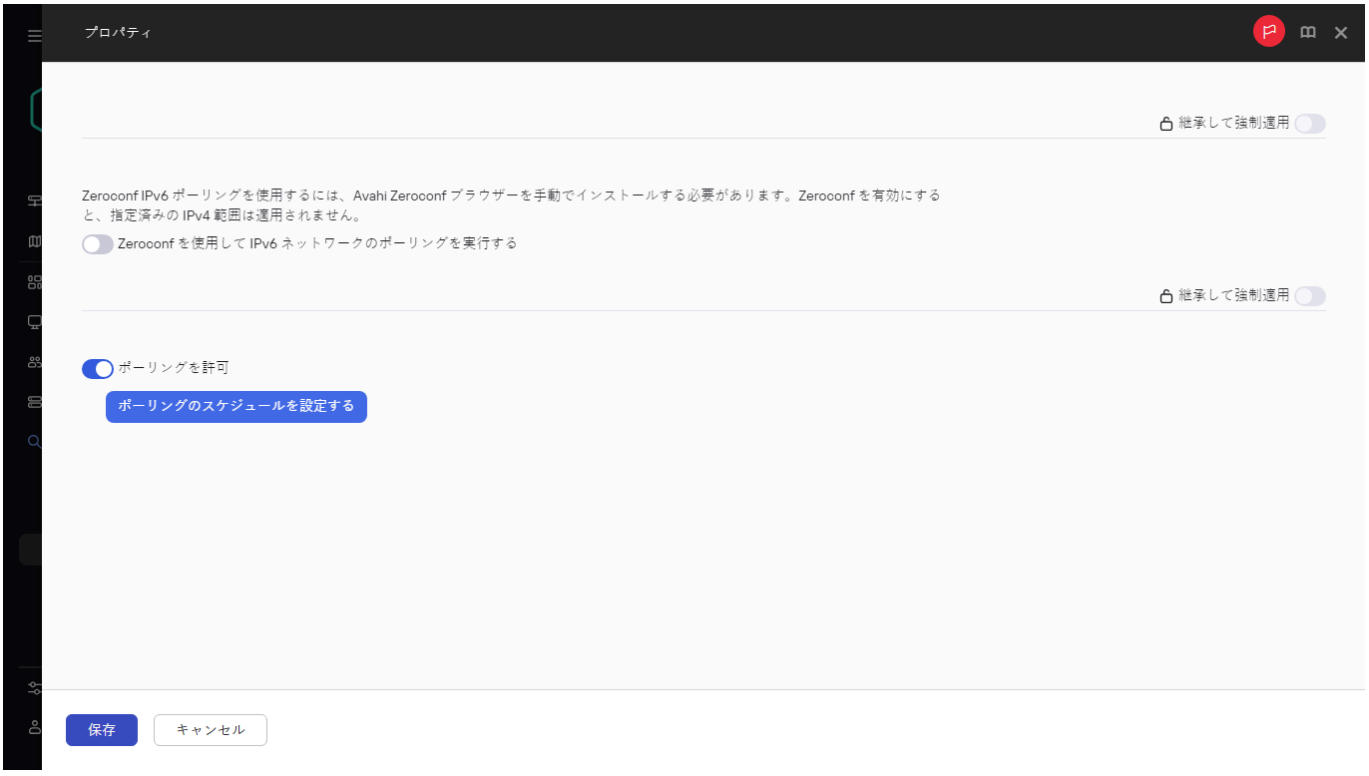
*IP アドレス範囲のポーリング設定の表示と変更を行うには：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。




IP 範囲リスト。

2. ［**プロパティ**］をクリックします。
   IP ポーリングのプロパティウィンドウが開きます。




IP ポーリングのプロパティ

3. ［**ポーリングを許可**］を使用して、IP ポーリングをオンまたはオフにします。

4. ポーリングスケジュールを設定します。既定では、IP ポーリングは 420 分（7 時間）ごとに実行されます。

   ポーリング間隔の指定時には、指定する値が［IP アドレスの有効期間］の値を超えないように注意してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。

   ポーリングスケジュールのオプション：

   - **N 日ごと**

     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

   - **N 分ごと**

     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

   - **曜日ごと**

     指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

   - **毎月、選択した週の指定日**

     毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

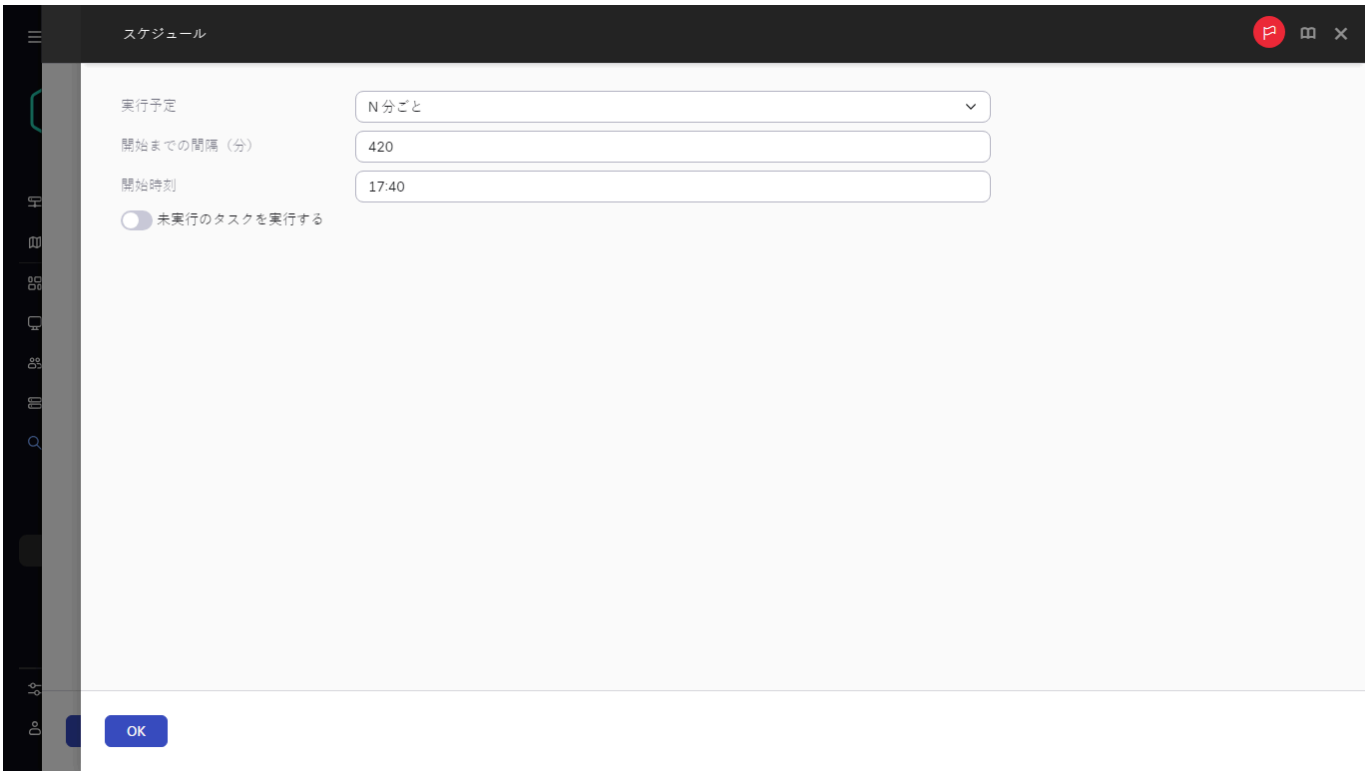
   - **未実行のタスクを実行する**

ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

既定では、このオプションはオフです。




ポーリングスケジュールの設定

5. ［**保存**］をクリックします。

プロパティが保存され、すべての IP アドレス範囲に適用されます。

## 手動でのポーリングの実行

*手動でポーリングを実行するには：*

［**ポーリングを開始する**］をクリックします。

# IP アドレス範囲の追加と変更

Kaspersky Security Center Linux は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center Linux がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center Linux は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center Linux は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。自動的に定義された IP アドレス範囲を編集したり、カスタム IP アドレス範囲を追加できます。

IPv4 アドレスに対してのみ範囲を作成できます。Zeroconf ポーリングを有効にしている場合は、Kaspersky Security Center Linux はネットワーク全体をポーリングします。

*新しい IP アドレス範囲を追加するには：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。




IP 範囲リスト。

2. 新しい IP アドレス範囲を追加するには、［**追加**］をクリックします。

3. 表示されたウィンドウで、次の設定を行います：

- **IP アドレス範囲の名前**

  IP アドレス範囲の名前。「192.168.0.0/24」のように、指定した IP アドレス範囲自体を名前として使用することもできます。

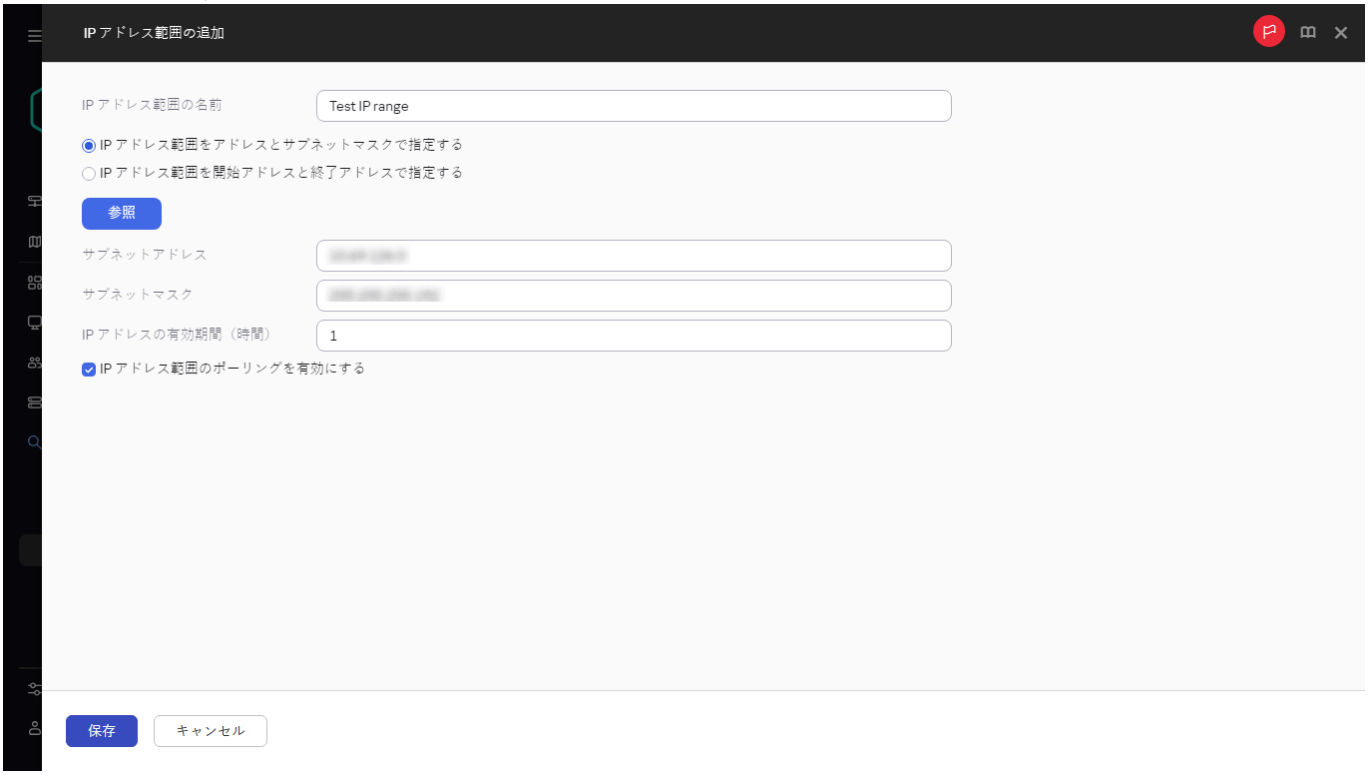
- **IP 区間またはサブネットアドレスとマスク**

  開始 IP アドレスと終了 IP アドレスを指定するか、サブネットアドレスとサブネットマスクを指定して、IP アドレス範囲を設定します。［**参照**］をクリックして、既存の IP アドレス範囲を選択することもできます。

- **IP アドレスの有効期間（時間）**

  このパラメータの指定時には、値がポーリングのスケジュールで指定したポーリング間隔を超えるように指定してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。

4. 追加したサブネットまたは IP アドレスの区間をポーリングするには、［**IP アドレス範囲のポーリングを有効にする**］をオンにします。そうでない場合、追加したサブネットまたは IP 区間を対象としたポーリングは実行されません。




IP 範囲設定の指定

5. ［**保存**］をクリックします。

IP アドレス範囲のリストに新しい IP アドレス範囲が追加されます。

［**ポーリングを開始する**］を使用して、IP アドレス範囲ごとに個別にポーリングを実行できます。既定では、ポーリング結果の有効期間は 24 時間で、これは IP アドレスの有効期間と同じ長さです。

*既存の IP アドレス範囲にサブネットを追加するには：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。
2. サブネットを追加する IP アドレス範囲の名前をクリックします。
3. ウィンドウが表示されたら、［**追加**］をクリックします。
4. サブネットアドレスとサブネットマスクを指定するか、開始 IP アドレスと終了 IP アドレスを指定して、IP アドレス範囲を指定します。または、［**参照**］をクリックして既存のサブネットを追加することもできます。
5. ［**保存**］をクリックします。

   IP アドレス範囲に新しいサブネットが追加されます。
6. ［**保存**］をクリックします。

IP アドレス範囲の新しい設定が保存されます。

サブネットは、個数の制限なく必要な数だけ追加できます。名前のある IP アドレス範囲同士での範囲の重複は許可されていませんが、1 つの IP アドレス範囲内の名前のないサブネット（IP 区間同士）にはそうした制限はありません。IP アドレス範囲ごとのポーリングを個別にオンまたはオフに切り替えることができます。

# Zeroconf ポーリング

この検索方法は Linux ベースのディストリビューションポイントでのみサポートされます。

Kaspersky Security Center Linux は IPv6 アドレスのデバイスを含むネットワークを検索できるようになりました。この場合、IP 範囲は指定されず、Kaspersky Security Center Linux はネットワーク全体をゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して検索します。Zeroconf の使用を開始するには、ネットワークをポーリングする Linux デバイス（管理サーバーまたはディストリビューションポイント）で avahi-browse ユーティリティをインストールする必要があります。

*Zeroconf ポーリングを有効にするには：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。
2. ［**プロパティ**］をクリックします。
3. ウィンドウが表示されたら、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにします。

その後、Kaspersky Security Center Linux はネットワークの検索を開始します。この場合、指定された IP 範囲は無視されます。

# ドメインコントローラーのポーリング

Kaspersky Security Center Linux は、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングをサポートしています。Samba ドメインコントローラーの場合、Samba 4 が Active Directory ドメインコントローラーとして使用されます。

ドメインコントローラーをポーリングすると、管理サーバーまたはディストリビューションポイントは、ドメイン構造、ユーザーアカウント、セキュリティ グループ、およびドメインに含まれるデバイスの DNS 名に関する情報を取得します。

すべてのネットワークに接続されたデバイスがドメインのメンバーである場合は、ドメインコントローラーのポーリングを使用することを推奨します。ネットワークに接続されたデバイスの一部がドメインに含まれていない場合、これらのデバイスはドメインコントローラーのポーリングでは検出できません。

サーバーは、Microsoft Active Directory のポーリング中に ICMP エコー要求（ping コマンドと同じ）を送信します。

## 必須条件

ドメインコントローラーをポーリングする前に、ファイアウォールまたはプロキシサーバー経由でドメインコントローラーへの接続を許可していることを確認してください。また、ドメインコントローラーで次のプロトコルが有効になっていることを確認してください。

- ライトウェイトディレクトリアクセスプロトコル（LDAP）
- 簡易認証およびセキュリティ層（SASL）

  このプロトコルは、SASL 認証を使用してドメインコントローラーへの接続が確立される場合に使用されます。管理サーバーおよびディストリビューションポイントは、DIGEST-MD5 メカニズムのみをサポートします。
- セキュアソケットレイヤー経由の軽量ディレクトリアクセスプロトコル（LDAPS）

  このプロトコルは、暗号化された接続を介してドメインコントローラーに接続する必要がある場合に使用されます。

ドメインコントローラーデバイスで次のポートが使用可能であることを確認してください：

- LDAP プロトコルおよび簡易認証（SASL を含む）の場合は 389
- LDAPS プロトコルの場合は 636

Microsoft Active Directory または Samba ドメインコントローラ内のすべての Linux ベースのホストに対して、`/etc/samba/smb.conf` ファイルで `netbios name` と `workgroup` パラメータを指定します。そうしないと、ポーリング結果に重複したホストが含まれる可能性があります。

# 管理サーバーを使用したドメインコントローラーのポーリング

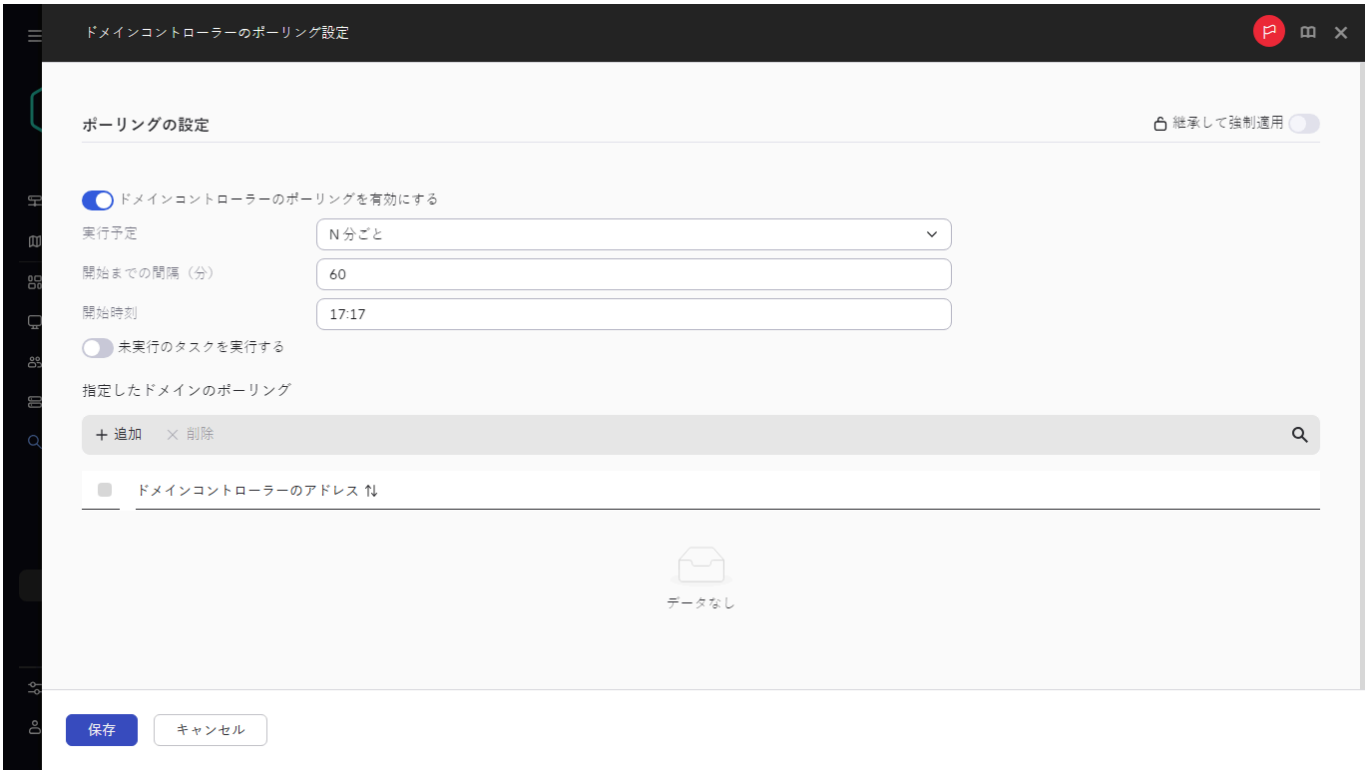
*管理サーバーを使用してドメインコントローラーをポーリングするには、次の手順を実行します：*

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**ドメインコントローラー**］の順に移動します。




ドメインコントローラーのポーリングウィンドウ

2. ［**ポーリングの設定**］をクリックします。
［**ドメインコントローラーのポーリング設定**］ウィンドウが開きます。




ドメインコントローラーのポーリング設定

3. ［**ドメインコントローラーのポーリングを有効にする**］をオンにします。

4. ［**指定したドメインのポーリング**］で［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

5. 必要に応じて、［**ドメインコントローラーのポーリング設定**］ウィンドウでポーリングスケジュールを指定します。既定では、時間は1時間です。次のポーリングで受信したデータは、古いデータと完全に置き換わります。

   ポーリングスケジュールには次のオプションがあります：

   - **N 日ごと**

     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。

     既定では、現在のシステム日時から、1日ごとにポーリングが実行されます。

   - **N 分ごと**

     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

   - **曜日ごと**

     指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

   - **毎月、選択した週の指定日**

     毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

   - **未実行のタスクを実行する**

     ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

     このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

     このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

     既定では、このオプションはオフです。

   ドメインのセキュリティグループ内のユーザーアカウントを変更した場合、ドメインコントローラーをポーリングしてから1時間後に、これらの変更が Kaspersky Security Center Linux に表示されます。

6. ［**保存**］をクリックして変更を適用します。

7. すぐにポーリングを実行するには、［**ポーリングを開始する**］をクリックします。

## ディストリビューションポイントを使用したドメインコントローラーのポーリング

ディストリビューションポイントを使用してドメインコントローラーをポーリングすることもできます。Windows または Linux ベースの管理対象デバイスは、ディストリビューションポイントとして機能できます。

Linux ディストリビューションポイントの場合、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングがサポートされています。
Windows ディストリビューションポイントの場合、Microsoft Active Directory ドメインコントローラーのポーリングのみがサポートされます。
Mac ディストリビューションポイントを使用したポーリングはサポートされていません。

*ディストリビューションポイントを使用してドメインコントローラーのポーリングを設定するには：*

1. ディストリビューションポイントのプロパティを開きます。
2. ［**ドメインコントローラーのポーリング**］セクションを選択します。
3. ［**ドメインコントローラーのポーリングを有効にする**］をオンにします。
4. ポーリングするドメインコントローラーを選択します。

   Linux ディストリビューションポイントを使用する場合は、［**指定したドメインのポーリング**］セクションで、［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

   Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

   - **現在のドメインのポーリング**
   - **ドメインフォレスト全体のポーリング**
   - **指定したドメインのポーリング**
5. 必要に応じて、［**ポーリングのスケジュールを設定する**］をクリックして、ポーリングスケジュールオプションを指定します。

   ポーリングは、指定されたスケジュールに従ってのみ開始されます。ポーリングを手動で開始することはできません。

ポーリングが完了すると、ドメイン構造が［**ドメインコントローラー**］セクションに表示されます。

デバイス移動ルールを設定しオンにしている場合、新たに検出されたデバイスは自動的に**管理対象デバイス**グループに含まれます。移動ルールがオンでない場合、新たに検出されたデバイスは自動的に**未割り当てデバイス**グループに含まれます。

検出されたユーザーアカウントは、Kaspersky Security Center Web コンソールでのドメイン認証に使用できます。

# 認証とドメインコントローラーへの接続

## ドメインをポーリングする際の認証とドメインコントローラーへの接続

ドメインコントローラーをポーリングする時、管理サーバーまたはディストリビューションポイントは、ドメインコントローラーへの初期接続を確立するための接続プロトコルを識別します。このプロトコルは、ドメインコントローラーへの今後のすべての接続に使用されます。ドメインコントローラーへの初期接続を確立する時に、ネットワークエージェントフラグ（KLNAG_LDAP_TLS_REQCERT および KLNAG_LDAP_SSL_CACERT）を使用して接続オプションを変更できます。この記事で説明されているように、klscflag を使用してネットワークエージェントフラグを構成できます。

ドメインコントローラーへの最初の接続は次のように行われます：

1. 管理サーバーまたはディストリビューションポイントは、LDAPS 経由でドメインコントローラーに接続しようとします。

   既定では、証明書の検証は必要ありません。証明書の検証を実施するには、 KLNAG_LDAP_TLS_REQCERT フラグを 1 に設定します。

   KLNAG_LDAP_TLS_REQCERT フラグに指定できる値：

   - 0 – 証明書が要求されますが、証明書が提供されない場合や証明書の検証が失敗した場合でも、TLS 接続は正常に作成されたと判断されます（既定値）。
   - 1 – LDAP サーバー証明書の厳密な検証が必要です。

   既定では、 KLNAG_LDAP_SSL_CACERT フラグが指定されていない場合、OS 依存の認証局（CA）へのパスが証明書チェーンへのアクセスに使用されます。KLNAG_LDAP_SSL_CACERT フラグを使用してカスタムパスを指定します。

2. LDAPS 接続が失敗した場合、管理サーバーまたはディストリビューションポイントは、SASL（DIGEST-MD5）を使用して、暗号化されていない TCP 接続経由でドメインコントローラーに接続しようとします。

## 管理サーバーにドメインユーザーを認証する際の認証とドメインコントローラーへの接続

ドメインユーザーが管理サーバー上で認証すると、管理サーバーはドメインコントローラーへの接続を確立するためのプロトコルを識別します。

ドメインコントローラーへの接続は次のように行われます：

1. 管理サーバーは、LDAPS 経由でドメインコントローラーへの接続を試行します。

   LDAP サーバー証明書の厳密な検証が必要です。

   既定では、 KLNAG_LDAP_SSL_CACERT フラグが指定されていない場合、OS 依存の認証局（CA）へのパスが証明書チェーンへのアクセスに使用されます。KLNAG_LDAP_SSL_CACERT フラグを使用してカスタムパスを指定します。

2. LDAPS 接続が失敗すると、ドメインコントローラーへの接続エラーが発生し、他の接続プロトコルは使用されません。

### フラグの設定

klscflag ユーティリティを使用してフラグを設定できます。

コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。管理サーバーデバイスでは、klscflag ユーティリティはインストールディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

たとえば、次のコマンドは証明書の検証を強制します：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

# Samba ドメインコントローラーの設定

Kaspersky Security Center Linux は、Samba 4 上でのみ実行される Linux ドメインコントローラーをサポートします。

Samba ドメインコントローラーは、Microsoft Active Directory ドメインコントローラーと同じスキーマ拡張をサポートします。Samba 4 スキーマ拡張機能を使用すると、Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーとの完全な互換性を有効にすることができます。これはオプションのアクションです。

Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にすることを推奨します。これにより、Kaspersky Security Center Linux と Samba ドメインコントローラー間の適切な対話が保証されます。

*Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にするには、次の手順を実行します：*

1. RFC2307 スキーマ拡張を使用するには、次のコマンドを実行します：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba ドメインコントローラーでスキーマのアップデートを有効にします。これを行うには、ファイル `/etc/samba/smb.conf` に以下の行を追加します。

   ```
   dsdb:schema update allowed = true
   ```

   スキーマのアップデートがエラーで完了した場合は、スキーママスターとして機能するドメインコントローラーの完全な復元を実行する必要があります。

Samba ドメイン コントローラ内のすべての Linux ベースのホストに対して、`/etc/samba/smb.conf` ファイルで `netbios name` と `workgroup` パラメータを指定します。そうしないと、ポーリング結果に重複したホストが含まれる可能性があります。

# 機器のインベントリ

機器の在庫管理に使用するハードウェアリスト（[**操作**] → [**リポジトリ**] → [**ハードウェア**]）は、自動と手動の 2 つの方法で追加されます。各ネットワークポーリングの後、検出されたすべてのデバイスが自動的にリストに追加されます。ただし、ネットワークをポーリングしない場合は、デバイスを手動で追加することもできます。ルーター、プリンター、デバイスハードウェアなど、他のデバイスを手動でリストに追加できます。

デバイスの詳細情報の確認と編集は、デバイスのプロパティで行うことができます。

ハードウェアリストには、次の種別のデバイスが含まれます：

- コンピューター
- モバイルデバイス
- ネットワークデバイス
- 仮想デバイス
- OEM コンポーネント
- コンピューター周辺機器
- 接続されているデバイス
- VoIP 電話
- ネットワークリポジトリ

管理者は、検出されたデバイスに*企業用*属性を割り当てることができます。この属性は、デバイスのプロパティで手動で割り当てることができます。また、この属性を自動的に割り当てる基準を管理者が指定することもできます。この場合、*企業用*属性はデバイスの種類に応じて割り当てられます。

Kaspersky Security Center Linux では、機器を抹消することができます。これを行うには、デバイスのプロパティで［**抹消済み**］オプションを選択します。抹消済みデバイスは機器リストに表示されません。

管理者は［**ハードウェア**］フォルダー内のプログラマブルロジックコントローラー（PLC）のリストを管理することができます。PLC リストの管理方法の詳細については、『*Kaspersky Industrial CyberSecurity for Nodes User Guide*』に記載されています。

# 新しいデバイスに関する情報の追加

*ネットワーク上の新しいデバイスに関する情報を追加するには：*

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**ハードウェア**］の順に選択します。
2. ［**追加**］をクリックして、[**新しいデバイス**］ウィンドウを開きます。
3. ［**新しいデバイス**］ウィンドウの［**デバイス種別**］から、追加したいデバイス種別を選択します。

4. ［**OK**］をクリックします。

   デバイスのプロパティウィンドウの［**全般**］セクションが表示されます。

5. ［**全般**］セクションの各フィールドにデバイスに関する情報を入力します。［**全般**］セクションには、次の設定項目があります：

   - **企業用デバイス**：デバイスに*企業用*属性を割り当てたい場合は、チェックボックスをオンにします。この属性を使用して、［**ハードウェア**］フォルダーでデバイスを検索できます。
   - **抹消済み**。［**ハードウェア**］フォルダーのデバイスのリストにデバイスが表示されないようにする場合は、このチェックボックスをオンにします。

6. ［**適用**］をクリックします。

   ［**ハードウェア**］フォルダーのワークスペースに新しいデバイスが表示されます。

# 企業用デバイスの定義に使用する基準の設定

*企業用デバイスの検出基準を設定するには：*

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**ハードウェア**］の順に選択します。
2. ［**ハードウェア**］ページの上部にある［**企業用デバイスのルールの設定**］をクリックします。

   ［**企業用デバイスのルールの設定**］パネルが呼び出されます。
3. ［**企業用デバイスのルールの設定**］パネルで、［**デバイスに企業用デバイス属性を自動で設定**］を有効にします。*エンタープライズ*属性が自動的に割り当てられるデバイスタイプを指定します。

   このオプションは、ネットワークポーリングによって追加されたデバイスにのみ影響します。手動で追加したデバイスの場合は、*企業*属性を手動で設定してください。
4. ［**OK**］をクリックします。

企業用デバイスの検出条件が設定されました。

# VDI 向け動的モードのクライアントデバイスでの使用

一時的な仮想マシンを使用して、企業ネットワークに仮想インフラストラクチャを導入できます。Kaspersky Security Center Linux は一時的な仮想マシンを検出し、それらに関する情報を管理サーバーのデータベースに追加します。一時的な仮想マシンの使用を終了した後、このマシンは仮想インフラストラクチャから削除されます。ただし、削除された仮想マシンに関する記録は、管理サーバーのデータベースに保存可能です。また、存在しない仮想マシンが Kaspersky Security Center Web コンソールに表示されることがあります。

存在しない仮想マシンに関する情報が保存されるのを防ぐため、Kaspersky Security Center Linux は仮想デスクトップインフラストラクチャ（VDI）向け動的モードをサポートしています。管理者は、一時的な仮想マシンにインストールされるネットワークエージェントのインストールパッケージのプロパティで、VDI 向け動的モードのサポートを有効にできます。

一時的な仮想マシンが無効になっている場合、ネットワークエージェントは管理サーバーに仮想マシンが無効化されていることを通知します。仮想マシンが正常に無効化されると、その仮想マシンは管理サーバーに接続されているデバイスのリストから削除されます。仮想マシンの無効化でエラーが発生し、無効化された仮想マシンに関する通知をネットワークエージェントが管理サーバーに送信しない場合、バックアップシナリオが使用されます。このシナリオでの仮想マシンは、管理サーバーとの同期に 3 回失敗すると、管理サーバーに接続されているデバイスのリストから削除されます。

# ネットワークエージェントインストールパッケージのプロパティでの VDI 向け動的モードの有効化

*VDI 向け動的モードを有効にするには：*

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
2. ネットワークエージェントのインストールパッケージのコンテキストメニューで［**プロパティ**］を選択します。

   ［**プロパティ**］ウィンドウが表示されます。
3. ［**プロパティ**］ウィンドウで［**詳細**］セクションを選択します。
4. ［**詳細**］セクションで、［**VDI 向け動的モードを有効にする**］を選択します。

ネットワークエージェントがインストールされるデバイスが VDI の一部になります。

# VDI から管理グループへのデバイスの移動

*VDI を構成するデバイスを管理グループへ移動するには：*

1. ［**アセット（デバイス）**］-［**移動ルール**］タブの順に移動します。
2. ［**追加**］をクリックします。
3. ［**ルールの条件**］タブで、［**仮想マシン**］タブを選択します。
4. ［**仮想マシン**］ルールを［**はい**］に設定し、［**仮想デスクトップインフラストラクチャの一部**］を［**はい**］に設定します。
5. ［**保存**］をクリックします。

# クライアントデバイスの管理

Kaspersky Security Center Linux では、クライアントデバイスを管理することができます。

- クラスタやサーバーアレイなどの管理対象デバイスの設定とステータスを表示します。
- ディストリビューションポイントの設定。
- タスクの管理。

管理グループを使用すると、クライアントデバイスを1つのユニットとして管理できるセットにまとめることができます。クライアントデバイスは1つの管理グループにのみ含めることができます。［**ルールの条件**］に基づいてデバイスをグループに自動的に割り当てることができます。

- デバイス移動ルールの作成。
- デバイス移動ルールのコピー。
- デバイス移動ルールの条件。

デバイスの抽出を使用すると、条件に基づいてデバイスをフィルタリングできます。抽出を作成したり、デバイスを検索したり、管理グループ間でデバイスを配置したりするために、デバイスにタグを付けることもできます。

# 管理対象デバイスの設定

*管理対象デバイスの設定を表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、目的のデバイス名のリンクをクリックします。

選択したデバイスのプロパティウィンドウが表示されます。

次のタブは、設定の主なグループを表すプロパティ ウィンドウの上部に表示されます。

- **全般**

このタブは次のセクションで構成されています。

- ［**全般**］セクションには、クライアントデバイスに関する全般的な情報が表示されます。情報は、クライアントデバイスと管理サーバーとの前回の同期中に受信されたデータに基づいて提供されます：

  - **名前**

    このフィールドでは、管理グループ内のクライアントデバイスの名前を表示したり変更したりできます。

  - **説明**

    このフィールドでは、クライアントデバイスの補足的な説明を入力できます。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **デバイスの所有者**

    デバイス所有者の名前。［**デバイスの所有者の管理**］をクリックすることにより、ユーザーをデバイスの所有者として割り当てたり削除したりすることができます。

  - **グループの完全名**

    クライアントデバイスが属する管理グループ。

  - **前回の定義データベースのアップデート**

    定義データベースまたはアプリケーションをデバイス上で前回アップデートした日付。

  - **管理サーバーへの接続**

    クライアントデバイスにインストールされたネットワークエージェントが管理サーバーに最後に接続した日時。

  - **前回の可視**

    デバイスが前回ネットワークで検出された日時。

  - **ネットワークエージェントのバージョン**

    インストールされているネットワークエージェントのバージョン。

- **作成**

  Kaspersky Security Center Linux 内でデバイスが作成された日付。

- **管理サーバーから切断しない**

  このオプションをオンにすると、管理対象デバイスと管理サーバー間の継続的な接続が維持されます。このような接続を提供するプッシュサーバーを使用していない場合は、このオプションを使用することをお勧めします。

  このオプションがオフで、プッシュサーバーが使用されていない場合、管理対象デバイスは、データの同期または情報の送信のためにのみ管理サーバーに接続します。

  ［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

  このオプションは、管理対象デバイスでは既定でオフになっています。このオプションは、管理サーバーがインストールされているデバイスでは既定でオンになっており、オフにしようとしてもオンのままになります。

- **セッション**

  このセクションには、現在デバイスにログインしているユーザーに関する情報を含むテーブルが含まれています。表には、対応する列に次のデータが表示されます：

  - ユーザー名
  - SAM アカウント名
  - ユーザープリンシパル名
  - メールアドレス

  ドメインユーザーのセッションに関する情報を正しく表示するには、ドメインコントローラーポーリングを使用する必要があります。

- ［**ネットワーク**］セクションには、クライアントデバイスのネットワークプロパティに関する次の情報が表示されます：

  - **IP アドレス**

    デバイスの IP アドレス。

  - **Windows ドメイン**

    デバイスを含むワークグループ。

  - **DNS 名**

    クライアントデバイスの DNS ドメイン名。

  - **NetBIOS 名**

クライアントデバイスの名前。

- **IPv6 アドレス**

- ［**システム**］セクションには、クライアントデバイスにインストールされているオペレーティングシステムに関する情報が表示されます。
  - **オペレーティングシステム**
  - **CPU アーキテクチャ**
  - **デバイス名**
  - **仮想マシンの種別**

    仮想マシンの製造元。

  - **動的仮想マシン（VDI の一部）**

    この行には、クライアントデバイスが VDI の一部である動的仮想マシンかどうかが表示されます。

- ［**プロテクション**］セクションには、次のようなクライアントデバイスにおけるアンチウイルスによる保護に関する現在のステータスが表示されます：

  - **可視**

    クライアントデバイスの可視性のステータス。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **ステータスの説明**

    クライアントデバイスの保護と管理サーバーへの接続のステータス。

  - **保護ステータス**

    クライアントデバイスのリアルタイム保護に関する現在のステータスが表示されます。

    デバイスのステータスに変更があると、新しいステータスは、クライアントデバイスと管理サーバーが同期された後にのみデバイスのプロパティウィンドウに表示されます。

  - **前回の完全スキャン**

    クライアントデバイスで前回のマルウェアスキャンが実行された日時。

  - **ウイルスが検知されました**

    セキュリティ製品のインストール後（最初のスキャンの場合）またはウイルスカウンターを前回リセットした後に、クライアントデバイスで検知された脅威の合計数。

  - **駆除できていないオブジェクト**

    クライアントデバイスにおける未処理ファイルの数。

    このフィールドは、モバイルデバイス上の未処理ファイルの数をスキップします。

  - **ディスク暗号化ステータス**

    デバイスのローカルドライブでのファイル暗号化の現在のステータス。ステータスの説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

    ファイルは、Kaspersky Endpoint Security for Windows がインストールされている管理対象デバイスでのみ暗号化できます。

- ［**製品が定義したデバイスのステータス**］セクションには、デバイスにインストールされている管理対象アプリケーションによって定義されたデバイスのステータスに関する情報が表示されます。このデバイスのステータスは、Kaspersky Security Center Linux によって定義されたものとは異なる場合があります。

- **アプリケーション**

  このタブには、クライアントデバイスにインストールされているすべてのカスペルスキー製品が一覧表示されます。このタブには、選択したカスペルスキー製品（ネットワークエージェントを除く）を開始および停止できる［**開始**］と［**停止**］があります。管理対象デバイスで管理サーバーからの受信プッシュ通知用にポート 15000 UDP が使用可能な場合は、これらのボタンを使用できます。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、［**開始**］と［**停止**］も使用できます。そうしないと、アプリケーションを起動または停止しようとすると、エラーメッセージが表示されます。また、アプリケーション名をクリックすると、アプリケーションに関する一般情報、デバイスで発生したイベントのリスト、およびアプリケーション設定が表示されます。

- **アクティブなポリシーとポリシーのプロファイル**

  このタブには、管理対象デバイスに現在割り当てられているポリシーとポリシープロファイルが一覧表示されます。

- **タスク**

  ［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、タスクの開始と停止、タスク設定の変更、実行結果の表示など、クライアントデバイスのタスクを管理できます。タスクのリストは、管理サーバーとの前回のクライアント同期セッション中に受信されたデータに基づいて提供されます。管理サーバーは、タスクステータスに関する情報をクライアントデバイスに要求します。管理対象デバイスで管理サーバーからのプッシュ通知を受信するためにポート 15000 UDP が使用可能な場合は、タスクのステータスが表示され、タスクを管理するためのボタンが有効になります。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、タスクによるアクションも利用できます。

  接続に失敗すると、ステータスは表示されず、ボタンは無効になります。

- **イベント**

  ［**イベント**］タブでは、選択したクライアントデバイスについて管理サーバーに記録されたイベントが表示されます。

- **セキュリティ問題**

  ［**セキュリティ問題**］タブでは、クライアントデバイスでのセキュリティ問題を表示、編集、作成できます。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。たとえば、定期的にマルウェアを自分のリムーバブルドライブからデバイスに移しているユーザーがいた場合、管理者はこの件のセキュリティ問題を作成できます。管理者はセキュリティ問題のテキストに、概要説明と推奨される処分（ユーザーに下す懲戒処分など）を記載したり、ユーザーへのリンクを追加することもできます。

  必要な処分がすべて行われたセキュリティ問題は、*処理済み*と呼ばれます。未処理のセキュリティ問題がある場合、デバイスのステータスを*緊急*または*警告*に変更する条件として選択できます。

  このセクションには、デバイス用に作成したセキュリティ問題のリストがあります。セキュリティ問題は、重要度と種別で分類されます。セキュリティ問題のタイプは、セキュリティ問題を作成するカスペルスキー製品によって定義されます。［**処理済み**］列のチェックボックスをオンにすると、リストにある処理済みのセキュリティ問題を強調表示できます。

- **タグ**

  ［**タグ**］タブでは、クライアントデバイスの検索に使用されるキーワードのリストを管理できます。また、既存のタグのリストの表示、リストからのタグの割り当て、自動タグ付けルールの設定、新規タグの追加、既存のタグの名称変更、タグの削除なども可能です。

- **詳細**

このタブは次のセクションで構成されています。

- **アプリケーションレジストリ**。このセクションでは、クライアントデバイス上にインストールされたアプリケーションのレジストリとそのアップデートを表示し、アプリケーションレジストリの表示を設定することができます。

  インストール済みアプリケーションの情報は、クライアントデバイスにインストールされているネットワークエージェントから必要な情報が管理サーバーに送信されている場合に供給されます。管理サーバーへの情報の送信は、ネットワークエージェントまたはそのポリシーのプロパティウィンドウにある［**リポジトリ**］セクションで設定できます。

  アプリケーション名をクリックすると、アプリケーションの詳細とアプリケーションにインストールされているアップデートパッケージのリストを表示するウィンドウが開きます。

- **実行ファイル**。このセクションには、クライアントデバイスにある実行ファイルが表示されます。

- **ディストリビューションポイント**。このセクションでは、デバイスがインタラクトするディストリビューションポイントのリストについて説明します。

  - **ファイルへのエクスポート**

    ［**ファイルへのエクスポート**］をクリックすると、デバイスがインタラクトするディストリビューションポイントのリストがファイルに保存されます。既定では、デバイスのリストは CSV ファイルにエクスポートされます。

  - **プロパティ**

    ［**プロパティ**］をクリックすると、デバイスがインタラクトするディストリビューションポイントが表示および設定されます。

- **ハードウェアレジストリ**。このセクションでは、クライアントデバイスにインストールされているハードウェアに関する情報を表示できます。

  Windows が動作しているデバイスにネットワークエージェントがインストールされている場合、ネットワークエージェントはデバイスのハードウェアに関する以下の情報を管理サーバーに送信します：

  - メモリ
  - 大容量ストレージデバイス
  - マザーボード
  - CPU
  - ネットワークアダプター
  - モニター
  - ビデオアダプター
  - サウンドカード

Linux または macOS を実行しているデバイスにネットワークエージェントがインストールされている場合、この情報がオペレーティングシステムから提供されると、ネットワークエージェントはデバイスのハードウェアに関する次の情報を管理サーバーに送信します：

- 合計 RAM 容量
- 大容量記憶装置の合計容量
- マザーボード
- CPU
- ネットワークアダプター

- **適用可能なアップデート**。このセクションには、デバイスで検出されたがインストールされていないソフトウェアアップデートのリストが表示されます。
- **ソフトウェアの脆弱性**。このセクションには、クライアントデバイスにインストールされているサードパーティのソフトウェアの脆弱性に関する情報が表示されます。

  脆弱性をファイルに保存するには、保存する脆弱性に隣接するチェックボックスをオンにして、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

  このセクションには、次の設定項目があります：

  - **修正可能な脆弱性のみ表示**

    このオプションを有効にすると、パッチを使用して修正できる脆弱性が表示されます。

    このオプションをオフにすると、パッチを使用して修正できる脆弱性と、パッチがリリースされていない脆弱性の両方が表示されます。

    既定では、このオプションはオンです。

  - **脆弱性のプロパティ**

    リストにあるソフトウェアの脆弱性の名前をクリックすると、選択したソフトウェアの脆弱性のプロパティが別のウィンドウに表示されます。ウィンドウで次の操作を実行できます：

    - 対象の管理対象デバイスではこのソフトウェアの脆弱性を無視するようにする（Kaspersky Security Center Web コンソールで操作）。
    - 脆弱性に対して推奨される修正のリストを表示する。
    - 脆弱性の修正をするソフトウェアのアップデートを手動で指定する（Kaspersky Security Center Web コンソールで操作）。
    - 脆弱性の該当数を表示する。
    - 脆弱性を修正するための既存のタスクのリストを表示したり、脆弱性を修正するためのタスクを新規作成する。

- **リモート診断**。このセクションでは、クライアントデバイスのリモート診断を実行できます。

PostgreSQL、MariaDB、または MySQL DBMS を使用する場合、[**イベント**] タブには、選択したクライアントデバイスのイベントの不完全なリストが表示されることがあります。これは、DBMS が非常に大量のイベントを保存する場合に発生します。次のいずれかを実行すると、表示されるイベントの数を増やすことができます：

- 不要なイベントを削除します。
- 不要なイベントの保存期間を短縮します。

デバイスの管理サーバーに記録されたイベントの完全なリストを表示するには、レポートを使用します。

# クライアントデバイスと管理サーバー間の接続の手動確認：Klnagchk ユーティリティ

klnagchk ユーティリティを使用すると、クライアントデバイスと管理サーバー間の接続を確認し、接続設定に関する詳細情報を取得できます。klnagchk ユーティリティはネットワークエージェントのインストールフォルダーにあります。

klnagchk ユーティリティは、コマンドラインから起動すると、次の処理を実行します（使用するキーによって異なります）：

- デバイスにインストールされたネットワークエージェントから管理サーバーへの接続に使用される設定値を画面に表示するかログに記録する
- ネットワークエージェントの統計情報（前回の起動以降）とユーティリティ処理結果をイベントログファイルに記録するか画面に表示する
- ネットワークエージェントと管理サーバー間の接続の確立を試行する

  接続の試行に失敗した場合、ICMP パケットを送信して、管理サーバーがインストールされているデバイスの状態を確認します。

*klnagchk ユーティリティを使用して、クライアントデバイスと管理サーバー間の接続を確認するには、*

ネットワークエージェントがインストールされているデバイスで、ローカル管理者アカウントのコマンドラインから klnagchk ユーティリティを起動します。

ユーティリティのコマンドライン構文は次の通りです：

```
klnagchk [-logfile <ファイル名>] [-sp] [-savecert <証明書ファイルのパス>] [-restart][-sendhb]
```

キーの説明：

- `-logfile <ファイル名>`ーネットワークエージェントと管理サーバー間の接続設定値とユーティリティの処理結果をログファイルに記録します。

  既定では、情報は標準出力ストリーム（stdout）に保存されます。このキーを使用しない場合、設定、結果、エラーメッセージは画面に表示されます。

- `-sp`ープロキシサーバー上のユーザー認証パスワードを表示します。

  このライセンスは、プロキシサーバー経由で管理サーバーへの接続が確立される場合に使用されます。

- `-savecert <ファイル名>`ー管理サーバーへのアクセス認証用の証明書を指定したファイルに保存します。

- `-restart`ーユーティリティの処理完了後にネットワークエージェントを再起動します。

- `-sendhb`ーネットワークエージェントと管理サーバーの同期を開始します。

起動後、klnagchk ユーティリティはネットワークエージェントの設定情報ファイルにアクセスし、接続パラメータを表示します。これらのパラメータは、ネットワークエージェントのインストール時およびネットワークエージェントのポリシー設定で指定されます：

- `Current device`ークライアントデバイスの Windows ネットワークでの名前。

- `Network Agent version`ーデバイスにインストールされているネットワークエージェントのバージョンの（パッチまで含む）完全な数字。

- `Administration Server address`ー管理サーバーのアドレス。

- `Use SSL`ー管理サーバーに接続する時にセキュアな接続が使用されるかどうかを示すパラメータ。

  指定可能な値：

  - 0ーセキュアな接続は使用されません。

  - 1ーセキュアな接続が使用されます。

- `Compress traffic`ークライアントデバイスと管理サーバー間のトラフィックが圧縮されるかどうかを示すパラメータ。

- `Numbers of the Administration Server SSL ports`ーセキュアな接続を使用する場合の管理サーバーとの通信に有効なポート番号。

- `Numbers of the Administration Server ports`ー通常の接続を使用する場合に管理サーバーと通信するために有効なポート番号。

- `Use proxy server`ープロキシサーバーが使用されるかどうかを示すパラメータ。

  指定可能な値：

  - 0ープロキシサーバーは使用されません。

  - 1ープロキシサーバーが使用されます。

- `Address`ープロキシサーバーのアドレスとポート（コロンで区切られます）。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。

- `User name`ープロキシサーバーにアクセスするためのユーザー名。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。

- `Password`ープロキシサーバーにアクセスするためのパスワード。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。プロキシサーバーのパスワードを表示するには、コマンドで `sp` キーを使用する必要があります。

- `Administration Server certificate`ークライアントデバイスに管理サーバー証明書があるかどうかを示すパラメータ。たとえば、ネットワークエージェントが管理サーバーに一度も正常に接続したことがない場合は、証明書が存在しない可能性があります。

  指定可能な値：

  - `not installed`ークライアントデバイスに管理サーバー証明書がありません。
  - `available`ークライアントデバイスに管理サーバー証明書があります。

- `Open UDP port`ーネットワークエージェントが管理サーバーからの同期要求を受信するために UDP ポートを使用するかどうかを示すパラメータ。

  指定可能な値：

  - 0ー管理サーバーからの同期要求を受信するための UDP ポートが閉じられています。
  - 1ー管理サーバーからの同期要求を受信するために UDP ポートが開かれています。

- `Numbers of UDP ports`ーネットワークエージェントで使用できる UDP ポートの数。
- `Location name`ーデバイスのネットワーク上の場所。
- `State of network location`ークライアントデバイスを 1 つの管理サーバー接続プロファイルから別の接続プロファイルに切り替えることができるかどうかを示すパラメータ。

  指定可能な値：

  - `Enabled`ークライアントデバイスの管理サーバー接続プロファイルを切り替えることができます。
  - `Disabled`ークライアントデバイスの管理サーバー接続プロファイルを切り替えることはできません。

- `Profile to use`ー管理サーバーの接続プロファイル。
- `Condition`ークライアントデバイスが接続されているネットワークの IP アドレスとサブネットマスク。
- `Synchronization interval (min)`ー同期の標準間隔。
- `Connection timeout (in seconds)`ー接続タイムアウト。
- `Send / receive timeout (in seconds)`ー読み取り / 書き込み操作の接続タイムアウト。
- `Device ID`ーネットワーク内のデバイス識別子。`Device ID` は、特定の管理サーバーによって管理されるクライアントデバイス間で一意です。
- `Locations of connection gateways`ー接続ゲートウェイを介してクライアントデバイスを管理サーバーに接続するためのパラメータ。
- `Location of distribution points`ーディストリビューションポイントを介してクライアントデバイスを管理サーバーに接続するためのパラメータ。

- **Connection with server**ー接続ゲートウェイが管理サーバーに継続的に接続されているかどうかを示すパラメータ。このパラメータは、クライアントデバイスが接続ゲートウェイとして機能する場合にのみ表示されます。

  指定可能な値：

  - **active**ー接続ゲートウェイは管理サーバーに継続的に接続されています。
  - **inactive**ー接続ゲートウェイは管理サーバーに継続的に接続されていません。

- **Connection with server through connection gateway**ー接続ゲートウェイを介した管理サーバーへの接続が正しく確立されているかどうかを示すパラメータ。このパラメータは、クライアントデバイスが接続ゲートウェイとして機能する場合にのみ表示されます。

  指定可能な値：

  - **active**ー接続ゲートウェイを介した管理サーバーへの接続が正しく確立されています。
  - **inactive**ー接続ゲートウェイを介した管理サーバーへの接続が正しく確立されていません。

また、klnagchk ユーティリティの出力には、次のいずれかの行が含まれる場合があります：

- **Administration Server is installed on this device**ー klnagchk ユーティリティは管理サーバーデバイスで実行されます。
- **This device has been assigned a connection gateway but is not yet registered on Administration Server**ー klnagchk ユーティリティは、ネットワークエージェントがインストールされているデバイス上で、接続ゲートウェイモードで実行されます。設定された接続ゲートウェイは管理サーバーからの接続を待機していますが、管理サーバーが管理対象デバイス中のデバイスをリストしません。管理サーバーが接続ゲートウェイへの接続を開始するようにする必要があります。
- **This device is a connection gateway**ーklnagchk ユーティリティは、接続ゲートウェイとして機能するデバイス上で実行されます。
- **Acts as a distribution point**ーklnagchk ユーティリティは、ディストリビューションポイントとして機能するデバイス上で実行されます。

klnagchk ユーティリティは、ネットワークエージェントサービスのステータスをチェックします。サービスが実行されていない場合、ユーティリティは停止します。サービスが実行中の場合、ユーティリティは次の接続統計を表示します：

- **Total number of synchronization requests**ークライアントデバイスから管理サーバーへの接続試行回数。
- **The number of successful synchronization request**ークライアントデバイスから管理サーバーへの接続試行が成功した回数。
- **Total number of synchronizations**ークライアントデバイス設定と管理サーバー設定の同期試行回数。
- **The number of successful synchronizations**ークライアントデバイス設定と管理サーバーの同期試行が成功した回数。
- **Date/time of the last request for synchronization**ー最後の接続の日時。

管理サーバーとネットワークエージェント間の接続を分析する時は、`Total number of synchronization requests`と`The number of successful synchronization request`パラメータを使用する必要があります。クライアントデバイスの設定は、管理サーバーの設定が変更された場合（たとえば、新しいタスクが追加された場合やポリシー設定が変更された場合）のみ、管理サーバーの設定と同期されます。それ以外の場合、`Total number of synchronizations`と`The number of successful synchronizations`のパラメータ値は変更されません。

ネットワークエージェントを管理サーバーに接続する際に発生する問題のトラブルシューティング方法の詳細については、「Kaspersky Security Center Linux の FAQ」を参照してください。

# デバイス移動ルール

*デバイス移動ルール*を使用して、管理グループにデバイスへの割り当てを自動化することを推奨します。デバイス移動ルールは、3 つのメイン部分から構成されます。それは、名前、実行条件（デバイス属性を使用した論理式）、および対象管理グループです。デバイス属性がルールの実行条件を満たしている場合は、このルールによりデバイスが対象管理グループに移動されます。

デバイス移動ルールにはすべて優先度が設定されています。管理サーバーは優先度の昇順に従って、デバイス属性が各ルールの実行条件を満たしているかどうかを確認します。デバイス属性がルールの実行条件を満たしている場合、そのデバイスは対象グループに移動され、このデバイスに対するルール処理が完了します。デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールは暗黙的に作成できます。たとえば、インストールパッケージまたはリモートインストールタスクのプロパティで、ネットワークエージェントをデバイスにインストールした後にそのデバイス移動先の管理グループを指定できます。さらに、［**アセット（デバイス）**］→［**移動ルール**］セクションで Kaspersky Security Center Linux の管理者が、デバイス移動ルールを明示的に作成できます。

既定では、デバイス移動ルールは、管理グループに対してデバイスを最初にワンタイムで割り当てることを目的としています。このルールにより、［未割り当てデバイス］グループから一度だけデバイスが移動されます。デバイスがこのルールによって一度移動されている場合は、デバイスを手動で［未割り当てデバイス］グループに戻したとしても、このデバイスが再度移動されることはありません。これは移動ルールを適用する際に推奨される方法です。

一部の管理グループに割り当て済みであるデバイスを移動できます。これを実行するには、ルールのプロパティで［**どの管理グループにも属していないデバイスのみ移動する**］をオフにします。

一部の管理グループに割り当て済みのデバイスに対して移動ルールを適用すると、管理サーバーの負荷が大幅に増大します。

［**どの管理グループにも属していないデバイスのみ移動する**］は、自動的に作成された移動ルールのプロパティでロックされています。このようなルールは、［*アプリケーションをリモートでインストールする*］タスクを追加するか、スタンドアロンインストールパッケージを作成する時に作成されます。

単一のデバイスに繰り返し適用される移動ルールを作成することができます。

単一のデバイスをあるグループから別のグループに繰り返し移動させないでください（たとえば、該当するデバイスに特別なポリシーを適用するために、特別なグループタスクを実行するか、または特定のディストリビューションポイントを使用してデバイスをアップデートする）。

このような処理は、管理サーバーとネットワークのトラフィックの負荷を極端に増大させるため、サポートされていません。また、Kaspersky Security Center Linux の操作原理と競合する可能性もあります（特に、アクセス権限、イベント、レポートの分野において）。ポリシーのプロファイル、デバイスの抽出のタスク、標準シナリオに従ったネットワークエージェントの割り当てなどを使用して、別のソリューションを見つける必要があります。

# デバイス移動ルールの作成

デバイスを自動的に管理グループに割り当てるデバイス移動ルールを設定できます。

*移動ルールを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。




2. ［**追加**］をクリックします。［**新規ルール**］ウィンドウが表示されます。



3. 表示されたウィンドウの［**全般**］タブで、次の情報を指定します：

- **ルール名**

  新しいルールの名前を入力します。

  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **アクティブなルール**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールの適用**

  次の中からいずれかを選択できます：

  - **各デバイスにつき1回**

    指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

  - **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**

    指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

  - **ルールを永続的に適用**

    管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

4. ［**ルールの条件**］タブで、デバイスを管理グループに移動する基準を少なくとも1つ指定します。

5. ［**保存**］をクリックします。

移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

リストでの順位が高いほど、ルールの優先度が高くなります。移動ルールの優先度を上げたり下げたりするには、マウスを使用してルールをリスト内でそれぞれ上下に移動します。

［**ルールを永続的に適用**］をオンにした場合、優先度設定に関係なく移動ルールが適用されます。このようなルールは、管理サーバーが自動的に設定したスケジュールに従って適用されます。

デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

# デバイス移動ルールのコピー

異なる管理グループで同一のルールを使用する場合などに、移動ルールをコピーできます。

既存の移動ルールをコピーするには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。
   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に移動します。

   移動ルールのリストが表示されます。




2. コピーするルールに隣接するチェックボックスをオンにします。




3. ［**コピー**］をクリックします。

4. 表示されるウィンドウで、必要に応じて［**全般**］タブで次の情報を変更します。ただし、設定を変更せずにルールのコピーのみを行う場合は、設定を変更する必要はありません：

- **ルール名**

  新しいルールの名前を入力します。

  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **アクティブなルール**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールの適用**

  次の中からいずれかを選択できます：

  - **各デバイスにつき1回**

    指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

  - **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**

    指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

  - **ルールを永続的に適用**

    管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。




5. ［**ルールの条件**］タブで、自動的に移動するデバイスの基準を少なくとも 1 つ指定します。

6. ［**保存**］をクリックします。

新しい移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

# デバイス移動ルールの条件

クライアントデバイスを管理グループに移動するルールを作成またはコピーする場合、［**ルールの条件**］タブで、デバイスを移動するための条件を設定します。次の基準に従って、移動するデバイスを決定できます：

- クライアントデバイスに割り当てられたタグ。
- ネットワークパラメータ。たとえば、指定した範囲の IP アドレスを持つデバイスを移動することができます。
- ネットワークエージェントや管理サーバーなど、クライアントデバイスにインストールされた管理対象アプリケーション。
- クライアントデバイスである仮想マシン。

以下では、デバイス移動ルールにこの情報を指定する方法について説明します。

ルールに複数の条件を指定すると、AND 論理演算子が機能し、すべての条件が同時に適用されます。オプションを何も選択しない場合や、一部のフィールドを空白のままにした場合には、そのような条件は適用されません。

## ［タグ］タブ

このタブでは、クライアントデバイスの説明に追加済みのデバイスタグに基づいてデバイス移動ルールを設定できます。このためには、必要なタグを選択します。また、次のオプションをオンにすることもできます：

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、指定したタグを持つすべてのデバイスがデバイス移動ルールから除外されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

- **少なくとも 1 個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択したタグを少なくとも 1 個持つクライアントデバイスにデバイス移動ルールが適用されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

## ［ネットワーク］タブ

このタブでは、デバイス移動ルールで考慮するデバイスのネットワークデータを指定できます：

- **デバイスの DNS 名**

  移動するクライアントデバイスの DNS ドメイン名。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

  Kaspersky Security Center Linux で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、デバイス移動ルールは機能しません。

- **DNS ドメイン**

  デバイス移動ルールは、指定されたメイン DNS サフィックスに含まれるすべてのデバイスに適用されます。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

- **管理サーバー接続用 IP アドレス**

  このオプションを有効にすると、クライアントデバイスを管理サーバーに接続するための IP アドレスを設定できます。これを行うには、必要なすべての IP アドレスが含まれる IP 範囲を指定します。

  既定では、このオプションはオフです。

- **デバイスが配置されている IP アドレス範囲**

  このオプションをオンにすると、［**IP アドレス範囲**］セクションで以前に追加した IP 範囲を選択できます。関連するデバイスは、選択した IP 範囲に含まれている必要があります。

  既定では、このオプションはオフです。

- **接続プロファイルが変更されました**

  次のいずれかの値を選択します：

  - **はい**：デバイス移動ルールは、接続プロファイルが変更されたクライアントデバイスにのみ適用されます。
  - **いいえ**：デバイス移動ルールは、接続プロファイルが変更されていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **別の管理サーバーの管理対象**

  次のいずれかの値を選択します：

  - **はい**：デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
  - **いいえ**：デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

## ［デバイスの所有者］タブ

このタブでは、デバイスの所有者、セキュリティグループのメンバーシップ、およびロールに基づいて、デバイスの移動ルールを設定できます：

- **デバイスの所有者**

  内部セキュリティグループからデバイスの所有者のユーザー名を選択します。このセクションでは、ユーザーとユーザーのロールについて詳しく説明します。

  > デバイスの所有者として登録できるユーザーは1人だけです。

- **デバイスの所有者が属している Active Directory セキュリティグループ**

  デバイスの所有者が属している外部 Active Directory セキュリティグループを選択します。

  > ユーザーは、Active Directory セキュリティグループの一部になることも、この Active Directory セキュリティグループに含まれるグループの一部になることもできます。

- **デバイス所有者のロール**

  デバイスの所有者に割り当てられたロールを選択します。ユーザーのロールの詳細については、この記事をご覧ください。

- **内部セキュリティグループでのデバイスの所有者のメンバーシップ**

  デバイスの所有者が属する内部セキュリティグループを選択します。

# ［アプリケーション］タブ

このタブでは、クライアントデバイスにインストールされている管理対象アプリケーションとオペレーティングシステムに基づいてデバイス移動ルールを設定できます：

- **ネットワークエージェントがインストール済み**

  次のいずれかの値を選択します：

  - **はい**：デバイス移動ルールは、ネットワークエージェントがインストールされたクライアントデバイスにのみ適用されます。
  - **いいえ**：デバイス移動ルールは、ネットワークエージェントがインストールされていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **アプリケーション**

  クライアントデバイスにインストールされている必要がある管理対象アプリケーションを指定して、デバイス移動ルールがこれらのデバイスに適用されるようにします。たとえば、**Kaspersky Security Center 15.3 ネットワークエージェント** や **Kaspersky Security Center 15.3 管理サーバー** を選択できます。

  管理対象アプリケーションを選択しない場合、条件は適用されません。

- **OS のバージョン**

  オペレーティングシステムのバージョンに基づいてクライアントデバイスを選別できます。この目的のために、クライアントデバイスにインストールされている必要があるオペレーティングシステムを指定します。その結果、選択したオペレーティングシステムがインストールされたクライアントデバイスにデバイス移動ルールが適用されます。

  このオプションを有効にしない場合、条件は適用されません。既定では、このオプションはオフです。

- **OS のビット数**

  オペレーティングシステムのビットサイズによってクライアントデバイスを選別できます。［**OS のビット数**］フィールドで、次のいずれかの値を選択できます：

  - **不明**
  - **x86**
  - **AMD64**
  - **IA64**

  *クライアントデバイスのオペレーティングシステムのビットサイズを確認するには：*

  1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションの順に選択します。
  2. 右側にある［**列の設定**］（）をクリックします。
  3. ［**OS のビット数**］オプションを選択し、［**保存**］ボタンをクリックします。

     その後、管理対象デバイスごとにオペレーティングシステムのビットサイズが表示されます。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **ユーザー証明書**

  次のいずれかの値を選択します：

  - **インストール**：デバイス移動ルールは、モバイル証明書を持つモバイルデバイスにのみ適用されます。
  - **未インストール**：デバイス移動ルールは、モバイル証明書のないモバイルデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **OS のビルド**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号に対してデバイス移動ルールを設定することもできます。

- **OS のリリース番号**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  選択したオペレーティングシステムのリリース ID が、入力したリリース番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース番号を除くすべてのリリース番号に対してデバイス移動ルールを設定することもできます。

## ［仮想マシン］タブ

このタブでは、クライアントデバイスが仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかに応じて、デバイス移動ルールを設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のいずれかのオプションを選択できます：

  - **該当なし**：条件は当てはまりません。
  - **いいえ**：仮想マシンでないデバイスを移動します。
  - **はい**仮想マシンであるデバイスを移動します。

- **仮想マシンの種別**

- **仮想デスクトップインフラストラクチャの一部**

  このドロップダウンリストで、次のいずれかのオプションを選択できます：

  - **該当なし**：条件は当てはまりません。
  - **いいえ**：VDI の一部ではないデバイスを移動します。
  - **はい**VDI を構成するデバイスを移動します。

### ［ドメインコントローラー］タブ

このタブでは、ドメイン組織単位に含まれるデバイスを移動する必要があることを指定できます。指定したドメイン組織単位のすべての子組織単位からデバイスを移動することもできます：

- **デバイスが含まれている次の組織単位**

  このオプションをオンにすると、デバイス移動ルールは、オプションの下のリストで指定されたドメインコントローラー組織ユニットのデバイスに適用されます。

  既定では、このオプションはオフです。

- **子組織単位を含める**

  このオプションをオンにすると、抽出には、指定したドメインコントローラー組織単位のすべての子組織単位（OU）のデバイスが含まれます。

  既定では、このオプションはオフです。

- **子組織単位のデバイスを対応するサブグループへ移動する**
- **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**
- **ドメインに存在しないサブグループを削除する**
- **デバイスが含まれている次のドメインセキュリティグループ**

  このオプションをオンにすると、デバイス移動ルールは、オプションの下のリストで指定されたドメインセキュリティグループのデバイスに適用されます。

  既定では、このオプションはオフです。

# デバイスを管理グループへ手動で追加

デバイス移動ルールを作成してデバイスを管理グループに自動的に移動したり、選択した管理グループにデバイスを追加することで、デバイスを管理グループ間で手動で移動したりすることができます。このセクションでは、デバイスを管理グループに手動で追加する手順を説明します。

*特定の管理グループに 1 台以上のデバイスを手動で追加するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。




管理対象デバイスのリスト

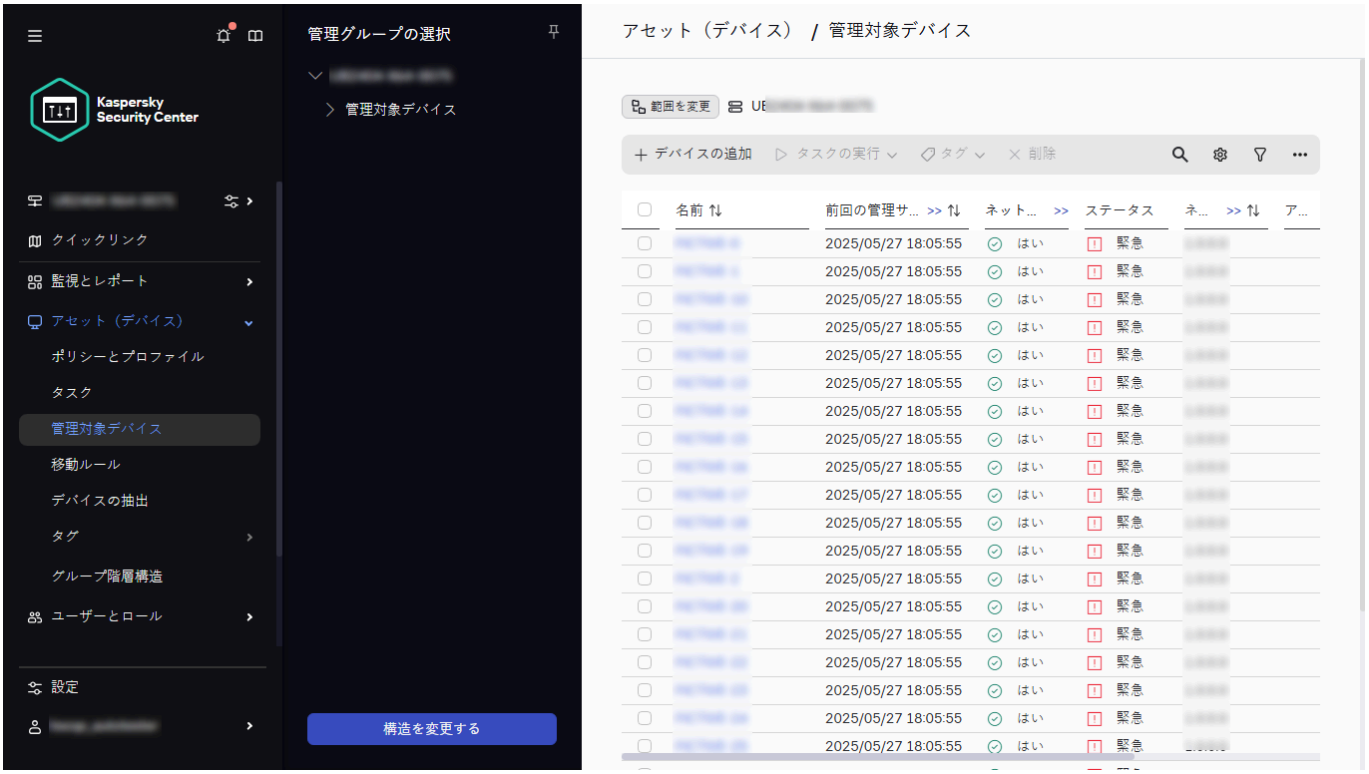
2. デバイスを追加する管理グループを選択します：

   - ルートグループ用：
     この場合は次のステップに進むことができます。
   - サブグループの場合：

     a. ページ上部の［**スコープの変更**］をクリックします。

     b. 開いたウィンドウで、サブグループの名前をクリックします。

選択したグループへのパスがページの上部に表示されます。必要に応じて、管理グループ名のリンクをクリックしてグループに移動できます。既定では、パス内の最後のリンクは非アクティブです。




管理グループの選択

3. ［**デバイスの追加**］をクリックします。

   デバイス移動ウィザードが起動します。

4. 管理グループに追加するデバイスのリストを作成します。

> デバイスへの接続時に、またはデバイスの検出後に、管理サーバーのデータベースに既に情報が追加されているデバイスのみを追加できます。

デバイスをリストに追加する方法を選択します：

- ［**デバイスの追加**］をクリックして、次のいずれかの方法でデバイスを指定します：
  - 管理サーバーによって検出されたデバイスのリストからデバイスを選択します。
  - デバイスの IP アドレスまたは IP アドレス範囲を指定します。
  - デバイスの DNS 名を指定します。

    > デバイス名のフィールドには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。

- ［**デバイスをファイルからインポート**］をクリックして、テキストファイルからデバイスのリストをインポートします。各デバイスのアドレスまたは名前をそれぞれの行に指定する必要があります。

  > ファイルには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。




管理グループに移動するデバイスの選択

5. 管理グループに追加するデバイスのリストを表示します。デバイスを追加または削除することでリストを編集できます。

6. リストが正しいことを確認したら、［**次へ**］をクリックします。

ウィザードによってデバイスリストが処理され、結果が表示されます。正常に処理されたデバイスが管理グループに追加され、管理サーバーによって作成された名前でデバイスのリストに表示されます。

# デバイスまたはクラスターを手動で管理グループに移動する

管理グループ間で、または未割り当てデバイスのグループから管理グループにデバイスを移動できます。

管理グループからクラスタまたはサーバーアレイを別の管理グループに移動することもできます。クラスタまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスタとそのノードのいずれかが常に同じ管理グループに属しているためです。［**デバイス**］タブで単一のクラスタノードを選択すると、［**グループへ移動**］が使用できなくなります。

*特定の管理グループに 1 台以上のデバイスまたはクラスタを移動するには：*

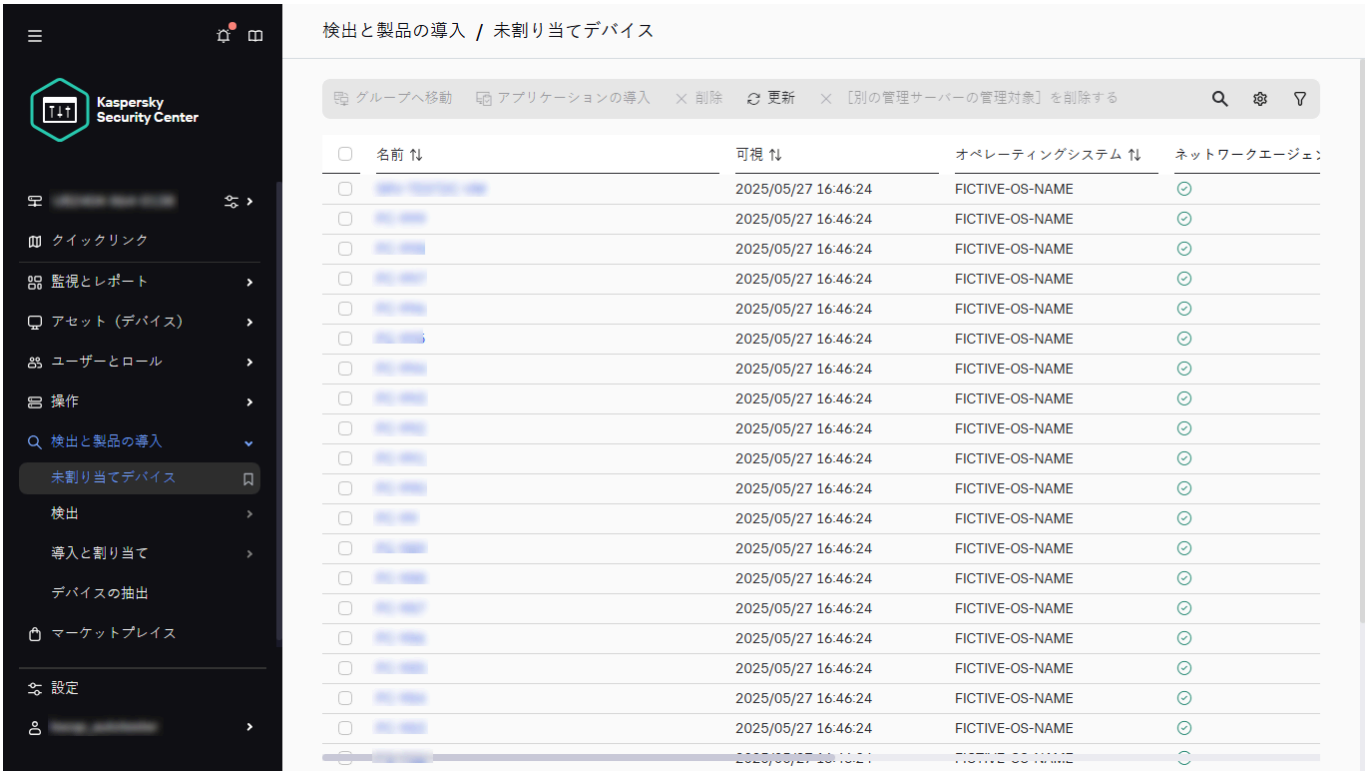
1. デバイスの移動元の管理グループを開きます。開くには、次のいずれかの操作を行います：

   - 管理グループを開くには、メインメニューで［**アセット（デバイス）**］→［**管理対象デバイス**］に移動し、必要な管理グループを選択します。

     - ルートグループの場合は、次の手順に進むことができます。

     - サブグループの場合は、ページ上部の［**スコープの変更**］をクリックし、開いたウィンドウで必要な管理グループを選択します。

   - ［**未割り当てデバイス**］のグループを開くには、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。




未割り当てデバイスのリスト

2. 管理グループにクラスタまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］セクションは、［**デバイス**］タブと［**クラスターとサーバーアレイ**］タブの 2 つのタブに分割されます。移動するオブジェクトのタブを開きます。

3. 別のグループに移動するデバイスまたはクラスタに隣接するチェックボックスをオンにします。

4. ［**グループへ移動**］をクリックします。

5. 管理グループの階層で、選択したデバイスまたはクラスタの移動先の管理グループに隣接するチェックボックスをオンにします。

6. ［**移動**］をクリックします。

選択したデバイスまたはクラスタが、選択した管理グループに移動します。

# クラスタとサーバーアレイについて

Kaspersky Security Center Linux はクラスタ技術をサポートしています。クライアントデバイスにインストールされたアプリケーションがサーバーアレイの一部であることを確認する情報が、ネットワークエージェントから管理サーバーに送信されると、このクライアントデバイスはクラスタノードになります。

管理グループにクラスタまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］ページには 2 つのタブが表示されます。1つは個々のデバイス用で、もう1つはクラスタおよびサーバーアレイ用です。管理対象デバイスがクラスターノードとして検出されると、クラスターは個別のオブジェクトとして［**クラスターとサーバーアレイ**］タブに追加されます。

クラスタまたはサーバーアレイノードは、他の管理対象デバイスとともに［**デバイス**］タブにリスト表示されます。個別のデバイスとしてノードのプロパティを表示したり、他の操作を実行したりできますが、クラスタノードを削除したり、そのクラスタとは別に他の管理グループに移動したりすることはできません。クラスタ全体の削除または移動のみが可能です。

クラスタまたはサーバーアレイで実行できる操作は次の通りです：

- プロパティを表示する
- クラスタまたはサーバーアレイを別の管理グループに移動する

  クラスターまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスターとそのノードのいずれかが常に同じ管理グループに属しているためです。

- 削除

  クラスタまたはサーバーアレイの削除は、クラスタまたはサーバーアレイが組織のネットワークに存在しなくなった場合にのみ行うことを推奨します。クラスタがまだネットワーク上に表示され、ネットワークエージェントとカスペルスキーセキュリティ製品がまだクラスタノードにインストールされている場合、Kaspersky Security Center Linux は、削除されたクラスタとそのノードを管理対象デバイスのリストに自動的に戻します。

# クラスターまたはサーバーアレイのプロパティ

*クラスタまたはサーバーアレイの設定を表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**クラスターとサーバーアレイ**］の順に移動します。

   クラスタとサーバーアレイのリストが表示されます。

2. 必要なクラスタまたはサーバーアレイの名前をクリックします。

選択したクラスタまたはサーバーアレイのプロパティウィンドウが表示されます。

## 全般

［**全般**］セクションには、クラスタまたはサーバーアレイに関する一般情報が表示されます。情報は、管理サーバーでクラスタノードの前回の同期中に受信されたデータに基づいて提供されます。

- **名前**
- **説明**
- **Windows ドメイン**

  クラスタまたはサーバーアレイを含む Windows ドメインまたはワークグループ。

- **NetBIOS 名**

  クラスタまたはサーバーアレイの Windows ネットワーク名。

- **DNS 名**

  クラスタまたはサーバーアレイの DNS ドメインの名前。

## タスク

［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、開始、停止、タスク設定の変更、実行結果の表示など、クラスタまたはサーバーアレイに割り当てられたタスクを管理できます。リストされているタスクは、クラスタノードにインストールされているカスペルスキーセキュリティ製品に関連するものです。Kaspersky Security Center Linux は、クラスタノードからタスクリストとタスクステータスの詳細を受け取ります。接続に失敗すると、ステータスは表示されません。

## ノード

このタブには、クラスタまたはサーバーアレイに含まれるノードのリストが表示されます。ノード名をクリックすると、デバイスのプロパティウィンドウが表示されます。

## カスペルスキー製品

プロパティウィンドウには、クラスタノードにインストールされているカスペルスキーのセキュリティ製品に関連する情報と設定を含む追加のタブが含まれている場合もあります。

# ディストリビューションポイントと接続ゲートウェイの調整

Kaspersky Security Center Linux の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する設定をデバイスに適用する別の方法として、*ポリシーのプロファイル*を使用する方法があります。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の組織図とネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス

- 複数の小規模なリモートオフィス

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

# ディストリビューションポイントの概要

ネットワークエージェントがインストールされたデバイスはディストリビューションポイントとして使用できます。このモードでは、ネットワークエージェントはアップデートを配布でき、アップデートは管理サーバーまたはカスペルスキーサーバーから取得できます。後者の場合は、ディストリビューションポイントのアップデートのダウンロードを構成します。

組織ネットワークにディストリビューションポイントを導入する目的は次の通りです：

- 管理サーバーの負荷の低減
- トラフィックの最適化
- 組織ネットワークで接続経路を確保しにくい場所にあるデバイスへの管理サーバーアクセスの提供。NAT の内側に構成したネットワークでディストリビューションポイント（管理サーバーに関して）を使用すると、管理サーバーは次の処理を実行できます：
  - IPv4 または IPv6 ネットワークの UDP を経由したデバイスへの通知の送信
  - IPv4 または IPv6 ネットワークの検索
  - 初期導入の実行
  - プッシュサーバーとしての動作

1つの管理グループに対して、1つのディストリビューションポイントが割り当てられます。この場合、ディストリビューションポイントの範囲には、管理グループとそのすべてのサブグループ内にあるすべてのデバイスが含まれます。ただし、ディストリビューションポイントとして動作しているデバイスは、割り当てられている管理グループに含まれていなくてもかまいません。

ディストリビューションポイントを接続ゲートウェイとして動作させることができます。この場合、ディストリビューションポイントの範囲内のデバイスは、管理サーバーと直接接続されずゲートウェイを介して接続されます。このモードは、管理サーバーと管理対象デバイスの間を直接には接続できない場合に有効です。

Linux ベースのデバイスをディストリビューションポイントとして使用する場合、ディストリビューションポイントの対象範囲に多数のデバイスが含まれると、開くことができるファイルの既定の最大数では不十分になる可能性があるため、klnagent サービスのファイル記述子の上限を引き上げることを強く推奨します。

# ディストリビューションポイントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

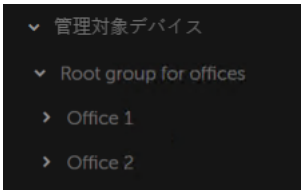
管理グループの構造は、次の方法で構築することが可能です：

- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。
- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する1台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

# ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。




管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

# ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ディストリビューションポイントの自動割り当ては、できるだけ使用しないでください。ディストリビューションポイントの自動割り当てが有効になっており、クライアントデバイスの数が非常に多い場合、管理サーバーがディストリビューションポイントの割り当てと設定を行います。

## 用途専用のディストリビューションポイントの使用

特定のデバイスをディストリビューションポイントとして使用する場合（たとえば、この用途専用で割り当てられたサーバー）、ディストリビューションポイントの自動割り当ては使用しないでください。また、ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

| ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 300 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 300 以上 | 許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数） |

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

| 各ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 10 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 10～100 | 1 |
| 100 以上 | 許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数） |

## 通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

| ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 300 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 300 以上 | N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要） |

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

| 各ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 10 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 10～30 | 1 |
| 31～300 | 2 |
| 300 以上 | N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要） |

ディストリビューションポイントがシャットダウンされた（もしくは、何らかの理由により使用できない）場合も、ディストリビューションポイントの対象範囲に含まれる管理対象デバイスは管理サーバーにアクセスしてアップデートを取得できます。

# ディストリビューションポイントの自動的な割り当て

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center Linux が選択します。

*ディストリビューションポイントを自動的に割り当てるには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを自動的に割り当て**］をオンにします。

   ディストリビューションポイントとしてのデバイスの自動割り当てが有効な場合、手動でディストリビューションポイントを設定したりディストリビューションポイントのリストを編集したりすることはできません。

4. ［**保存**］をクリックします。

管理サーバーが自動的にディストリビューションポイントを割り当てて設定します。

# ディストリビューションポイントの手動での割り当て

Kaspersky Security Center Linux で、ディストリビューションポイントとして動作するデバイスを手動で指定できます。

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center Linux が選択します。何らかの理由（たとえば、この用途専用で割り当てられたサーバーを使用する、など）により自動割り当てが選択できない場合、ディストリビューションポイント数の計算と設定を行った後に、手動でディストリビューションポイントを割り当てることができます。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

*ディストリビューションポイントとして動作するデバイスを手動で指定するには：*

1. メインメニューで、管理サーバー名をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを手動で割り当て**］をオンにします。
4. ［**割り当て**］をクリックします。
5. ディストリビューションポイントとして動作させるデバイスを選択します。
   デバイスを選択する際は、ディストリビューションポイントの動作とディストリビューションポイントとして動作するデバイスの要件を確認してください。
6. 選択したディストリビューションポイントの受け持ち範囲に含める管理グループを選択します。

7. ［**OK**］をクリックします。

   追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。

8. 新しく追加したディストリビューションポイントをリストからクリックし、プロパティウィンドウを開きます。

9. プロパティウィンドウでディストリビューションポイントを設定します。

- ［General］セクションには、ディストリビューションポイントとクライアントデバイスの間の通信の設定があります。

  - **SSL ポート**

    SSL を使用したクライアントデバイスとディストリビューションポイントの間の暗号化接続で使用する SSL ポートの番号。

    既定では、ポート 13000 が使用されます。

  - **マルチキャストを使用する**

    このオプションをオンにすると、グループ内にあるクライアントデバイスへのインストールパッケージの自動配布に IP マルチキャストが使用されます。

    IP マルチキャストを使用すると、インストールパッケージからクライアントデバイスのグループに製品をインストールするのに必要な時間が短縮されます。一方で、1 台のクライアントデバイスに製品をインストールする場合は、インストールの時間は長くなります。

  - **マルチキャスト IP アドレス**

    マルチキャストで使用される IP アドレス。224.0.0.0 ～ 239.255.255.255 の範囲で IP アドレスを定義できます。

    既定では、Kaspersky Security Center Linux は定められた範囲内で一意の IP マルチキャストアドレスを自動的に割り当てます。

  - **IP マルチキャストポート番号**

    IP マルチキャストのポート番号。

    既定では、ポート番号は 15001 です。管理サーバーがインストールされたデバイスがディストリビューションポイントとして指定された場合、既定では SSL 接続でポート 13001 が使用されます。

  - **リモートデバイスのディストリビューションポイントアドレス**

    リモートデバイスがディストリビューションポイントに接続するために使用する IPv4 アドレス。

  - **アップデートの配信**

アップデートは、次のアップデート元から管理対象デバイスに配布されます：

- このオプションがオンの場合は、このディストリビューションポイントです。
- このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

アップデートの配信にディストリビューションポイントを使用している場合は、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **インストールパッケージの配布**

インストールパッケージは、次の配布元から管理対象デバイスに配布されます：

- このオプションがオンの場合は、このディストリビューションポイントです。
- このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

インストールパッケージの配信にディストリビューションポイントを使用すると、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **プッシュサーバーを実行**

Kaspersky Security Center Linux で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

- **プッシュサーバーのポート**

プッシュサーバー用のポート番号です。使用されていないポートの番号を入力できます。

- ［**Scope**］セクションで、ディストリビューションポイントがアップデートを配信する管理グループを指定します。
- ［**アップデート元**］セクションで、ディストリビューションポイントのアップデート元を選択します。
  - **アップデート元**

ディストリビューションポイントのアップデート元を選択します：

- ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
- タスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートのダウンロードタスクを使用**］をオンにして、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを指定します：
  - そのようなタスクが既にデバイスにある場合は、リストからタスクを選択します。
  - タスクがデバイスに存在しない場合、［**タスクの作成**］をクリックし、タスクを作成します。新規タスクウィザードが起動します。ウィザードの指示に従ってください。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオンです。

- ディストリビューションポイントがインターネットへの接続時にプロキシサーバーを使用する場合は、**インターネット接続設定**サブセクションで次の設定を指定できます：

  - **プロキシサーバーを使用する**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバー接続を設定できます。

    既定では、このチェックボックスはオフです。

  - **プロキシサーバーアドレス**

    プロキシサーバーのアドレス。

  - **ポート番号**

    接続に使用されるポート番号。

  - **ローカルアドレスにプロキシサーバーを使用しない**

    このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

    既定では、このオプションはオフです。

  - **プロキシサーバー認証**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

    既定では、このチェックボックスはオフです。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

- ［**KSN プロキシ**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます：

  - **ディストリビューションポイントで KSN プロキシを有効にする**

    ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

    ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。

    既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

    アクティブ / パッシブモードのクラスタのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

  - **KSN リクエストを管理サーバーに転送する**

    ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

    既定では、このオプションはオンです。

  - **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

    ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

  - **KPSN への接続時にプロキシサーバーの設定を無視する**

    ディストリビューションポイントのプロパティまたはネットワークエージェントのポリシーでプロキシサーバー設定が構成済みであるにも関わらず、ネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、このオプションをオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

    このオプションは［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］をオンにした場合に使用できます。

  - **ポート**

管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポートを使用**

  UDP ポートを経由して KSN プロキシサーバーと管理対象デバイスを接続する場合は、［**UDP ポートを使用**］をオンにして、UDP ポート番号を指定します。既定では、このオプションはオンです。

- **UDP ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する UDP ポートの番号。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- **HTTPS を使用する**

  管理対象デバイスが HTTPS ポート経由で KSN プロキシサーバーに接続する必要がある場合は、［**HTTPS を使用する**］をオンにし、［**HTTPS の使用時に経由するポート**］の番号を指定します。HTTPS プロキシサーバーに接続する既定のポートは 17111 です。

- **HTTPS ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する HTTPS ポートの番号。HTTPS プロキシサーバーに接続する既定のポートは 17111 です。

- ［**接続ゲートウェイ**］セクションでは、ネットワークエージェントインスタンスと管理サーバー間の接続のゲートウェイとして機能するようにディストリビューションポイントを設定できます。

  - **接続ゲートウェイ**

    ネットワークの構成が原因で、管理サーバーとネットワークエージェント間の直接接続を確立できない場合は、ディストリビューションポイントを使用して、管理サーバーとネットワークエージェント間の接続ゲートウェイとして機能させることができます。

    ディストリビューションポイントがネットワークエージェントと管理サーバー間の接続ゲートウェイとして機能する必要がある場合は、このオプションをオンにします。既定では、このオプションはオフです。

  - **管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**

    管理サーバーがローカル エリア ネットワーク上の非武装地帯（DMZ）の外にある場合、リモートデバイスにインストールされたネットワークエージェントは管理サーバーに接続できません。ディストリビューションポイントをリバース接続の接続ゲートウェイとして使用できます（管理サーバーがディストリビューションポイントへの接続を確立します）。

    管理サーバーを DMZ の接続ゲートウェイに接続する必要がある場合は、このオプションをオンにします。

  - **Kaspersky Security Center Web コンソールのローカルポートを開く**

DMZ 内またはインターネット上にある Web コンソールのポートを開くために DMZ 内の接続ゲートウェイが必要な場合は、このオプションをオンにします。Web コンソールからディストリビューションポイントへの接続に使用するポート番号を指定します。既定のポート番号は 13299 です。

このオプションは、［**管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**］をオンにした場合に使用できます。

接続ゲートウェイとして機能するディストリビューションポイントを介してモバイルデバイスを管理サーバーに接続する場合、次のオプションを有効にできます。

- **モバイルデバイス用にポートを開く（管理サーバーの SSL 認証のみ）**

  接続ゲートウェイでモバイル デバイス用のポートを開き、モバイルデバイスがディストリビューションポイントへの接続に使用するポート番号を指定する必要がある場合は、このオプションをオンにします。既定のポート番号は 13292 です。モバイルデバイスは管理サーバー証明書を確認します。接続を確立するときは、管理サーバーのみが認証されます。

- **モバイルデバイス用にポートを開く（SSL 相互認証）**

  管理サーバーとモバイル デバイスの双方向認証に使用されるポートを開くために接続ゲートウェイが必要な場合は、このオプションをオンにします。モバイルデバイスは管理サーバー証明書をチェックし、管理サーバーはモバイルデバイスの証明書をチェックします。次のパラメータを指定します：

  - モバイル デバイスがディストリビューションポイントへの接続に使用するポート番号。既定のポート番号は 13293 です。
  - モバイル デバイスで使用される接続ゲートウェイの DNS ドメイン名。ドメイン名はコンマで区切ります。指定したドメイン名は、ディストリビューションポイント証明書に含まれます。モバイル デバイスが使用するドメイン名がディストリビューションポイント証明書の共通名と一致しない場合、モバイル デバイスはディストリビューションポイントに接続しません。

    デフォルトの DNS ドメイン名は、接続ゲートウェイの FQDN 名です。

どちらの場合も、証明書はディストリビューションポイントでの TLS セッションの確立時にのみチェックされます。証明書は管理サーバーによるチェックのために転送されません。モバイルデバイスとの TLS セッションが確立されると、ディストリビューションポイントは管理サーバー証明書を使用して、モバイルデバイスと管理サーバー間の同期用のトンネルを作成します。双方向 SSL 認証用にポートを開く場合、モバイルデバイス証明書を配布する唯一の方法は、インストールパッケージを使用することです。

- ディストリビューションポイントによるドメインコントローラーのポーリングを設定します。
  - **ドメインコントローラーのポーリング**

ドメインコントローラーのデバイス検出を有効にできます。

［**ドメインコントローラーのポーリングを有効にする**］をオンにすると、ポーリングの対象となるドメインコントローラーを選択し、それらのポーリングスケジュールを指定することもできます。

Linux ディストリビューションポイントを使用する場合は、［**指定したドメインのポーリング**］セクションで［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

- **現在のドメインのポーリング**
- **ドメインフォレスト全体のポーリング**
- **指定したドメインのポーリング**

- ディストリビューションポイントによる IP 範囲のポーリングを設定します。
  - **IP 範囲のポーリング**

    デバイスの検索は IPv4 範囲および IPv6 ネットワークで有効にできます。

    ［**IP アドレス範囲のポーリングを有効にする**］をオンにすると、対象範囲を追加して実行スケジュールを設定できます。スキャン対象範囲のリストに IP アドレス範囲を追加できます。

    ［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークのポーリングを行います。この場合、ディストリビューションポイントはネットワーク全体を検索するため、指定した IP 範囲は無視されます。ディストリビューションポイントが Linux を実行している場合は、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］を使用できます。Zeroconf IPv6 ポーリングを使用するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

- ［**詳細**］セクションで、配信されたデータの格納用にディストリビューションポイントが使用するフォルダーを指定します。
  - **既定のフォルダーを使用する**

    このオプションをオンにすると、ディストリビューションポイント上でネットワークエージェントがインストールされているフォルダーが使用されます。

  - **指定したフォルダーを使用する**

    このオプションをオンにすると、この下のフィールドで、フォルダーのパスを指定できます。ディストリビューションポイントのローカルフォルダーまたは組織ネットワーク内の任意のデバイス上にあるフォルダーを指定できます。

    ネットワークエージェントの実行時にディストリビューションポイントで使用されるユーザーアカウントには、指定したフォルダーへの読み取りおよび書き込みアクセス権限が必要です。

10. ［**OK**］をクリックします。

選択されたデバイスがディストリビューションポイントとして使用されます。

# 管理グループに割り当てられたディストリビューションポイントのリストの編集

特定の管理グループに割り当てられたディストリビューションポイントのリストを表示し、ディストリビューションポイントを追加または削除してこのリストを編集できます。

*管理グループに割り当てられたディストリビューションポイントのリストの表示と編集を行うには：*

1. メインメニューで、[**アセット（デバイス）**] → [**管理対象デバイス**] の順に移動します。
2. ページ上部の [**スコープの変更**] をクリックして、割り当てられたディストリビューションポイントを表示する管理グループを選択し、開いたウィンドウで必要なグループの名前をクリックします。

   これにより、[**ディストリビューションポイント**] メニュー項目をオンにします。

   選択したグループへのパスがページの上部に表示されます。必要に応じて、このパスで管理グループ名のリンクをクリックしてグループに移動できます。既定では、パス内の最後のリンクは非アクティブです。
3. メインメニューで、[**アセット（デバイス）**] → [**ディストリビューションポイント**] の順に選択します。
4. 管理グループに新しいディストリビューションポイントを追加するには、[**割り当て**] をクリックします。
5. 割り当てられたディストリビューションポイントを削除するには、リストからデバイスを選択し、[**割り当て解除**] をクリックします。

   変更内容に応じて、新しいディストリビューションポイントがリストに追加されるか、既存のディストリビューションポイントがリストから削除されます。

# プッシュサーバーの有効化

Kaspersky Security Center Linux で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

ディストリビューションポイントをプッシュサーバーとして使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。ローカルタスクの実行と停止、管理対象アプリケーションの統計の受信、トンネルの作成など、一部の操作には継続的な接続が必要です。ディストリビューションポイントをプッシュサーバーとして使用する場合は、管理対象デバイスで [**管理サーバーから切断しない**] をオンにしたり、ネットワークエージェントの UDP ポートにパケットを送信したりする必要はありません。

プッシュサーバーは、最大 50,000 件の同時接続の負荷をサポートします。

*ディストリビューションポイントでプッシュサーバーを有効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. プッシュサーバーを有効にするディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。
4. ［**全般**］セクションで、［**プッシュサーバーを実行**］をオンにします。
5. ［**プッシュサーバーのポート**］フィールドで、ポート番号を入力します。使用されていないポートの番号を入力できます。
6. ［**リモートホストのアドレス**］フィールドで、ディストリビューションポイントデバイスの IP アドレスまたは名前を指定します。
7. ［OK］をクリックします。

選択したディストリビューションポイントでプッシュサーバーが有効になります。

# klnagent サービスのファイル記述子の上限を引き上げる

Linux ベースのディストリビューションポイントの対象範囲に多数のデバイスが含まれる場合、開くことができるファイル（ファイル記述子）の既定の制限では不十分な場合があります。これを回避するために、klnagent サービスのファイル記述子の上限を引き上げることができます。

*klnagent サービスのファイル記述子の上限を引き上げるには：*

1. ディストリビューションポイントとして機能する Linux ベースのデバイスで、ファイル `/lib/systemd/system/klnagent64.service` を開き、`[Service]` セクションの `LimitNOFILE` パラメータでファイル記述子のハード上限とソフト上限を指定します：

   `LimitNOFILE=< ソフトリソース制限 >:< ハードリソース制限 >`

   たとえば、`LimitNOFILE=32768:131072` と指定します。ファイル記述子のソフト上限はハード上限以下でなければならないことに注意してください。

2. パラメータが正しく指定されていることを確認するには、次のコマンドを実行します。

   `systemd-analyze verify klnagent64.service`

   パラメータが誤って指定されている場合、このコマンドは次のいずれかのエラーを出力する可能性があります：

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     このエラーが発生した場合、`LimitNOFILE` 行の記号が正しく指定されていません。入力した行を確認して修正する必要があります。

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     このエラーが発生した場合、入力したファイル記述子のソフト上限がハード上限を超えています。入力した行をチェックして、ファイル記述子のソフト上限がハード上限以下であることを確認する必要があります。

3. 次のコマンドを実行して、systemd プロセスを再読み込みします：

   `systemctl daemon-reload`

4. 次のコマンドを実行して、ネットワークエージェントサービスを再起動します：

   `systemctl restart klnagent`

5. 指定したパラメータが正しく適用されていることを確認するには、次のコマンドを実行します：

   `less /proc/< nagent プロセス ID >/limits`

   `< nagent プロセス ID >`パラメータは、ネットワークエージェントプロセスの識別子です。識別子を取得するには、次のコマンドを実行します：

   `ps -ax | grep klnagent`

Linux ベースのディストリビューションポイントでは、開くことができるファイルの上限が引き上げられました。

# デバイスのステータスの概要

Kaspersky Security Center Linux は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center Linux はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center Linux が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK*または*OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

| 条件 | 条件の説明 | 設定可能な値 |
| --- | --- | --- |
| セキュリティ製品がインストールされていません | デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。 | • 切り替えスイッチをオン<br>• 切り替えスイッチをオフ |
| ウイルスが多数検知されました | マルウェアスキャンタスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。 | 0 より大きい値 |
| リアルタイム保護レベルが管理者の設定と異なります | デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。 | • 停止<br>• 一時停止<br>• 実行中 |
| マルウェアのスキャンが長期間実行されていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャンタスク*もローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。 | 1日より大きい値 |
| 定義データベースがアップデートされていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。 | 1日より大きい値 |
| 長期間接続されていません | デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。 | 1日より大きい値 |
| アクティブな脅威を検知しました | ［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。 | 0 項目より大きい値 |
| 再起動が必要です | デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。 | 0 分より大きい値 |
| 競合アプリケーションがインストールされています | デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| ソフトウェアの脆弱性が検知されました | デバイスはネットワーク上で可視でネットワークエージェントもインストールされていますが、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された重要度の脆弱性を検知しました。 | • 緊急<br>• 高<br>• 中<br>• 脆弱性を修正できない場合は無視する<br>• 修正プログラムがインストール用に割り当てられている場合は無視する |
| ライセンスの有効期間が終了しました | デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |

| 条件 | 条件の説明 | 設定可能な値 |
| --- | --- | --- |
| ライセンスの有効期間がまもなく終了します | デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。 | 0 日より大きい値 |
| Windows Update 更新プログラムのチェックが長期間実行されていません | デバイスはネットワーク上で可視ですが、*Windows Update の同期の実行*タスクが実行されていない状態が指定期間を越えて続いています。 | 1 日より大きい値 |
| 暗号化ステータスが無効です | デバイスにネットワークエージェントはインストールされていますが、デバイスの暗号化結果が割り当て条件として指定されているものと合致しました。 | • ユーザーが拒否したため、ポリシーに準拠していない（外部デバイスのみ）。<br>• エラーにより、ポリシーに準拠していない。<br>• ポリシーを適用したら再起動する必要がある。<br>• 暗号化ポリシーが指定されていない。<br>• サポートされていない。<br>• ポリシーを適用するとき。 |
| モバイルデバイスの設定がポリシーに適合していません | コンプライアンスルールをチェックしたところ、モバイルデバイスの設定が Kaspersky Endpoint Security for Android ポリシーで指定された設定と異なります。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| 未処理のセキュリティ問題が検出されました | 未処理のセキュリティ問題がデバイス上でいくつか見つかりました。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| 製品が定義したデバイスのステータス | デバイスのステータスが管理対象アプリケーションによって定義されています。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| デバイスに空き容量がありません | デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。 | 0 MB より大きい値。 |
| デバイスが管理対象外になりました | デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| プロテクションが無効です | デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。<br>この場合、セキュリティ製品の状態は*停止中*またはエラーとなり、*開始中*、*実行中*、*中断中*とは異なります。 | 0 分より大きい値 |
| セキュリティ製品が実行されていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |

Kaspersky Security Center Linux では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、**定義データベースがアップデートされていません**条件の値が**3 日より大きい値**の場合はクライアントデバイスに*警告*ステータスが割り当てられ、条件値が**7 日より大きい値**の場合は*緊急*ステータスが割り当てられます。

Kaspersky Security Center Linux を旧バージョンからアップグレードしても、ステータスを*緊急*または*警告*に割り当てるための**定義データベースがアップデートされていません**条件の値は変更されません。

Kaspersky Security Center Linux によってデバイスにステータスが割り当てられると、一部の条件（上表の条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは定義データベースがアップデートされていません条件を満たしていたために、*緊急*ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスには*OK*ステータスが割り当てられます。

# デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

*デバイスのステータスの「緊急」への切り替えを有効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。

5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［緊急］ステータスを割り当てる条件をオンにします。




> 親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「緊急」ステータスが割り当てられます。

*デバイスのステータスの「警告」への切り替えを有効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［警告］ステータスを割り当てる条件をオンにします。

> 親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。

7. リストの左上にある［**編集**］をクリックします。

8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。

9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

# デバイスの抽出

*デバイスの抽出*は、特定の条件を指定してデバイスをフィルタリングできる機能です。デバイスの抽出を使用して、複数のデバイスを管理できます。たとえば、デバイスの抽出に含まれるデバイスのみを対象とするレポートを表示したり、デバイスの抽出に含まれるデバイスすべてを別のグループに移動したりできます。

Kaspersky Security Center Linux では、様々な*定義済みの抽出*（例：「**「緊急」ステータスのデバイス**、**プロテクションが無効です**、**アクティブな脅威を検知しました**）を使用できます。定義済みの抽出は削除できません。*ユーザー定義の抽出*を追加で作成し設定できます。

ユーザー定義の抽出では、抽出範囲を「すべてのデバイス」「管理対象デバイス」「未割り当てデバイス」から選択できます。抽出条件のパラメータを指定できます。デバイスの抽出では、異なるパラメータを指定した複数の抽出条件を作成できます。たとえば、2 つの条件を作成し、それぞれに異なる IP アドレス範囲を指定できます。複数の条件を指定した場合、デバイスの抽出はいずれかの条件に 1 つでも一致するデバイスを表示します。これに対して、1 つの条件内で複数のパラメータが指定されている場合、すべてのパラメータを満たすことが求められます。たとえば、1 つの条件内で IP アドレス範囲とインストールされている製品名の両方が指定されている場合、該当する製品がインストールされていてなおかつ IP アドレスが指定した範囲内のデバイスのみが表示されます。

# デバイスの抽出からデバイスリストを表示

Kaspersky Security Center Linux には、デバイスの抽出からデバイスのリストを表示できます。

*デバイスの抽出からデバイスリストを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。

2. 抽出リストで、デバイスの抽出の名前をクリックします。
   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。

3. デバイステーブルのデータは、次のようにしてグループ化およびフィルタリングできます：

   - 設定アイコン（⚙）をクリックし、テーブルに表示する列を選択します。

   - フィルターアイコン（ ⛛ ）をクリックしてから、呼び出したメニューでフィルター条件を指定して適用します。
     デバイスをフィルタリングしたテーブルが表示されます。

デバイスの抽出で1つまたは複数のデバイスを選択し、［**新規タスク**］をクリックして、これらのデバイスに適用されるタスクを作成できます。

デバイスの抽出で選択したデバイスを別の管理グループに移動するには、［**グループへ移動**］をクリックし、ターゲットの管理グループを選択します。

# デバイスの抽出の作成

*デバイスの抽出を作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. ［**追加**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. 新しい抽出の名前を入力します。
4. デバイスの抽出に含めるデバイスを含むグループを指定します：
   - ［**デバイスの検索**］ - 選択基準を満たし、［**管理対象デバイス**］または［**未割り当てデバイス**］グループに含まれるデバイスを検索します。
   - ［**管理対象デバイスの検索**］ - 選択基準を満たし、［**管理対象デバイス**］グループに含まれるデバイスを検索します。
   - ［**未割り当てデバイスの検索**］ - 選択基準を満たし、［**未割り当てデバイス**］グループに含まれるデバイスを検索します。

   ［**セカンダリ管理サーバーのデータを含める**］を有効にして、選択基準を満たし、セカンダリ管理サーバーによって管理されているデバイスを検索できるようにします。
5. ［**追加**］をクリックします。
6. 表示されたウィンドウで、この抽出に含めるデバイスが満たす必要のある条件を指定し、［**OK**］をクリックします。
7. ［**保存**］をクリックします。

デバイスの抽出が作成され、リストに追加されます。

# デバイスの抽出の設定

*デバイスの抽出を設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. 関連するユーザー定義のデバイス抽出を選択し、［**プロパティ**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。

3. ［**全般**］タブで、［**新規の条件**］をクリックします。

4. この抽出に含めるデバイスが満たす必要のある条件を指定します。

5. ［**保存**］をクリックします。

   設定が適用され保存されます。

以下に、デバイスを抽出に割り当てる条件について説明します。条件は論理演算子「OR」を使用して結合されます。抽出には、少なくとも1つの条件を満たすデバイスが含まれます。

## 全般

［**全般**］セクションでは、抽出条件の名前を変更したり、条件を反転させたりすることができます：

**抽出の条件を反転させる**

このオプションをオンにすると、指定した抽出条件の選択状態が反転します。指定した条件に合致しないすべてのデバイスが、抽出に含まれるようになります。

既定では、このオプションはオフです。

## ネットワークインフラストラクチャ

［**ネットワーク**］サブセクションでは、ネットワークデータを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **デバイス名**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **ドメイン**

  指定したワークグループに含まれるデバイスをすべて表示します。

- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。

- **説明**

デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。

［**説明**］で検索に使用する表現として、次の文字を使用できます：

- 1つの単語：
  - ***** -文字数不定の任意の文字列を表します。

    **例**：

    **Server** または **Server's** などの単語を記述するには、**Server*** と入力します。

  - **?** -任意の1文字を表します。

    **例**：

    **SUSE Linux Enterprise Server 12** や **SUSE Linux Enterprise Server 15** などの単語を記述するには、「**SUSE Linux Enterprise Server 1?**」と入力します。

    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。

- 複数の単語による検索：
  - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    **例**：

    **Secondary** または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。

  - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    **例**：

    **Secondary** と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。

  - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    **例**：

    **Secondary** が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。

  - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    **例**：

    **Secondary Server** という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

- **別の管理サーバーの管理対象**

  次のいずれかの値を選択します：

  - **はい**：デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
  - **いいえ**：デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

［**ドメインコントローラー**］サブセクションでは、ドメインメンバーシップに基づいてデバイスを選択範囲に含める基準を設定できます：

- **デバイスが配置されているドメイン組織単位**

  このオプションをオンにすると、入力フィールドで指定されたドメイン組織単位のデバイスが選択されます。

  既定では、このオプションはオフです。

- **デバイスが属しているドメインセキュリティグループ**

  このオプションをオンにすると、入力フィールドで指定されたドメインセキュリティグループのデバイスが選択されます。

  既定では、このオプションはオフです。

［**ネットワーク活動**］サブセクションでは、ネットワークアクティビティを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **ディストリビューションポイントとして動作**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - **いいえ**：ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
  - **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **接続プロファイルが切り替えられました**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
  - **いいえ**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

  このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

  過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

  このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

  このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

  既定では、このオプションはオフです。

- **デバイスが可視**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

  - **はい**：ネットワークで現在可視のデバイスを抽出に含めます。
  - **いいえ**：ネットワークで現在不可視のデバイスを抽出に含めます。
  - **値を選択しない**：基準は適用されません。

## デバイスのステータス

［**管理対象デバイスのステータス**］サブセクションでは、管理対象アプリケーションからのデバイスのステータスの説明を基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスのステータス**

  ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「*警告*」）を選択します。

- **リアルタイム保護のステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

- **デバイスステータスの説明**

  このフィールドで、「*OK*」、「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

［**管理対象アプリケーションのコンポーネントのステータス**］サブセクションでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

  サーバーコラボレーションの保護ステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

  メールサーバーの保護のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor ステータス**

  Endpoint Sensor のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

［**管理対象アプリケーションのステータスに影響がある問題**］サブセクションでは、管理対象アプリケーションで検知される可能性のある問題のリストを基にデバイスを抽出に含めるために使用する基準を設定できます：選択した問題のうち1つ以上の問題が存在するデバイスが抽出に含まれます複数のアプリケーションを対象とする問題については、同じ問題をすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

## システムの詳細

［**オペレーティングシステム**］セクションでは、オペレーティングシステム種別を基にデバイスを抽出に含める場合に使用する基準を指定できます。

- **プラットフォームの種別**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビット数**

  ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（[**不明**]、[**x86**]、[**AMD64**]、[**IA64**]）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS のビルド**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース番号**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

［**仮想マシン**］セクションでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかによってデバイスを抽出に含めるための基準を設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のオプションを選択できます：

  - **未定義**。
  - **いいえ**：仮想マシンでないデバイスを検索します。
  - **はい**：仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

  このドロップダウンリストで、仮想マシンの製造元を選択できます。

  このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

  このドロップダウンリストで、次のオプションを選択できます：

  - **未定義**。
  - **いいえ**：仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
  - **はい**：仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

［**ハードウェアレジストリ**］サブセクションでは、取り付けたハードウェアを基にデバイスを抽出に含めるための基準を設定できます：

ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

- **デバイス**

  このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **デバイス名**

  指定された名前のデバイスが抽出に含まれます。

- **説明**

  デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

  デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **デバイスの製造元**

  デバイスの製造元の名前。このフィールドで指定された製造元のデバイスが抽出に含まれます。

  コンピューターの製造元名は、デバイスのプロパティウィンドウで入力できます。

- **シリアル番号**

  このフィールドで指定されたシリアル番号が付けられたすべてのハードウェアユニットが抽出に含まれます。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **ユーザー**

  このフィールドで指定されたユーザーのすべてのハードウェアユニットが抽出に含まれます。

- **場所**

  デバイスまたはハードウェアユニットの場所（本社、支社など）。このフィールドで指定された場所に導入されるコンピューターまたはその他のデバイスが抽出に含まれます。

  デバイスの場所は、そのデバイスのプロパティウィンドウにおいて、あらゆる形式で記載できます。

- **CPU クロック周波数（MHz）（最小）**

  CPU の最小クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **CPU クロック周波数（MHz）（最大）**

  CPU の最大クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最小）**

  仮想 CPU コアの最小数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最大）**

  仮想 CPU コアの最大数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最小）**

  デバイス上のハードディスクの最小容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最大）**

  デバイス上のハードディスクの最大容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最小）**

  デバイスの RAM の最小サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最大）**

  デバイスの RAM の最大サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

## サードパーティ製ソフトウェアの詳細

［**アプリケーションレジストリ**］サブセクションでは、インストール済みのアプリケーションを基にデバイスを検索するための基準を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

  選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

  デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

  このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

  既定では、このオプションはオフです。

- **互換性がないセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、選択したタグがいずれも説明に含まれないデバイスが抽出に含まれます。

  このオプションをオフにすると、基準が適用されません。

  既定では、このオプションはオフです。

［**脆弱性とアップデート**］サブセクションでは、Windows Update をどこから取得するかを基にデバイスを抽出に含める場合に使用する基準を指定できます：

**WUA の管理サーバーへの切り替え**

このドロップダウンリストから、次のいずれかを選択できます：

- **はい**：これを選択すると、Windows Update の更新プログラムを管理サーバーから受信するデバイスが検索結果に含まれます。
- **いいえ**：これを選択すると、Windows Update の更新プログラムを他の提供元から受信するデバイスが検索結果に含まれます。

## カスペルスキー製品の詳細

［**カスペルスキー製品**］サブセクションでは、選択した管理対象アプリケーションを基にデバイスを抽出に含めるための基準を設定できます：

- **アプリケーション名**

  カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

  リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

  アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

  カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

  製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  このフィールドが空白の場合、この基準は適用されません。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **モジュールの最終アップデート期間を選択**

  このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **デバイスを管理サーバーで管理する**

  ドロップダウンリストで、Kaspersky Security Center Linux で管理されているデバイスを抽出に含めることができます：

  - **はい**Kaspersky Security Center Linux で管理されているデバイスが抽出に含まれます。
  - **いいえ**：Kaspersky Security Center Linux により管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされています**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**：セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - **いいえ**：セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

［**アンチウイルスによる保護**］サブセクションでは、保護ステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **定義データベースのレコード数**

  このオプションを有効にすると、定義データベースのレコード数でクライアントデバイスを検索できます。入力フィールドで、定義データベースのレコード数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回マルウェアスキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回マルウェアスキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知された脅威**

  このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

［**暗号化**］サブセクションでは、選択した暗号化アルゴリズムを基にデバイスを抽出に含めるための基準を設定できます：

**暗号化アルゴリズム**

Advanced Encryption Standard（AES）対称ブロック暗号アルゴリズム。ドロップダウンリストから、暗号化キーのサイズ（56 ビット、128 ビット、192 ビット、または 256 ビット）を選択できます。

指定可能な値：*AES56*、*AES128*、*AES192*、または *AES256*。

［**製品コンポーネント**］サブセクションには、対応する管理プラグインが Kaspersky Security Center Web コンソールにインストールされているアプリケーションのコンポーネントのリストが含まれています。

［**製品コンポーネント**］サブセクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

  アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。次のステータスのいずれかを選択できます：*N/A*、*停止*、*一時停止*、*開始中*、*実行中*、*失敗*、*インストールされていない*、*ライセンスでサポートされていない*。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

  製品から送信されるステータス：

  - *停止* - コンポーネントが無効で、現在動作していません。
  - *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
  - *開始中* - コンポーネントが利用開始プロセスを実行中です。
  - *実行中* - コンポーネントが有効で正常に動作しています。
  - *エラー* - コンポーネントの動作中にエラーが発生しました。
  - *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。
  - *ライセンスでサポートされていない* - ライセンスは選択したコンポーネントをカバーしていません。

  他のステータスとは異なり、［*N/A*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

  リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

## タグ

［**タグ**］セクションでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスを抽出に含めるための基準を設定できます：

**少なくとも 1 個のタグが一致する場合に適用する**

このオプションをオンにすると、選択されたタグを1つ以上説明に含むデバイスが検索結果に表示されます。

このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

既定では、このオプションはオフです。

基準にタグを追加するには、[**追加**]をクリックし、[**タグ**]入力フィールドをクリックしてタグを選択します。選択したタグを持つデバイスをデバイスの抽出に含めるか除外するかを指定します。

- **このタグが割り当てられているすべてのデバイス**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **このタグが割り当てられていないすべてのデバイス**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

## ユーザー

[**ユーザー**]セクションでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを抽出に含めるための基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにすると、基準を設定するためのユーザーアカウントを選択できます。選択したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも1回システムにログインしたユーザー**

  このオプションをオンにする場合は、[**参照**]をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムに少なくとも1回ログインしたデバイスが検索結果に含まれます。

### デバイスの所有者

［**デバイスの所有者**］セクションでは、デバイスの登録所有者、そのロール、セキュリティグループのメンバーシップに応じて、抽出に含めるデバイス基準を設定できます。

- **デバイスの所有者**

  内部セキュリティグループからデバイスの所有者のユーザー名を選択します。このセクションでは、ユーザーとユーザーのロールについて詳しく説明します。

  デバイスの所有者として登録できるユーザーは1人だけです。

- **デバイスの所有者が属している Active Directory セキュリティグループ**

  デバイスの所有者が属している外部 Active Directory セキュリティグループを選択します。

  ユーザーは、Active Directory セキュリティグループの一部になることも、この Active Directory セキュリティグループに含まれるグループの一部になることもできます。

- **デバイス所有者のロール**

  デバイスの所有者に割り当てられたロールを選択します。ユーザーのロールの詳細については、この記事をご覧ください。

- **内部セキュリティグループでのデバイスの所有者のメンバーシップ**

  デバイスの所有者が属する内部セキュリティグループを選択します。

# デバイスの抽出からデバイスリストをエクスポート

Kaspersky Security Center Linux には、デバイスの抽出からデバイスに関する情報を CSV または TXT ファイルに保存できます。

*デバイスの抽出からデバイスリストを表示するには：*

1. デバイスの抽出からデバイスを含むテーブルを開きます。
2. 次のいずれかの方法を使用して、抽出するデバイスを選択します：
   - 特定のデバイスを選択するには、その横にあるチェックボックスをオンにしてください。
   - 現在のテーブルページからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**現在のページをすべて選択**］をオンにします。
   - テーブルからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**すべて選択**］をオンにします。
3. ［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。テーブルに含まれる抽出したデバイスに関するすべての情報がエクスポートされます。

フィルター条件をデバイステーブルに適用した場合、エクスポートされるのは、表示された列からフィルター処理されたデータのみです。

# 抽出で管理グループからデバイスを削除

デバイスの抽出作業を行う場合は、デバイスを削除する必要がある管理グループに切り替えずに、この抽出に含まれる管理グループからデバイスを削除することができます。

*管理グループからデバイスを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出リストで、デバイスの抽出の名前をクリックします。

   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。
3. 削除するデバイスを選択し、［**削除**］をクリックします。

   選択したデバイスが対応する管理グループから削除されます。

# デバイスのタグ

Kaspersky Security Center Linux では、デバイスに*タグ付け*できます。タグは、デバイスのグループ化、説明、または検索に使用できる文字列値です。デバイスに割り当てられたタグは、抽出の作成、デバイスの検索、および各管理グループへのデバイスの割り当てに使用できます。

デバイスには、手動または自動でタグ付けできます。個々のデバイスにタグを付ける場合は、手動タグ付けを使用できます。自動タグ付けは、Kaspersky Security Center Linux によって次のいずれかの方法で実行されます：

- 指定されたタグ付けルールに従います。
- アプリケーションによって。

同じタグを割り当てるために異なるタグ付け方法を使用することは推奨しません。たとえば、タグがルールによって割り当てられる場合、このタグをデバイスに手動で割り当てることは推奨しません。

タグがルールによって割り当てられる場合、指定されたルールが満たされるとデバイスは自動的にタグ付けされます。個々のルールは各タグに対応します。ルールは、デバイス、オペレーティングシステム、デバイスにインストールされたアプリケーションのネットワークプロパティ、およびその他のデバイスのプロパティに適用されます。たとえば、CentOS オペレーティングシステムが実行されているすべてのデバイスに `[CentOS]` タグを割り当てるルールを設定できます。その後、デバイスの抽出を作成する場合にこのタグを使用できます。これにより、すべての CentOS のデバイスを抽出し、タスクを割り当てることができます。

タグごとに追加できる自動タグ付けルールは1つだけです。同じタグに対して新しいルールを作成すると、以前のルールは置き換えられます。

次の場合は、デバイスからタグが自動的に削除されます：

- タグの割り当てルールの条件をデバイスが満たさなくなった場合。
- タグを割り当てるルールがオフになったあるいは削除された場合。

管理サーバーごとのタグのリストとタグ付けルールのリストは、プライマリ管理サーバーとセカンダリ管理サーバーを含むその他のすべての管理サーバーとは影響関係を持ちません。タグ付けのルールは、ルールが作成された管理サーバーのデバイスに対してのみ適用されます。

# デバイスタグの作成

*デバイスのタグを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. ［**タグ**］にタグ名を入力します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに新しいタグが表示されます。

# デバイスタグの名前変更

*デバイスタグの名前を変更するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 名前を変更するタグの名前をクリックします。
   タグのプロパティウィンドウが表示されます。
3. ［**タグ**］でタグ名を変更します。
4. ［**保存**］をクリックして変更内容を保存します。

デバイスタグのリストに更新したタグが表示されます。

# デバイスタグの削除

手動で割り当てられたタグのみ削除できます。

*手動で割り当てられたデバイスタグを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
   タグのリストが表示されます。
2. 削除したいデバイスタグを選択します。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**はい**］をクリックします。

デバイスタグが削除されます。削除されたタグが割り当てられていたすべてのデバイスから、このタグが自動的に削除されます。

自動タグ付けルールによってデバイスに割り当てられたタグを削除しても、ルールは削除されず、デバイスがルール条件を初めて満たした時に、タグが新しいデバイスに割り当てられます。自動タグ付けルールを削除すると、ルール条件で指定されたタグは、割り当てられているすべてのデバイスから削除されますが、タグのリストからは削除されません。必要に応じて、リストからタグを手動で削除できます。

このタグがアプリケーションまたはネットワークエージェントによってデバイスに割り当てられている場合、削除されたタグはデバイスから自動的に削除されません。デバイスからタグを削除するには、klscflag ユーティリティを使用します。

# タグを割り当てられているデバイスの表示

*タグを割り当てられているデバイスを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 割り当て先のデバイスを確認するタグの横の［**デバイスの表示**］をクリックします。

   メインメニューの［**管理対象デバイス**］セクションにリダイレクトされ、［**デバイスの表示**］リンクをクリックしたタグでデバイスがフィルタリングされます。
3. デバイスタグのリストに戻るには、ブラウザーの［**戻る**］をクリックします。

タグが割り当てられているデバイスを表示した後、新しいタグを作成して割り当てるか、既存のタグを他のデバイスに割り当てることができます。この場合、タグによるフィルターを削除し、デバイスを抽出してからタグを割り当てる必要があります。

# デバイスに割り当てられているタグの表示

*デバイスに割り当てられているタグを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。

   選択したデバイスに割り当てられているタグのリストが表示されます。［**タグの割り当て**］列では、タグがどのように割り当てられたかを確認できます。

ツールバーで次の操作を実行できます：

- デバイスに別のタグを割り当てます。
- 既に割り当てられているタグを削除します。
- 管理サーバーに存在するすべてのデバイスタグを表示します。

割り当てられたタグをデバイス上でローカルに表示することはできません。

# デバイスへの手動でのタグ付け

*デバイスを手動でタグ付けするには：*

1. メニューを移動して、別のタグを追加するデバイスに割り当てられているタグを表示します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウで、次のいずれかを実行します：
   - 新しいタグを作成して割り当てるには、［**新しいタグを作成する**］を選択して新しいタグの名前を入力します。
   - 既存のタグを選択するには、［**既存のタグを割り当てる**］を選択し、ドロップダウンリストから目的のタグを選択します。
4. ［**OK**］をクリックして変更を適用します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したタグがデバイスに割り当てられます。

# デバイスに割り当てたタグの削除

*デバイスからタグを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。
4. 削除するタグに隣接するチェックボックスをオンにします。
5. リストの上部にある［**タグを解除しますか？**］をクリックします。
6. 表示されたウィンドウで［**はい**］をクリックします。

タグがデバイスから削除されます。

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションまたはネットワークエージェントによってデバイスに割り当てられたタグを手動で削除することはできません。これらのタグを削除するには、klscflag ユーティリティを使用します。

# デバイスの自動タグルールの表示

*デバイスの自動タグルールを表示するには：*

次のいずれかの手順を実行します：

- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**自動タグルール**］の順に選択します。
- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に移動し、［**自動タグルールの設定**］をクリックします。
- デバイスに割り当てられているタグを確認し、［**設定**］をクリックします。

デバイスの自動タグルールのリストが表示されます。

# デバイスの自動タグルールの編集

*デバイスの自動タグルールを編集するには：*

1. デバイスの自動タグルールを表示します。
2. 編集するルールの名前をクリックします。
   ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を編集します：
   a. ［**ルール名**］で、ルール名を変更します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
4. 次のいずれかの手順を実行します：
   - 新しい条件を追加する場合は、［**追加**］をクリックし、開いたウィンドウで新しい条件の設定を指定します。
   - 既存の条件を編集するには、編集する条件の名前をクリックし、条件設定を編集します。
   - 条件を削除するには、削除する条件の横のチェックボックスを選択し、［**削除**］をクリックします。
5. 設定ウィンドウで、［**OK**］をクリックします。
6. ［**保存**］をクリックして変更内容を保存します。

編集後のルールがリストに表示されます。

# デバイスの自動タグルールの作成

*デバイスの自動タグルールを作成するには：*

1. デバイスの自動タグルールを表示します。
2. ［**追加**］をクリックします。
   新規ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を設定します：
   a. ［**ルール名**］で、ルール名を入力します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
   c. ［**タグ**］で、新しいデバイスタグの名前を入力するか、リストから既存のデバイスタグを選択します。
      名前は 256 文字以下でなければなりません。
4. 条件セクションで［**追加**］をクリックして新しい条件を追加します。
   新しい条件の設定ウィンドウが表示されます。
5. 条件の名前を入力します。
   名前は 256 文字以下でなければなりません。名前は、1 つのルール内で一意である必要があります。
6. 次の条件によりルールのトリガーを設定します：複数の条件を選択できます。
   - **ネットワーク** - デバイスのネットワークプロパティ（デバイスの DNS 名、デバイスが IP サブネットに含まれるかなど）。

     Kaspersky Security Center Linux で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、自動タグ付けルールが機能しません。
   - **アプリケーション** - デバイス上のネットワークエージェントの存在、オペレーティングシステムの種別、バージョン、アーキテクチャ。
   - **仮想マシン** - デバイスが仮想マシンの特定の種別に属しているかどうか。
   - **アプリケーションレジストリ** - デバイス上の異なる製造元によるアプリケーションの存在。

7. ［**OK**］をクリックして変更内容を保存します。

   必要に応じて、1つのルールに対して複数の条件を設定できます。この場合、タグは少なくとも1つの条件を満たすデバイスに割り当てられます。

8. ［**保存**］をクリックして変更内容を保存します。

新しく作成されたルールは、選択した管理サーバーによって管理されているデバイスに適用されます。デバイスの設定がルールの条件を満たす場合、そのデバイスにタグが割り当てられます。

設定後、ルールは次の状況で適用されます：

- サーバーの負荷に応じて、自動的かつ定期的に適用
- ルールの編集後に適用
- 手動でのルール実行時に適用
- ルールの条件に合致するデバイスの設定の変更やデバイスのグループの設定の変更を管理サーバーが検知した後に適用

複数のタグ付けルールを作成できます。複数のタグ付けルールを作成しており、それらのルールのそれぞれの条件が同時に満たされる場合は、1つのデバイスに複数のタグを割り当てることができます。すべての割り当てられたタグのリストは、デバイスのプロパティで確認できます。

# デバイスの自動タグルールの実行

ルールを実行すると、ルールのプロパティで指定されたタグが、ルールのプロパティで指定された条件に合致するデバイスに割り当てられます。有効なルールのみを実行できます。

*デバイスの自動タグルールを実行するには：*

1. デバイスの自動タグルールを表示します。
2. 実行する有効なルールに隣接するチェックボックスをオンにします。
3. ［**ルールを実行**］をクリックします。

   選択したルールが実行されます。

# デバイスの自動タグルールの削除

*デバイスの自動タグルールを削除するには：*

1. デバイスの自動タグルールを表示します。
2. 削除するルールに隣接するチェックボックスをオンにします。

3. ［**削除**］をクリックします。

4. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

選択したルールが削除されます。このルールのプロパティで指定されていたタグは、このタグが割り当てられていたすべてのデバイスから割り当て解除されます。

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

# klscflag ユーティリティを使用したデバイスタグの管理

デバイスにタグのセットを割り当てるには、タグを割り当てるクライアントデバイスで klscflag ユーティリティを実行する必要があります。

klscflag ユーティリティは、デバイスに割り当てられている既存のタグを上書きします。つまり、希望のタグセットをコマンドで指定することで、タグを追加したり削除することができます。このユーティリティには、個々のタグを追加または削除するための個別のコマンドはありません。代わりに、タグのセット全体を変更します。

klscflag などのコマンドでタグ名を指定する場合は、すべて大文字にするなど、大文字と小文字を統一したアプローチを使用することをお勧めします。すべて大文字を使用すると、DBMS 構成に応じて、大文字と小文字のみが異なるタグで発生する潜在的な問題を回避できます。

*klscflag ユーティリティを使用してデバイスに 1 つ以上のタグを割り当てるには：*

1. ルート権限を持つアカウントを使用してコマンドプロンプトを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、ネットワークエージェントがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/klnagent64/sbin/ です。

2. 次のコマンドのいずれかを入力します：

   - タグのセットを割り当てるには：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"タグ名 1\",\"タグ名 2\",\"タグ名 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     ここで、**[\"タグ名 1\",\"タグ名 2\",\"タグ名 3\"]** は、デバイスに割り当てるタグのリストです。

     角かっこを空のままにすると、デバイスからすべてのタグが削除されます：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - 既存のタグセットに新しいタグを割り当てるには：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"新しいタグ名\",\"タグ名 1\",\"タグ名 2\",\"タグ名 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     ここで、**新しいタグ名** はデバイスに割り当てるタグの名前であり、**タグ名 1**、**タグ名 2**、**タグ名 3** はデバイスに既に割り当てられているタグの名前です。

   - デバイスに既に割り当てられている他のタグを削除せずに特定のタグを削除するには、アップデートされたタグのセットを使用してコマンドを実行します。

     たとえば、現在のタグが **タグ名 1**、**タグ名 2**、**タグ名 3** で、**タグ名 2** を削除する場合は、次のコマンドを実行します：

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"タグ名 1\",\"タグ名 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. ネットワークエージェントサービスを再起動します。

   klscflag ユーティリティは、指定されたタグをデバイスに割り当てます。

4. klscflag ユーティリティが指定されたタグを正常に割り当てたことを確認するには、デバイスに割り当てられたタグを表示します。

または、デバイスタグを手動で割り当てることもできます。

# データ暗号化と保護機能

データ暗号化により、ノート PC やハードディスクの盗難や紛失が発生した場合に機密データや企業データが意図せず漏洩するリスクが軽減されます。また、不正なユーザーやアプリケーションによるアクセスを防止できます。

Kaspersky Endpoint Security for Windows がインストールされた Windows ベースの管理対象デバイスがネットワークに含まれている場合、データ暗号化機能を使用できます。この場合、Windows オペレーティングシステムを実行しているデバイスでは、次の種類の暗号化を管理できます：

- BitLocker ドライブ暗号化
- Kaspersky Disk Encryption

Kaspersky Endpoint Security for Windows のこれらのコンポーネントを使用すると、暗号化を有効または無効にする、暗号化されたドライブのリストを表示する、暗号化に関するレポートを生成して表示する、などの操作を実行できます。

暗号化を設定するには、Kaspersky Security Center Linux で Kaspersky Endpoint Security for Windows ポリシーを定義します。Kaspersky Endpoint Security for Windows は、アクティブなポリシーに基づいて、暗号化と復号化を実行します。ルールの編集方法と暗号化機能の詳細については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

現在、管理サーバーの階層の暗号化管理は Web コンソールでは利用できません。暗号化されたデバイスを管理するには、プライマリ管理サーバーを使用します。

ユーザーインターフェイス設定を使用して、暗号化管理の機能に関連するインターフェイス要素の一部を表示または非表示にすることができます。

# 暗号化されたドライブのリストの表示

Kaspersky Security Center Linux で、暗号化されたドライブの詳細や、ドライブレベルで暗号化されたデバイスの詳細を表示できます。ドライブ上の情報が復号されると、そのドライブはリストから自動的に削除されます。

*暗号化されたドライブのリストを表示するには、*

メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

セクションがメニューにない場合、非表示になっています。セクションを表示させるには、ユーザーインターフェイスの設定で、［**データ暗号化と保護機能の表示**］を有効にします。

暗号化されたドライブのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。これを行うには、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

# 暗号化イベントのリストの表示

デバイス上でデータの暗号化または復号化タスクを実行する時、Kaspersky Endpoint Security for Windows は、次の種類のイベントに関する Kaspersky Security Center Linux 情報を送信します：

- ディスクの空き容量が不足しているため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- ライセンスの問題で、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アクセス権がないため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アプリケーションが暗号化されたファイルへのアクセスをブロックされている
- 不明なエラー

*デバイスでのデータの暗号化中に発生したイベントのリストを表示するには：*

メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化イベント**］の順に移動します。

セクションがメニューにない場合、非表示になっています。セクションを表示させるには、ユーザーインターフェイスの設定で、［**データ暗号化と保護機能の表示**］を有効にします。

暗号化されたドライブのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。これを行うには、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

または、すべての管理対象デバイスの暗号化イベントのリストを確認することができます。

*管理対象デバイスの暗号化イベントを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. 管理対象デバイスの名前をクリックします。
3. ［**全般**］タブで、［**プロテクション**］セクションに移動します。
4. ［**データ暗号化エラーの表示**］をクリックします。

# 暗号化レポートの作成と表示

次のレポートを作成できます：

- 管理対象デバイスの暗号化ステータスレポート：様々な管理対象デバイスのデータ暗号化について詳細を確認できます。たとえば、暗号化ルールが設定されたポリシーが適用されるデバイスの数が表示されます。また、再起動が必要なデバイスの数なども確認できます。さらに、各デバイスの暗号化技術とアルゴリズムに関する情報も含まれています。

- 大容量ストレージデバイスの暗号化ステータスレポート：管理対象デバイスの暗号化ステータスレポートと類似の情報が含まれますが、大容量ストレージデバイスとリムーバブルドライブのデータのみが表示されます。

- 暗号化されたドライブへのアクセス権に関するレポート：暗号化されたドライブへのアクセス権を持つユーザーアカウントが表示されます。

- ファイル暗号化のエラーに関するレポート：デバイスでデータの暗号化または復号化タスクを実行した時に発生したエラーの情報を含みます。

- 暗号化されたファイルへのアクセスのブロックに関するレポート：暗号化されたファイルへのアクセスのブロックに関する情報を含みます。このレポートは、暗号化されたファイルやドライブに不正なユーザーまたはアプリケーションがアクセスしようとした場合に役立ちます。

［**監視とレポート**］→［**レポート**］セクションの順に移動して、レポートを生成できます。または、［**操作**］→［**データ暗号化と保護機能**］セクションの順に移動して、次の暗号化レポートを生成できます：

- 大容量ストレージデバイスの暗号化ステータスレポート

- 暗号化されたドライブへのアクセス権に関するレポート

- ファイル暗号化のエラーに関するレポート

*［**データ暗号化と保護機能**］セクションで暗号化レポートを生成するには：*

1. インターフェイスのオプションで、［**データ暗号化と保護機能の表示**］がオンであることを確認します。

2. ポリシーのプロパティで、［**イベントの設定**］タブを開きます。

3. **緊急**セクションで、 **イベントの追加**をクリックし、 *ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました*イベントの横にあるチェックボックスをオンにします。

4. ［**OK**］をクリックします。

5. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］の順に移動します。

6. 次のいずれかのセクションを開きます：

   - **暗号化されたドライブ**：大容量ストレージデバイスの暗号化ステータスレポート、または暗号化されたドライブへのアクセス権に関するレポートが生成されます。

   - **暗号化イベント**：ファイル暗号化エラーのレポートが生成されます。

7. 生成するレポートの名前をクリックします。

レポート作成が開始されます。

# 暗号化されたドライブへのオフラインモードでのアクセス権の付与

管理対象デバイスに Kaspersky Endpoint Security for Windows がインストールされていない場合などに、ユーザーは、暗号化されたデバイスへのアクセスを要求できます。要求を受信したら、アクセスキーファイルを作成してユーザーに送信できます。すべてのユースケースと詳細な手順については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

*暗号化されたドライブへのオフラインモードでのアクセス権を付与するには：*

1. ユーザーからアクセス要求ファイル（拡張子が FDERTC のファイル）を取得します。Kaspersky Endpoint Security for Windows でファイルを生成するには、Kaspersky Endpoint Security for Windows のヘルプの指示に従ってください。
2. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

   暗号化されたドライブのリストが表示されます。
3. ユーザーがアクセスを要求したドライブを選択します。
4. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
5. 表示されるウィンドウで、Kaspersky Endpoint Security for Windows プラグインを選択します。
6. Kaspersky Endpoint Security for Windows のヘルプに記載された指示に従ってください（セクションの最後にある Kaspersky Security Center Web コンソールの手順を参照してください）。

その後、受信したファイルを適用して暗号化されたドライブにアクセスし、ドライブに保存されているデータを読み取ることができます。

# クライアントデバイスの管理サーバーの変更

特定のクライアントデバイスの管理サーバーを別のものに変更することができます。このためには、［*管理サーバーの変更*］タスクを使用します。

*クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：*

1. デバイスを管理する管理サーバーに接続します。

2. 管理サーバーの変更タスクを作成します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。新規タスクウィザードの［**新規タスク**］ウィンドウで［**Kaspersky Security Center 15.3**］を選択して、タスク種別に［**管理サーバーの変更**］を選択します。その後、管理サーバーを変更するデバイスを指定します：

   - **管理グループにタスクを割り当てる**

     任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

     たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

     タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

   - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

     タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

     特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

   - **デバイスの抽出にタスクを割り当てる**

     デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

     たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

3. 作成したタスクを実行します。

タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

管理サーバーで暗号化とデータ保護をサポートしている場合、［*管理サーバーの変更*］タスクを作成しようとすると、警告が表示されます。その警告には、デバイスに暗号化されたデータが保存される場合、新しいサーバーがデバイスの管理を開始すると、ユーザーは以前に処理したことがある暗号化データにしかアクセスできなくなることが示されます。それ以外の暗号化されたデータにはアクセスできなくなります。暗号化されたデータにアクセスできなくなるケースの詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# 複数の管理サーバー間での競合の回避

ネットワーク上に複数の管理サーバーがある場合、これらの管理サーバー上で同じクライアントデバイスが可視になる可能性があります。この結果、たとえば、管理サーバーが別の管理サーバーによって既にインストールされているアプリケーションをインストールしたり、その他の競合が発生したりする可能性があります。別の管理サーバーによって管理されているデバイスにアプリケーションがインストールされないようにするには、アプリケーションのリモートインストールタスクのプロパティで［**この管理サーバーで管理されているデバイスにのみインストール**］をオンにする必要があります。

［**この管理サーバーで管理されているデバイスにのみインストール**］をオンにし、*アプリケーションのリモートインストール*タスクを実行すると、デバイスが別の管理サーバーによって管理されているかどうかを確認するチェックが実行されます。別の管理サーバーによって管理されるデバイスの場合、［**別の管理サーバーの管理対象**］属性値は `true` に設定されます。*アプリケーションのリモートインストール*タスクはこれらのデバイスには適用されません。

［**別の管理サーバーの管理対象**］属性値は、管理対象デバイスのリストと未割り当てデバイスのリストの［**別の管理サーバーの管理対象**］列に表示されます。

また、［**別の管理サーバーの管理対象**］属性は、次の用途の識別条件としても使用できます：

- 管理対象デバイスの表示
- デバイスの抽出
- デバイス移動ルール
- 自動タグルール

*別の管理サーバーの管理対象属性をリセットするには：*

1. Kaspersky Security Center Web コンソールのメインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。
2. 必要なデバイスを選択し、［［**別の管理サーバーの管理対象**］**を削除する**］をクリックします。

   ［**別の管理サーバーの管理対象**］属性がリセットされます。

# 管理サーバーに接続されたデバイスを接続ゲートウェイ経由で別の管理サーバーに移動する

管理サーバーに接続されているデバイスを、接続ゲートウェイを介して別の管理サーバーに移動できます。たとえば、別のバージョンの管理サーバーをインストールし、時間がかかる可能性があるためデバイスにネットワークエージェントを再インストールしたくない場合に、これが必要になることがあります。

手順に記載されているコマンドは、管理者権限を持つアカウントでクライアントデバイス上で実行する必要があります。

*接続ゲートウェイを介して接続されたデバイスを別の管理サーバーに移動するには：*

1. klmover ユーティリティを `-address <サーバーのアドレス>` パラメータを指定して実行し、新しい管理サーバーに切り替えます。
2. `klnagchk -nagwait -tl 4` コマンドを実行します。
3. 新しい接続ゲートウェイを設定するには、次のコマンドを実行します：
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<ゲートウェイ IP または名前>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `gateway_ip_or_name` は、インターネットからアクセス可能な接続ゲートウェイのアドレスです。
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` は、接続ゲートウェイがリッスンしている TCP ポートの番号です。
4. `klnagchk -restart -tl 4` コマンドを実行して、ネットワークエージェントサービスを開始します。

デバイスは新しい管理サーバーに移動され、新しく接続されたゲートウェイを介して接続されます。

# デバイスが不可視の時の処理の表示と設定

グループ内のクライアントデバイスがアクティブでない場合、通知を受け取ることができます。こうしたデバイスを自動的に削除することもできます。

*グループ内のデバイスがアクティブでない場合の処理を表示したり設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 目的の管理グループの名前をクリックします。




管理グループの階層

管理グループのプロパティウィンドウが開きます。

3. プロパティウィンドウで［**設定**］タブに移動します。

4. ［**継承**］セクションで、次のオプションの有効と無効を切り替えます：

- **親グループから継承する**

  クライアントデバイスが属する親グループからこのセクションの設定が継承されます。このオプションをオンにすると、［**ネットワーク上のデバイスのアクティビティ**］の設定がロックされ変更できなくなります。

  このオプションは管理グループに親グループが存在する場合にのみ利用できます。

  既定では、このオプションはオンです。

- **設定を子グループへ強制的に継承させる**

  設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

  既定では、このオプションはオフです。




管理グループのロパティ

5. ［**デバイスのアクティビティ**］セクションで、次のオプションの有効と無効を切り替えます：

- **次の期間デバイスが不可視の場合管理者に通知（日）**

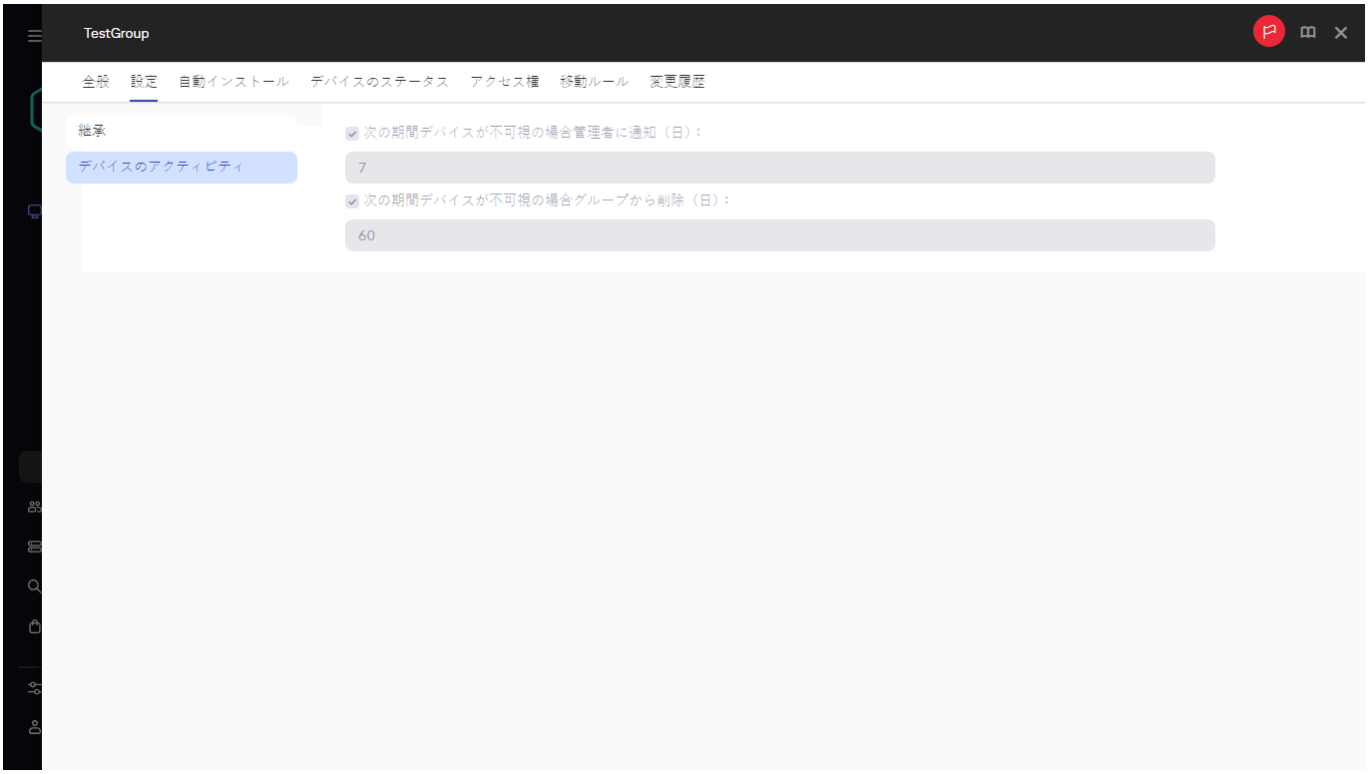
  このオプションをオンにすると、管理者が非アクティブなデバイスについて通知を受け取ります。［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定できます。既定の期間は 7 日です。

  既定では、このオプションはオンです。

- **次の期間デバイスが不可視の場合グループから削除（日）**

  このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定の期間は 60 日です。

  既定では、このオプションはオンです。




管理グループのロパティ

6. ［**保存**］をクリックします。

変更内容が保存され、適用されます。

# デバイスのユーザーへのメッセージの送信

*メッセージをデバイスのユーザーに送るには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

新規タスクウィザードが起動します。

3. ［**タスク種別**］ドロップダウンリストで、［**ユーザーにメッセージを送信**］を選択します。

4. タスクの適用対象として、1つのオプションをオンにして管理グループ、デバイスの抽出、またはデバイスを指定します。

5. 作成したタスクを実行します。

タスクの完了後、作成したメッセージが、選択したデバイスのユーザーに送信されます。［**ユーザーにメッセージを送信**］タスクは、Windows を実行しているデバイスでのみ使用できます。

# クライアントデバイスのリモートでの起動、停止、再起動

Kaspersky Security Center Linux では、クライアントデバイスをリモートで管理できます（起動、停止、再起動）。

*クライアントデバイスをリモートで管理するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. ［**追加**］をクリックします。
新規タスクウィザードが起動します。

3. ［**タスク種別**］ドロップダウンリストから、［**デバイスの管理**］を選択します。

4. タスクの適用対象として、1つのオプションをオンにして管理グループ、デバイスの抽出、またはデバイスを指定します。

5. コマンド（オン、オフ、または再起動）を選択します。

6. 必要に応じて、電源オフおよび再起動コマンドに対して次の設定を構成します：

   - ［**ユーザーへ処理を確認する**］スイッチをオンにして、ユーザープロンプトメッセージと、プロンプトを繰り返したりデバイスを再起動またはオフにしたりするまでの時間間隔を指定します。

   - **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）** チェックボックスをオンにして、時間を指定します。

> これらの設定は Windows クライアントデバイスにのみ適用されます。タスクが完了すると、Linux デバイスはすぐに再起動されるか、電源がオフになります。

7. 作成したタスクを実行します。

タスクの完了後、選択したデバイスでコマンド（起動、停止、再起動）が実行されます。

# 管理対象デバイスへのリモートアクセス

Kaspersky Security Center Linux を使用すると、管理対象デバイスへのリモート接続を確立できます。管理者は、デバイスにインストールされているネットワークエージェントを使用して、管理対象デバイスのデスクトップへのリモートアクセスを取得できます。ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。デバイスとの接続を確立すると、管理者はそのデバイスに保存されている情報へのフルアクセス権を取得できます。そのため、そのデバイスにインストールされているアプリケーションを管理することが可能です。

リモート接続を確立する方法は、Kaspersky Security Center Web コンソールがインストールされているデバイスで使用されているプラットフォームによって異なります。Kaspersky Security Center Web コンソールは、管理サーバーデバイス以外のデバイス、つまり Windows ベースまたは Linux ベースのデバイスにインストールできます。

Linux デバイスにインストールされた Kaspersky Security Center Web コンソールから、次の接続を確立できます：

- Linux ベースの管理対象デバイスに次のものを使用して接続します：
  - リモートデスクトップ接続（RDP）
  - 仮想ネットワークコンピューティング（VNC）
- 次の方法を使用して Windows ベースの管理対象デバイスに：
  - リモートデスクトップ接続（RDP）
  - 仮想ネットワークコンピューティング（VNC）

Windows デバイスにインストールされた Kaspersky Security Center Web コンソールから、次の接続を確立できます：

- Linux ベースの管理対象デバイスに次のものを使用して接続します：
  - リモートデスクトップ接続（RDP）
  - 仮想ネットワークコンピューティング（VNC）
- 次の方法を使用して Windows ベースの管理対象デバイスに：
  - リモートデスクトップ接続（RDP）
  - Windows デスクトップ共有（WDS）

デバイスへのリモート接続を確立するには、以下のものが必要です：

- klsctunnel ユーティリティ

  カスペルスキーユーティリティは、管理対象デバイスと管理サーバー間の接続をトンネリングするために使用されます。

  Kaspersky Security Center Linux では、Kaspersky Security Center Web コンソールから管理サーバーを経由し、ネットワークエージェントを経由して管理対象デバイスの指定したポートに TCP 接続をトンネリングすることができます。トンネリングは、Kaspersky Security Center Web コンソールと対象デバイスが直接接続できない場合に、Kaspersky Security Center Web コンソールがインストールされたデバイス上のクライアントアプリケーションを、管理対象デバイス上の TCP ポートに接続するために設計されています。

  クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

  - リモートデバイスが NAT を使用するローカルネットワークに接続されている。
  - リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

  このユーティリティは、Kaspersky Security Center Web コンソールまたは手動でリモート接続が確立された時にダウンロードできます。klsctunnel ユーティリティは管理サーバーデバイスにインストールされます。

  klsctunnel ユーティリティは、すべてのタイプのリモート接続（RDP、VNC、WDS）に使用されます。

- RDP または VNC クライアント

  RDP または VNC クライアントは、管理サーバーデバイスにインストールされます。このクライアントを使用すると、klsctunnel ユーティリティによって提供されるローカル接続のアドレスとポートを使用して、管理対象デバイスへのリモートアクセスを取得できます。

  ユーザーの現在のリモートデスクトップのセッションへの RDP 接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、通知なくセッションから切断されます。

- Windows デスクトップ共有（Windows ベースの管理対象デバイスのみ）

  この機能により、このセッションのユーザーを切断することなく、クライアントデバイスでの既存のセッションに接続することができます。この場合、管理者とデバイスのセッションユーザーが、デスクトップのアクセスを共有します。

  リモートデスクトップの既存のセッションに接続する場合、デバイスのセッションユーザーは管理者から接続要求を受信します。デバイスのリモートからの動作とその結果に関する情報は、Kaspersky Security Center Linux により作成されるレポートに保存されません。

  管理者はリモートクライアントデバイスでのユーザー操作の監査を設定できます。監査中に、管理者が開いている（または変更している）クライアントデバイスのファイルの情報が保存されます。

# Kaspersky Security Center Web コンソールを搭載した Linux ベースのデバイスから Linux ベースの管理対象デバイスへのリモートアクセス

## 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Linux を実行している管理対象デバイスには、ネットワークエージェントバージョン 15.3 以降がインストールされています。
- Linux を実行している管理対象デバイスに、RDP サーバーがインストールされます（リモートデスクトップ接続を使用して管理対象デバイスに接続する場合）。
- Linux を実行している管理対象デバイスに、VNC サーバーがインストールされます（仮想ネットワークコンピューティングを使用して管理対象デバイスに接続する場合）。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。
- 管理者には、RDP 接続を確立するための［**RDP セッションの開始**］権限があります（リモートデスクトップ接続を使用して管理対象デバイスに接続する場合）。
- 管理者には、VNC のトンネル接続を確立するための［**トンネリング接続の開始**］権限を持っています（仮想ネットワークコンピューティングを使用して管理対象デバイスに接続する場合）。

*Linux ベースのデバイスで開いた Kaspersky Security Center Web コンソール管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。

2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。




管理対象デバイスのリスト

3. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティをダウンロードする時は、次の点に注意してください：

   - klsctunnel ユーティリティの最新バージョンを取得するには、管理サーバーがカスペルスキーのアップデートサーバーにアクセスできることを確認してください。

     *「管理サーバーのリポジトリへのアップデートのダウンロード」*タスクを実行し、アップデートのソースとしてカスペルスキーのアップデートサーバーを選択できます。タスクが正常に完了すると、管理サーバーはカスペルスキーのアップデートサーバーにアクセスできるようになります。

   - ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードし、それを管理サーバーデバイスの /var/opt/kaspersky/klnagent ディレクトリに配置します。

4. ［**リモートデスクトップに接続**］ウィンドウで、接続ポートを指定します。既定では、ポート 3389 が使用されます。

5. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

6. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   klsctunnel ユーティリティは、リモートアクセスクライアントのローカル接続のアドレスとポートを表示します。

   このユーティリティを使用すると、管理者はトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

7. リモートアクセスクライアント（RDP または VNC）を実行し、klsctunnel ユーティリティによって提供されるアドレスとポートを使用して管理対象デバイスに接続します。

管理対象デバイスへの接続が確立され、リモートアクセスクライアントウィンドウでデスクトップが使用できるようになります。

# Kaspersky Security Center Web コンソールを搭載した Linux ベースのデバイスから Windows ベースの管理対象デバイスへのリモートアクセス

## リモートデスクトップ接続（RDP）

**必須条件**

導入を開始する前に、次が完了していることを確認してください：

- 対象の管理対象デバイスのオペレーティングシステム設定でリモート接続を許可する必要があります。
- Windows を実行している管理対象デバイスには、ネットワークエージェントバージョン 13.0 以降がインストールされています。
- 管理者には、RDP 接続を確立するための［**RDP セッションの開始**］権限があります。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。

*Linux ベースのデバイスで開いた Kaspersky Security Center Web コンソールから RDP を使用して Windows ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。
2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。
3. ［**リモートデスクトップに接続**］ウィンドウで、［**RDP**］接続タイプを選択します。

4. 管理対象デバイスのオペレーティングシステム設定でリモート接続が許可されていない場合は、［**設定の変更**］をクリックして、リモート接続を集中的に許可します。

   設定が正しく適用された場合、通知が表示されます。また、管理対象デバイスの［**設定**］→［**システム**］→［**リモートデスクトップ**］セクションで、［**リモートデスクトップを有効にする**］がオンになっています。

   管理対象デバイスのオペレーティングシステム設定でリモート接続が許可されている場合、［**設定の変更**］は表示されません。

5. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティをダウンロードする時は、次の点に注意してください：

   - klsctunnel ユーティリティの最新バージョンを取得するには、管理サーバーがカスペルスキーのアップデートサーバーにアクセスできることを確認してください。

     *「管理サーバーのリポジトリへのアップデートのダウンロード」*タスクを実行し、アップデートのソースとしてカスペルスキーのアップデートサーバーを選択できます。タスクが正常に完了すると、管理サーバーはカスペルスキーのアップデートサーバーにアクセスできるようになります。

   - ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードし、それを管理サーバーデバイスの /var/opt/kaspersky/klnagent ディレクトリに配置します。

6. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

7. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   klsctunnel ユーティリティは、リモートデバイスへの接続のアドレスとポートを表示します。

   このユーティリティを使用すると、管理者はトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

8. RDP クライアントを実行し、klsctunnel ユーティリティによって提供されるアドレスとポートを使用して管理対象デバイスに接続します。

管理対象デバイスへの接続が確立され、RDP クライアントウィンドウでデスクトップが使用できるようになります。

ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、通知なくセッションから切断されます。

## 仮想ネットワークコンピューティングシステム（VNC）

### 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Windows を実行している管理対象デバイスには、ネットワークエージェントバージョン 13.0 以降がインストールされています。
- Windows を実行している管理対象デバイスには、VNC サーバーがインストールされています。

- 管理者には、VNC のトンネル接続を確立するための［**トンネリング接続の開始**］権限があります。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。

*Linux ベースのデバイスで開いた Kaspersky Security Center Web コンソールから VNC を使用して Windows ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。
2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。
3. ［**リモートデスクトップに接続**］ウィンドウで、接続タイプとして［**VNC**］を選択します。
4. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードしてください。
5. ［**リモートデスクトップに接続**］ウィンドウで、VNC 接続ポートを指定します。既定では、ポート 5900 が使用されます。
6. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。
7. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   klsctunnel ユーティリティは、VNC クライアントのローカル接続のアドレスとポートを表示します。

   このユーティリティを使用すると、リモートユーザーはトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。
8. VNC クライアントを実行し、klsctunnel ユーティリティによって提供されるアドレスとポートを使用して管理対象デバイスに接続します。

管理対象デバイスへの接続が確立され、VNC クライアントウィンドウでデスクトップが使用できるようになります。

# Kaspersky Security Center Web コンソールを搭載した Windows ベースのデバイスから Linux ベースの管理対象デバイスへのリモートアクセス

## リモートデスクトップ接続（RDP）

**必須条件**

導入を開始する前に、次が完了していることを確認してください：

- Linux を実行している管理対象デバイスには、RDP サーバーがインストールされています。
- Linux を実行している管理対象デバイスには、ネットワークエージェントバージョン 15.3 以降がインストールされています。
- 管理者には、RDP 接続を確立するための［**RDP セッションの開始**］権限があります。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。

*Windows ベースのデバイスで開いた Kaspersky Security Center Web コンソールから RDP を使用して Linux ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。
2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。
3. ［**リモートデスクトップに接続**］ウィンドウで、［**RDP**］接続タイプを選択します。
4. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティをダウンロードする時は、次の点に注意してください：

   - klsctunnel ユーティリティの最新バージョンを取得するには、管理サーバーがカスペルスキーのアップデートサーバーにアクセスできることを確認してください。

     *「管理サーバーのリポジトリへのアップデートのダウンロード」*タスクを実行し、アップデートのソースとしてカスペルスキーのアップデートサーバーを選択できます。タスクが正常に完了すると、管理サーバーはカスペルスキーのアップデートサーバーにアクセスできるようになります。
   - ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードし、それを管理サーバーデバイスの /var/opt/kaspersky/klnagent ディレクトリに配置します。
5. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。
6. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   これを行うには、［**プロキシサーバーを使用する**］をオンにし、接続設定を指定します。

7. ［**ポートを開く**］をクリックします。

   リモートデスクトップ接続のログインウィンドウが開きます。

8. Kaspersky Security Center Web コンソールに現在ログインしているアカウントの認証情報を指定し、管理対象デバイスに接続します。

   klsctunnel ユーティリティは、リモートデバイスへの接続のアドレスとポートを表示します。

   このユーティリティを使用すると、管理者はトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

デバイスへの接続が確立されると、Microsoft Windows のリモートデスクトップ接続ウィンドウにデスクトップが表示されます。

ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、通知なくセッションから切断されます。

## 仮想ネットワークコンピューティングシステム（VNC）

### 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Linux を実行している管理対象デバイスには、ネットワークエージェントバージョン 15.3 以降がインストールされています。
- Linux を実行している管理対象デバイスには、VNC サーバーがインストールされています。
- 管理者には、VNC のトンネル接続を確立するための［**トンネリング接続の開始**］権限があります。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。

*Windows ベースのデバイスで開いた Kaspersky Security Center Web コンソールから VNC を使用して Linux ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。
2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。
3. ［**リモートデスクトップに接続**］ウィンドウで、接続タイプとして［**VNC**］を選択します。
4. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードしてください。
5. ［**リモートデスクトップに接続**］ウィンドウで、VNC 接続ポートを指定します。既定では、ポート 5900 が使用されます。

6. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

7. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   これを行うには、［**プロキシサーバーを使用する**］をオンにし、接続設定を指定します。

8. ［**ポートを開く**］をクリックします。

   klsctunnel ユーティリティは、VNC クライアントのローカル接続のアドレスとポートを表示します。

   このユーティリティを使用すると、リモートユーザーはトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

9. VNC クライアントを実行し、klsctunnel ユーティリティによって提供されるアドレスとポートを使用して管理対象デバイスに接続します。

管理対象デバイスへの接続が確立され、VNC クライアントウィンドウでデスクトップが使用できるようになります。

# Kaspersky Security Center Web コンソールを搭載した Windows ベースのデバイスから Windows ベースの管理対象デバイスへのリモートアクセス

## リモートデスクトップ接続（RDP）

### 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Windows を実行している管理対象デバイスには、ネットワークエージェントバージョン 13.0 以降がインストールされています。
- 管理者には、RDP 接続を確立するための［**RDP セッションの開始**］権限があります。
- RDP 接続のトンネリング用のポートが開かれています（管理サーバーのプロパティウィンドウの［**接続ポート**］セクションで、［**RDP 接続のトンネリング用にポートを開く**］がオンになっています）。
- 管理対象デバイスのオペレーティングシステム設定でリモート接続が許可されています。

*Windows ベースのデバイスで開いた Kaspersky Security Center Web コンソールから RDP を使用して Windows ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。

2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。

3. ［**リモートデスクトップに接続**］ウィンドウで、接続タイプとして［**リモートデスクトップ接続**］を選択します。

4. 管理対象デバイスのオペレーティングシステム設定でリモート接続が許可されていない場合は、［**設定の変更**］をクリックして、リモート接続を集中的に許可します。

   設定が正しく適用された場合、通知が表示されます。また、管理対象デバイスの［**設定**］→［**システム**］→［**リモートデスクトップ**］セクションで、［**リモートデスクトップを有効にする**］がオンになっています。

   管理対象デバイスのオペレーティングシステム設定でリモート接続が許可されている場合、［**設定の変更**］は表示されません。

5. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティをダウンロードする時は、次の点に注意してください：

   - klsctunnel ユーティリティの最新バージョンを取得するには、管理サーバーがカスペルスキーのアップデートサーバーにアクセスできることを確認してください。

     *「管理サーバーのリポジトリへのアップデートのダウンロード」*タスクを実行し、アップデートのソースとしてカスペルスキーのアップデートサーバーを選択できます。タスクが正常に完了すると、管理サーバーはカスペルスキーのアップデートサーバーにアクセスできるようになります。

   - ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードし、それを管理サーバーデバイスの /var/opt/kaspersky/klnagent ディレクトリに配置します。

6. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

7. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   これを行うには、［**プロキシサーバーを使用する**］をオンにし、接続設定を指定します。

8. ［**ポートを開く**］をクリックします。

   リモートデスクトップ接続のログインウィンドウが開きます。

9. Kaspersky Security Center Web コンソールに現在ログインしているアカウントの認証情報を指定し、管理対象デバイスに接続します。

   klsctunnel ユーティリティは、リモートデバイスへの接続のアドレスとポートを表示します。

   このユーティリティを使用すると、管理者はトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

デバイスへの接続が確立されると、Microsoft Windows のリモートデスクトップ接続ウィンドウにデスクトップが表示されます。

ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、通知なくセッションから切断されます。

## Windows デスクトップ共有（WDS）

### 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Windows を実行している管理対象デバイスには、ネットワークエージェントバージョン 13.0 以降がインストールされています。
- 管理者には、WDS 接続を確立するための［**既存の RDP セッションへの接続**］権限があります。
- 脆弱性とパッチ管理のライセンスが使用可能です。
- Microsoft Windows Vista 以降の Windows オペレーティングシステムが管理ステーションにインストールされている。管理サーバーをホストしているデバイスのオペレーティングシステムの種別により、Windows デスクトップ共有を使用した接続に制限が適用されることはありません。

  使用する Windows のエディションに Windows デスクトップ共有機能が含まれているかどうかを確認して、Windows レジストリに CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} ライセンスがあることを確認します。
- Microsoft Windows Vista 以降の Windows オペレーティングシステムがクライアントデバイスにインストールされている。

*Windows ベースのデバイスで開いた Kaspersky Security Center Web コンソールから VNC を使用して Windows ベースの管理対象デバイスに接続するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションに移動するか、デバイスの抽出を開きます。
2. リモートで接続する管理対象デバイスの横にあるチェックボックスをオンにし、［**リモートデスクトップに接続**］をクリックします。

   ［**リモートデスクトップに接続**］ウィンドウが開きます。

   複数のデバイス、モバイルデバイス、または macOS を実行しているデバイスを選択した場合、［**リモートデスクトップに接続**］は無効になります。
3. ［**リモートデスクトップに接続**］ウィンドウで、接続タイプとして［**Windows デスクトップ共有**］を選択します。

   脆弱性とパッチ管理ライセンスが使用できない場合は、エラーメッセージが表示されます。
4. ［**ダウンロード**］をクリックして klsctunnel ユーティリティをダウンロードし、実行します。

   ユーティリティファイルをダウンロードできない場合は、エラーメッセージが表示されます。この場合は、ユーティリティを手動でダウンロードしてください。

5. 選択したデバイスでアクティブな使用可能なユーザーセッションのリストで、接続するセッションを選択します。

   リモートユーザーは接続を許可する必要があります。リモートユーザーが接続を拒否した場合、またはタイムアウト期間中にリモートユーザーが接続を許可しなかった場合は、エラーメッセージが表示されます。

6. ［**blob の生成**］をクリックして、エンコードされた接続パラメータを含むテキスト BLOB を生成し、そのテキストをコピーして klsctunnel ユーティリティの対応するフィールドに貼り付けます。

   BLOB には、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定が含まれています。BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

7. klsctunnel ユーティリティでプロキシサーバーを使用する場合は、プロキシサーバーの接続設定を指定します。

   これを行うには、［**プロキシサーバーを使用する**］をオンにし、接続設定を指定します。

8. ［**ポートを開く**］をクリックします。

   klsctunnel ユーティリティは、VNC クライアントのローカル接続のアドレスとポートを表示します。

   このユーティリティを使用すると、リモートユーザーはトンネル接続を閉じることができます。トンネル接続が閉じられると、リモートデスクトップへの現在の接続が終了します。

デスクトップ共有が新しいウィンドウで開始されます。デバイスと対話する場合は、メニューアイコン（  ）をウィンドウの左上でクリックし、［**対話モード**］を選択します。

# モバイルデバイスの管理

Kaspersky Security Center によるモバイルデバイス保護の管理は、モバイルデバイス管理機能を使用して行われます。保護アプリケーションを有効にする には、各モバイルデバイスにライセンスを追加する必要があります。組織内の従業員が所有するモバイルデバイスを管理する場合は、モバイルデバイス管理を有効にして設定してください。

モバイルデバイス管理を使用して、従業員の Android デバイスおよび iOS デバイスを管理できます。保護は、モバイルデバイスにインストールされた Kaspersky Endpoint Security for Android アプリと iOS デバイス管理システムによって提供されます。このモバイルアプリにより、モバイルデバイスを Web の脅威、ウイルス、その他の脅威をもたらすプログラムから保護します。Kaspersky Security Center Web コンソールを使用した一元管理のため、Kaspersky Security Center Web がインストールされたデバイスに次の Web 管理プラグインをインストールする必要があります：

- カスペルスキーモバイルデバイスの保護と管理

  Kaspersky Mobile Devices Protection and Management プラグインを使用すると、Kaspersky Security Center Web コンソールで Android および iOS を実行しているデバイスを管理できます。

- iOS MDM サーバー設定

  iOS MDM サーバー設定プラグインを使用すると、iOS デバイスを管理サーバーに接続し、iOS デバイスを管理するために使用される iOS MDM サーバーの設定を構成できます。

モバイルデバイスへの保護の導入および管理の詳細については、Kaspersky Security for Mobile のヘルプ および Kaspersky Secure Mobility Management のヘルプ を参照してください。

# Firebase Cloud Messaging の使用

Android デバイスへのコマンドのタイムリーな配信を確実にするために、Kaspersky Security Center Linux はプッシュ通知のメカニズムを使用します。プッシュ通知は、Firebase Cloud Messaging（以下、FCM）を介して Android デバイスと管理サーバー間で交換されます。Kaspersky Security Center Linux Web コンソールで、Firebase Cloud Messaging サービスの設定を指定することで、サービスに Android デバイスを接続できます。

Firebase Cloud Messaging の設定を取得するには、Google アカウントが必要です。

*FCM の使用を有効化するには：*

1. Kaspersky Security Center Linux Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**Mobile**］→［**Devices**］を選択します。
2. 3 ドットメニュー（⋮）を開き、［**Forced Android device synchronization**］を選択します。
3. ［**Firebase project number**］フィールドに、FCM 送信者 ID を指定します。
4. ［**Private key**］フィールドで、秘密鍵ファイルを選択します。

   管理サーバーとの次回の同期時に、Android デバイスが管理する Android デバイスが、Firebase Cloud Messaging に接続されます。

別の Firebase プロジェクトに切り替える場合は、FCM が再開されるまで 10 分間待つ必要があります。

FCM サービスは、以下のアドレス範囲で実行されます：

- Android デバイス側では、以下のアドレスのポート 443（HTTPS）、5228（HTTPS）、5229（HTTPS）、および 5230（HTTPS）に対するアクセスが必要です：
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Google の ASN 15169 に一覧表示されたすべての IP アドレス
- 管理サーバー側では、以下のアドレスのポート 443（HTTPS）に対するアクセスが必要です：
  - fcm.googleapis.com
  - Google の ASN 15169 に一覧表示されたすべての IP アドレス

Web コンソールの管理サーバーのプロパティで、プロキシサーバー設定が指定されている場合、その設定が FCM との対話に使用されます。

### FCM の設定：送信者 ID と秘密鍵ファイルの取得

*FCM を設定するには：*

1. Google ポータルで登録します。
2. Firebase コンソールへ移動します。
3. 次のいずれかの手順を実行します：
   - 新しいプロジェクトを作成するには、［**プロジェクトの作成**］をクリックし、画面の指示に従います。
   - 既存のプロジェクトを開きます。
4. 歯車アイコンをクリックし、［**プロジェクト設定**］を選択します。
   ［**プロジェクト設定**］ウィンドウが開きます。
5. ［**クラウドメッセージング**］タブを選択します。
6. ［**Firebase Cloud Messaging API (V1)**］セクションの［**送信者 ID**］フィールドから関連する送信者 ID を取得します。
7. ［**サービスアカウント**］タブを選択し、［**新しい秘密鍵の生成**］をクリックします。
8. 開いたウィンドウで、［**鍵の生成**］をクリックして秘密鍵ファイルを生成し、ダウンロードします。

Firebase Cloud Messaging が設定されました。

## 公開鍵基盤との統合

公開鍵認証基盤（PKI）を介して、Microsoft 認証局（CA）との証明書の発行を統合できます。PKI との統合は、管理サーバーによるドメインユーザー証明書の発行を簡素化することを目的としています。統合後、証明書が自動的に発行されます。

証明書を発行するための PKI との統合を設定する方法の詳細については、Kaspersky Secure Mobility Management ヘルプを参照してください。

指定された設定で PKI 統合を実行し、特定の種類の証明書のソースとして機能するように PKI を割り当てることができます。PKI 統合設定では、すべての種類の証明書に対して個別の既定テンプレートを設定できます。

PKI 統合を使用して証明書を発行する場合の詳細：

- PKI 統合は既定で無効になっています。PKI を有効にして設定する方法の詳細については、Kaspersky Secure Mobility Management ヘルプを参照してください。
- 証明書の発行は、管理サーバーと Microsoft CA 間の統合を可能にするネットワークエージェント Windows を使用して実行されます。ネットワークエージェントがインストールされているデバイスは複数存在する可能性があるため、**Issuance rules** で Microsoft CA に接続するデバイスを指定できます。このデバイスには、PKI との統合が実行されるアカウントの証明書リポジトリに登録エージェント（EA）証明書がインストールされている必要があります。証明書はドメインの CA の管理者によって発行されます。

- PKI との統合を実行するアカウントはドメインユーザーである必要があり、*サービスとしてログイン*する権限を持っている必要があります。

- Kaspersky Security Center Linux は、一度に 1 つの PKI（Microsoft CA）統合のみで動作します。

# 管理グループの管理

このセクションでは、管理グループの管理方法について説明します。

管理グループには次の処理を行うことができます：

- 任意の階層レベルのネストされたグループを管理グループに追加する
- デバイスを管理グループに追加する
- 個々のデバイスとグループ全体を別のグループに移動して、管理グループの階層を変更する
- ネストされたグループとデバイスを管理グループから削除する
- セカンダリ管理サーバーおよび仮想管理サーバーを管理グループに追加する
- 任意の管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動する
- グループに含まれているデバイスに自動的にインストールされるカスペルスキー製品を定義する

管理する管理グループ（またはその管理グループが属する管理サーバー）の［**管理グループの管理**］領域で［Modify］権限を付与されている場合にのみ、これらの処理を実行できます。

# 管理グループの作成

Kaspersky Security Center のインストール直後に、［**管理対象デバイス**］と呼ばれる管理グループが 1 つだけ管理グループの階層に含まれます。管理グループの階層の作成時に、仮想マシンおよびデバイスを［**管理対象デバイス**］グループに追加したり、ネストされたグループを追加したりできます。



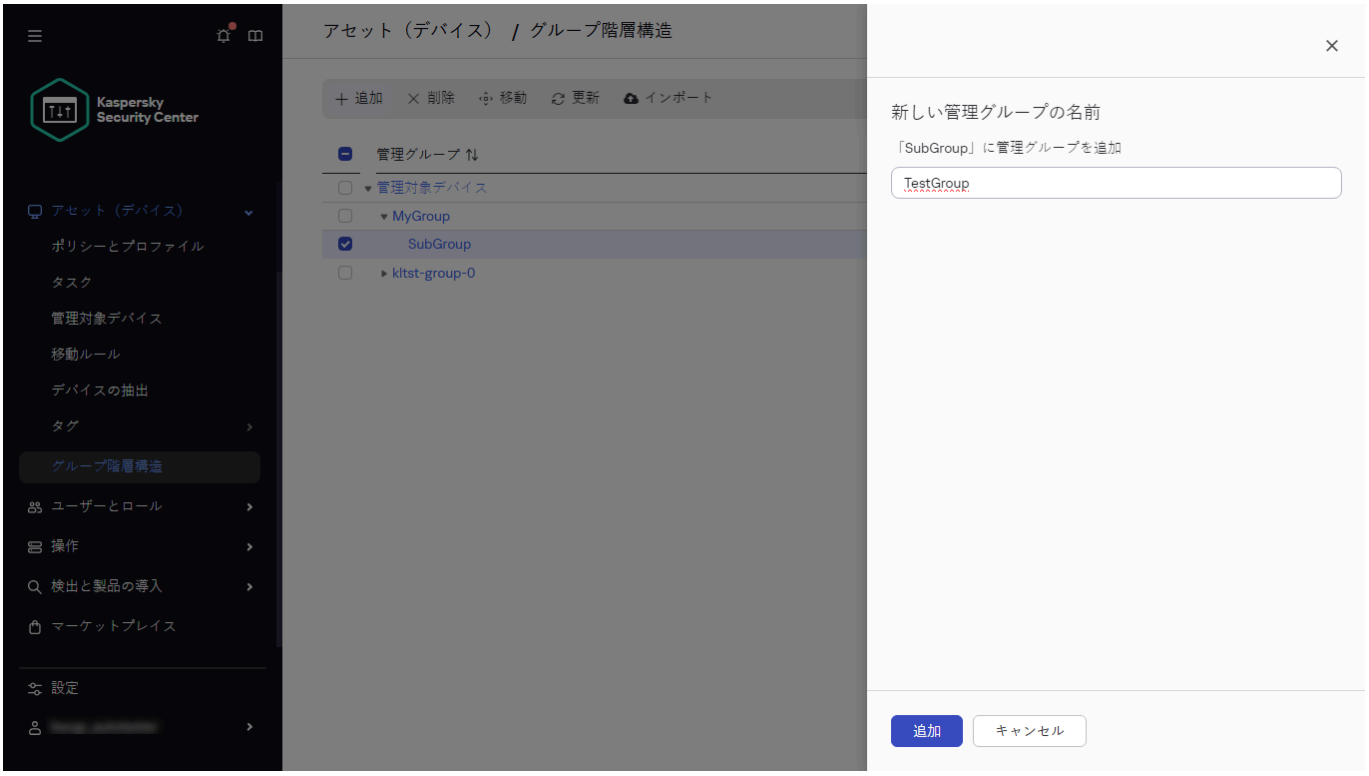

管理グループ階層の表示

*管理グループを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 管理グループの構成で、新しい管理グループを含める管理グループを選択します。




3. ［**追加**］をクリックします。
4. 表示される［**新しい管理グループの名前**］ウィンドウで、グループの名前を入力して［**追加**］をクリックします。




指定した名前の新しい管理グループが管理グループの階層に表示されます。

*管理グループの構造を作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. ［**インポート**］をクリックします。

新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

# 管理グループ内のデバイスでのアプリケーションの自動インストール

管理グループ内のクライアントデバイスにカスペルスキー製品を自動的にリモートインストールする際に、使用するインストールパッケージを指定できます。

*管理グループ内のデバイスでのアプリケーションの自動インストールを設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］し、必要な管理グループの名前をクリックします。
2. 開いたプロパティウィンドウで、［**自動インストール**］タブを選択します。
3. デバイスにインストールするアプリケーションのインストールパッケージを選択し、次に［**保存**］ボタンをクリックします。

   同じアプリケーションのバージョンのみが異なる複数のインストールパッケージを選択した場合は、最新バージョンのインストールパッケージが保存されます。

インストールパッケージを選択すると、管理グループ内のデバイスにアプリケーションをインストールするためのグループタスクがアプリケーションごとに作成されます。管理グループにクライアントデバイスが追加されるとすぐにそのクライアントデバイスで実行されます。

# 管理グループの移動

ネストされた管理グループは、グループ階層内で移動できます。

グループを移動すると、すべてのネストされたグループ、セカンダリ管理サーバー、デバイス、グループポリシー、およびタスクも一緒に移動します。移動したグループには、管理グループ階層内の新しい位置に対応するすべての設定が適用されます。

グループの名前は、階層の1レベル内で一意である必要があります。管理グループを移動するフォルダー内に同じ名前のグループが既にある場合は、後者の名前を変更してください。移動するグループの名前を変更しなかった場合は、移動すると、**(1)**、**(2)** のような **(<次の連番>)** 形式のインデックスが名前に自動的に追加されます。

［**管理対象デバイス**］グループの名前を変更したり移動したりすることはできません。

*管理グループを管理グループ階層の別のレベルに移動するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］を選択し、移動する管理グループの横にあるチェックボックスをオンにします。
2. ツールバーの［**移動**］をクリックします。
3. 開いたウィンドウで、管理グループを移動する場所を選択し、［**移動**］をクリックします。

ウィンドウが閉じられ、管理グループはグループ階層の別のレベルに移動されます。

# 管理グループの削除

このグループ用に作成されたセカンダリ管理サーバー、ネストされたグループ、クライアントデバイス、グループタスク、またはポリシーを含む管理グループを削除すると、それらもすべて削除されます。

管理グループを削除する前に、そのグループからセカンダリ管理サーバー、ネストされたグループ、クライアントデバイスをすべて削除する必要があります。

*管理グループを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］を選択し、削除する管理グループの横にあるチェックボックスをオンにします。
2. ツールバーの［**削除**］をクリックします。

選択した管理グループが削除されます。

# カスペルスキー製品の導入

このセクションでは、Kaspersky Security Center Web コンソールを使用して、企業ネットワーク内のクライアントデバイスにカスペルスキー製品を導入する方法について説明しています。

# シナリオ：カスペルスキー製品の導入

このシナリオは、Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入方法を説明しています。導入には、クイックスタートウィザードと製品導入ウィザードを使用する方法と、すべての必要なステップを手動で完了させる方法があります。

次の製品は、Kaspersky Security Center Web コンソールを使用して導入できます：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

## 実行するステップ

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **アプリケーションの Web 管理プラグインのダウンロード**

   このステップはクイックスタートウィザードの一部として実行できます。ウィザードを実行しないことを選択した場合は、プラグインを手動でダウンロードしてください。

2. **インストールパッケージのダウンロードと作成**

   このステップはクイックスタートウィザードの一部として実行できます。

   クイックスタートウィザードを使用すると、Web 管理プラグインと一緒にインストールパッケージをダウンロードできます。ウィザードの実行中にこのオプションを選択しない場合は、手動でパッケージをダウンロードする必要があります。

   Kaspersky Security Center Linux を使用してカスペルスキー製品をインストールできないデバイスがある場合（リモートワークで働く従業員のデバイスなど）、製品のスタンドアロンインストールパッケージを作成できます。スタンドアロンパッケージを使用してカスペルスキー製品をインストールする場合、リモートインストールタスクを作成して実行したり、Kaspersky Endpoint Security for Windows のタスクを作成、設定したりする必要はありません。

   または、カスペルスキー Web サイトからネットワークエージェントの配布パッケージおよびセキュリティ製品をダウンロードすることもできます。何らかの理由で本製品のリモートインストールができない場合は、ダウンロードした配布パッケージを使用してアプリケーションをローカルにインストールできます。

3. **リモートインストールタスクの作成、設定、実行**

   このステップは製品導入ウィザードの一部です。製品導入ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。

   異なる管理グループや異なるデバイスの抽出を対象に、複数のリモートインストールタスクを手動で作成することもできます。これらのタスクでは、同一製品の異なるバージョンを導入できます。

   ネットワーク上ですべてのデバイスが検出済みであることを確認してから、リモートインストールタスクを実行します。

SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

オペレーティングシステムRED OS 7.3.4 以降またはMSVSPHERE 9.2以降を使用するデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントを正しく機能させるために libxcrypt-compat パッケージをインストールしてください。

4. **タスクの作成と設定**

   Kaspersky Endpoint Security のアップデートタスクを設定する必要があります。

   このステップはクイックスタートウィザードの一部です：既定の設定を使用してタスクは自動的に作成、設定されます。ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。クイックスタートウィザードを使用する場合は、タスクのスケジュールがお客様の要件に合致しているかを確認します（既定では、タスクの実行予定は［**手動**］に設定されていますが、別のオプションも選択できます）。

5. **ポリシーの作成**

   手動またはクイックスタートウィザードを使用して Kaspersky Endpoint Security のポリシーを作成します。ポリシーは既定の設定を使用できます。また、いつでも必要に応じてポリシーの既定の設定を変更できます。

6. **結果の検証**

   導入が正しく完了しているかの確認：アプリケーションごとにポリシーとタスクが設定済みで、これらのアプリケーションが管理対象デバイスにインストールされていることを確認します。

### 結果

これらのステップがすべて完了すると、次の状態を実現できます：

- すべての必要なポリシーとタスクが、選択したアプリケーションに対して作成されている。
- タスクのスケジュールが必要に応じて設定されている。
- 指定したデバイス上で、選択したアプリケーションが導入されているか、導入スケジュールが設定されている。

# カスペルスキー製品向けの管理プラグインの追加

Kaspersky Endpoint Security for Linux や Kaspersky Endpoint Security for Windows などのカスペルスキー製品を導入するには、製品の Web 管理プラグインを追加してインストールする必要があります。

*カスペルスキー製品の Web 管理プラグインをダウンロードするには：*

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に移動します。




インストールされている Web プラグインのリスト

2. ウィンドウが表示されたら、［**追加**］をクリックします。
   使用可能なプラグインのリストが表示されます。

3. 使用可能なプラグインのリストから、プラグイン名（「Kaspersky Endpoint Security for Linux」など）をクリックして、ダウンロードするプラグインを選択します。
   プラグインの説明ページが表示されます。

4. プラグインの説明ページで、［**プラグインのインストール**］をクリックします。

5. インストールが完了したら、［**OK**］をクリックします。

Web 管理プラグインが既定の設定でダウンロードされ、Web 管理プラグインのリストに表示されます。

ファイルからプラグインを追加したり、ダウンロードされたプラグインをアップデートすることができます。Web 管理プラグインは、カスペルスキーの Web サイトからダウンロードできます。

*ファイルから Web 管理プラグインをダウンロードまたはアップデートするには：*

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に選択します。

2. プラグインのファイルおよびファイルの署名を指定します：

   - ［**ファイルから追加**］をクリックしてファイルからプラグインをダウンロードします。
   - ［**ファイルからアップデート**］をクリックしてファイルからプラグインのアップデートをダウンロードします。

3. ファイルおよびファイルの署名を指定します。

4. 指定したファイルをダウンロードします。

Web 管理プラグインがファイルからダウンロードされ、Web 管理プラグインのリストに表示されます。

# インストールパッケージ

*インストールパッケージ*は、カスペルスキー製品のリモートインストール用に作成されたファイルのセットです。インストールパッケージには、アプリケーションをインストールし、インストール後にすぐに実行させるのに必要な設定の範囲が含まれます。設定は、アプリケーションの既定値になります。インストールパッケージは、アプリケーション配布キットに含まれる拡張子が KPD および KUD のファイルを使用して作成されます。

インストールパッケージを作成するには、次の方法を使用します：

- 含まれている*記述子*を基にして、指定した配布パッケージから自動的に作成（インストールと結果分析のルール、およびその他の情報を含む kud 拡張子のファイル）。
- 標準またはサポートされているアプリケーション用の ZIP、CAB、TAR、または TAR.GZ アーカイブファイルから。

作成されたインストールパッケージは、サブフォルダーとファイルが格納されているフォルダーとして階層的に編成されます。インストールパッケージには元の配布パッケージの他に、編集可能な設定（インストールを完了するために必要なオペレーティングシステムの再起動を処理するための、インストーラーの設定とルールを含む）と小規模な予備モジュールが含まれています。

サポートされている個別のアプリケーションに固有のインストール設定の値は、インストールパッケージの作成時に Kaspersky Security Center Web コンソールのユーザーインターフェイスで定義できます。Kaspersky Security Center Linux のツールを使用してアプリケーションをリモートインストールする際には、インストールパッケージをデバイスに配布します。これで、アプリケーションのインストーラーを実行することにより、すべての管理者定義の設定がアプリケーションで使用できるようになります。カスペルスキー製品のインストールにサードパーティ製のツールを使用する際に必要になるのは、デバイスでインストールパッケージ全体（つまり、配布パッケージとその設定）を使用できるようにすることだけです。Kaspersky Security Center Linux によってインストールパッケージが作成され、共有フォルダーの専用サブフォルダーに保存されます。

> インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。

Microsoft Windows のグループポリシーを使用した導入はサポートされていません。

Kaspersky Security Center Linux のインストール直後には、自動的にいくつかのインストールパッケージが作成されます。これらのインストールパッケージはインストールの準備が完了しており、Microsoft Windows 用のネットワークエージェントパッケージとセキュリティ製品パッケージを含んでいます。

> インストールパッケージのプロパティでアプリケーション用のライセンスを設定できますが、インストールパッケージへの読み取り権限は簡単に取得されてしまうため、このライセンス配信方法は避けるのが適切です。この場合、ライセンスの自動配信またはライセンスのインストールタスクを使用する必要があります。

# カスペルスキー製品のインストールパッケージのダウンロードおよび作成

管理サーバーがインターネットにアクセスできる場合、カスペルスキーの Web サーバーからカスペルスキー製品のインストールパッケージを作成できます。

*カスペルスキー製品のインストールパッケージのダウンロードと作成を実行するには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   画面表示による通知のリストでも、カスペルスキー製品の新しいパッケージに関する通知を確認できます。新しいパッケージに関する通知が表示されている場合、通知に隣接するリンクをクリックし、使用可能なインストールパッケージのリストを表示できます。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。




インストールパッケージのリスト

2. ［**追加**］をクリックします。

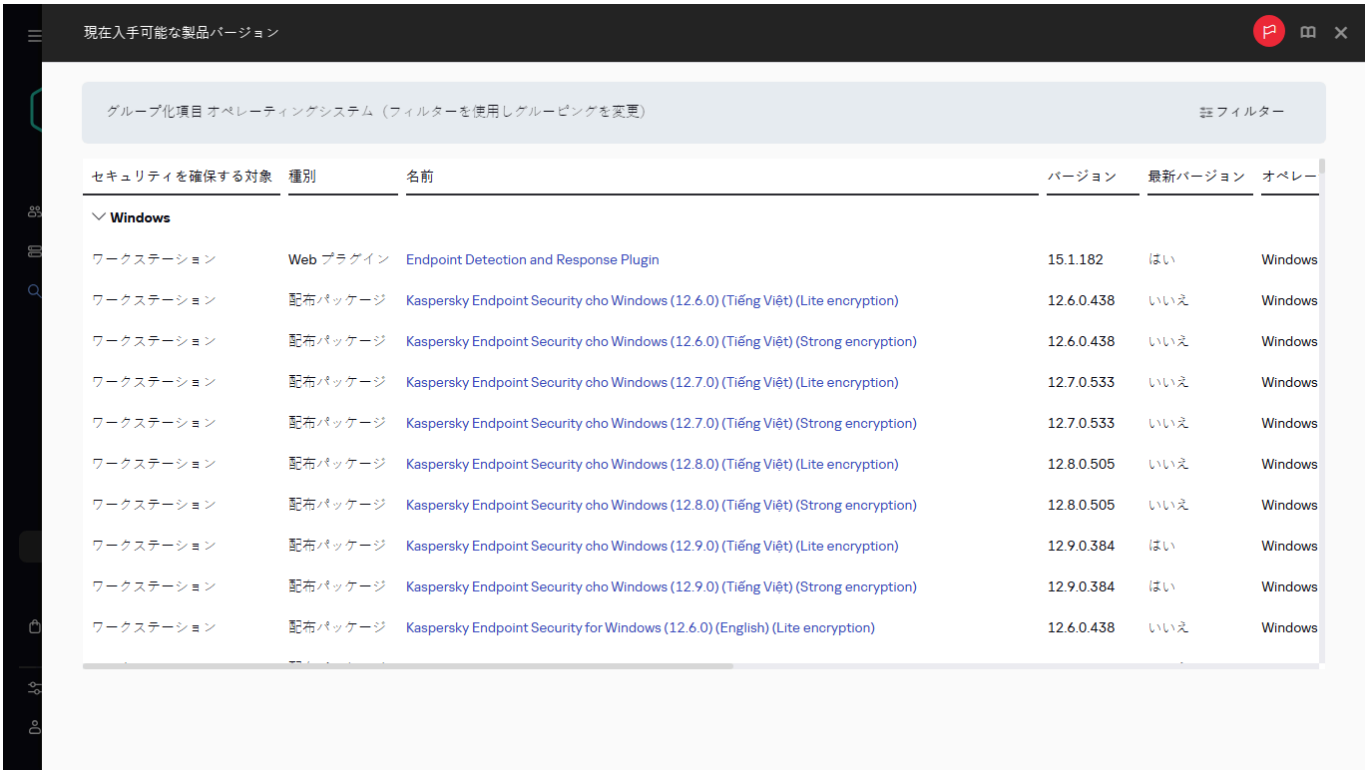
   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。




インストールパッケージの種類の選択

カスペルスキーの Web サーバーで使用可能なインストールパッケージのリストが表示されます。リストには、Kaspersky Security Center Linux の現在のバージョンと互換性のあるアプリケーションのインストールパッケージのみが含まれています。

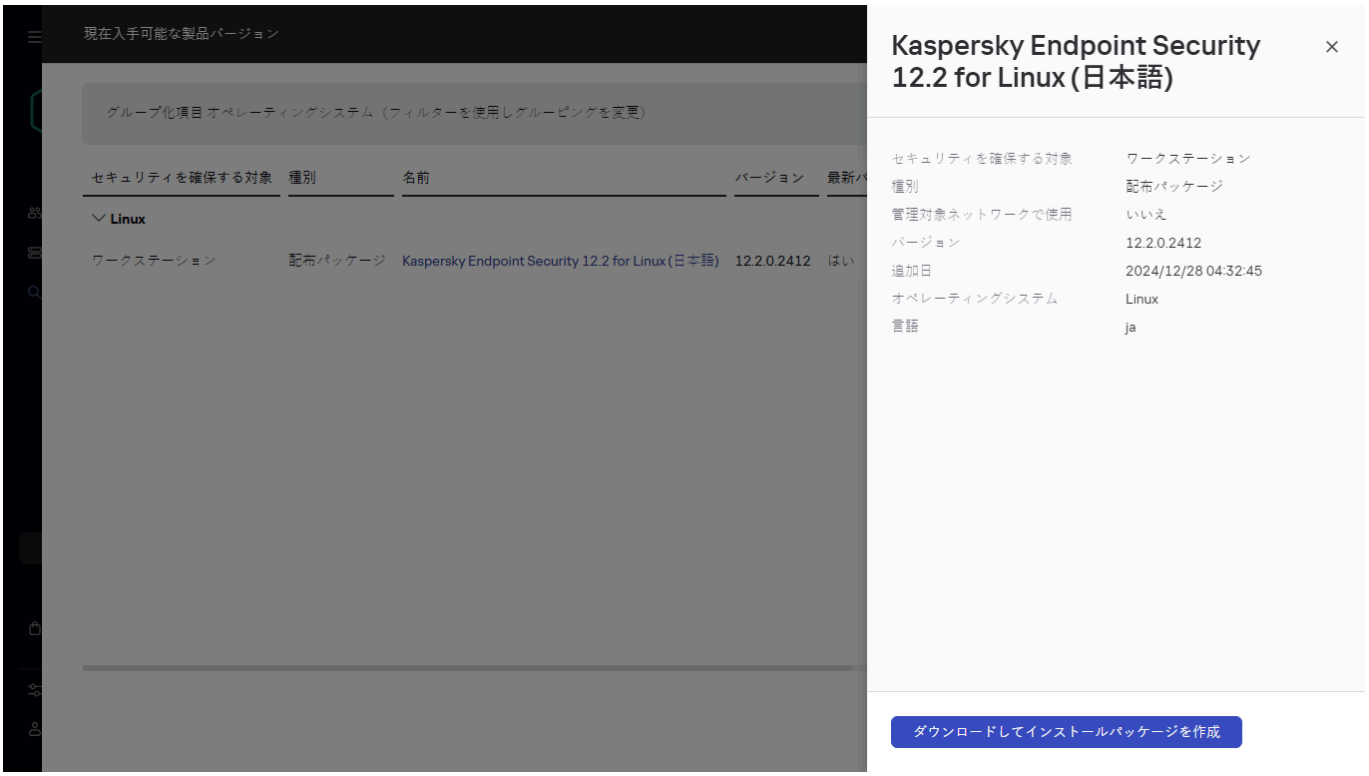



使用可能なインストールパッケージのリスト

4. インストーパッケージの名前（たとえば「Kaspersky Endpoint Security for Linux」）をクリックします。

インストールパッケージに関する情報を確認できるウィンドウが表示されます：

適用法令および規則に準拠している場合、高度な暗号化を実装する暗号化ツールを含むインストールパッケージをダウンロードして使用できます。組織のニーズに合致した Kaspersky Endpoint Security for Windows のインストールパッケージをダウンロードするには、組織内のクライアントデバイスの所在地における法令などを確認してください。




インストールパッケージのダウンロード

5. 情報を確認し、［**ダウンロードしてインストールパッケージを作成**］をクリックします。

配布パッケージをインストールパッケージに変換できない場合、［**配布パッケージをダウンロード**］の代わりに［**ダウンロードしてインストールパッケージを作成**］が表示されます。

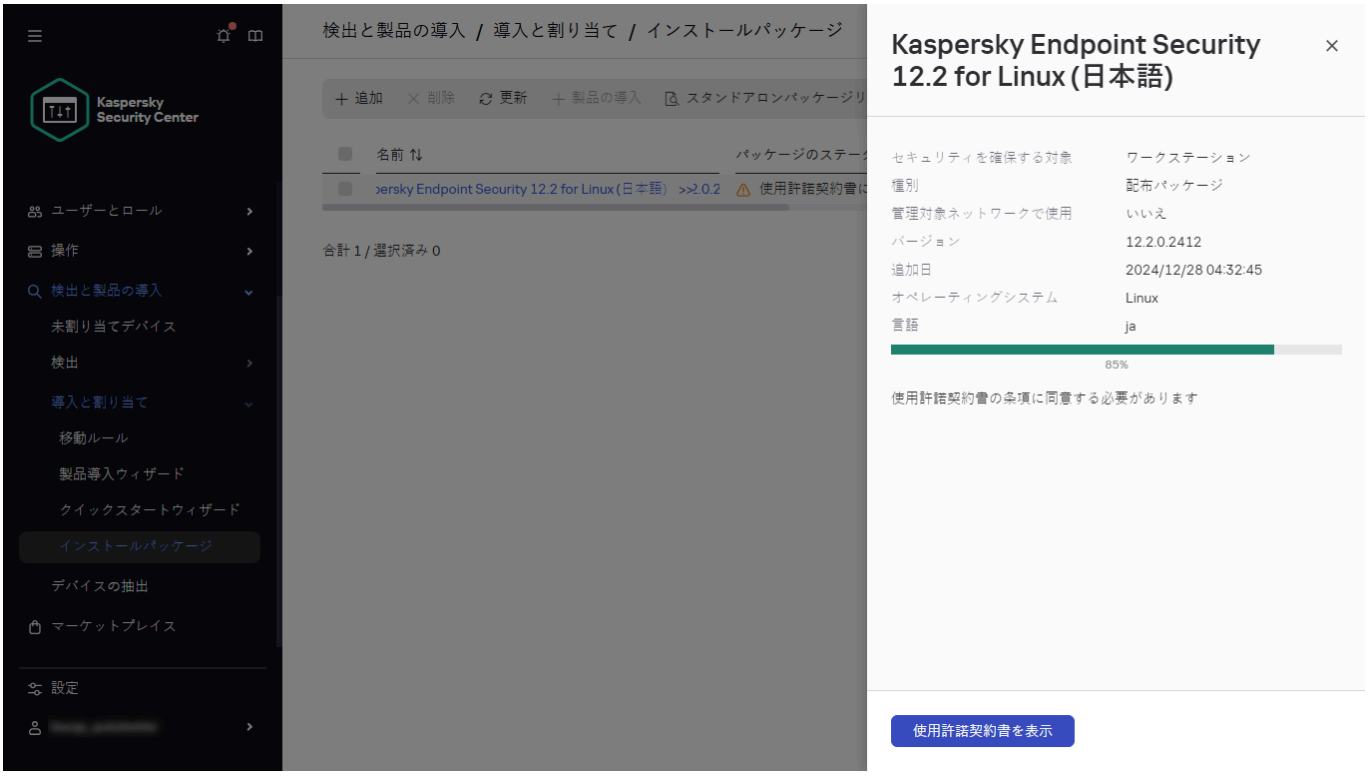
インストールパッケージ（または配布パッケージ）の管理サーバーへのダウンロードが開始されます。ウィザードのウィンドウを閉じることができます。この場合、ダウンロードプロセスはバックグラウンドモードで続行されます。インストールパッケージのダウンロードステータスを追跡したり、［**パッケージのステータス**］列でステータスをフィルター処理したり並べ替えたりすることができます。

ダウンロードプロセスが停止し、ダウンロードの状況が［**使用許諾契約書に同意する**］に切り替わったら、インストールパッケージ名をクリックして、説明のステップ 6 に進みます。既定では、**実行中**および**使用許諾契約書に同意する**ステータスのインストールパッケージがリストの先頭に配置されます。

選択した配布パッケージ内のデータサイズが現在の上限を超えている場合、エラーメッセージが表示されます。上限の値を変更し、インストールパッケージの作成に進んでください。

6. 一部のカスペルスキー製品では、ダウンロードプロセスの途中で［**使用許諾契約書を表示**］が表示されます。この場合は、次の操作を実行します：

   a. ［**使用許諾契約書を表示**］をクリックし、使用許諾契約書（EULA）の内容を確認します。




インストールパッケージのダウンロード

   a. 画面に表示された EULA の内容を確認し、［**同意する**］をクリックします。

      使用許諾契約書に同意するとダウンロードを進めることができます。［**同意しない**］をクリックすると、ダウンロードが中止されます。




EULA に同意する

7. ダウンロードが完了したら、［**閉じる**］をクリックします。

選択したインストールパッケージが管理サーバーの共有フォルダーのパッケージ用サブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。




インストールパッケージのリスト

# ファイルからのインストールパッケージの作成

以下のような用途でカスタムインストールパッケージを使用できます：

- タスクなどを使用して、サードパーティ製を含む任意のアプリケーション（例：テキストエディター）をクライアントデバイスにインストールするため。
- スタンドアロンインストールパッケージを作成するため。

カスタムインストールパッケージは、複数のファイルを含んだフォルダーです。カスタムインストールパッケージは、*圧縮ファイル*を元に作成します。圧縮ファイルには、カスタムインストールパッケージに含める必要のあるファイルが含まれているようにします。

カスタムインストールパッケージを作成するときに、コマンドラインのパラメータを指定できます（例：製品をサイレントモードでインストールするためのパラメータ）。

*カスタムインストールパッケージを作成するには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで使用可能なインストールパッケージのリストが表示されます。




インストールパッケージのリスト

2. ［**追加**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**インストールパッケージをファイルから作成する**オンにします。



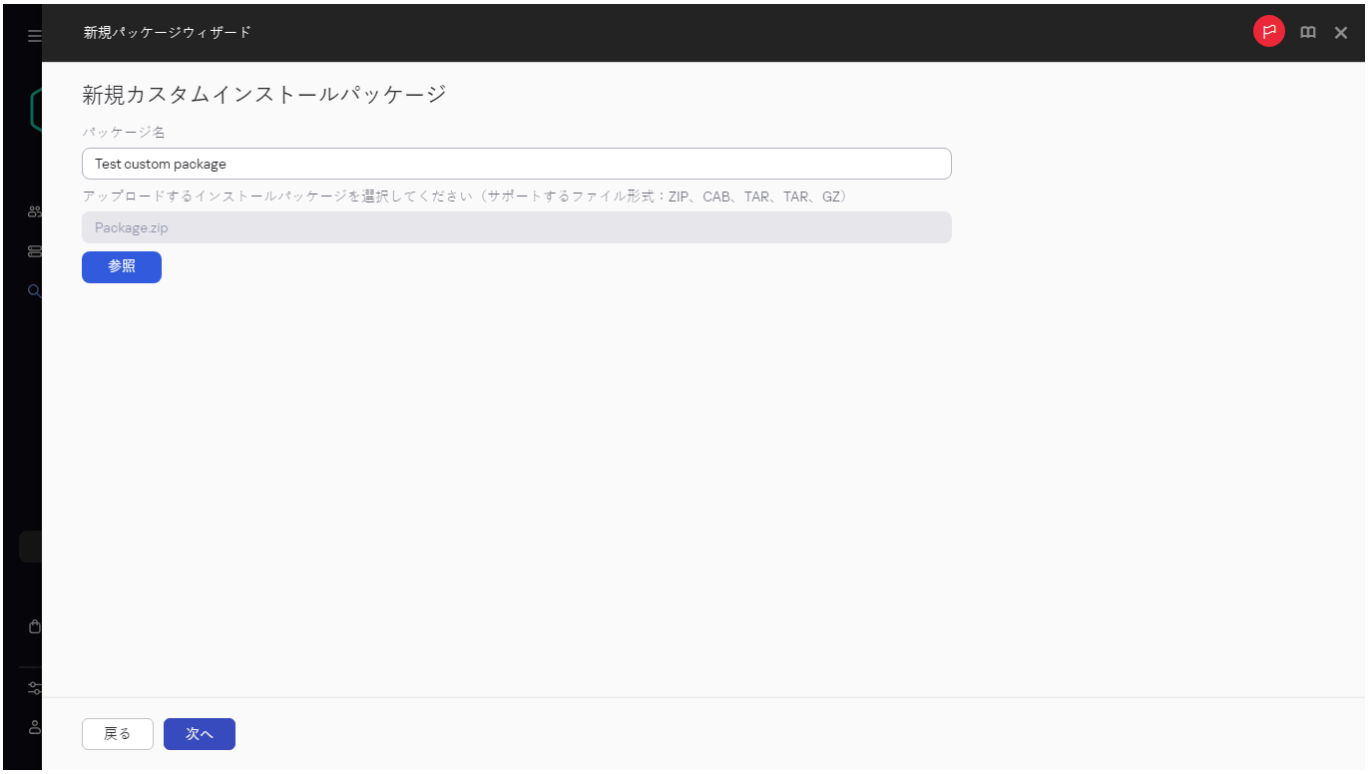

インストールパッケージの種類の選択

4. パッケージ名を指定して、［**参照**］をクリックします。

5. 表示されるウィンドウで、使用可能なディスクにあるアーカイブファイルを選択します。

   ZIP、CAB、TAR、または TAR.GZ ファイルをアップロードできます。インストールパッケージを SFX ファイル（自己解凍型の圧縮ファイル）から作成することはできません。

   管理サーバーへのファイルのアップロードが開始されます。



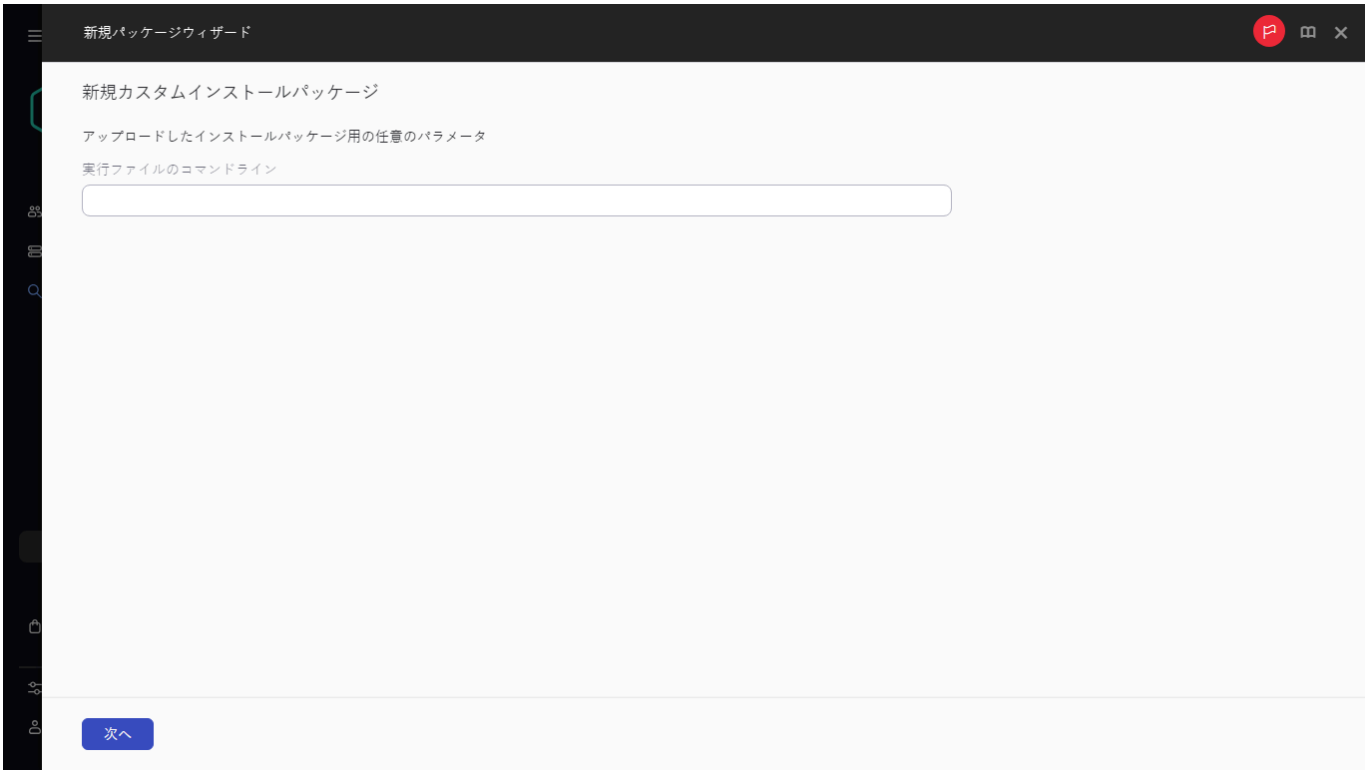

インストールパッケージファイルの指定

6. カスペルスキー製品のファイルを指定した場合、製品の使用許諾契約書（EULA）を確認して同意するよう求められることがあります。続行するには、EULA に同意する必要があります。EULA の条項をすべて確認して理解した上で同意する場合にのみ［**この使用許諾契約書の条項に同意する**］を選択します。

   また、プライバシーポリシーについても確認と同意を求められることがあります。続行するには、プライバシーポリシーに同意する必要があります。プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解し、同意する場合にのみ［**プライバシーポリシーに同意する**］を選択します。

7. 指定された圧縮ファイルから展開されたファイルのリストから実行ファイルを選択し、実行ファイルのコマンドラインパラメータを指定します。

   インストールパッケージから製品をサイレントモードでインストールするためのコマンドラインのパラメータを指定できます。コマンドラインのパラメータの指定は省略可能です。




オプションのコマンドラインパラメータの指定

   カスタムインストールパッケージを作成するプロセスが開始されます。

   プロセスが終了すると、ウィザードで通知されます。

   インストールパッケージが作成されなかった場合も、メッセージで通知されます。

8. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

管理サーバーで利用できるインストールパッケージのリストで、カスタムインストールパッケージの名前をクリックすることで次の操作を実行できます：

- インストールパッケージのプロパティとして以下の情報を表示する：
  - **名前**：カスタムインストールパッケージの名前。
  - **パッケージのステータス**：インストールパッケージのダウンロードステータス。
  - **ソース**：アプリケーションの開発元の名前。
  - **アプリケーション**：カスタムインストールパッケージに含まれるアプリケーションの名前。
  - **バージョン**：アプリケーションのバージョン。
  - **言語**：カスタムインストールパッケージに含まれるアプリケーションの言語。
  - **サイズ（MB）**：インストールパッケージのサイズ。
  - **オペレーティングシステム**：インストールパッケージが対象とするオペレーティングシステムの種別。
  - **作成**：インストールパッケージの作成日時。
  - **変更**：インストールパッケージの変更日時。
  - **種別**：インストールパッケージの種別。
- コマンドラインのパラメータを変更します。

# スタンドアロンインストールパッケージの作成

組織内の管理者とユーザーがデバイスに手動でアプリケーションをインストールするために、スタンドアロンインストールパッケージを使用できます。

スタンドアロンインストールパッケージは実行ファイルで、Web サーバーまたは共有フォルダーに保存したり、メールで送信したり、別の方法でクライアントデバイスに転送したりできます。クライアントデバイスで受け取った実行ファイルをローカルで起動することで、Kaspersky Security Center Linux を使用せずにアプリケーションをインストールすることが可能となります。カスペルスキー製品およびサードパーティ製品のスタンドアロンインストールパッケージを作成できます。サードパーティ製品のインストールパッケージを作成するには、カスタムインストールパッケージを作成する必要があります。

スタンドアロンインストールパッケージが第三者にアクセスされないように必ず注意してください。

*スタンドアロンインストールパッケージを作成するには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのリストでインストールパッケージを選択し、リストの上にある［**製品の導入**］をクリックします。




インストールパッケージのリスト

3. ［**スタンドアロンパッケージを使用**］を選択します。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。




スタンドアロンインストールパッケージの作成

4. 選択したアプリケーションとネットワークエージェントを合わせてインストールする場合、［**このアプリケーションと同時にネットワークエージェントをインストールする**］がオンになっていることを確認します。

   既定では、このオプションはオンです。デバイスにネットワークエージェントがインストール済みかどうかが不明な場合は、このオプションをオンにすることを推奨します。ネットワークエージェントがデバイスにインストールされている場合、ネットワークエージェントを含めたインストールパッケージがインストールされたときにネットワークエージェントが新しいバージョンにアップデートされます。

   このオプションがオフの場合、デバイスにはネットワークエージェントはインストールされず、デバイスは管理対象外のデバイスになります。

   選択したアプリケーションのスタンドアロンインストールパッケージが既に管理サーバー上に存在する場合、ウィザードに通知が表示されます。この場合、次のいずれかのオプションを選択する必要があります：

   - **スタンドアロンインストールパッケージの作成**：新しいバージョンのアプリケーションのスタンドアロンインストールパッケージを新規に作成し、なおかつ旧バージョンのアプリケーションで作成したスタンドアロンインストールパッケージも保持する場合などにこのオプションを選択します。新しいスタンドアロンインストールパッケージは別のフォルダーに配置されます。

   - **既存のスタンドアロンインストールパッケージを使用**：既存のスタンドアロンインストールパッケージを使用する場合は、このオプションをオンにします。パッケージの作成プロセスは開始されません。

   - **既存のスタンドアロンインストールパッケージを再構築**：同じアプリケーションのインストールパッケージを再作成する場合、このオプションを選択します。スタンドアロンインストールパッケージは、同じフォルダーに保存されます。

5. ［**管理対象デバイスのリストへ移動**］ステップで、既定では［**デバイスを移動しない**］オプションがオンになっています。ネットワークエージェントのインストール後にクライアントデバイスをどの管理グループにも移動したくない場合は、オプションの選択を変更しないでください。

   ネットワークエージェントのインストール後にクライアントデバイスを移動したい場合は、［**未割り当てデバイスをこのグループへ移動**］を選択し、クライアントデバイスの移動先の管理グループを指定します。既定では、デバイスは［**管理対象デバイス**］グループに移動されます。




クライアントデバイスを移動する管理グループの選択

6. スタンドアロンインストールパッケージの作成プロセスが完了したら、［**完了**］をクリックします。

   ［Stand-alone Installation Package Creation Wizard］が閉じます。

スタンドアロンインストールパッケージが作成され、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。インストールパッケージのリストの上にある［**スタンドアロンパッケージリストの表示**］をクリックすると、スタンドアロンパッケージのリストを確認できます。

# ネットワークエージェントのインストールパッケージ設定

*ネットワークエージェントのインストールパッケージを設定するには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで使用可能なインストールパッケージのリストが表示されます。

2. ネットワークエージェントインストールパッケージの名前をクリックします。

ネットワークエージェントのインストールパッケージのプロパティウィンドウが表示されます。

ネットワークエージェントインストールパッケージの設定は、次のタブにグループ化されています：

- ［**全般**］タブ
  このタブには、インストールパッケージに関する次の情報が表示されます：
  - インストールパッケージ名
  - インストールパッケージでインストールされるアプリケーションの名前とバージョン
  - インストールパッケージのサイズ
  - インストールパッケージの作成日
  - インストールパッケージのフォルダーのパス
- ［**設定**］タブ
  このタブには、ネットワークエージェントをインストール後すぐに正常に機能させるのに必要な設定が示されます。
  - ［**設定**］セクション
    - **既定のフォルダーにインストールする**
      このオプションをオンにすると、ネットワークエージェントは、フォルダー <ドライブ名>:\Program Files\Kaspersky Lab\NetworkAgent にインストールされます。このフォルダーがない場合は、フォルダーが自動的に作成されます。
      既定では、このオプションがオンです。
    - **指定したフォルダーにインストールする**
      このオプションをオンにすると、ネットワークエージェントは、入力フィールドで指定したフォルダーにインストールされます。
    - **アンインストール用パスワードを使用する**
      このオプションをオンにすると、アンインストール用パスワード（Windows オペレーティングシステム実行中のデバイスのネットワークエージェントのみに使用可能）を入力できます。
      既定では、このオプションはオフです。
    - **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**
      このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。
      ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。
      既定では、このオプションはオフです。

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

  このオプションをオンにすると、管理サーバー、ネットワークエージェント、Kaspersky Security Center Web コンソール、および iOS MDM サーバー用にダウンロードされたすべてのアップデートとパッチが自動的にインストールされます。

  このオプションをオフにすると、ダウンロードされたすべてのアップデートとパッチは、アップデートとパッチのステータスを［*承認*］に変更した後にインストールされます。［*未定義*］ステータスのアップデートとパッチはインストールされません。

  既定では、このオプションはオンです。

- ［**接続**］セクション

  このセクションでは、ネットワークエージェントから管理サーバーへの接続を設定できます：接続を確立するために、SSL または UDP プロトコルを使用できます。接続を設定するには、次の設定を指定します：

  - **管理サーバーアドレス**

    管理サーバーがインストールされたデバイスのアドレス。

  - **ポート番号**

    接続に使用されるポート番号。

  - **SSL ポート**

    SSL プロトコルによる接続に使用されるポート番号。

  - **サーバー証明書を使用する**

    このオプションを有効にすると、ネットワークエージェントによる管理サーバーへのアクセス認証には、［**証明書ファイルの選択**］ボタンをクリックして指定した証明書ファイルが使用されます。

    このオプションをオフにすると、［**管理サーバーアドレス**］フィールドで指定したアドレスへのネットワークエージェントからかの初回接続時に、管理サーバーから証明書ファイルを受信します。

    管理サーバーへの接続時にネットワークエージェントで管理サーバー証明書を自動受信することはセキュアでないため、このオプションの無効化は推奨されません。

    既定では、このオプションはオフです。

  - **SSL 接続を使用する**

    このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

    既定では、このオプションはオフです。セキュアな接続を保つために、このオプションを無効にしないことを推奨します。

  - **UDP ポートを使用する**

このオプションをオンにすると、ネットワークエージェントは UDP ポート経由で管理サーバーに接続されます。これにより、クライアントデバイスを管理し、それらに関する情報を受け取ることができます。

ネットワークエージェントがインストールされている管理対象デバイスで,UDP ポートを開放する必要があります。したがって、このオプションを無効にしないことを推奨します。

既定では、このオプションはオンです。

- **UDP ポート**

  このフィールドでは、UDP プロトコル経由で管理サーバーがネットワークエージェントに接続するポートを指定できます。

  既定の UDP ポート番号は 15000 です。

- **プロキシサーバーを使用しない**

  このオプションをオンにすると、デバイスを管理サーバーに接続するために直接接続が使用されます。

- **プロキシサーバーを使用する**

  このオプションをオンにする場合は、プロキシサーバーのパラメータを指定します：

  - **プロキシサーバーアドレス**
  - **プロキシサーバーのポート**

  プロキシサーバーで認証が必要な場合は、［**プロキシサーバー認証**］をオンにし、プロキシサーバーへの接続を確立するアカウントの**ユーザー名**と**パスワード**を指定します。プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

- **Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**

  このオプションをオンにすると、ネットワークエージェントによって使用されるポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

  既定では、このオプションはオフになっています。

  このオプションは、Windows を実行するデバイス向けのネットワークエージェントインストールパッケージでのみ使用できます。

- ［**詳細**］セクション

  このセクションでは、接続ゲートウェイの使用方法を設定できます。

  **接続ゲートウェイ**設定グループでは、デバイスと管理サーバー間の接続方法を構成できます：

  - **DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**

このオプションをオンにすると、ネットワークエージェントが非武装地帯（DMZ）の接続ゲートウェイとして使用され、管理サーバーへの接続、通信、およびデータ転送中のネットワークエージェント上のデータの安全が確保されます。

- **接続ゲートウェイを使用して管理サーバーに接続する**

  このオプションをオンにすると、管理サーバーへの接続数を減らすため、接続ゲートウェイを使用して管理サーバーへの接続が確立されます。この場合、接続ゲートウェイとして機能するデバイスのアドレス［**接続ゲートウェイアドレス**］フィールドに入力します。

**仮想マシン**設定グループでは、ネットワークに仮想マシンが含まれている場合に仮想デスクトップインフラストラクチャ（VDI）の接続を構成できます。

- **VDI 向け動的モードを有効にする**

  このオプションをオンにすると、仮想マシンにインストールされたネットワークエージェントで仮想デスクトップインフラストラクチャ（VDI）向け動的モードが有効になります。

  既定では、このオプションはオフです。

- **VM 向けに設定を最適化する**

  このオプションをオンにすると、ネットワークエージェントの設定で次の機能が無効にされます：

  - インストールされたソフトウェアに関する情報の取得
  - ハードウェアに関する情報の取得
  - 検知された脆弱性に関する情報の取得
  - 必要なアップデートに関する情報の取得

  既定では、このオプションはオフです。

Linux デバイスにネットワークエージェントをインストールした後、ユーザーにデバイスの所有者として登録するように自動的に要求する場合は、**ネットワークエージェントのインストール後にユーザー登録ユーティリティの実行を許可する**オプションをオン有効にします。

このオプションを有効にすると、デバイスの所有者ユーティリティとしてのユーザー登録は、ネットワークエージェントのインストール後に実行されます。既定では、このオプションはオフです。

- ［**タグ**］セクション

  ［**タグ**］セクションには、ネットワークエージェントのインストール後にクライアントデバイスに追加できるキーワード（タグ）のリストが表示されます。リストへのタグの追加、リストからのタグの削除、タグの名前の変更を行うことができます。

  タグの横のチェックボックスがオンの場合、そのタグは、ネットワークエージェントのインストール時に、管理対象デバイスに自動的に追加されます。

  タグに隣接するチェックボックスをオフにすると、ネットワークエージェントのインストール時に、管理対象デバイスに自動的には追加されません。タグは手動でデバイスに追加できます。

  リストからタグを削除すると、そのタグは、そのタグが追加されたすべてのデバイスから自動的に削除されます。

自動タグ付けルールは、 Linux および macOS を実行するデバイス向けのネットワークエージェントインストールパッケージには適用されません。

- ［**スタンドアロンパッケージ**］タブ

  このタブで、次の操作を実行できます：

  - 利用可能なスタンドアロンインストールパッケージのリストの表示。
  - ［**公開**］をクリックして、スタンドアロンインストールパッケージを Web サーバーに公開する。スタンドアロンインストールパッケージへのリンクを管理者から受け取ったユーザーは、公開されたスタンドアロンインストールパッケージをダウンロードできます。
  - ［**公開の取り消し**］をクリックして、スタンドアロンインストールパッケージの Web サーバーへの公開を中止する。公開を取り消したスタンドアロンインストールパッケージは、取り消し操作を行った管理者およびその他の管理者しかダウンロードできません。
  - ［**ダウンロード**］をクリックして、スタンドアロンインストールパッケージを操作中のデバイスにダウンロードする。
  - ［**メールで送信**］をクリックして、スタンドアロンインストールパッケージへのリンクをメールで送信する。
  - ［**削除**］をクリックして、スタンドアロンインストールパッケージを削除する。

- ［**変更履歴**］タブ

  このタブでは、インストールパッケージのリビジョンの履歴を確認できます。リビジョンの比較、リビジョンの表示、リビジョンのファイル保存、リビジョンの説明の追加と編集ができます。

# Kaspersky Security Center Linux で作成された実行中のスタンドアロンパッケージ

上述のネットワークエージェントとその他のアプリケーションの初期導入方法は、適用される条件をすべて満たすことができないため、常に実装できるわけではありません。そのような場合は、Kaspersky Security Center Linux で、管理者によって適切なインストール設定が行われているインストールパッケージを使用して、*スタンドアロンインストールパッケージ*と呼ばれる共通の実行ファイルを作成できます。スタンドアロンインストールパッケージは、妥当であると判断される場合（Web サーバーへの外部アクセスが対象デバイスのユーザー用に設定されている場合）、内部 Web サーバー（Kaspersky Security Center Linux に含まれる）上、あるいは Kaspersky Security Center Web コンソールに含まれる排他的に導入された Web サーバー上のいずれかで公開されます。また、スタンドアロンパッケージは別の Web サーバーにコピーできます。

Kaspersky Security Center Linux を使用して、現在使用されている Web サーバー上のスタンドアロンパッケージファイルのリンクを記載したメールメッセージを、特定のユーザーに送信できます。そうすることで、（対話モードで、またはサイレントインストールのキー「-s」を使用して）ファイルを実行するようユーザーに促すことができます。Web サーバーにアクセスできないデバイスのユーザーには、スタンドアロンインストールパッケージをメールメッセージに添付して送信できます。管理者は、スタンドアロンパッケージをリムーバブルドライブにコピーし、関連のデバイスに配布し、後で実行することもできます。

スタンドアロンパッケージは、ネットワークエージェントパッケージ、別のアプリケーションのパッケージ（セキュリティ製品のパッケージなど）、またはその両方から作成できます。スタンドアロンパッケージをネットワークエージェントパッケージと別のアプリケーションから作成した場合、インストールはネットワークエージェントを使用して起動されます。

スタンドアロンパッケージをネットワークエージェントから作成する場合、ネットワークエージェントのインストールが完了した際に、新しいデバイス（管理グループのいずれにも割り当てられていないデバイス）が自動的に割り当てられる管理グループを指定できます。

スタンドアロンパッケージは、パッケージに含まれるアプリケーションのインストール結果が表示される対話モードで実行することも（既定）、サイレントモードで実行することもできます（キー「-s」を使用して実行した場合）。サイレントモードは、スクリプト（オペレーティングシステムイメージが導入された後に実行されるように設定されているスクリプトなど）からインストールする場合に使用できます。サイレントモードでは、インストール結果はプロセスのリターンコードから判断します。

Linux 用のスタンドアロンネットワークエージェントには、nmap ユーティリティからのオプションの依存関係があります。nmap ユーティリティが見つからないか、バージョン 6.0 より前の場合、ブロードキャスト DHCP 検出機能はサポートされません。

# スタンドアロンパッケージを使用したアプリケーションのインストール

Kaspersky Security Center で、アプリケーションインストール用のスタンドアロンパッケージを作成できます。スタンドアロンパッケージは実行ファイル形式で、Web サーバーやメールなどを利用してクライアントデバイスに送信できます。この実行ファイルをクライアントデバイスにダウンロードすると、Kaspersky Security Center を使用せずにアプリケーションをインストールすることが可能となります。

Linux 用のスタンドアロンネットワークエージェントには、nmap ユーティリティからのオプションの依存関係があります。nmap ユーティリティが見つからないか、バージョン 6.0 より前の場合、ブロードキャスト DHCP 検出機能はサポートされません。

*スタンドアロンインストールパッケージを使用してアプリケーションをインストールするには：*

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. 必要なアプリケーションのインストールパッケージの横にあるチェックボックスをオンにし、［**製品の導入**］をクリックします。
3. 開いたウィンドウで、［**スタンドアロンパッケージを使用**］を選択し、［**次へ**］をクリックします。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
4. ［**スタンドアロンインストールパッケージの作成**］をオンにします。
5. ネットワークエージェントのインストール後に、デバイスを管理グループに移動するかどうかを指定します。
6. ウィザードの最後のステップで、スタンドアロンインストールパッケージをクライアントデバイスに転送する方法を選択し、［**終了**］をクリックして、ウィザードを終了します。
7. スタンドアロンインストールパッケージをクライアントデバイスに送信します。
8. クライアントデバイスでスタンドアロンインストールパッケージを実行します。

これにより、スタンドアロンパッケージに指定されている設定を用いてクライアントデバイスにアプリケーションをインストールできます。

スタンドアロンインストールパッケージは作成時に、Web サーバー上に自動的に公開されます。スタンドアロンパッケージをダウンロードするリンクは、作成済みスタンドアロンインストールパッケージのリストに表示されます。必要に応じて、特定のスタンドアロンパッケージの公開を取り消したり、Web サーバーに再度公開したりすることができます。スタンドアロンインストールパッケージのダウンロードに使用される既定のポートは 8060 です。

# セキュリティ製品のインストールパッケージで定義データベースをアップデートする

セキュリティ製品の配布パッケージと一緒に出荷された定義データベース（自動パッチのモジュールを含む）は、保護の導入を開始する前にアップデートすることが可能です。導入を開始する前に、（選択したインストールパッケージのコンテキストメニューで関連コマンドを使用するなどして）アプリケーションのインストールパッケージ内のデータベースをアップデートすることは有用です。そうすることで、対象デバイスへの保護製品の導入を完了するために必要な再起動の回数が低減されます。

# カスタムインストールパッケージのデータサイズの上限の変更

カスタムインストールパッケージの作成中に展開されるデータサイズの総量には上限があります。既定の制限は 1 GB です。

現在設定されている上限値を超えるサイズのデータが含まれる圧縮ファイルをアップロードしようとすると、エラーメッセージが表示されます。サイズが大きい配布パッケージからインストールパッケージを作成する場合は、上限値を増やす必要が生じる場合があります。

*カスタムインストールパッケージのサイズの上限値を変更するには：*

1. 管理サーバーデバイスで、管理サーバーのインストールに使用したアカウントでコマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center Linux のインストールフォルダー（通常は /opt/kaspersky/ksc64/sbin）に変更します。
3. 管理サーバーのインストールの種別に応じて、root アカウントで次のいずれかのコマンドを入力します：
   - 通常のローカルインストール：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <バイト数>
     ```

   - Kaspersky Security Center Linux フェールオーバークラスタへのインストール：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <バイト数> --stp klfoc
     ```

   <バイト数> は、16 進数または 10 進数形式のバイト数です。

   たとえば、必要な制限が 2 GB の場合、10 進値 2147483648 または 16 進値 0x80000000 を指定できます。この場合、管理サーバーのローカルインストールでは、次のコマンドを使用できます：

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

カスタムインストールパッケージのデータサイズの上限が変更されます。

# セカンダリ管理サーバーへのインストールパッケージの配布

Kaspersky Security Center Linux を使用すると、カスペルスキー製品およびサードパーティ製品のインストールパッケージを作成したり、インストールパッケージをクライアントデバイスに配布したり、パッケージからアプリケーションをインストールしたりできます。プライマリ管理サーバーの負荷を最適化するために、インストールパッケージをセカンダリ管理サーバーに配布できます。その後、セカンダリサーバーがパッケージをクライアントデバイスに送信すると、クライアントデバイスでアプリケーションのリモートインストールを実行できます。

*セカンダリ管理サーバーにインストールパッケージを配布するには：*

1. セカンダリ管理サーバーがプライマリ管理サーバーに接続されていることを確認します。
2. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

   タスクのリストが表示されます。
3. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
4. ［**新規タスク設定**］ページの［**アプリケーション**］ドロップダウンリストで、**Kaspersky Security Center** を選択します。次に、［**タスク種別**］ドロップダウンリストから［**インストールパッケージの配布**］を選択し、タスク名を指定します。
5. ［**タスク範囲**］ページで、次のいずれかの方法で、タスクが割り当てられるデバイスを選択します。

   - 特定の管理グループ内のすべてのセカンダリ管理サーバー用のタスクを作成する場合は、そのグループを選択して、グループタスクを作成します。
   - 特定のセカンダリ管理サーバー用のタスクを作成する場合は、それらのサーバーを選択して、タスクを作成します。
6. ［**配布したインストールパッケージ**］ページで、セカンダリ管理サーバーにコピーするインストールパッケージを選択します。
7. *インストールパッケージの配布*タスクを実行するアカウントを指定します。自身のアカウントを使用して、［**既定のアカウント**］**オプションをオンのままにすることもできます。**または、必要なアクセス権を持つ別のアカウントを指定してタスクを実行することもできます。この場合は［**アカウントの指定**］をオンにしてそのアカウントの資格情報を入力してください。
8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにして、タスクのプロパティウィンドウを開き、既定のタスク設定を変更できます。変更しない場合は、後でいつでもタスク設定を変更できます。
9. ［**終了**］をクリックします。

   セカンダリ管理サーバーにインストールパッケージを配布するために作成されたタスクが、タスクリストに表示されます。
10. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待つことができます。

タスクが完了すると、選択したインストールパッケージが、指定したセカンダリ管理サーバーにコピーされます。

# スタンドアロンインストールパッケージのリストの表示

スタンドアロンインストールパッケージのリストを表示し、それぞれのスタンドアロンインストールパッケージのプロパティを確認できます。

*すべてのインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：*

リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストで、パッケージのプロパティが次のように表示されます。

- **パッケージ名**：パッケージに含まれるアプリケーション名とバージョン番号を組み合わせて自動的に作成されるスタンドアロンインストールパッケージの名前。
- **アプリケーション名**：スタンドアロンインストールパッケージに含まれるアプリケーションの名前。
- **アプリケーションのバージョン**。
- **ネットワークエージェントのインストールパッケージ名**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **ネットワークエージェントのバージョン**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **サイズ**：ファイルのサイズ（MB 単位）。
- **グループ**：ネットワークエージェントのインストール後にクライアントデバイスが移動する管理グループの名前。
- **作成日時**：スタンドアロンインストールパッケージが作成された日時。
- **変更日時**：スタンドアロンインストールパッケージが変更された日時。
- **パス**：スタンドアロンインストールパッケージが保存されているフォルダーのパス。
- **URL**：スタンドアロンインストールパッケージをダウンロードできる URL。
- **ファイルのハッシュ**：このプロパティは、スタンドアロンインストールパッケージが第三者による改竄を受けておらず、管理者が作成してユーザーに送信したのと同じファイルがユーザーの手元にあるかどうかを検証するために使用します。

*特定のインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：*

リストからインストールパッケージを選択し、リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストを使用して、次の操作を実行できます：

- ［**公開**］をクリックして、スタンドアロンインストールパッケージを Web サーバーに公開する。スタンドアロンインストールパッケージへのリンクを管理者から受け取ったユーザーは、公開されたスタンドアロンインストールパッケージをダウンロードできます。
- ［**公開の取り消し**］をクリックして、スタンドアロンインストールパッケージの Web サーバーへの公開を中止する。公開を取り消したスタンドアロンインストールパッケージは、取り消し操作を行った管理者およびその他の管理者しかダウンロードできません。
- ［**ダウンロード**］をクリックして、スタンドアロンインストールパッケージを操作中のデバイスにダウンロードする。
- ［**メールで送信**］をクリックして、スタンドアロンインストールパッケージへのリンクをメールで送信する。
- ［**削除**］をクリックして、スタンドアロンインストールパッケージを削除する。

# Linux 用のネットワークエージェントのインストール

組織内でデバイスを管理するには、各デバイスにネットワークエージェントをインストールする必要があります。組織用デバイスに配信された Kaspersky Security Center Linux を導入すると、通常はそのデバイスでネットワークエージェントのインストールが開始されます。

Linux 管理対象デバイスにネットワークエージェントを最初にインストールするには、次の方法があります：

- SSH 経由で管理対象デバイスに接続し、リモートインストールタスクを実行します。
- 管理対象デバイスでパッケージのインストールを実行します。

デバイスにネットワークエージェントをインストールすると、このネットワークエージェントを介してそのデバイスにカスペルスキー製品のリモートインストールを実行できるようになります。インストールするアプリケーションの配布パッケージは、管理者が定義したインストール設定とともに、ネットワークエージェントと管理サーバー間の通信チャネルを介して転送されます。配布パッケージを転送するには、転送配布用のノードを使用します。例：ディストリビューションポイント、マルチキャストによる配布など。

管理対象ネットワーク内に製品を導入するための方法と戦略を選択する際には、いくつかの要素について検討する必要があります（部分的なリスト）：

- 組織ネットワークの設定。
- デバイスの合計数。
- 組織ネットワーク上で、いずれのドメインにも属していないデバイスの有無、およびそのデバイスに関して管理者権限を付与されている統一アカウントの有無。
- 管理サーバーとデバイス間のチャネルの容量。
- 管理サーバーとリモートサブネット間の通信の種別、およびそのサブネット内のネットワークチャネルの容量。
- 導入の開始時にリモートデバイスに適用されるセキュリティ設定。これらのパラメータを使用すると、管理対象デバイスへのリモート接続を確立し、インストールを開始できます。

# Linux デバイスの準備と Linux デバイスへのネットワークエージェントのリモートインストール

ネットワークエージェントのインストールは、次の 2 つの手順で実行されます：

- Linux デバイスの準備
- ネットワークエージェントのリモートインストール

## Linux デバイスの準備

*Linux で動作するデバイスにネットワークエージェントをリモートインストールのために準備するには：*

1. Linux 用ネットワークエージェントをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
2. アプリケーションインターフェイスを使用するか、カスペルスキー Web サイトからネットワークエージェントインストールパッケージをダウンロードします。
3. 対象となる Linux デバイスに次のソフトウェアがインストールされていることを確認します：
   - Sudo（Ubuntu 10.04 の場合、Sudo バージョンは 1.7.2p1 以降）
   - Perl 言語インタープリターのバージョン 5.10 以降

4. デバイスの構成をテストします：

   a. デバイスに SSH クライアント（PuTTY など）で接続できることを確認します。

      デバイスに接続できない場合、ファイル `/etc/ssh/sshd_config` を開き、次の設定をそれぞれの値に変更します：

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > デバイスに問題なく接続できる場合は、/etc/ssh/sshd_config ファイルを変更しないでください。そうしないと、リモートインストールタスクの実行時に SSH 認証エラーが発生する可能性があります。

      必要に応じてファイルを保存し、`sudo service ssh restart` コマンドを使用して SSH サービスを再起動します。

   b. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。

   c. sudo で `visudo` コマンドを使用し、sudoers 構成ファイルを開きます。

      開いたファイルの末尾に次の行を追加します：**<ユーザー名>** `ALL = (ALL) NOPASSWD: ALL`。この場合、**<ユーザー名>** は、SSH を経由してデバイスを接続するために使用するユーザーアカウントです。Astra Linux オペレーティングシステムを使用している場合は、ファイル /etc/sudoers の最後の行に次のテキストを追加します：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. sudoers ファイルを保存して閉じます。

   e. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。

5. systemd 初期化システムを搭載したオペレーティングシステムを実行しているデバイスにネットワークエージェントをインストールする場合は、`/etc/systemd/logind.conf` ファイルを開き、次のいずれかを実行します：

   - `KillUserProcesses` 設定の値として［no］を指定します：`KillUserProcesses=no`。
   - `KillExcludeUsers` の設定にリモートインストールを実行するアカウントのユーザー名を入力します。例：`KillExcludeUsers=root`。

   **Astra Linux ターゲットデバイス**

   対象デバイスが Astra Linux を実行している場合は、`export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 文字列をファイル `/home/<ユーザー名>/.bashrc` に追加します。**<ユーザー名>** は、SSH を使用したデバイス接続に使用されるユーザーアカウントです。

   **OSnova ターゲットデバイス**

   ターゲットデバイスで OSnova が実行されている場合は、次の手順を実行します：

   a. `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` ファイルを開き、`#KillUserProcess=yes` 行をコメントアウトします。

   b. `/usr/lib/NESS/pam-user-session` ファイルを開き、`#loginctl terminate-session "$XDG_SESSION_ID"` 行をコメントアウトします。

   変更した設定を適用するには、Linux デバイスを再起動するか、次のコマンドを実行してください：

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

6. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

7. Astra Linux オペレーティング システムが閉鎖ソフトウェア環境モードで実行されているデバイスにネットワークエージェントをインストールする場合は、追加の手順を実行して Astra Linux デバイスを準備します。

8. Ubuntu Server または Ubuntu Desktop バージョン 10.04 を実行しているデバイスにネットワークエージェントをインストールする場合は、追加の手順を実行してこれらのデバイスを準備します。

9. オペレーティングシステム RED OS 7.3.4 以降または MSVSPHERE 9.2 以降を使用するデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントを正しく機能させるために libxcrypt-compat パッケージをインストールしてください。

### ネットワークエージェントのリモートインストール

*Linux デバイスにネットワークエージェントをリモートインストールするには、次の手順に従います：*

1. インストールパッケージをダウンロードして作成します：

   a. パッケージのインストール前に、このパッケージが依存するプログラムやライブラリのすべてがデバイスにインストールされていることを確認してください。

   パッケージの依存関係は、パッケージのインストール先の Linux ディストリビューションに含まれるユーティリティで確認できます。それらのユーティリティについて詳しくは、オペレーティングシステムのマニュアルを参照してください。

   b. リモートインストールパッケージを作成するには、次のファイルを使用します：

   - klnagent.kpd
   - akinstall.sh
   - ネットワークエージェントの DEB または RPM パッケージ

2. 次の設定でリモートインストールタスクを作成します：

   - 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。
   - ［**タスクを実行するアカウントの選択**］ページで、SSH でデバイスに接続するために使用するユーザーアカウントの設定を指定します。

3. リモートインストールタスクを実行します。`su` コマンドのオプションを使用して、環境を保持します: `-m, -p, --preserve-environment`。

# ネットワークエージェントをインストールする SUSE Linux Enterprise Server 15 デバイスの準備

閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスにネットワークエージェントをインストールする前に、2 つの準備手順を実行する必要があります。1 つは以下の手順にある手順、もう 1 つは Linux デバイスの一般的な準備手順です。

*SUSE Linux Enterprise Server 15 オペレーティングシステムのデバイスにネットワークエージェントを準備するには：*

ネットワークエージェントのインストール前に、次のコマンドを実行します：

```
$ sudo zypper install insserv-compat
```

これにより、insserv-compat パッケージのインストールと、ネットワークエージェントの適切な設定が可能になります。

`rpm -q insserv-compat` コマンドを実行し、パッケージがインストール済みかどうかをチェックします。

多くの SUSE Linux Enterprise Server 15 デバイスがネットワークに存在する場合、会社のインフラストラクチャを設定、管理する専用のソフトウェアを使用できます。このソフトウェアを使用することで、必要なすべてのデバイスに insserv-compat パッケージを一度に自動的にインストールできます。たとえば、Puppet、Ansible、Chef を使用したり、独自のスクリプトを作成したりできます。都合のよい方法を使用してください。

デバイスに SUSE Linux Enterprise の GPG 署名ライセンスがない場合は、次の警告が表示される場合があります：`Package header is not signed!` 警告を無視するには、[`i`] をオンにします。

SUSE Linux Enterprise Server 15 デバイスの準備が完了したら、ネットワークエージェントを配信してインストールします。

# ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備します

閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスにネットワークエージェントをインストールする前に、2 つの準備手順を実行する必要があります。1 つは以下の手順にある手順、もう 1 つは Linux デバイスの一般的な準備手順です。

ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

*ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備するには：*

1. ファイル `/etc/digsig/digsig_initramfs.conf` を開き、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. コマンドラインで次のコマンドを実行して、適合パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 製品のライセンスにディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 前の手順で作成したディレクトリに製品のライセンス /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg を配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Kaspersky Security Center Linux 配布キットに kaspersky_astra_pub_key.gpg ライセンスが含まれていない場合は、以下のリンクをクリックしてダウンロードできます：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. RAM ディスクをアップデートします：

   ```
   update-initramfs -u -k all
   ```

   システムを再起動します。

6. すべての Linux デバイスに共通の準備手順を実行します。

デバイスが準備されました。これで、ネットワークエージェントのインストールに進むことができます。

# OpenSSH バージョン 6.4 以前を使用するデバイスをネットワークエージェントのインストーラー用に準備する

OpenSSH バージョン 6.4 以前を使用するデバイスにネットワークエージェントをインストールする前に、2 つの準備手順を実行する必要があります。この記事で説明する手順と、あらゆる Linux デバイス向けの一般的な準備手順です。

開始前、必要なネットワークエージェントインストールファイルをカスペルスキーの Web サイトからダウンロードします。

ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

*OpenSSH バージョン 6.4 以前を使用するデバイスをネットワークエージェントのインストール用に準備するには：*

1. Kaspersky Security Center Linux 管理サーバーがインストールされているデバイスでは、OpenSSH バージョン 6.4 以前のデバイスにネットワークエージェントをインストールできるように、SSH 接続の有効な暗号化アルゴリズムの許可リストを無効にしてください。

   これを行うには、コマンドラインで次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

   許可リストを無効にすると、SSH 接続のセキュリティに影響する可能性があります。

2. OpenSSH バージョン 6.4 以前を使用するデバイスで、あらゆる Linux デバイスに共通の準備手順を実行します。

デバイスが準備されました。これで、ネットワークエージェントのインストールに進むことができます。

# Linux 用ネットワークエージェントのサイレントモードでのインストール（応答ファイルを使用）

Linux デバイスにネットワークエージェントをインストールするには、インストールパラメータのカスタムセット（変数と各変数の値）を含むテキストファイルである応答ファイルを使用します。この応答ファイルを使用すると、インストールをサイレントモードで、つまりユーザーの参加なしで実行できます。

*Linux 用ネットワークエージェントのインストールをサイレントモードで実行するには：*

1. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

   オペレーティングシステム RED OS 7.3.4 以降またはMSVSPHERE 9.2以降を使用するデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントを正しく機能させるために libxcrypt-compat パッケージをインストールしてください。

2. 使用許諾契約書をお読みください。次の手順は、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

3. たとえば、次のように応答ファイルの完全な名前（パスを含む）を入力して、ルートまたはユーザー環境の KLAUTOANSWERS 環境変数の値を設定します：

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. 環境変数で指定したディレクトリに応答ファイル（TXT 形式）を作成します。応答ファイルに、VARIABLE_NAME=variable_value 形式の変数のリストを追加します。各変数は個別の行に配置します。

   応答ファイルを正しく使用するには、3 つの必須変数の最小セットをファイルに含める必要があります：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   オプションの変数を追加して、リモートインストールに関するより具体的なパラメータを使用することもできます。次の表に、応答ファイルに含めることができるすべての変数を一覧で示します：

   **サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数**

サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数

| 変数名 | 必須 | 説明 | 指定可能な値 |
|---|---|---|---|
| KLNAGENT_SERVER | 使用する | 完全修飾ドメイン名（FQDN）または IP アドレスとして提示される管理サーバー名が含まれます。 | DNS 名または IP アドレス。 |
| KLNAGENT_AUTOINSTALL | 使用する | サイレントインストールモードを有効にするかどうかを定義します。 | 1 - サイレントモードが有効です。ユーザーが、インストール中に操作を要求されることはありません。<br><br>その他 - サイレントモードは無効です。ユーザーは、インストール中に操作を要求される場合があります。 |
| EULA_ACCEPTED | 使用する | ユーザーがネットワークエージェントの使用許諾契約書（EULA）に同意するかどうかを定義します。定義されていない場合は、EULA に同意しないものとして解釈できます。 | 1 - この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する。<br><br>その他の値または値なし - 使用許諾契約書の条項に同意しない（インストールは実行されません）。 |
| KLNAGENT_PROXY_USE | 使用しない | 管理サーバーとの接続でプロキシ設定を使用するかどうかを定義します。既定値は 0 です。 | 1 - プロキシ設定が使用されます。<br><br>その他 - プロキシ設定は使用されません。 |
| KLNAGENT_PROXY_ADDR | 使用しない | 管理サーバーとの接続に使用されるプロキシサーバーのアドレスを定義します。 | DNS 名または IP アドレス。 |
| KLNAGENT_PROXY_LOGIN | 使用しない | プロキシサーバーへのログインに使用するユーザー名を定義します。 | 既存のユーザー名。 |
| KLNAGENT_PROXY_PASSWORD | 使用しない | プロキシサーバーへのログインに使用するパスワードを定義します。 | オペレーティングシステムのパスワード形式で許可されている英数字のセット。 |
| KLNAGENT_VM_VDI | 使用しない | 動的仮想マシンを作成するために、ネットワークエージェントをイメージにインストールするかどうかを定義します。 | 1 - ネットワークエージェントがイメージにインストールされ、その後、動的仮想マシンの作成に使用されます。<br><br>その他 - インストール中にイメージは使用されません。 |
| KLNAGENT_VM_OPTIMIZE | 使用しない | ネットワークエージェントの設定をハイパーバイザー向けに最適化するかどうかを定義します。 | 1 - ネットワークエージェントの既定のローカル設定が変更され、ハイパーバイザーでの使用が最適化されます。 |
| KLNAGENT_TAGS | 使用しない | ネットワークエージェントのインスタンスに割り当てられたタグを一覧表示します。 | セミコロンで区切られた 1 つまたは複数のタグ名。 |
| KLNAGENT_UDP_PORT | 使用しない | ネットワークエージェントが使用する UDP ポートを定義します。既定値は 15000 です。 | 既存のポート番号。 |
| KLNAGENT_PORT | 使用しない | ネットワークエージェントが使用する非 TLS ポートを定義します。既定値は 14000 です。 | 既存のポート番号。 |
| KLNAGENT_SSLPORT | 使用しない | ネットワークエージェントが使用する TLS ポートを定義します。既定値は 13000 です。 | 既存のポート番号。 |

| | | | |
|---|---|---|---|
| KLNAGENT_USESSL | 使用しない | 接続にトランスポート層セキュリティ（TLS）を使用するかどうかを定義します。 | 1（既定） - TLSが使用されます。<br><br>その他 - TLS は使用されません。 |
| KLNAGENT_GW_MODE | 使用しない | 接続ゲートウェイを使用するかどうかを定義します。 | 1（既定） - 現在の設定は変更されません（最初の呼び出しで、接続ゲートウェイは指定されません）。<br><br>2 - 接続ゲートウェイは使用されません。<br><br>3 - 接続ゲートウェイが使用されます。KLNAGENT_GW_ADDRESS が必要です。<br><br>4 - ネットワークエージェントのインスタンスが、非武装地帯（DMZ）で接続ゲートウェイとして使用されます。サーバー証明書が必要です。 |
| KLNAGENT_GW_ADDRESS | 使用しない | 接続ゲートウェイのアドレスを定義します。この値は、KLNAGENT_GW_MODE=3 の場合にのみ適用されます。 | DNS 名または IP アドレス： |
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | いいえ | ネットワークエージェントのインストール後に、デバイスの所有者としてのユーザー登録ユーティリティを実行できるようにします。オフにすると、ユーザーはデバイスの所有者として登録できなくなります。 | 1–デバイスの所有者としてのユーザー登録ユーティリティは、ネットワークエージェントのインストール後に実行されます。<br><br>その他–オフになっています。 |
| PTCH_ALLOW_APPLY_NONAPROVED_PATCHES | いいえ | *未定義*ステータスのネットワークエージェントに対してダウンロードしたアップデートを自動的にインストールするかどうかを定義します。 | true（既定） - アップデートが自動的にインストールされます。<br><br>false - アップデートは自動的にインストールされません。 |

5. ネットワークエージェントをインストールします：

- RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# yum install ./klnagent-<ビルド番号>.i386.rpm`

- RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# yum install ./klnagent64-<ビルド番号>.x86_64.rpm`

- RPM パッケージから ARM アーキテクチャの 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# yum install ./klnagent64-<ビルド番号>.aarch64.rpm`

- DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent_<ビルド番号>_i386.deb`

- DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_amd64.deb`

- ARM アーキテクチャの 64 ビットオペレーティングシステムに DEB パッケージからネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_arm64.deb`

ユーザー環境にネットワークエージェントをインストールするには、コマンドの前に `sudo -E` を追加します。たとえば、RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

`$ sudo -E yum install ./klnagent-<ビルド番号>.i386.rpm`

Linux 用ネットワークエージェントのインストールはサイレントモードで開始されます。ユーザーが、プロセス中に操作を要求されることはありません。

# 対話モードでの Linux 用ネットワークエージェントのインストール

この記事では、インストールパラメータを段階的に指定して、対話モードで Linux デバイスにネットワークエージェントをインストールする方法について説明します。あるいは、アンサーファイル（インストールパラメータのカスタムセットである変数とそれぞれの値を含むテキストファイル）を使用することもできます。この応答ファイルを使用すると、インストールをサイレントモードで、つまりユーザーの参加なしで実行できます。

オペレーティングシステム RED OS 7.3.4 以降または MSVSPHERE 9.2 以降を使用するデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントを正しく機能させるために libxcrypt-compat パッケージをインストールしてください。

*対話モードでネットワークエージェントをインストールするには：*

1. ネットワークエージェントのインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

   - RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     `# yum -i klnagent-<ビルド番号>.i386.rpm`

   - RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     `# yum -i klnagent64-<ビルド番号>.x86_64.rpm`

   - Arm アーキテクチャの 64 ビットオペレーティングシステムに RPM パッケージからネットワークエージェントをインストールするには：

     `# yum -i klnagent64-<ビルド番号>.aarch64.rpm`

   - DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     `# apt install ./klnagent_<ビルド番号>_i386.deb`

   - DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     `# apt install ./klnagent64_<ビルド番号>_amd64.deb`

   - Arm アーキテクチャの 64 ビットオペレーティングシステムに DEB パッケージからネットワークエージェントをインストールするには：

     `# apt install ./klnagent64_<ビルド番号>_arm64.deb`

2. ネットワークエージェントの構成を実行します：

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. 使用許諾契約書（EULA）をお読みください。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。次に、確認が表示されてから次の値を入力します：

   - EULA の内容を確認して同意する場合は「y」を入力します。

   - EULA の内容に同意しない場合は「n」を入力します。ネットワークエージェントを使用するには、EULA の内容に同意する必要があります。

   - EULA を再度表示するには、「r」と入力します。

4. 管理サーバーの DNS 名または IP アドレスを入力します。

5. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。

6. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。

7. ネットワークエージェントと管理サーバー間のトラフィックに SSL 暗号化を使用する場合は、「y」と入力します。それ以外の場合は「n」と入力します。

8. ネットワークエージェントを設定するには、次のオプションのいずれかを選択します：

   - [1] - 接続ゲートウェイを設定しないでください。
     デバイスは接続ゲートウェイとして機能せず、接続ゲートウェイを介して管理サーバーに接続しません。
   - [2] – 接続ゲートウェイを使用しません。
     デバイスは接続ゲートウェイを介して管理サーバーに接続しません。
   - [3] – 接続ゲートウェイを使用してサーバーに接続する
     デバイスは接続ゲートウェイを介して管理サーバーに接続します。
   - [4] – 接続ゲートウェイとして使用します。
     デバイスは接続ゲートウェイとして機能します。

ネットワークエージェントは Linux デバイスにインストールされます。

# ネットワークエージェントをインストールしたデバイスでのファイルシステムロールバックのサポート

Kaspersky Security Center Linux は配信アプリケーションです。ネットワークエージェントがインストールされたデバイスでファイルシステムを以前の状態にロールバックすると、データの非同期を引き起こし、Kaspersky Security Center Linux が正しく機能しなくなります。

ファイルシステム（またはその一部）をロールバックできるのは、次の場合です：

- ハードディスクのイメージをコピーする場合
- 仮想インフラストラクチャを使用して仮想マシンの状態を復元する場合
- バックアップコピーまたは復元ポイントからデータを復元する場合

ネットワークエージェントがインストールされたデバイスのサードパーティ製ソフトウェアが、/var/opt/kaspersky/klnagent ディレクトリに影響を与えるシナリオは、Kaspersky Security Center Linux にとって重要なシナリオのみです。そのため、可能な場合は復元手順からこのフォルダーを常に除外する必要があります。

一部の組織では、職場のルールでデバイスのファイルシステムのロールバックが規定されているため、バージョン 10 Maintenance Release 1 より、Kaspersky Security Center Linux では、ネットワークエージェントがインストールされたデバイスでのファイルシステムのロールバックがサポートされるようになりました（管理サーバーとネットワークエージェントはバージョン 10 Maintenance Release 1 以降でなければなりません）。これらのデバイスは検出されると、完全にデータがクレンジングおよび同期化された管理サーバーに自動的に再接続されます。

Kaspersky Security Center Linux では、既定でファイルシステムのロールバック検出機能が有効になっています。

ネットワークエージェントがインストールされているデバイスでは、/var/opt/kaspersky/klnagent ディレクトリのロールバックはデータの完全な再同期には大量のリソースが必要になるため、できるだけ避けてください。

管理サーバーがインストールされたデバイスでは、システムステータスのロールバックは禁じられています。管理サーバーが使用するデータベースのロールバックも同様に禁じられています。

管理サーバーの状態は、標準の klbackup ユーティリティを使用する場合にのみバックアップコピーから復元できます。

# Windows 用のネットワークエージェントのインストール

また、組織の Windows ベースのデバイスにネットワークエージェントをインストールし、管理サーバーを使用してそれらを管理することもできます。

Microsoft Windows XP では、ネットワークエージェントがカスペルスキーのサーバーから（ディストリビューションポイントとして）アップデートを直接ダウンロードする操作と、（ディストリビューションポイントとして）KSN プロキシサーバーとして機能する操作を正しく実行しない可能性があります。

Windows 管理対象デバイスにネットワークエージェントを最初にインストールするには、次の方法があります：

- Windows ディストリビューションポイントでリモートインストールタスクを実行します。
- ネットワークエージェント用の Windows インストールパッケージ（MSI）とサードパーティツールを使用して、アプリケーションをリモートインストールします。
- 管理対象デバイス上でアプリケーションインストーラーを実行します。
- Kaspersky Security Center Linux が生成したスタンドアロンパッケージに対して、デバイスユーザーリンクを送信します。スタンドアロンパッケージは、選択したアプリケーションの配布パッケージを含む、設定が定義された実行モジュールです。

# Windows 用ネットワークエージェントをインタラクティブモードでインストールする

*ネットワークエージェントをデバイスにローカルインストールするには：*

1. デバイス上で、インターネットからダウンロードした配布パッケージの ksc_<バージョン番号>.<ビルド番号>_full_<ローカライズ言語>.exe ファイルを実行します。

   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。

2. 製品の選択ウィンドウで、［**Kaspersky Security Center ネットワークエージェントのみのインストール**］をクリックしてネットワークエージェントのセットアップウィザードを起動します。ウィザードの指示に従います。

   インストールウィザードの実行中、ネットワークエージェントの詳細設定を行うことができます（下記参照）。

3. デバイスを特定の管理グループの接続ゲートウェイとして使用する場合は、セットアップウィザードの［**接続ゲートウェイ**］ウィンドウで、［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］をオンにします。

4. 仮想マシンへのインストール時にネットワークエージェントを設定するには：

   a. 仮想マシンのイメージから動的仮想マシンを作成する場合は、ネットワークエージェントの仮想デスクトップインフラストラクチャ（VDI）向け動的モードを有効にします。これを行うには、セットアップウィザードの［**詳細設定**］ウィンドウで［**VDI 向け動的モードを有効にする**］をオンにします。

      仮想マシンのイメージから動的仮想マシンを作成する計画がない場合、この手順は省略します。

   b. ネットワークエージェントの動作を VDI 向けに最適化します。これを行うには、セットアップウィザードの［**詳細設定**］ウィンドウで［**VM 向けに設定を最適化する**］をオンにします。

      デバイス起動時の実行ファイルの脆弱性スキャンが実行されなくなります。また、次のオブジェクトの情報が管理サーバーに送信されなくなります：

      - ハードウェアレジストリ
      - デバイスにインストールされているアプリケーション
      - ローカルクライアントデバイスにインストールする必要がある Microsoft Windows の更新プログラム
      - ローカルクライアントデバイスで検知されたソフトウェアの脆弱性

      これらの情報の送信は、ネットワークエージェントのプロパティまたはネットワークエージェントポリシーの設定で有効にできます。

セットアップウィザードが終了すると、ネットワークエージェントがデバイスにインストールされます。

これでネットワークエージェントサービスのプロパティを表示したり、Microsoft Windows の標準ツール（コンピューターの管理 / サービス）でネットワークエージェントのアクティビティの開始、終了、監視をしたりすることができるようになります。

# Windows 用ネットワークエージェントをサイレントモードでインストールする

ネットワークエージェントは、サイレントモードでインストールできます。インストール中にパラメータを対話形式で入力する必要はありません。サイレントインストールでは、ネットワークエージェント用の Windows インストーラーパッケージ（MSI）が使用されます。MSI ファイルは、Kaspersky Security Center Linux 配布パッケージのフォルダー Packages\NetAgent\exec にあります。

MSI パッケージからのネットワークエージェントのインストールはサイレントモードでのみ可能であり、MSI パッケージからの対話型インストールはサポートされていません。

*ネットワークエージェントをサイレントモードでローカルデバイスにインストールするには：*

1. 使用許諾契約書をお読みください。以下のコマンドは、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

2. 次のコマンドを実行します：

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <セットアップパラメータ>
   ```

   ここで、**<セットアップパラメータ>**には、パラメータと対応する値のペアをスペースで区切って並べます（例：`PROP1=PROP1VAL PROP2=PROP2VAL`）。

   パラメータ部分には、「`EULA=1`」というパラメータを含める必要があります。そうしない場合、ネットワークエージェントがインストールされません。

Kaspersky Security Center の標準接続設定、およびリモートデバイスのネットワークエージェントを使用している場合は、コマンドを実行します：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` はログ記録のためのキーです。ログはネットワークエージェントのインストール中に作成され、C:\windows\temp\nag_inst.log に保存されます。

nag_inst.log に加えて、アプリケーションはインストールログを含む $klssinstlib.log ファイルを作成します。このファイルは、%windir%\ temp フォルダーまたは %temp% フォルダーに保存されます。トラブルシューティングの目的で、お客様またはカスペルスキーテクニカルサポートのスペシャリストが、nag_inst.log と $klssinstlib.log の両方のログファイルを必要とする場合があります。

管理サーバーに接続するポートを追加で指定する必要がある場合、次のコマンドを実行します：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

パラメータ `SERVERPORT` は管理サーバーに接続するためのポート番号に対応しています。

ネットワークエージェントをサイレントモードでインストールする時に使用可能なパラメータの名前と値を［ネットワークエージェントのインストールパラメータ］セクションに示します。

Windows インストーラーを使用してネットワークエージェントをアップグレードする場合は、次のコマンドを実行します：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

# デバイスのイメージの取得とコピーを使用した導入

オペレーティングシステムとその他のソフトウェアもインストール（または再インストール）する必要があるデバイスにネットワークエージェントをインストールする必要がある場合は、そのデバイスのイメージをキャプチャしてコピーするメカニズムを使用できます。

*ハードディスクイメージの取得とコピーによる導入を実行するには：*

1. オペレーティングシステムと関連するソフトウェア（ネットワークエージェントとセキュリティ製品を含む）がインストールされた基準デバイスを作成します。
2. デバイスの基準イメージを取得し、Kaspersky Security Center Linux の専用タスクを使用して、そのイメージを新しいデバイスに配信します。

   ディスクイメージをキャプチャしてインストールするには、組織で使用可能なサードパーティ製ツールを使用します。

## サードパーティ製のツールを使用したディスクイメージのコピー

ネットワークエージェントがインストールされたデバイスのイメージの取得にサードパーティ製のツールを適用する際には、次のいずれかの方法を使用します：

- 基準デバイスでネットワークエージェントサービスを停止し、-dupfix キーにより klmover ユーティリティを実行します。klmover ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。イメージ取得の操作が完了するまで、ネットワークエージェントサービスを引き続き実行しないでください。
- イメージの導入後にオペレーティングシステムを初めて起動する際には、対象デバイスでネットワークエージェントサービスを最初に実行する前（必須要件）に、-dupfix キーにより klmover が実行されていることを確認してください。klmover ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。
- ネットワークエージェントのディスククローンモードを使用します。

ハードディスクイメージが正しくコピーされていない場合は、この問題を解決できます。

ネットワークエージェントがインストールされていないデバイスのイメージをキャプチャすることもできます。これを行うには、対象デバイスでイメージの導入を実行してから、ネットワークエージェントを導入します。この方法を使用する場合は、デバイスからスタンドアロンイントールパッケージを含むネットワークフォルダーへのアクセスを提供します。

# ネットワークエージェントのディスククローンモード

新しいデバイスにソフトウェアをインストールする際、基準となるデバイスのハードディスクを複製する方法が一般的です。基準となるデバイスのハードディスク上でネットワークエージェントが標準モードで動作していると、次の問題が発生します：

新しいデバイス上に、ネットワークエージェントを含む基準ディスクイメージが導入されると、Kaspersky Security Center Web コンソール上ではそれらのデバイスが1つのデバイスとして表示されます。この問題は、管理サーバーが Kaspersky Security Center Web コンソール上でデバイスと記録を関連付けるために使用する内部データが、複製の結果として新しいデバイスで同一になるために発生します。

*ネットワークエージェントのディスククローンモード*を使用すると、複製後、Kaspersky Security Center Web コンソール上での新しいデバイスの表示の問題を回避できます。新しいデバイスに、ディスクを複製してネットワークエージェントとソフトウェアを導入する場合はこのモードを使用します。

ディスククローンモードでは、ネットワークエージェントは動作を継続しますが、管理サーバーには接続しません。ネットワークエージェントは、クローンモードを終了する時に、Kaspersky Security Center Web コンソール上で管理サーバーが複数のデバイスを単一の記録に関連付ける原因となる内部データを削除します。基準デバイスのイメージの複製が完了すると、新しいデバイスが Kaspersky Security Center Web コンソール上で正しく（個別の記録で）表示されます。

## ネットワークエージェントのディスククローンモードの使用シナリオ

1. 基準となるデバイスにネットワークエージェントをインストールします。
2. ネットワークエージェントの管理サーバーへの接続を klnagchk ユーティリティを使用して確認します。
3. ネットワークエージェントのディスククローンモードを有効にします。
4. ソフトウェアとパッチをデバイスにインストールし、必要な回数再起動します。
5. 基準デバイスのハードディスクを必要な数のデバイス上に複製します。
6. 複製されたコピーは次の条件を満たす必要があります：
   a. デバイス名を変更する必要があります。
   b. デバイスを再起動する必要があります。
   c. ディスククローンモードを無効にする必要があります。

## Klmover ユーティリティを使用したディスククローンモードの有効化および無効化

*ネットワークエージェントのディスククローンモードを有効または無効にするには：*

1. ネットワークエージェントがインストールされた複製元デバイス上で klmover ユーティリティを実行します。

   Klmover ユーティリティはネットワークエージェントのインストールフォルダーにあります。

2. ディスククローンモードを有効にするには、Linux コマンドシェルで次のコマンドを入力します：

   ```
   ./klmover -cloningmode 1
   ```

   ネットワークエージェントがディスククローンモードに切り替わります。

3. ディスククローンモードの現在のステータスを要求するには、コマンドプロンプトで次のコマンドを入力します：

   ```
   ./klmover -cloningmode
   ```

   ユーティリティウィンドウに、ディスククローンモードが有効か無効かが表示されます。

4. ディスククローンモードを無効にするには、ユーティリティのコマンドラインで次のコマンドを入力します：

   ```
   ./klmover -cloningmode 0
   ```

# ネットワークエージェントのインストールパラメータ

以下の表では、ネットワークエージェントをインストールする際に設定できる MSI プロパティについて説明しています。EULA と SERVERADDRESS を除き、すべてのパラメータの指定は省略可能です。

サイレントモードでのネットワークエージェントのインストールのパラメータ

| MSI プロパティ | 説明 | 設定可能な値 |
|---|---|---|
| EULA | 使用許諾契約書の条項の同意 | • 1- この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する。<br>• 0 – 使用許諾契約書の条件に同意しません（インストールは実行されません）。<br>• 値なし – 使用許諾契約書の条件に同意しません（インストールは実行されません）。 |
| DONT_USE_ANSWER_FILE | 応答ファイルからインストールの設定を読み込む | • 1 – 使用しない。<br>• その他の値または値なし – 読み取り。 |
| INSTALLDIR | ネットワークエージェントのインストールフォルダーへのパス | 文字列値 |
| SERVERADDRESS | 管理サーバーのアドレス（必須） | 文字列値 |
| SERVERPORT | 管理サーバーに接続するためのポートの番号 | 数値 |
| SERVERSSLPORT | SSL プロトコルを使用した管理サーバーへの暗号化接続用ポートの番号 | 数値 |
| USESSL | SSL 接続を使用するかどうか | • 1 – 使用する<br>• その他の値または値なし – 使用しない |
| OPENUDPPORT | UDP ポートを開くかどうか | • 1 – 開く<br>• その他の値または値なし – 開かない |
| UDPPORT | UDP ポート番号 | 数値 |
| USEPROXY | プロキシサーバーを使用するかどうか。<br>互換性のため、ネットワークエージェントのインストールパッケージ設定でプロキシ接続設定を指定することは推奨されません。 | • 1 – 使用する<br>• その他の値または値なし – 使用しない |
| PROXYLOCATION (PROXYADDRESS:PROXYPORT) | プロキシサーバーに接続するためのプロキシアドレスとポートの番号 | 文字列値 |
| PROXYLOGIN | プロキシサーバーに接続するためのアカウント | 文字列値 |
| PROXYPASSWORD | プロキシサーバーに接続するためのアカウントのパスワード（インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。） | 文字列値 |

| MSI プロパティ | 説明 | 設定可能な値 |
| --- | --- | --- |
| GATEWAYMODE | 接続ゲートウェイの使用モード | • 0 – 接続ゲートウェイを使用しない<br>• 1– このネットワークエージェントを接続ゲートウェイとして使用する<br>• 2 – 接続ゲートウェイを使用して管理サーバーに接続する |
| GATEWAYADDRESS | 接続ゲートウェイアドレス | 文字列値 |
| CERTSELECTION | 証明書を取得する方法 | • GetOnFirstConnection – 管理サーバーから証明書を取得する<br>• GetExistent – 既存の証明書を選択する。このオプションを選択する場合、CERTFILE プロパティを指定する必要があります |
| CERTFILE | 証明書ファイルのパス | 文字列値 |
| VMVDI | 仮想デスクトップインフラストラクチャ（VDI）向け動的モードを有効にする | • 1 – 有効にする<br>• 0 – 有効にしない<br>• 値なし – 有効にしない |
| LAUNCHPROGRAM | インストール後にネットワークエージェントサービスを開始するかどうか。VMVDI=1 の場合、パラメータは無視されます。 | • 1 – 開始する<br>• その他の値または値なし – 開始しない |
| NAGENTTAGS | ネットワークエージェントのタグ（応答ファイルで付与されているタグよりも優先されます） | 文字列値 |

# リモートインストールタスクを使用したアプリケーションのインストール

Kaspersky Security Center Linux では、リモートインストールタスクを使用してデバイスにアプリケーションをリモートインストールできます。このタスクは、専用のウィザードを使用して作成しデバイスに割り当てます。タスクを簡単にデバイスに割り当てるには、次のいずれかの方法を使用し、ウィザードウィンドウでデバイス（最大 1000 台）を指定できます：

- **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。
- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**：タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。
- **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。既定の抽出または作成済みのカスタム抽出を指定できます。選択できるデバイスは最大 1000 台までです。

ネットワークエージェントがインストールされていないクライアントデバイスにアプリケーションをインストールする際に発生する可能性のある問題を回避するには、Kaspersky Security Center Linux のリモートインストールタスクによる強制導入の説明通りに実行する必要があります。

# Kaspersky Security Center Linux でのリモートインストールタスクの概要

Kaspersky Security Center Linux には、アプリケーションをリモートインストールするための様々なメカニズムが用意されており、リモートインストールタスクとして実装されています（強制インストール、ハードドライブイメージのコピーによるインストール）。リモートインストールタスクは、特定のデバイスまたは選択したデバイスと指定した管理グループの両方に対して作成できます（このタスクは Kaspersky Security Center Web コンソールの［**タスク**］フォルダーに表示されます）。タスクを作成する際には、このタスク内にインストールする（ネットワークエージェントや別のアプリケーン用の）インストールパッケージを選択し、リモートインストール方法を定義するための特定の設定を指定することができます。さらに、リモートインストールタスクの作成と結果の監視に基づいた、リモートインストールウィザードも使用できます。

管理グループのタスクは、指定したグループに含まれるデバイスと、その管理グループ内のすべてのサブグループにあるすべてのデバイスの両方に影響を与えます。タスクは、対応する設定がそのタスク内で有効な場合、1つのグループまたはそのサブグループのいずれかに含まれるセカンダリ管理サーバーのデバイスに対応しています。

特定のデバイスに対するタスクでは、タスクが開始された時点での選択内容に従って、実行ごとにクライアントデバイスのリストが更新されます。選択内容に、セカンダリ管理サーバーに接続されているデバイスが含まれている場合は、そのデバイスでもタスクが実行されます。これらの設定とインストール方法の詳細については、このセクションの後半を参照してください。

セカンダリ管理サーバーに接続されているデバイスでリモートインストールタスクの操作を正常に実行するには、対応するセカンダリ管理サーバーに対して前もって、タスクで使用するインストールパッケージをリレーしておく必要があります。

# アプリケーションのリモートインストール

このセクションでは、管理グループ内のデバイス、特定のアドレスを持つデバイス、または選択したデバイスにアプリケーションをリモートインストールする方法について説明します。

*アプリケーションを特定のデバイスにインストールするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。
3. ［**タスク種別**］で、［**アプリケーションのリモートインストール**］を選択します。

4. 次のいずれかのオプションをオンにします：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

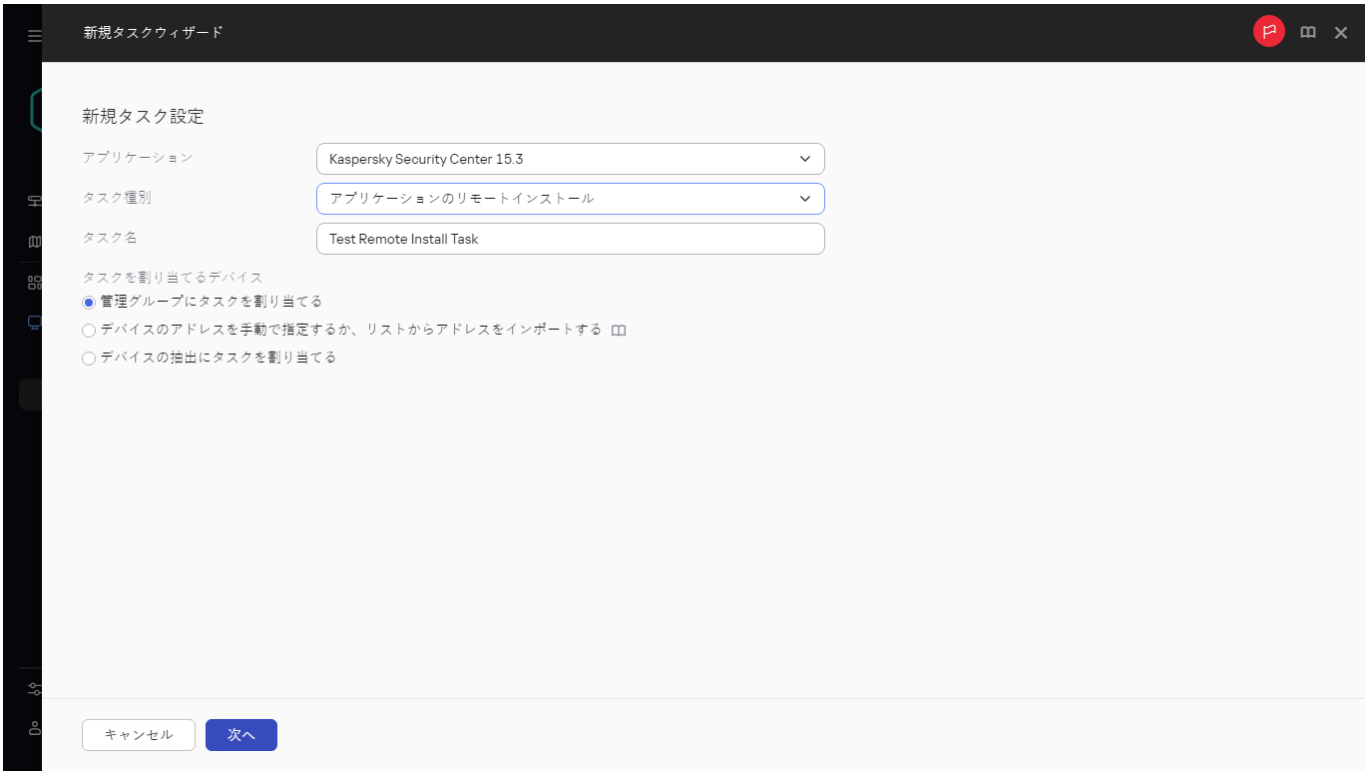
  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

指定したデバイスに対して、アプリケーションのリモートインストールタスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ1になります。




アプリケーションのリモートインストールタスクの作成

5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

   使用可能な設定は、前のステップでオンにしたオプションによって異なります。

6. ［**インストールパッケージ**］ステップで、次の設定を指定します：

- ［**インストールパッケージの選択**］で、インストールするアプリケーションのインストールパッケージを選択します。
- ［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。
  - **ネットワークエージェントを使用する**

    このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

    このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

    ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

    既定では、このオプションはオンです。

  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

    このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

    ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

    既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

    Network Agent がインストールされていないデバイスに Windows 用のアプリケーション（Windows 用ネットワークエージェントを含む）をインストールするには、Windows ベースのディストリビューションポイントを使用するのが唯一の方法です。したがって、Windows アプリケーションをインストールする場合：

    - このオプションをオンにします。
    - ターゲットのクライアントデバイスにディストリビューションポイントが割り当てられていることを確認します。
    - ディストリビューションポイントが Windows ベースであることを確認します。

  - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

    このオプションをオンにすると、管理サーバーを通じてクライアントデバイスのオペレーティングシステムツールを使用してクライアントデバイスにファイルが送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

    既定では、このオプションはオンです。

- ［**同時ダウンロード数の上限**］で、管理サーバーが同時にファイルを送信できるクライアントデバイスの最大許容数を指定します。
- ［**インストール試行回数の上限**］で、インストーラーの最大許容実行回数を指定します。

試行回数がこのパラメータで指定された回数を超えると、Kaspersky Security Center Linux はこのデバイスでインストーラーを起動しなくなります。*アプリケーションのリモートインストールタスク*を再開するには、［**インストール試行回数の上限**］パラメータの値を増やしてタスクを開始します。または、*アプリケーションのリモートインストールタスク*を新規作成することもできます。

- あるカスペルスキー製品から別のアプリケーションに移行する場合、現在のアプリケーションがパスワードで保護されているときは、［**現在のカスペルスキー製品をアンインストールするためのパスワード**］フィールドにパスワードを入力します。移行中は、現在の Kaspersky アプリケーションがアンインストールされることに注意してください。

  ［**現在のカスペルスキー製品をアンインストールするためのパスワード**］フィールドは、［**インストールパッケージの強制ダウンロード**］設定グループで［**ネットワークエージェントを使用する**］をオンにした場合にのみ使用できます。

  アンインストールパスワードは、*アプリケーションをリモートでインストールするタスク*を使用して Kaspersky Endpoint Security for Windows をインストールする場合、Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows への移行シナリオでのみ使用できます。他のコンポーネントをインストールする時にアンインストールパスワードを使用すると、インストールエラーが発生する可能性があります。

  移行シナリオを正常に完了するには、次の前提条件が満たされていることを確認してください：

  - Kaspersky Security Center ネットワークエージェント 14.2 for Windows 以降を使用しています。
  - Windows を実行しているデバイスにアプリケーションをインストールしています。

- 詳細設定を行います：

  - **アプリケーションが既にインストールされている場合は再インストールしない**

    このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

    このオプションをオフにすると、アプリケーションは常にインストールされます。

    既定では、このオプションはオンです。

  - **ダウンロード前に OS の種別を確認する**

    ファイルをクライアントデバイスに送信する前に、Kaspersky Security Center Linux はインストールユーティリティの設定がクライアントデバイスのオペレーティングシステムに適用可能であるかどうかを確認します。設定を適用できない場合、ファイルを送信せず、アプリケーションのインストールを試行しません。たとえば、様々なオペレーティングシステムを実行しているデバイスが存在する管理グループのデバイスにアプリケーションをインストールするには、インストールタスクを管理グループに割り当ててから、このオプションをオンにして、必要なオペレーティングシステム以外を実行しているデバイスをスキップできます。

  - **Active Directory のグループポリシーにパッケージのインストールを割り当てる**

このオプションをオンにすると、Active Directory のグループポリシーを使用してインストールパッケージがインストールされます。

このオプションは、ネットワークエージェントのインストールパッケージが選択されている場合に使用可能になります。

既定では、このオプションはオフです。

- **実行中のアプリケーションを終了するよう告知する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

- 本製品をインストールするデバイスを選択します：

  - **全デバイスにインストール**

    他の管理サーバーで管理されているクライアントデバイスにもアプリケーションがインストールされます。

    既定ではこのオプションが選択されます。ネットワーク内に管理サーバーが1台しかない場合は、この設定を変更する必要はありません。

  - **この管理サーバーで管理されているデバイスにのみインストール**

    アプリケーションはこの管理サーバーによって管理されているデバイスにのみインストールされます。ネットワーク内に複数の管理サーバーがあり、管理サーバー間での競合を回避したい場合は、このオプションを選択してください。

- インストール後に、デバイスを管理グループに移動するかどうかを指定します：

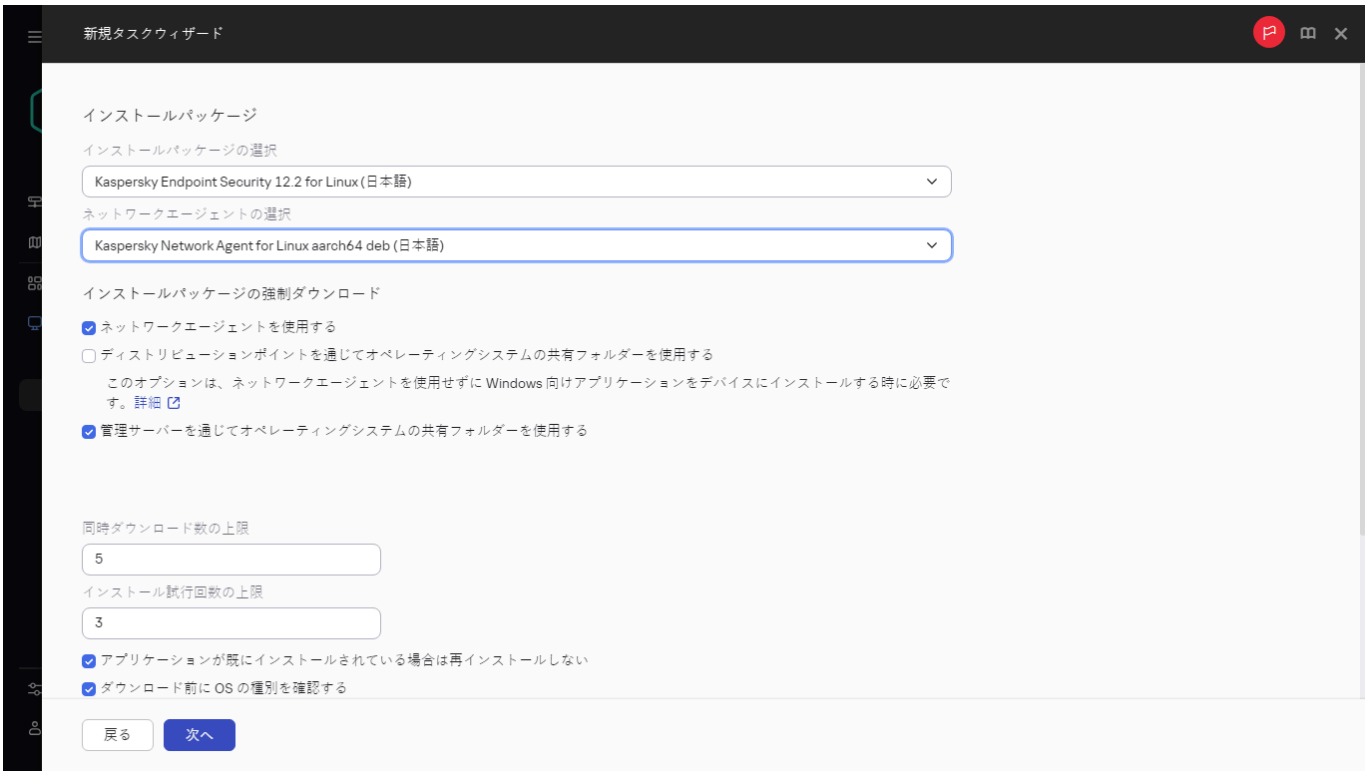
  - **デバイスを移動しない**

    デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

  - **未割り当てデバイスを選択したグループへ移動する（選択できるグループは1つのみ）**

    指定した管理グループにデバイスが移動されます。

  既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。




タスク設定の指定

7. ウィザードのこのステップでは、アプリケーションのインストール中にデバイスを再起動する必要があるかどうかを指定します。

- **デバイスを再起動しない**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されません。

- **デバイスを再起動する**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されます。

8. 必要に応じて、［**デバイスにアクセスするアカウントの選択**］ステップで、*アプリケーションのリモートインストールタスク*を開始するために使用されるアカウントを追加します。

   - **アカウントが不要（ネットワークエージェントインストール済み）**

     このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

     クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

   - **アカウントが必要（ネットワークエージェントの使用なし）**

     リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントまたは SSH 証明書を指定して、アプリケーションをインストールできます。

     - **ローカルアカウント**。このオプションをオンにする場合、アプリケーションのインストーラーを実行するユーザーアカウントを指定します。［**追加**］をクリックし、［**ローカルアカウント**］を選択してから、ユーザーアカウントの資格情報を指定します。

       タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

     - **SSH 証明書**。Linux ベースのクライアントデバイスにアプリケーションをインストールする場合、ユーザーアカウントの代わりに SSH 証明書を指定できます。［**追加**］をクリックし、［**SSH 証明書**］を選択してから、証明書の秘密鍵と公開鍵を指定します。

       秘密鍵を生成するには、ssh-keygen ユーティリティを使用できます。Kaspersky Security Center Linux は PEM 形式の秘密鍵をサポートしますが、ssh-keygen ユーティリティは既定で SSH 鍵を OPENSSH 形式で生成します。OPENSSH 形式は Kaspersky Security Center Linux ではサポートされていません。サポートされる PEM 形式で秘密鍵を作成するには、ssh-keygen コマンドに -m PEM オプションを追加します。例：

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<ユーザーのメールアドレス>"
       ```

9. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

10. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

    または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

リモートインストールタスクが完了すると、指定したデバイスに選択したアプリケーションがインストールされます。

# セカンダリ管理サーバーへのアプリケーションのインストール

*セカンダリ管理サーバーにアプリケーションをインストールするには：*

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。

2. インストールするアプリケーションに対応するインストールパッケージが、選択したそれぞれのセカンダリ管理サーバー上で使用可能であるか確認してください。セカンダリサーバーのいずれにもインストールパッケージが見つからない場合は、配布します。この目的のために、タスク種別［**インストールパッケージの配布**］でタスクを作成します。

3. セカンダリ管理サーバーでリモートアプリケーションのインストール用のタスクを作成します。タスク種別として［**セカンダリ管理サーバーへのアプリケーションのリモートインストール**］を選択します。

   新規タスクウィザードは、ウィザードで選択したアプリケーションを特定のセカンダリ管理サーバーにリモートインストールするタスクを作成します。

4. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションがセカンダリ管理サーバーにインストールされます。

# ネットワークエージェントがインストールされたデバイスへのアプリケーションのリモートインストール

プライマリ管理サーバー（またはそのセカンダリ管理サーバーのいずれか）に接続された操作可能なネットワークエージェントがデバイスにインストールされた場合、このデバイスのネットワークエージェントのアップグレードや、ネットワークエージェント経由でサポートされる任意のアプリケーションのインストール、アップグレード、削除が可能です。

このオプションは、リモートインストールタスクのプロパティで［**ネットワークエージェントを使用する**］をオンにすることができます。

このオプションをオンにすると、管理者によってインストール設定が定義されたインストールパッケージは、ネットワークエージェントと管理サーバー間の通信チャネルを経由して対象デバイスに送信されます。

管理サーバーの負荷を最適化し、管理サーバーとデバイス間のトラフィックを最小化するには、すべてのリモートネットワークまたはすべてのブロードキャストドメインでディストリビューションポイントを割り当てるのが適切な方法です（「ディストリビューションポイントについて」および「管理グループの構造の構築とディストリビューションポイントの割り当て」を参照）。この場合、インストールパッケージとインストーラーの設定は、ディストリビューションポイント経由で管理サーバーから対象デバイスに配布されます。

さらに、ディストリビューションポイントをインストールパッケージのブロードキャスト（マルチキャスト）配信に使用できるため、アプリケーション導入時のネットワークトラフィックを大幅に削減できます。

ネットワークエージェントと管理サーバー間の通信チャネルを経由してインストールパッケージを対象デバイスに送信する場合、送信の準備が整っているすべてのインストールパッケージは、/var/opt/kaspersky/klnagent_srv/1093/.working/ フォルダーにもキャッシュされます。複数の様々な種別の大規模インストールパッケージと、多数のディストリビューションポイントを使用する場合、このフォルダーのサイズは急増する可能性があります。

FTServer フォルダーからファイルを手動で削除することはできません。元のインストールパッケージが削除された場合、FTServer フォルダーから関連データが自動的に削除されます。

ディストリビューションポイントによって受信されたデータは、/var/opt/kaspersky/klnagent_srv/1103/ フォルダーに保存されます。

$FTCITmp フォルダーからファイルを手動で削除することはできません。このフォルダーのデータを使用するタスクが完了すると、このフォルダーの中身は自動的に削除されます。

インストールパッケージは、管理サーバーとネットワークエージェント間の通信チャネルを経由して、ネットワーク送信用に最適化されたフォーマットで中間リポジトリから配布されるため、各インストールパッケージの元のフォルダーに保存されたインストールパッケージへの変更は許可されていません。そのような変更は、管理サーバーによって自動的に登録されません。インストールパッケージのファイルを手動で変更する必要がある場合は、Kaspersky Security Center Web コンソールでインストールパッケージの設定を編集しなければなりません（ただし、このようなシナリオは回避することが推奨されます）。Kaspersky Security Center Web コンソールでインストールパッケージの設定を編集すると、対象デバイスへの送信準備が整っているキャッシュ内のパッケージイメージが、管理サーバーによってアップグレードされてしまいます。

サーバーは、リモートインストール中に ICMP エコー要求（ping コマンドと同じ）を対象デバイスに送信します。

# macOS デバイスへのアプリケーションのリモートインストール

*リモートインストールタスクを使用して、macOS を実行しているデバイスにアプリケーションをインストールするには：*

1. インストールパッケージと .sh インストールスクリプトで構成されるアーカイブを作成します。
2. 新規タスクウィザードの［**ダウンロード前に OS の種別を確認する**］オプションを無効にしてください。

あるいは、［**スクリプトをリモートで実行**］タスクを使用することもできます。次の記事では、このタスクのファイルを構成する方法について説明します：［スクリプトをリモートで実行］タスクを使用してデバイスにアプリケーションをリモートでインストールします。

# リモートインストールタスクに含まれるデバイス再起動を管理する

アプリケーションのリモートインストールを完了するには（特に Windows では）、通常はデバイスの再起動が必要です。

Kaspersky Security Center Linux のリモートインストールタスクを使用する場合、新規タスクウィザード、または作成したタスクのプロパティウィンドウ（[**OS の再起動**] セクション）で、Windows デバイスに再起動が必要な際に実行する以下の操作を選択できます：

- **デバイスを再起動しない**：自動再起動は実行されません。インストールを完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、サーバーや、継続的な操作が不可欠なその他のデバイスのインストールタスクに適切です。

- **デバイスを再起動する**：インストールの完了に再起動が必要な場合は常に、デバイスは自動的に再起動されます。このオプションは、定期的に操作が一時停止（シャットダウンまたは再起動）されるデバイスのインストールタスクに有用です。

- **ユーザーに処理を確認する**：手動での再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。[**ユーザーに処理を確認する**] は、ユーザーにとって最も好都合な時間に再起動できることが要求されるワークステーションに最適です。

# Kaspersky Security Center Linux のリモートインストールタスクを使用した強制的な導入

ネットワークエージェントやその他のアプリケーションの初期導入を実行するには、各デバイスにローカル管理者権限を持つユーザーアカウントがあることを前提として、Kaspersky Security Center Linux のリモートインストールタスクを使用して、選択したインストールパッケージを強制的にインストールできます。

管理サーバーがデバイスに直接アクセスできない場合は、強制インストールを適用することもできます。たとえば、デバイスが分離されたネットワーク上に配置されている場合や、管理サーバーが DMZ にあり、デバイスがローカルネットワーク上に配置されている場合が考えられます。

初期導入の場合、ネットワークエージェントはインストールされません。そのため、リモートインストールタスクの設定では、ネットワークエージェントを使用してアプリケーションのインストールに必要なファイルの配布を選択することはできません。管理サーバーまたはディストリビューションポイントを介してオペレーティングシステムリソースを使用してファイルを配布することのみを選択できます。

管理サーバーサービスは、ターゲットデバイスに対する管理者権限を持つアカウントで実行する必要があります。または、リモートインストールタスクの設定で、admin$ 共有にアクセスできるアカウントを指定することもできます。

既定では、リモートインストールタスクは、管理サーバーが実行されているアカウントの資格情報を使用してデバイスに接続します。これは、リモートインストールタスクが実行されるアカウントではなく、admin$ 共有にアクセスするために使用されるアカウントであることを明確にすることが重要です。インストールは LocalSystem アカウントで実行されます。

対象デバイスを指定する方法として、明示的に指定する（リストを使用）、対象デバイスが属する Kaspersky Security Center Linux の管理グループを選択する、または特定の基準に基づいてデバイスの抽出内容を作成するのいずれかを使用できます。インストールの開始時刻は、タスクのスケジュールによって定義されます。タスクのプロパティで [**未実行のタスクを実行する**] 設定をオンにすると、対象デバイスの電源をオンにした直後または対象デバイスを対象管理グループに移動した際に、タスクを実行できます。

強制インストールは、インストールパッケージの対象デバイスへの送信、その後の各対象デバイスの admin$ リソースへのファイルコピー、これらのデバイス上でのサポートデバイスのリモート登録で構成されます。インストールパッケージの対象デバイスへの送信は、ネットワーク対話を保証する Kaspersky Security Center Linux 機能を介して実施されます。この場合、次の条件を満たしている必要があります：

- 対象デバイスには、管理サーバー側またはディストリビューションポイント側からアクセスできます。
- ネットワーク上で、対象デバイスの名前解決が正常に機能しています。
- 対象デバイスで、管理共有（admin$）が有効のままである。
- 対象デバイスでは次のシステムサービスが実行されています：
  - サーバー（LanmanServer）
    既定では、このサービスは実行されています。
  - DCOM サーバープロセスランチャー（DcomLaunch）
  - RPC エンドポイントマッパー（RpcEptMapper）
  - リモートプロシージャコール（RpcSs）
- Windows 管理インストルメンテーションを介したリモートアクセスを可能にするために、対象デバイスでポート TCP 445 が開かれます。

  > TCP 139、UDP 137、および UDP 138 は古いプロトコルで使用されており、現在のアプリケーションには必要ありません。

  管理サーバーおよびディストリビューションポイントから対象デバイスへの接続には、ファイアウォールで動的な送信アクセスポートを許可する必要があります。
- ネットワークエージェントを導入する時、Active Directory ドメインポリシーのセキュリティ設定により、NTLM プロトコルの動作が可能になります。
- Microsoft Windows XP を実行している対象デバイスで、シンプルファイル共有モードが無効になっている。
- 対象デバイスでは、アクセス共有とセキュリティモデルは「*クラシック – ローカルユーザーはローカルユーザー自身として認証*」に設定されます。決して「*ゲストのみ – ローカルユーザーはゲストとして認証*」に設定できません。
- 対象デバイスをドメインに属させるか、または管理者権限を付与された統一アカウントを対象デバイスで前もって作成する。

Windows Server 2003 以降の Active Directory ドメインに参加していないデバイスにネットワークエージェントまたはその他のアプリケーションを正常に展開するには、そのデバイスでリモート UAC を無効にする必要があります。リモート UAC は、ネットワークエージェントやその他のアプリケーションの強制導入に必要な admin$ にローカル管理アカウントがアクセスできない原因の 1 つです。リモート UAC を無効にしても、ローカル UAC には影響しません。

まだいずれの Kaspersky Security Center Linux の管理グループにも割り当てられていない新しいデバイスへのインストール時には、リモートインストールタスクのプロパティを開き、ネットワークエージェントのインストール後にデバイスの移動先の管理グループを指定できます。

グループタスクの作成時には、選択したグループ内のネストされたすべてのグループにあるすべてのデバイスに対して、各グループタスクが影響を与えることに注意してください。このため、サブグループ内でインストールタスクが重複しないようにする必要があります。

アプリケーションを強制インストールするためのタスクを作成する簡単な方法は、自動インストールです。この処理を実行するには、管理グループのプロパティを開いてから、インストールパッケージのリストを開き、このグループのデバイスにインストールする必要があるパッケージを選択しなければなりません。そうすると、このグループとそのすべてのサブグループ内にあるすべてのデバイスに、選択したインストールパッケージが自動的にインストールされます。パッケージのインストールに要する時間は、ネットワークのスループットとネットワーク接続されているデバイスの合計数に応じて異なります。

インストールパッケージを対象デバイスに配信する際に管理サーバーの負荷を軽減するには、インストールタスクでディストリビューションポイント経由のインストールを選択できます。ただし、このインストール方法では、ディストリビューションポイントとして動作しているデバイスの負荷が大幅に増大するのでご注意ください。したがって、ディストリビューションポイントの要件を満たすデバイスを選択することを推奨します。ディストリビューションポイントを使用する場合は、対象デバイスをホストする分離された各サブネットにディストリビューションポイントが存在することを確認する必要があります。

小容量チャネルを介して管理サーバーと通信するサブネット内のデバイスへのインストールを実行する際に、同じサブネット内のデバイス間で大容量チャネルが使用できる場合は、ディストリビューションポイントをローカルインストールのセンターとして使用することも役に立ちます。

さらに、［/var/opt/kaspersky/klnagent_srv/］フォルダーのパーティションの空きディスク容量は、インストールされたアプリケーションの配布パッケージの合計サイズより何倍も大きな容量にする必要があります。

# サイレントモードでアプリケーションをインストールする

*アプリケーションをサイレントモードでインストールするには：*

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. 必要なアプリケーションのインストールパッケージの横にあるチェックボックスをオンにするか、そのアプリケーション用に新しいパッケージを作成します。

インストールパッケージは、管理サーバーで指定された共有フォルダー内のサブフォルダー Packages 内にあります。各インストールパッケージは、個別のサブフォルダー内に格納されています。

3. 次のいずれかの方法で、必要なインストールパッケージを格納するためのフォルダーを開きます：

   - 管理サーバーからクライアントデバイスに関連するインストールパッケージに対応するフォルダーをコピーします。コピーしたフォルダーをクライアントデバイスで開きます。
   - クライアントデバイスから、管理サーバーの必須インストールパッケージに対応する共有フォルダーを開きます。

   Microsoft Windows Vista がインストールされたデバイスに共有フォルダーがある場合は、［**ユーザーアカウント制御：管理者承認モードですべての管理者を実行する**］の値を「**無効**」にする必要があります（［**スタート**］→［**コントロールパネル**］→［**管理ツール**］→［**ローカルセキュリティポリシー**］→［**セキュリティオプション**］）。

4. 選択したアプリケーションに応じて次の手順を実行します：

   - Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers、Kaspersky Security Center の場合、サブフォルダー exec に移動し、/s キーを指定して実行ファイル（exe 拡張子のファイル）を実行します。
   - その他のカスペルスキー製品の場合は、開かれたフォルダーから /s キーを指定して実行ファイル（exe 拡張子のファイル）を実行します。

   `EULA=1` および `PRIVACYPOLICY=1` キーを指定して実行ファイルを実行すると、使用許諾契約書とプライバシーポリシーそれぞれの内容をすべて確認し、理解した上で条項に同意したことになります。また、プライバシーポリシーに記載されているように、データが処理されて送信されること（第三国への送信を含む）も理解したことになります。使用許諾契約書とプライバシーポリシーの本文は、Kaspersky Security Center Linux の配布キットに含まれています。アプリケーションのインストールまたは以前のバージョンのアプリケーションをアップグレードするには、使用許諾契約書とプライバシーポリシーに同意する必要があります。

# ネットワークエージェントのリモートインストール用の macOS デバイスの準備

macOS 管理対象デバイスにネットワークエージェントを最初にインストールするには、次の方法があります：

- macOS ディストリビューションポイントでリモートインストールタスクを実行します。
- Kaspersky Security Center Linux が生成したスタンドアロンパッケージに対して、デバイスユーザーリンクを送信します。スタンドアロンパッケージは、選択したアプリケーションの配布パッケージを含む、設定が定義された実行モジュールです。

*ネットワークエージェントをリモートでインストールする macOS 搭載デバイスを準備するには：*

1. 対象となる macOS デバイスに、sudo がインストールされていることを確認します。
2. デバイスの構成をテストします：
   a. クライアントデバイスでポート 22 が開いていることを確認します。これを行うには、［**システム環境設定**］で［**共有**］ペインを開き、［**リモートログイン**］がオンになっていることを確認します。

      SSH 経由でクライアントデバイスに接続できるのはポート 22 を介した場合のみです。ポート番号は変更できません。

      `ssh <デバイス名>` コマンドを使用して macOS デバイスにリモートでログインできます。［**共有**］ペインで、［**アクセスを許可する**］を使用して、macOS デバイスへのアクセスを許可するユーザーの範囲を設定できます。

   b. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。

      端末で `sudo visudo` コマンドを使用して sudoers 設定ファイルを開きます。開いたファイルの `User privilege specification` エントリで、次のように指定します。`username ALL = (ALL) NOPASSWD: ALL`。この場合、`username` は SSH を経由してデバイスを接続するために使用するユーザーアカウントを表します。

   c. sudoers ファイルを保存して閉じます。

   d. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。
3. インストールパッケージをダウンロードして作成します：
   a. 次のいずれかの方法で、ネットワークエージェントのインストールパッケージをダウンロードします：
      - アプリケーションインターフェイスを使用することで
      - https://support.kaspersky.co.jp/ のテクニカルサポートサイトから関連バージョンのネットワークエージェントをダウンロードする
      - テクニカルサポート担当者にインストールパッケージをリクエストする
   b. リモートインストールパッケージを作成するには、次のファイルを使用します：
      - klnagent.kud
      - install.sh
      - klnagentmac.dmg
4. 次の設定でリモートインストールタスクを作成します：
   - 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。
   - ［**タスクを実行するアカウントの選択**］ページで、SSH を使用したデバイス接続に使用するユーザーアカウントの設定を指定します。

作成したタスクを使用したネットワークエージェントのリモートインストールに対して、クライアントデバイスの準備ができています。

# 仮想インフラストラクチャ

Kaspersky Security Center Linux では仮想マシンの使用をサポートします。ネットワークエージェントとセキュリティ製品を各仮想マシンにインストールできます。また、ハイパーバイザーレベルで仮想マシンを保護できます。前者の場合、標準セキュリティ製品または Kaspersky Security for Virtualization Light Agent のいずれかを使用して、仮想マシンを保護できます。後者の場合、Kaspersky Security for Virtualization Agentless を使用できます。

Kaspersky Security Center Linux は、以前の状態への仮想マシンのロールバックをサポートします。

# 仮想マシンの負荷を軽減するヒント

Kaspersky Security Center Linux の一部の機能は、仮想マシンに対してはそれほど有効性がないと考えられます。ネットワークエージェントを仮想マシンにインストールする場合は、それらの機能の無効化を検討することが推奨されます。

ネットワークエージェントを仮想マシンまたは仮想マシンの生成を目的とするテンプレートにインストールする場合、以下の操作を実行してください：

- リモートインストールを実行している場合、ネットワークエージェントのインストールパッケージのプロパティウィンドウの［**詳細**］セクションで、［**VDI 向けに設定を最適化する**］をオンにします。
- ウィザードを使用して対話型インストールを実行している場合、ウィザードウィンドウで［**ネットワークエージェントの設定を仮想インフラストラクチャ用に最適化します**］をオンにします。

これらのオプションを選択すると、ネットワークエージェントの設定が変更されるため、以下の機能は（ポリシーを適用する前に）既定で引き続き無効化されます：

- インストールされたソフトウェアに関する情報の取得
- ハードウェアに関する情報の取得
- 検知された脆弱性に関する情報の取得
- 必要なアップデートに関する情報の取得

これらの機能は同一のソフトウェアと仮想ハードウェアを使用しているため、通常は仮想マシンでは必須ではありません。

機能の無効化は取り消すことができます。無効にした機能が必要になった場合、ネットワークエージェントのポリシーを使用して、またはネットワークエージェントのローカル設定を使用して有効にすることができます。ネットワークエージェントのローカル設定は、Kaspersky Security Center Web コンソールで関連デバイスのコンテキストメニューからアクセスできます。

# 動的仮想マシンのサポート

Kaspersky Security Center Linux では動的仮想マシンをサポートします。仮想インフラストラクチャが組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。動的仮想マシンは、管理者が準備したテンプレートに基づき、一意の名前で作成されます。ユーザーがしばらくの間仮想マシンで作業して、仮想マシンの電源をオフにすると、その仮想マシンは仮想インフラストラクチャから削除されます。Kaspersky Security Center Linux が組織ネットワークに導入されている場合、ネットワークエージェントがインストールされた仮想マシンが管理サーバーデータベースに追加されます。仮想マシンの電源をオフにした後は、対応するエントリも管理サーバーのデータベースから削除する必要があります。

仮想マシンのエントリの自動削除機能を活用するには、動的仮想マシンのテンプレートにネットワークエージェントをインストールする際に、次の場所で［**VDI 向け動的モードを有効にする**］をオンにします：

- リモートインストールの場合 – ネットワークエージェントのインストールパッケージのプロパティウィンドウで（［**詳細**］セクション）
- 対話型インストールの場合 – ネットワークエージェントのインストールウィザードで

ネットワークエージェントを物理デバイスにインストールする場合は、［**VDI 向け動的モードを有効にする**］をオンにしないでください。

動的仮想マシンのイベントを、それらの仮想マシンを削除した後もしばらくの間管理サーバーに保存したい場合、管理サーバーのプロパティウィンドウの［**イベントリポジトリ**］セクションで、［**デバイスの削除後にイベントを保管する**］をオンにし、イベントの最大保管時間（日数）を指定します。

# 仮想マシンのコピーのサポート

ネットワークエージェントがインストールされた仮想マシンをコピーする、またはネットワークエージェントがインストールされたテンプレートを使用して仮想マシンを作成する作業は、ハードディスクイメージを取得し、コピーしてネットワークエージェントを導入する場合と同一です。通常、仮想マシンをコピーする場合は、ディスクイメージをコピーしてネットワークエージェントを導入する場合と同じアクションを実行する必要があります。

ただし、以下に説明する 2 つの方法では、ネットワークエージェントでコピーが自動的に検出されます。そのため、「デバイスのハードディスクの取得とコピーによる導入」で説明する高度な操作を実行する必要はありません：

- ネットワークエージェントのインストール時に［**VDI 向け動的モードを有効にする**］をオンにした場合：オペレーティングシステムを再起動するたびに、この仮想マシンは、コピーされたかどうかに依存せず、新しいデバイスとして認識されます。
- VMware™、HyperV®、Xen® のいずれかのハイパーバイザーが使用されている場合：ネットワークエージェントでは、変更された仮想ハードウェアの ID によって、仮想マシンのコピーが検出されます。

仮想ハードウェアにおける変更の分析機能は、完全に信頼できるわけではありません。この方法を広く採用する前に、組織が現在使用しているハイパーバイザーのバージョンを用いて、小規模な仮想マシンのプールでテストする必要があります。

# Unix デバイスのリモートインストールを設定する

リモートインストールタスクを使用して Unix デバイスにアプリケーションをインストールする際、タスクに Unix 固有の設定を指定することができます。これらの設定はタスクが作成された後にタスクのプロパティで利用できるようになります。

*Unix 固有の設定をリモートインストールタスクで指定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. Unix 固有の設定を指定するリモートインストールタスクの名前をクリックします。
   タスクのプロパティウィンドウが開きます。
3. ［**アプリケーション設定**］→［**Unix 固有の設定**］の順に移動します。
4. 次の設定を指定します：
   - **root アカウントのパスワードを設定する（SSH での導入時のみ）**

     パスワードを指定しないと対象のデバイスで sudo コマンドが使用できない場合、このオプションを選択してルートアカウントのパスワードを指定します。Kaspersky Security Center Linux は対象デバイスにパスワードを暗号化して転送し、復号化してからこのパスワードを使用してルートアカウントに代わってインストール手順を開始します。

     Kaspersky Security Center Linux は SSH 接続を作成するためにユーザーアカウントや指定したパスワードを使用しません。

   - **ターゲットデバイスへの実行権限がある一時ディレクトリへのパスを指定する（SSH での導入時のみ）**

     対象デバイスの /tmp ディレクトリに実行権限がない場合、このオプションを選択してから実行権限のあるディレクトリへのパスを指定します。Kaspersky Security Center Linux は SSH 経由でアクセスする一時ディレクトリとして指定されたディレクトリを使用します。アプリケーションはインストールパッケージをそのディレクトリに配置し、インストールプロセスを実行します。
5. ［**保存**］をクリックします。

   指定したタスク設定が保存されます。

# 製品導入を監視する

Kaspersky Security Center Linux 導入を監視し、セキュリティ製品とネットワークエージェントが管理対象デバイスにインストールされていることを確認するには、監視とレポート機能を使用します：

- ダッシュボードの導入ウィジェットを使用して、導入をリアルタイムで監視します。
- レポートを使用して詳細情報を取得します。

# カスペルスキー製品の起動および停止

管理対象デバイスでカスペルスキー製品を起動および停止するには、*アプリケーションの開始または停止*タスクを使用できます。

*アプリケーションの開始または停止タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、タスクを作成するアプリケーションを選択します。
   以前にこれらのアプリケーションの管理 Web プラグインを追加している場合は、カスペルスキー製品がリストに表示されます。
4. ［**タスク種別**］リストから、［**アプリケーションのアクティベーション**］タスクを選択します。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
6. ［タスクを割り当てるデバイス］を選択します。
7. ［**アプリケーション**］ウィンドウで、次のように操作します：
   - タスクを作成するアプリケーションの名前の横にあるチェックボックスをオンにします。
   - ［**アプリケーションの開始**］または［**アプリケーションの停止**］オプションを選択します。
8. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ステップで、［**タスクの作成が完了したらタスクの詳細を表示する**］オプションを有効にします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
9. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。
10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
11. タスクのプロパティウィンドウで、必要性に応じて一般的なタスク設定を指定し、設定を保存します。

    タスクが指定した設定で作成されます。

タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

# サードパーティのセキュリティ製品からの移行とアンインストールの実施

カスペルスキーのセキュリティ製品を Kaspersky Security Center Linux を使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。Kaspersky Security Center Linux では、サードパーティ製品を削除する複数の方法が用意されています。

## 競合するアプリケーションの削除をアプリケーションのリモートインストールの設定時に指定

製品導入ウィザードのセキュリティ製品のリモートインストールの設定時に［**競合アプリケーションを自動的にアンインストールする**］をオンにできます。このオプションをオンにすると、管理対象デバイスにセキュリティ製品をインストールする前に、Kaspersky Security Center Linux は競合するアプリケーションを削除します。

## 専用タスクを使用した競合アプリケーションの削除

競合アプリケーションを削除するには、*アプリケーションのリモートアンインストールタスク*を使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［*アプリケーションのリモートアンインストール*］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

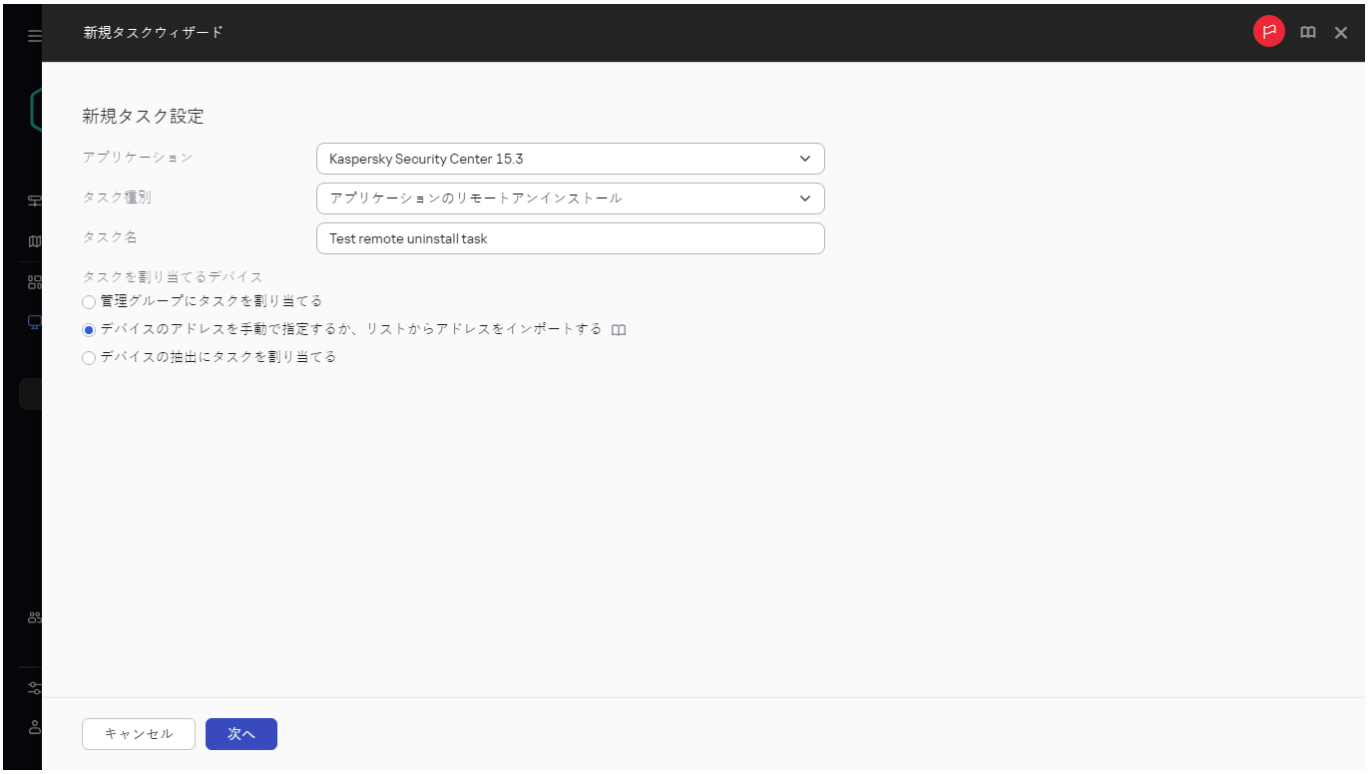
# アプリケーションまたはソフトウェアのアップデートのリモートでの削除

Linux を実行している管理対象デバイスのアプリケーションまたはソフトウェアアップデートは、ネットワークエージェントを使用した場合のみリモートから削除することができます。

*選択したデバイスからリモートでアプリケーションまたはソフトウェアのアップデートを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、［Kaspersky Security Center］を選択します。
4. ［**タスク種別**］リストで、［**アプリケーションのリモートアンインストール**］タスクタイプを選択します。

5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。




アプリケーションのリモートアンインストールタスクの作成

6. ［タスクを割り当てるデバイス］を選択します。
ウィザードの次のステップに進みます。




タスク範囲を指定します

7. 削除するソフトウェアの種類を選択してから、削除する特定のアプリケーション、アップデート、またはパッチを選択します。

- **管理対象アプリケーションをアンインストールする**

  カスペルスキー製品のリストが表示されます。削除するアプリケーションを選択します。

- **競合アプリケーションをアンインストールする**

  カスペルスキーのセキュリティ製品または Kaspersky Security Center Linux と互換性のないアプリケーションのリストが表示されます。削除するアプリケーションの隣にあるチェックボックスをオンにします。

- **アプリケーションレジストリからアプリケーションを削除する**

既定では、ネットワークエージェントは管理対象デバイスにインストールされているアプリケーションに関する情報を管理サーバーに送信します。インストールされているアプリケーションのリストは、アプリケーションレジストリに保存されます。

*アプリケーションレジストリからアプリケーションを選択するには：*

a. ［**アンインストールするアプリケーション**］をクリックし、削除するアプリケーションを選択します。

Kaspersky Security Center ネットワークエージェントを選択した場合、タスクを実行すると、削除プロセスが開始されたことを表「*正常に完了*」ステータスが表示されます。Kaspersky Security Center ネットワークエージェントが削除されても、ステータスは変わりません。タスクが失敗すると、ステータスは「*失敗*」に変わります。

b. アンインストールオプションを指定します：

- **アンインストールモード**

アプリケーションを削除する方法を選択します：

- **アンインストールコマンドを自動的に定義する**

  アプリケーションの製造元によって定義されたアンインストールコマンドがアプリケーションにある場合、Kaspersky Security Center Linux はこのコマンドを使用します。このオプションをオンにすることを推奨します。

- **アンインストールコマンドを指定する**

  アプリケーションのアンインストール用のコマンドを指定する場合は、このオプションをオンにします。

  まず、［**アンインストールコマンドを自動的に定義する**］をオンにしてアプリケーションを削除してみてください。自動的に定義されたコマンドによるアンインストールが失敗した場合は、独自のコマンドを使用してください。

  フィールドにインストールコマンドを入力し、次のオプションをオンにします。

  **既定コマンドが自動検知されない場合、このアンインストール用コマンドを使用**

  Kaspersky Security Center Linux は、選択されたアプリケーションに、アプリケーションの製造元が定義したアンインストールコマンドがあるかどうかを確認します。コマンドが見つかった場合、Kaspersky Security Center Linux は、［**アプリケーションのアンインストール用コマンド**］で指定されたコマンドの代わりにそのコマンドを使用します。

  このオプションをオンにすることを推奨します。

- **アプリケーションのアンインストール後に再起動する**

アンインストールが正常に完了した後で、アプリケーションが管理対象デバイスでオペレーティングシステムを再起動する必要がある場合、オペレーティングシステムは自動的に再起動されます。

- **指定したソフトウェアアップデート、パッチ、サードパーティ製品をアンインストールする**

  アップデート、パッチ、サードパーティ製品のリストが表示されます。削除する項目を選択します。

  表示されるリストは、アプリケーションとアップデートの一般的なリストであり、管理対象デバイスにインストールされているアプリケーションとアップデートには対応していません。項目を選択する前に、タスク範囲で定義されたデバイスにアプリケーションまたはアップデートがインストールされていることの確認を推奨します。アプリケーションまたはアップデートがインストールされているデバイスのリストを、プロパティウィンドウで表示できます。

  *デバイスのリストを表示するには：*

  a. アプリケーションまたはアップデートの名前をクリックします。

     プロパティウィンドウが表示されます。

  b. ［**デバイス**］セクションを開きます。

     インストールされているアプリケーションとアップデートのリストをデバイスのプロパティウィンドウで表示することもできます。

8. クライアントデバイスがアンインストールユーティリティをダウンロードする方法を指定します：

- **ネットワークエージェントを使用する**

  ファイルは、クライアントデバイスにインストールされているネットワークエージェントによってクライアントデバイスに配布されます。

  このオプションをオフにすると、ファイルは Linux オペレーティングシステムツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションは廃止されました。代わりに、［**ネットワークエージェントを使用する**］または［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］オプションを使用してください。

  ファイルは、管理サーバーのオペレーティングシステムツールを使用してクライアントデバイスに送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

  ファイルは、オペレーティングシステムのツールを使用してディストリビューションポイント経由でクライアントデバイスに送信されます。このオプションをオンにできるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

  ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールを使用して配布されます。

- **同時ダウンロード数の上限**

  管理サーバーが同時にファイルを送信できるクライアントデバイスの最大許容数。この数が大きいほど、アプリケーションのアンインストールは高速になりますが、管理サーバーの負荷が増大します。

- **アンインストール試行回数の上限**

［*アプリケーションのリモートアンインストール*］タスクの実行時に、パラメータで指定されたインストーラーの実行回数の範囲内で、管理対象デバイスから対象製品をアンインストールすることに失敗した場合、Kaspersky Security Center Linux はこの管理対象デバイスへのインストールユーティリティの配布を中止し、そのデバイス上でインストーラーを起動しなくなります。

［**アンインストール試行回数の上限**］パラメータを使用することで、管理対象デバイス上でのリソースの消費量とネットワークのトラフィック量を軽減できます（アンインストールの実行や MSI ファイルの実行によるリソース消費、エラーメッセージのトラフィック）。

タスクの開始が繰り返し試行されることは、デバイス上でインストールを阻害する問題が発生していることを示している可能性があります。管理者は、指定されたアンインストールの試行回数内で問題を解決してから、タスクを（手動でまたはスケジュールによって）再起動する必要があります。

指定された試行回数以内にアンインストールを実行できなかった場合、問題は解決不可能なものとして認識され、それ以上タスクの開始を試行することは不必要にリソースとトラフィックを消費してしまうものと判断されます。

タスクが作成されると、試行回数のカウンターは「`0`」にセットされます。デバイス上でインストーラーを実行してエラーが返されるたびに、カウンターの値が 1 ずつ増加します。

パラメータで指定した回数のインストールの試行が既に実行された後に、デバイスでアンインストールの準備が完了した場合は、［**アンインストール試行回数の上限**］パラメータの値を増やすことでアプリケーションをアンインストールするタスクを開始できます。または、［*アプリケーションのリモートアンインストール*］タスクを新規に作成することもできます。

- **ダウンロード前に OS の種別を確認する**

ファイルをクライアントデバイスに送信する前に、Kaspersky Security Center Linux はインストールユーティリティの設定がクライアントデバイスのオペレーティングシステムに適用可能であるかどうかを確認します。設定を適用できない場合、ファイルを送信せず、アプリケーションのインストールを試行しません。たとえば、様々なオペレーティングシステムを実行しているデバイスが存在する管理グループのデバイスにアプリケーションをインストールするには、インストールタスクを管理グループに割り当ててから、このオプションをオンにして、必要なオペレーティングシステム以外を実行しているデバイスをスキップできます。

ウィザードの次のステップに進みます。




タスク設定の指定

9. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**
  - **再起動するまでの時間（分）**

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

ウィザードの次のステップに進みます。

10. 必要に応じて、リモートアンインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  アプリケーションのリモートアンインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントまたは SSH 証明書を指定して、アプリケーションをアンインストールできます。

  - **ローカルアカウント**。このオプションをオンにする場合、アプリケーションのインストーラーを実行するユーザーアカウントを指定します。［**追加**］をクリックし、［**ローカルアカウント**］を選択してから、ユーザーアカウントの資格情報を指定します。

    タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

  - **SSH 証明書**。Linux ベースのクライアントデバイスからアプリケーションをアンインストールする場合、ユーザーアカウントの代わりに SSH 証明書を指定できます。［**追加**］をクリックし、［**SSH 証明書**］を選択してから、証明書の秘密鍵と公開鍵を指定します。

    秘密鍵を生成するには、ssh-keygen ユーティリティを使用できます。Kaspersky Security Center Linux は PEM 形式の秘密鍵をサポートしますが、ssh-keygen ユーティリティは既定で SSH 鍵を OPENSSH 形式で生成します。OPENSSH 形式は Kaspersky Security Center Linux ではサポートされていません。サポートされる PEM 形式で秘密鍵を作成するには、ssh-keygen コマンドに -m PEM オプションを追加します。

    例：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<ユーザーのメールアドレス>"
    ```

11. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。

    このオプションをオンにしない場合、タスクは既定の設定で作成されます。既定の設定からの変更は、後からいつでも実行できます。

12. ［**終了**］をクリックします。

    ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

    タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

    タスクが作成、設定され、［**アセット（デバイス）**］→［**タスク**］のタスクリストに表示されます。

13. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。

    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、選択したアプリケーションは選択したデバイスから削除されます。

## リモートアンインストールの問題

サードパーティ製アプリケーションのリモートアンインストールが、次の警告付きで終了する場合があります：「このデバイスでリモートアンインストールが警告付きで終了しました：削除対象のアプリケーションがインストールされていません。」この問題は、アンインストール対象のアプリケーションが既にアンインストールされているか、特定のユーザーに対してのみインストールされている場合に発生します。特定のユーザー用にインストールされたアプリケーション（「ユーザーごとのアプリケーション」とも表記）は、ユーザーがログインしていない場合は非表示になり、リモートアンインストールはできません。

この動作は、同じデバイス上で複数のユーザーが使用することを目的としたアプリケーション（「デバイスごとのアプリケーション」とも表記）とは異なります。デバイスごとのアプリケーションは、デバイスのすべてのユーザーに表示され、アクセス可能です。

したがって、ユーザーごとのアプリケーションは、ユーザーがログインしている時にアンインストールする必要があります。

## インストール済み製品の情報源

ネットワークエージェントは、次のレジストリライセンスから Windows デバイスにインストールされているソフトウェアに関する情報を取得します。

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  すべてのユーザーに対してインストールされたアプリケーションに関する情報が含まれます。

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  すべてのユーザーに対してインストールされたアプリケーションに関する情報が含まれます。

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  現在のユーザーに対してインストールされているアプリケーションに関する情報が含まれます。

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  特定のユーザーに対してインストールされたアプリケーションに関する情報が含まれます。

# リモートインストールのための Windows デバイスの準備

次のような理由によって、クライアントデバイスへのリモートインストールでエラーが返されることがあります：

- タスクが既に同じデバイスで正常に実行されている。

  この場合、タスクを再度実行する必要はありません。

- タスクの開始時点でデバイスが停止していた。

  この場合、デバイスを起動して、タスクを再起動してください。

- 管理サーバーと、クライアントデバイスにインストールされているネットワークエージェントとが接続されていない。

  原因を解明するには、クライアントデバイスのユーティリティ（klactgui）のリモート診断機能を使用してください。

- ネットワークエージェントがデバイスにインストールされていない場合、リモートインストール時に次の問題が生じることがあります：

  - クライアントデバイスで［**簡易ファイルの共有を無効にする**］オプションがオンになっています
  - サーバーのサービスがクライアントデバイスで実行されていない
  - クライアントデバイス上で必要なポートが閉じている
  - タスクの実行に使用されるアカウントに十分な権限がない

  ネットワークエージェントがインストールされていないクライアントデバイスにアプリケーションをインストールする際に発生する可能性のある問題を回避するには、Kaspersky Security Center Linux のリモートインストールタスクによる強制導入の説明通りに実行する必要があります。

以前は、リモートインストール用のデバイスを準備するために riprep ユーティリティを使用していました。これは現在、オペレーティングシステムを構成するための時代遅れの方法であると考えられています。riprep ユーティリティは、Windows XP および Windows Server 2003 R2 より新しいオペレーティングシステムでの使用は推奨されません。

# スクリプトをリモートで実行タスクの作成

クライアントデバイス上でインストールパッケージを実行し、アプリケーションをリモートでインストールするための*スクリプトをリモートで実行*タスクを作成できます。

インストールパッケージには、クライアントデバイスで実行するためのスクリプトのセットとファイル manifest.json を含む ZIP アーカイブが含まれています。このタイプのインストールパッケージの作成の詳細については、この記事を参照してください。

このタスクは、Linux 用ネットワークエージェントがインストールされているデバイスでのみ開始する必要があります。

*スクリプトをリモートで実行タスクを開始するには：*

1. **新規タスクウィザード**に移動し、**スクリプトをリモートで実行**タスクタイプを選択します。
2. タスク名を入力し、タスクを割り当てるデバイスを選択します。［**次へ**］をクリックします。
3. リモート実行用のファイル manifest.json を含む ZIP アーカイブに基づくインストールパッケージを選択します。

   タスクが既に完了しているデバイスで、タスクを再実行しない場合は、［**タスクが完了済みのデバイスではこのタスクを開始しない**］をオンにします。
4. タスクを実行するアカウントを選択します。

   既定アカウントを選択した場合、タスクはネットワークエージェント（root アカウント）によって実行されます。

   *スクリプトをリモートで実行*タスクが開始されると、割り当てられているアカウントを変更することはできません。タスクが割り当てられているアカウントを変更するには、タスク設定でタスクを停止し、正しいアカウント詳細で再度作成します。
5. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後でいつでも実行できます。
6. ［**終了**］をクリックします。

   *スクリプトをリモートで実行*タスクが作成され、タスクリストに表示されます。

ネットワークエージェントは、*スクリプトをリモートで実行*タスクからデータを受信した後、管理者とタスク設定で指定されたユーザーを除くすべてのユーザーに対して、受信したデータへのアクセスを制限します。

# マニフェストファイルに基づいてインストールパッケージを作成する

*マニフェストファイルに基づいてインストールパッケージを作成するには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. **ファイル manifest.json を含む ZIP アーカイブを基に［スクリプトをリモートで実行］タスクのインストールパッケージを作成する**］を選択します。

4. パッケージ名を指定して、［**参照**］をクリックします。

   開いたウィンドウで、インストールパッケージを作成するファイルを選択します。

5. 事前に準備しておいた圧縮ファイルを選択します。このタスク用のアーカイブを準備する方法については、この記事を参照してください。

   ファイルが Kaspersky Security Center Linux 管理サーバーにアップロードされ始めます。

   カスタムインストールパッケージを作成するプロセスが開始されます。

   プロセスが終了すると、ウィザードで通知されます。

   インストールパッケージが作成されなかった場合も、メッセージで通知されます。

6. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

管理サーバーで利用できるインストールパッケージのリストで、カスタムインストールパッケージの名前をクリックすることで次の操作を実行できます：

- インストールパッケージのプロパティとして以下の情報を表示する：
  - **名前：**カスタムインストールパッケージの名前。
  - **ソース：**アプリケーションの開発元の名前。
  - **バージョン：**アプリケーションのバージョン。
  - **作成：**インストールパッケージの作成日時。
  - **変更：**インストールパッケージの変更日時。
  - **パス：**管理サーバー上のカスタムインストールパッケージへのパス。
- パッケージ名とコマンドラインのパラメータを変更する。この操作は、カスペルスキー製品に基づいて作成されていないインストールパッケージでのみ実行できます。

# スクリプトをリモートで実行タスク用のアーカイブを準備する

ファイル manifest.json に基づく*スクリプトをリモートで実行*タスクのアーカイブは、次の要件を満たす必要があります。

- アーカイブ形式：ZIP。
- 合計サイズ：1 GB 以下。
- アーカイブ内のファイルとフォルダーの数に制限はありません。

- アーカイブのマニフェストファイルは以下のスキーマと一致し、manifest.json という名前にする必要があります。スキーマは、デバイス上でタスクが実行されるときにのみ検証されます。

  **マニフェストファイルの JSON スキーマと配列の説明**

JSON スキーマ

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

**マニフェストファイルの例**

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- アーカイブは次のように構造化する必要があります：

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json はタスクのマニフェストファイルです。

**<file1>, ...., <fileX>** は、実行されるスクリプトを含むファイルのセットです。

# スクリプトをリモートで実行タスクを使用して、デバイスにアプリケーションをリモートでインストールする

*スクリプトをリモートで実行*タスクを使用すると、カスタムインストールパッケージを作成して、クライアントデバイスにアプリケーションをリモートでインストールできます。

このタスク用のアーカイブを準備する方法については、この記事を参照してください。

クライアントデバイスにアプリケーションをリモートインストールするためのインストールパッケージを作成するには、このタスク用にアップロードするアーカイブに次のファイルが含まれている必要があります。

- <パッケージ名>.deb
- install.sh

  ```
  sudo apt-get install <パッケージ名>.deb
  ```

- manifest.json

アプリケーションのリモートインストール用の JSON スキーマ

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<必要に応じて引数を入力>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

配列の説明

1. `version` - マニフェストファイルとタスクのバージョン。
   現在、許容される値は 1 のみです。
2. `actions` 配列の要素によって、タスクで実行されるスクリプトの構成と順序が決まります。
   スクリプトの実行順序は、配列内の要素のインデックス（場所）に対応します。
3. `actions` 配列の各要素に対して、次の要素が定義されます。
   a. `type` - スクリプトから実行可能なコマンドのタイプ。現時点では、値は常に `execute` です。
   b. `path` - アーカイブ内のスクリプトファイルへのパス。
   c. `args` - 実行可能コマンドの一部としてスクリプトに渡される引数。
   d. `results` - タスクの結果に応じてさらなるアクションを定義する配列。
      1. `code` - スクリプトを返す値。
      2. `next` - 次に完了するアクション。`continue` アクションは次のスクリプト（`actions` 配列内の要素）の実行に進み、`break` アクションはタスクを停止します。
   e. `default_next` - スクリプトが `results` に含まれていない値を返した場合のアクション。

*スクリプトをリモートで実行*タスクが開始されると、ネットワークエージェントはアプリケーションを含むインストールパッケージをクライアントデバイスにアップロードします。クライアントデバイスがインストールパッケージを受信すると、このデバイス上のネットワークエージェントはファイル manifest.json を解析し、結果に応じてスクリプトとアクションの実行順序を定義して実行を開始します。

*スクリプトをリモートで実行*タスクが完了すると、アプリケーションがクライアントデバイスにインストールされます。

# スクリプトをリモートで実行するタスクの通知と監視を設定する

*スクリプトをリモートで実行*タスクの監視、イベント保存動作、および通知を設定できます。

*スクリプトをリモートで実行のステータスを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
2. タスクを選択し、［**デバイスの履歴**］をクリックします。
   タスクの進行状況が表示されます。

*イベント保存動作を設定するには：*

1. タスクのリストで、タスクをクリックして［**設定**］タブに移動します。
2. ［**通知**］セクションで、［**設定**］をクリックします。
3. タスクが完了した後のアプリケーションの動作については、次のいずれかのオプションを選択します。
   - **すべてのイベントを保存**する。
   - **タスクの進捗に関連したイベントを保存**：
   - **タスク実行結果のみ保存**：
     イベントは**デバイスの履歴**と**イベントリポジトリ**に保存されます。
     既定では、タスクの実行結果のみが保存されます。

     ［**すべてのイベントを保存**］を選択した場合は、タスクの実行結果のみが保存されます。
4. イベントを管理サーバーの定義データベース、管理サーバー上のイベントログ、またはデバイス上に保存する場合は、対応するオプションをオンにします。

通知の設定の詳細については、この記事を参照してください。

# ライセンス

このセクションでは、次の項目について説明します：

- Kaspersky Security Center Linux ライセンス管理に関連する一般的な概念
- 管理対象のカスペルスキー製品のライセンス管理に関する手順

# Kaspersky Security Center Linux のライセンス

このセクションでは、Kaspersky Security Center Linux のライセンス管理に関係する一般的な概念について説明します。

## 使用許諾契約書について

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で交わされる契約であり、製品の使用条件が定められています。

製品の使用を開始する前に、使用許諾契約書の条項をよく読んでください。

Kaspersky Security Center Linux とそのコンポーネント（ネットワークエージェントなど）にはそれぞれ個別の使用許諾契約書があります。

Kaspersky Security Center Linux の使用許諾契約書の条項は、次の方法で確認できます：

- Kaspersky Security Center のインストール中に確認する。
- Kaspersky Security Center の配布キットに含まれている license.txt を参照する。
- Kaspersky Security Center のインストールフォルダーにある license.txt を参照する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

Linux 用ネットワークエージェントの使用許諾契約書の条項は、次の方法で確認できます：

- カスペルスキーの Web サーバーからのネットワークエージェント配布パッケージのダウンロード時に確認する。
- Linux 向けネットワークエージェントのインストール中に確認する。
- Linux 向けネットワークエージェントの配布パッケージに含まれる license.txt を読んで確認する。
- Linux 向けネットワークエージェントのインストールフォルダーにある license.txt を読んで確認する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

製品のインストール時に使用許諾契約書に同意することにより、使用許諾契約書の条項を受諾したものと判断されます。使用許諾契約書の条項に同意しない場合は、製品のインストールを中止し、使用しないようにする必要があります。

# ライセンスについて

*ライセンス*は、署名されたライセンス契約（使用許諾契約書）の条件に基づいて提供される、Kaspersky Security Center Linux を使用する期限付きの権利です。

サービスの範囲と有効期間は、アプリケーションが使用されるライセンスによって異なります。

次のライセンス種別があります：

- *試用版*

  製品の試用を目的とした無償ライセンス。試用版ライセンスは通常、有効期間が短く設定されています。

  試用版ライセンスの有効期間が終了すると、Kaspersky Security Center Linux のすべての機能が無効になります。製品の使用を継続するには、製品版ライセンスを購入する必要があります。

  試用ライセンスに基づいてアプリケーションを使用できるのは、1回の試用期間のみです。

- *製品版*

  有料ライセンス。

  製品版ライセンスの有効期限が切れると、本製品の主要な機能が無効になります。Kaspersky Security Center の使用を継続するには、製品版ライセンスを更新する必要があります。商用ライセンスの有効期限が切れると、アプリケーションを引き続き使用できなくなり、デバイスから削除する必要があります。

  有効期間が終了する前、すべてのセキュリティ脅威から継続的に保護された環境を維持できるようにライセンスを更新することを推奨します。

# ライセンス証書について

*ライセンス証書*とは、ライセンス情報ファイルまたはアクティベーションコードに付随して受け取る文書です。

ライセンス証書には、提供されたライセンスに関する次の情報が含まれています：

- ライセンス ID または注文番号
- ライセンスが適用されるユーザーの情報
- 提供されたライセンスを使用したアクティベーションが可能である製品の情報
- ライセンスの上限（提供されたライセンスで使用可能な製品が使用できるデバイスの台数など）
- ライセンスの有効期間の開始日
- ライセンスの有効期間または有効期間の終了日
- ライセンス種別

# ライセンス情報について

*ライセンス情報*とは、使用許諾契約書の条項に基づいてアクティベーションを適用して製品を使用できる数値の並びです。ライセンス情報は、カスペルスキーによって生成されます。

製品にライセンス情報を追加するには、*ライセンス情報ファイル*を適用するか、*アクティベーションコード*を入力します。ライセンス情報は、製品に追加した後、インターフェイスに一意の英数字の並びで表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーがライセンス情報をブロックします。ライセンス情報がブロックされた際に、製品を使用したい場合は、別のライセンス情報を追加する必要があります。

ライセンスには、現在のライセンスまたは予備のライセンスがあります。

*現在のライセンス*：アプリケーションによって現在使用されているライセンス。現在のライセンスは、試用版または製品版のライセンス情報として追加できます。製品に指定できる現在のライセンスは1つのみで、2つ以上の現在のライセンスを指定することはできません。

*予備のライセンス*：アプリケーションを使用する権限をユーザーに付与する、現在使用されていないライセンス。予備のライセンスは、現在のライセンスの有効期間が終了すると、自動的に適用されます。予備のライセンスは、現在のライセンスが追加済みである場合にのみ、追加できます。

試用版のライセンスは、現在のライセンスとしてのみ追加できます。試用版のライセンスを予備のライセンスとして追加することはできません。

# プライバシーポリシーの表示

プライバシーポリシーは、https://www.kaspersky.co.jp/products-and-services-privacy-policy で参照できます。

プライバシーポリシーはオフラインでも使用可能です。

- Kaspersky Security Center Linux のインストール前にプライバシーポリシーを確認することができます。
- プライバシーポリシーは Kaspersky Security Center Linux のインストールフォルダーにある license.txt に含まれています。
- ファイル「privacy_policy.txt」は管理対象デバイスのネットワークエージェントのインストールフォルダーにあります。
- ネットワークエージェントの配布パッケージから privacy_policy.txt を解凍できます。

# Kaspersky Security Center のライセンスオプション

Kaspersky Security Center は次のモードで動作します：

- **管理コンソールの基本機能**

  Kaspersky Security Center は、アプリケーションがアクティベートされる前、または製品版ライセンスの有効期限が切れた後、このモードで動作します。Kaspersky Security Center と管理コンソールの基本機能は、企業ネットワークを保護するカスペルスキー製品の一部として提供されます。カスペルスキーの Web サイトからもダウンロードできます。

- **製品版ライセンス**

  管理コンソールの基本機能に含まれていない追加機能が必要な場合は、製品版ライセンスを購入する必要があります。

  管理サーバーのプロパティウィンドウでライセンスを追加する時は、Kaspersky Security Center Linux を使用できるようにするライセンスを必ず追加してください。この情報は、カスペルスキーの Web サイトにあります。各ソリューションの Web ページには、ソリューションに含まれるアプリケーションのリストが記載されています。管理サーバーは、サポートされていないライセンス（たとえば、Kaspersky Endpoint Security Cloud のライセンス）を受け入れる場合がありますが、そのようなライセンスは、管理コンソールの基本機能に加えて新しい機能を提供しません。

| 機能またはプロパティ | Kaspersky Security Center Linux 操作モード | |
|---|---|---|
| | ライセンスなし | 商用ライセンス |
| **管理コンソールの基本機能**<br>次の機能を使用できます：<br>• リモートオフィスまたはクライアント組織のネットワークを管理する仮想管理サーバーの作成<br>• 特定のデバイスをまとめて管理する管理グループの階層の作成<br>• アプリケーションのリモートインストール<br>• クライアントデバイスにインストールされたアプリケーションの一元的設定<br>• 組織のアンチウイルスセキュリティステータスの管理<br>• ユーザーロールの管理<br>• アプリケーションの動作に関する統計、レポートの検索、および緊急イベントの通知<br>• 隔離フォルダーまたはバックアップフォルダーに移動されたファイルおよび処理が延期されたファイルの一元的管理<br>• 暗号化とデータ保護の管理<br>• ネットワークポーリングによって検出されたハードウェアのリストの表示と手動編集<br>• リモートインストールに使用できるオペレーティングシステムイメージのリストの表示 | ✓ | ✓ |
| **脆弱性とパッチ管理：基本機能**<br>次のタスクに商用ライセンスは必要ありません：<br>• *脆弱性とアプリケーションのアップデートの検索*タスク<br>このタスクを使用して、Kaspersky Security Center Linux は管理対象デバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。<br>• ［*脆弱性の修正*］タスク<br>［*脆弱性の修正*］タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。このタスクを使用するには、タスクの設定で、脆弱性を修正するために使用するユーザー修正を手動で指定する必要があります。 | ✓ | ✓ |

| 機能またはプロパティ | Kaspersky Security Center Linux 操作モード | |
|---|---|---|
| | ライセンスなし | 商用ライセンス |
| **脆弱性とパッチ管理：高度な機能**<br>ソフトウェアアップデートの自動リモートインストールと脆弱性の自動修正のルールを定義できます。 | – | ✓ |
| **システム管理**<br>次の機能を使用できます：<br>• リモートデスクトップ接続という名前の Microsoft® Windows® コンポーネントによるクライアントデバイスへのリモート接続権限<br>• Windows デスクトップ共有によるクライアントデバイスへのリモート接続 | – | ✓ |
| **イベントを SIEM システムへエクスポートする方法：Syslog プロトコルを使用します**<br>Syslog プロトコルを使用すると、Kaspersky Security Center 管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントはすべてリレーできます。Syslog プロトコルは、標準メッセージロギングプロトコルです。任意の SIEM システムへのイベントのエクスポートに使用可能です。 | ✓ | ✓ |

# ライセンス情報ファイルについて

*ライセンス情報ファイル*は、拡張子が「key」のファイルで、カスペルスキーから提供されます。ライセンス情報ファイルは、製品のアクティベーションに使用します。

ライセンス情報ファイルは、Kaspersky Security Center を購入すると提供されます。

ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

製品のインストール後にライセンス情報ファイルを紛失した場合は、再入手できます。ライセンス情報ファイルは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。

ライセンス情報ファイルを再入手するには次の方法があります：

- ご購入元の販売代理店へ問い合わせる。
- カスペルスキーの Web サイト で、使用可能なアクティベーションコードを使用してライセンス情報ファイルを取得する。

# データ提供について

## サードパーティに送信されるデータ

製品のモバイルデバイス管理機能を使用する場合、プッシュ通知のメカニズムによって Android オペレーティングシステムを実行するデバイスにコマンドをタイムリーに配信する目的で、Google Firebase Cloud Messaging サービスが使用されます。ユーザーが Google Firebase Cloud Messaging サービスの使用を設定している場合、ユーザーは自動モードで Google Firebase Cloud Messaging サービスに以下の情報を提供することに同意するものとします：

- インスタンス ID。
- Google Firebase Cloud Messaging サービスのソフトウェア ID。
- インストールされているソフトウェアのバージョン。
- ソフトウェアの完全なバージョン。
- Google Play 版。
- ソフトウェア配布パッケージ名。
- 提供されるデータのスキーマバージョン。
- デバイスのオペレーティングシステムのバージョン。
- ソフトウェア ID。

Google Firebase Cloud Messaging サービスとの情報の交換をブロックするには、ユーザーが Google Firebase Cloud Messaging サービスの使用設定を出荷時の設定にロールバックする必要があります。

製品のモバイルデバイス管理機能を使用する場合、プッシュ通知のメカニズムによって iOS オペレーティングシステムを実行するデバイスにコマンドをタイムリーに配信する目的で、Apple Push Notification Service（APNs）が使用されます。ユーザーが iOS MDM サーバーに APNs 証明書をインストールし、iOS モバイルデバイスを製品に接続するために iOS MDM プロファイルを作成して一連の設定を行い、このプロファイルをモバイルデバイスにインストールした場合、そのユーザーは次の情報を APNs に自動モードで提供することに同意したものとします：

- トークン - デバイスのプッシュトークン。サーバーはデバイスにプッシュ通知を送信する時に、このトークンを使用します。
- PushMagic - プッシュ通知に含まれる必要のある文字列。この文字列の値はデバイスによって生成されます。

## ローカル環境で処理されるデータ

Kaspersky Security Center Linux は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。管理者は組織のネットワークのセキュリティレベルに関する詳細情報にアクセスし、カスペルスキー製品を使用して構築された保護システムのすべてのコンポーネントを設定できるようになります。Kaspersky Security Center Linux が実行する主要な機能は次の通りです：

- 組織のネットワーク内のデバイスおよびそのユーザーの検出
- デバイス管理用の管理グループ階層の作成
- デバイスへのカスペルスキー製品のインストール
- インストールされた製品の設定およびタスクの管理
- カスペルスキー製品およびサードパーティ製品のアップデートの管理、および脆弱性の検知と修正
- デバイス上でのカスペルスキー製品のアクティベーション
- ユーザーアカウントの管理
- デバイス上でのカスペルスキー製品の動作に関する情報の表示
- レポートの表示

主要な機能を実行するために、Kaspersky Security Center Linux は次の情報を取得し、保存し、処理することができます：

- Active Directory または Samba ドメインコントローラーをスキャンすること、または IP 間隔をスキャンすることを通じて受信した、組織のネットワーク上のデバイスに関する情報。管理サーバーは、データを独立して収集するか、ネットワークエージェントからデータを取得します。
- 組織単位、ドメイン、ユーザー、およびグループに関する Active Directory および Samba からの情報。管理サーバーは、それ自体でデータを取得するか、ディストリビューションポイントとして機能するように割り当てられたネットワークエージェントからデータを受信します。
- 管理対象デバイスの詳細情報。ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます。ユーザーはデバイスの表示名と説明を Kaspersky Security Center Web コンソールのインターフェイスに入力します：
  - デバイスの識別に必要な管理対象デバイスとそのコンポーネントの技術的な仕様情報：デバイスの表示名と説明、Windows ドメイン名と種別（Windows ドメイン内のデバイスが対象）、Windows 環境におけるデバイス名（Windows ドメイン内のデバイスが対象）、DNS ドメインと DNS 名、IPv4 アドレス、IPv6 アドレス、ネットワークロケーション、MAC アドレス、シリアル番号、オペレーティングシステムの種別、デバイスが仮想マシンかどうかの情報とハイパーバイザーの種別、およびデバイスが VDI の一部としての動的仮想マシンかどうかの情報。
  - 管理対象デバイスの監査および特定のパッチやアップデートが適用可能かどうかの判断に必要となる、管理対象デバイスとそのコンポーネントのその他の仕様情報：オペレーティングシステムのアーキテクチャ、オペレーティングシステムベンダー、オペレーティングシステムのビルド番号、オペレーティングシステムのリリース ID、オペレーティングシステムのロケーションフォルダー、（デバイスが仮想マシンの場合）仮想マシンの種別とデバイスを管理する仮想管理サーバーの名前。
  - 管理対象デバイス上の処理の詳細情報：前回のアップデートの日時、デバイスが前回ネットワークで検出された日時、再起動の待機ステータス、デバイスの電源を投入した日時。
  - デバイスのユーザーアカウントとその作業セッションの詳細情報。
- 管理対象デバイスでリモート診断を実行することによって受信したデータ：トレースファイル、システム情報、デバイスにインストールされているカスペルスキーアプリケーションの詳細、ダンプファイル、イベントログ、カスペルスキーテクニカルサポートから受信した診断スクリプトの実行結果。

- デバイスがディストリビューションポイントである場合、ディストリビューションポイントの動作統計情報。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。

- ユーザーが Kaspersky Security Center Web コンソールに入力したディストリビューションポイントの設定。

- 管理サーバーへのモバイルデバイスの接続に必要なデータ：証明書、モバイル接続ポート、管理サーバーの接続アドレス。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- モバイルプロトコル経由で送信されるモバイルデバイスの詳細情報。次に記載されたデータがモバイルデバイスから管理サーバーに送信されます：

  - アプリケーションに関する情報：アプリケーション名、アプリケーションのフルバージョン、アプリケーションのインストール日時、デバイスのリアルタイム保護ステータス、セッション ID。

  - アプリケーションが使用するライセンスに関する情報：ライセンスのシリアル番号とライセンスの種類、ライセンスのステータス、ライセンスの有効期間（日数）、ライセンスの生成日とライセンスの有効期限、ライセンスの提供先の会社名、サブスクリプションが使用されている場合の追加情報（サブスクリプションフラグ、有効期限とサブスクリプション更新までに使用可能な日数、サブスクリプションプロバイダーの Web アドレス、現在のサブスクリプションのステータスとステータスを取得した理由）、デバイスでアプリケーションがアクティブ化された日時、デバイスのライセンスの有効期限が切れる日時。

  - 管理対象デバイスに関する情報：デバイス名、デバイス ID、デバイスタイプ、デバイス IMEI（使用可能な場合）、デバイスのシリアル番号（使用可能な場合）、デバイスの製造元、デバイスの CPU ファミリー名、デバイスの所有者証明書の拇印、OS タイプ、OS バージョン、OS 名、デバイスの合計ディスク容量、デバイスが属するサーバーの名前、デバイスの IP アドレス、デバイスグループ名、ユーザーの識別名、ドメインの識別名、ワンタイムパスワードまたはドメインパスワード。

  - カスタムコマンドの実行結果に関する情報：コマンド ID、コマンド実行ステータス、コマンド実行結果。デバイス検索コマンドの場合：デバイスの緯度、経度、高度、移動速度。マグショットコマンドの場合：ロック解除を試行した時にモバイルデバイスの前面カメラで撮影された写真。

  - デバイススキャンに関する情報：最後のデバイススキャンの日時、スキャンが開始されたファイルシステム内の完全なパス、スキャンされたオブジェクトの数、検出された悪意のあるオブジェクトの数、ブロック、削除、および駆除されたオブジェクトの数、駆除できなかったオブジェクトの数、検証エラーの数、終了したプロセスの数。

  - 各アプリケーションコンポーネントの機能と各タスクのパフォーマンスに関する情報がイベントとして表示されます：

    - イベント ID。

    - 重要度。

    - イベント名とタイプ。

    - イベントの原因の説明。

    - イベントが発生した日時。

    - 盗難対策操作イベントに関する情報（デバイスのロック解除コード、デバイスの座標、コマンドの配信方法、削除されたデータのリスト）。

    - 検知されたオブジェクトまたはアクションの処理結果（デバイス上のファイル名、アプリケーション名、脅威名、脅威の種類、ファイルで実行されたアクションの種類、アクションの結果、発生した場合はエラーコード）。

    - トリガーされたコンプライアンスルールに関する情報（ルールの基準、適用されたアクション、発生した場合のアクション適用時のエラーの説明）。

    - アプリケーション操作エラーに関する情報（アプリケーションバージョン、OS バージョン、デバイス名、エラーの説明）。

    - Samsung KNOX のエラーに関する情報（エラーコード、ファイルをダウンロードできなかった URL）。

- アプリケーションに付与された権限に関する情報。
- 管理対象デバイスにインストールされている各アプリケーションに関する情報（アプリケーション名、インストール状態）。

- 使用許諾契約書（EULA）のグローバル承認に関する情報：EULA ID、EULA タイムスタンプ、EULA テキスト。
- Google Firebase Cloud Messaging の設定：送信者 ID、デバイス登録 ID。

- iOS MDM プロトコル経由で送信されるモバイルデバイスの詳細情報。次に記載されたデータがモバイルデバイスから管理サーバーに送信されます：
  - デバイスの識別に必要なモバイルデバイスとそのコンポーネントの技術的な仕様情報：デバイス名、機種、オペレーティングシステムの名前、バージョンとビルド番号、デバイスの機種番号、IMEI 番号、電話番号、UDID、MEID、シリアル番号、フルで使用可能なストレージ容量、モデムファームウェアのバージョン、Bluetooth の MAC アドレス、Wi-Fi の MAC アドレス、SIM カードの詳細情報（SIM カードの識別子の一部としての ICCID）。
  - 管理対象デバイスで使用されるモバイルネットワークの詳細情報：モバイルネットワークの種別、現在使用されているモバイルネットワークの名前、ホームモバイルネットワーク名、通信事業者の設定のバージョン、音声ローミングとデータローミングのステータス、ホームネットワークの国コード、居住国コード、現在使用されているネットワークの国コード、暗号化レベル。
  - モバイルデバイスのセキュリティ設定：パスワードの使用とポリシー設定への準拠、インストールされている証明書、アプリ、設定プロファイルのリスト。
  - 管理サーバーとの前回の同期の日時とデバイスの管理ステータス。
- モバイルデバイスへの転送用に指定されたファイルの詳細。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。
- デバイスにインストールされたカスペルスキー製品の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：
  - 管理対象デバイスにインストールされているカスペルスキー製品の設定：カスペルスキー製品の名前とバージョン、ステータス、リアルタイム保護のステータス、前回のデバイススキャンの日時、検知された脅威の数、駆除に失敗したオブジェクトの数、製品コンポーネントの使用可否の情報とそのステータス、カスペルスキー製品の設定およびタスクの詳細情報、現在のライセンスと予備のライセンスに関する情報、製品のインストールの日付と ID。
  - 製品動作の統計情報：管理対象デバイス上のカスペルスキー製品コンポーネントのステータス変化および製品コンポーネントによって開始されたタスクのパフォーマンスに関係するイベント。
  - カスペルスキー製品によって定義されたデバイスのステータス。
  - カスペルスキー製品によって割り当てられたタグ。
- Kaspersky Security Center Linux のコンポーネントおよび管理対象のカスペルスキー製品からのイベントに含まれるデータ。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。
- Kaspersky Security Center Linux と、イベントをエクスポートする SIEM システムとの統合に必要なデータ。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center Linux のコンポーネント、およびポリシーとポリシーのプロファイルに示される管理対象のカスペルスキー製品の設定。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center Linux のコンポーネントおよび管理対象のカスペルスキー製品のタスク設定。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- システム管理機能によって処理されたデータネットワークエージェントは、デバイスから管理サーバーに次の情報を転送します：

  - 管理対象デバイスで検出されたハードウェアに関する情報（ハードウェアのレジストリ）。

    Windows が動作しているデバイスにネットワークエージェントがインストールされている場合、ネットワークエージェントはデバイスのハードウェアに関する以下の情報を管理サーバーに送信します：

    - メモリ
    - 大容量ストレージデバイス
    - マザーボード
    - CPU
    - ネットワークアダプター
    - モニター
    - ビデオアダプター
    - サウンドカード

    Linux または macOS を実行しているデバイスにネットワークエージェントがインストールされている場合、この情報がオペレーティングシステムから提供されると、ネットワークエージェントはデバイスのハードウェアに関する次の情報を管理サーバーに送信します：

    - 合計 RAM 容量
    - 大容量記憶装置の合計容量
    - マザーボード
    - CPU
    - ネットワークアダプター

  - 管理対象デバイスにインストールされているアプリケーションおよびパッチの詳細情報（アプリケーションのレジストリ）。アプリケーションは、アプリケーションコントロール機能によってデバイス上で検知された実行ファイルに関する情報と比較できます。

  - 管理対象デバイスで検出されたサードパーティ製品の脆弱性に関する詳細情報。

  - 管理対象デバイスにインストールされているサードパーティ製品で利用できるアップデートの詳細情報。

- 管理対象デバイスのサードパーティ製品の脆弱性を修正するため、分離された管理サーバー上のアップデートをダウンロードするために必要なデータ。ユーザーは管理サーバーの klscflag ユーティリティを使用してデータを入力および送信します。

- アプリケーションのユーザーカテゴリ。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- アプリケーションコントロール機能を使用して管理対象デバイスで検出された実行ファイルの詳細。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- バックアップされたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 隔離されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 詳細分析のためにカスペルスキーの担当者から提出を依頼されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- アダプティブアノマリーコントロールルールのステータスとトリガーの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- デバイスコントロール機能によって検出された、管理対象デバイスに搭載されているデバイスまたは管理対象デバイスに接続している外部デバイス（メモリユニット、情報転送ツール、情報ハードコピーツール、接続バス）の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 暗号化された Windows ベースのデバイスと暗号化のステータスに関する情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：

- デバイスのデータ暗号化エラーのに関する情報。暗号化は、カスペルスキー製品のデータ暗号化機能によって実行されます。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：データの完全なリストは、該当する製品のヘルプファイルに記載されています。

- 管理対象のプログラマブルロジックコントローラー（PLC）のリスト。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 脅威開発チェーンの作成に必要なデータ。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 組織の従業員によるクラウドサービスへのアクセス試行に関する情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- Kaspersky Security Center と Kaspersky Managed Detection and Response サービスの統合に必要なデータ（Kaspersky Security Center Web コンソールには専用プラグインをインストールする必要があります）：統合開始トークン、統合トークン、およびユーザーセッショントークン。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールで統合開始トークンを入力します。Kaspersky MDR サービスは、専用プラグインを介して統合トークンとユーザーセッショントークンを転送します。

- 入力されたアクティベーションコードまたはライセンス情報ファイルの詳細。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- ユーザーアカウント：名前、説明、氏名、メールアドレス、メインの電話番号、パスワード、管理サーバーによって生成された秘密鍵、および二段階認証用のワンタイムパスワード。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- 管理オブジェクトの変更履歴。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- ユーザーがリビジョンを作成したデバイスの IP アドレス。IP アドレスは管理サーバーによって自動的に定義されます。

- 削除された管理オブジェクトのレジストリ。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- ファイルから作成されたインストールパッケージとインストール設定。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center Web コンソールでのカスペルスキーからの告知表示に必要なデータ。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center Web コンソールで管理対象アプリケーションのプラグインが機能するために必要なデータおよび日常の作業中に管理サーバーのデータベースにプラグインによって保存されるデータ。データの説明および提供方法については、対応するアプリケーションのヘルプファイルで説明されています。

- Kaspersky Security Center Web コンソールのユーザー設定：ローカリゼーション言語とインターフェイスのテーマ、監視パネルの表示設定、通知のステータスに関する情報（確認済みまたは未確認）、スプレッドシートの列のステータス（表示または非表示）、トレーニングモードの進捗状況。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- 管理対象デバイスから Kaspersky Security Center Linux コンポーネントへのセキュアな接続を確立するための証明書。ユーザーは管理サーバーの klsetsrvcert ユーティリティを使用してデータを入力および送信します。

- 組織の内部 Web リソースへの信頼を確立するための証明書。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- ユーザーが同意したカスペルスキーの法的条項に関する情報。

- ユーザーが Kaspersky Security Center Web コンソールまたはプログラムインターフェイス Kaspersky Security Center OpenAPI に入力する管理サーバーのデータ。

- ユーザーが Kaspersky Security Center Web コンソールで入力したあらゆるデータ。

上記のデータは、次の方法のいずれかが適用された場合に Kaspersky Security Center にLinux 表示される場合があります：

- ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- ネットワークエージェントが自動的にデータをデバイスから受信して、管理サーバーに送信します。

- ネットワークエージェントが、管理対象のカスペルスキー製品によって取得されたデータを受信して、管理サーバーに送信する。管理対象のカスペルスキー製品によって処理されるデータ一覧については、該当する製品のヘルプファイルに記載されています。

- 管理サーバーは、ネットワークに接続されたデバイスに関する情報を独自に取得するか、ディストリビューションポイントとして機能するように割り当てられたネットワークエージェントからデータを受信します。
- iOS MDM プロトコルまたはモバイルプロトコルを使用して、データがモバイルデバイスから管理サーバーに送信されます。

これらのデータは管理サーバーのデータベースに保存されます。ユーザー名とパスワードは暗号化された形式で保存されます。

ローカルで処理されたデータはすべて、ダンプファイル、トレースファイル、または Kaspersky Security Center Linux のコンポーネントのログファイル（インストーラーやユーティリティによって作成されたログファイルを含む）としてのみカスペルスキーに送信されます。

Kaspersky Security Center Linux コンポーネントのダンプファイル、トレースファイル、またはログファイルには、管理サーバー、ネットワークエージェント、および Kaspersky Security Center Web コンソールの任意のデータが含まれています。これらのファイルには、個人情報などの機密情報が含まれていることがあります。ダンプファイル、トレースファイル、ログファイルは、暗号化された形式でデバイスに保存されます。ダンプファイル、トレースファイル、ログファイルはカスペルスキーに自動では転送されませんが、管理者はテクニカルサポートからの要求に応じてこれらのファイルを手動でカスペルスキーに転送し、 Kaspersky Security Center Linux のパフォーマンスに関する問題を解決することができます。

カスペルスキーは、受け取ったすべての情報を法律およびカスペルスキーの内規に基づいて保護します。データはセキュアな接続で送信されます。

管理コンソールまたは Kaspersky Security Center Web コンソールのリンクを使用することで、ユーザーは次のデータが自動的に送信されることに同意したものとします：

- Kaspersky Security Center Linux のコード
- Kaspersky Security Center Linux のバージョン
- Kaspersky Security Center Linux の言語
- ライセンス識別子
- ライセンス種別
- ライセンスが代理店経由で購入されたかどうか

リンクの目的や位置によってリンク経由で提供されたデータのリスト。

カスペルスキーでは、取得したデータはすべて匿名形式で、また一般的な統計情報としてのみ使用します。統計情報のサマリーが最初に取得した情報から自動的に生成されますが、そのサマリーには個人情報などの機密情報は含まれていません。新しい情報が蓄積された後、以前のデータは即座に破棄されます（年に1回）。統計情報のサマリーは、無期限に保管されます。

# 定額制サービスについて

*Kaspersky Security Center Linux の定額制サービス*とは、選択した設定（有効期限、保護されるデバイスの台数）でのアプリケーションの使用を注文することです。Kaspersky Security Center Linux の定額制サービスをサービスプロバイダー（インターネットプロバイダーなど）に登録できます。定額制サービスは手動および自動で更新することができ、キャンセルすることもできます。

定額制サービスの期間は制限する（1年間など）ことも、無制限にすることもできます。制限された定額制サービスの期限を過ぎてKaspersky Security Centerを利用するには、更新する必要があります。サービスプロバイダーによって期限までに支払いが行われた場合、無制限の定額制サービスは自動的に更新されます。

制限された定額制サービスの期限が過ぎた場合は、更新するまでの猶予期間が与えられ、その期間はアプリケーションが機能し続けます。猶予期間の長さや利用できる機能はサービスプロバイダーによって定義されます。

Kaspersky Security Center Linuxを定額制サービスの形式で利用するには、サービスプロバイダーが提供するアクティベーションコードを適用する必要があります。

異なるKaspersky Security Center Linuxのアクティベーションコードを適用できるのは、定額制サービスの期限の経過後か、定額制サービスをキャンセルした時のみです。

サービスプロバイダーによっては、定額制サービスの管理に伴う操作が異なる可能性があります。サービスプロバイダーが定額制サービスの更新のための猶予期間を設定しないこともあり、その場合はアプリケーションを利用できなくなります。

定額制サービスの形式で利用する目的で購入されたアクティベーションコードでKaspersky Security Centerの旧バージョンをアクティベートすることはできません。

定額制サービスのもとアプリケーションを使用している場合、Kaspersky Security Center Linuxは、定額制サービスの有効期間が切れるまで、指定された間隔でアクティベーションサーバーへの接続を自動的に試みます。システムDNSを使用したサーバーへのアクセスが不可能な場合は、パブリックDNSサーバーが使用されます。定額制サービスは、サービスプロバイダーのWebサイトで更新することができます。

# Kaspersky Security Center Linuxのアクティベーション

追加機能を使用するには、Kaspersky Security Center Linuxをアクティベートします。このタスクを実行するには、管理サーバーのクイックスタートウィザードを使用することと管理サーバーのプロパティを使用することの2つの方法があります。

*Kaspersky Security Center Linuxをアクティベートするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ライセンス**］セクションを選択します。
3. ［**現在のライセンス**］で、［**選択**］をクリックします。
4. 開いたウィンドウで、Kaspersky Security Center Linuxのアクティベーションに使用するライセンスを選択します。ライセンスがリストにない場合は、［**新しいライセンスを追加**］をクリックし、新しいライセンスを指定します。
5. 必要に応じて、予備のライセンスを追加することもできます。これを行うには、［**予備のライセンス**］で［**選択**］をクリックし、既存のライセンスを選択するか、新しいライセンスを追加します。現在のライセンスがない場合は、予備のライセンスを追加できないことに注意してください。
6. ［**保存**］をクリックします。

# 管理されたカスペルスキー製品のライセンス

このセクションでは、管理対象のカスペルスキー製品のライセンスを Kaspersky Security Center で操作する方法について説明します。

Kaspersky Security Center Linux では、クライアントデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

Kaspersky Security Center でライセンスを追加すると、ライセンスの設定が管理サーバーで保存されます。アプリケーションでは、この情報に基づいて、ライセンス使用レポートを生成し、ライセンスの有効期限と、ライセンスのプロパティで設定されるライセンスの制限事項の違反について管理者に通知します。ライセンス使用の通知の設定は管理サーバーで設定できます。

# 管理対象アプリケーションのライセンスの管理

管理対象デバイスにインストールされているカスペルスキー製品には、各製品のライセンス情報ファイルまたはアクティベーションコードを適用してライセンスを付与する必要があります。ライセンス情報ファイルとアクティベーションコードは次の方法で展開できます：

- 自動配信
- 管理対象アプリケーションのインストールパッケージ
- 管理対象アプリケーションへのライセンスの追加タスク
- 管理対象アプリケーションの手動アクティベーション

上記のいずれかの方法で、新しい現在のライセンスまたは予備のライセンスを追加できます。カスペルスキー製品は、現時点で現在のライセンスを使用し、現在のライセンスの有効期限が切れた後に適用する予備のライセンスを保存します。ライセンスを追加するアプリケーションは、ライセンスが現在のライセンスか予備のライセンスかを定義します。ライセンスの定義は、新しいライセンスの追加方法には依存しません。

## 自動配信

異なる複数の管理対象アプリケーションを使用し、特定のライセンス情報ファイルまたはアクティベーションコードをデバイスに配信する必要がある場合は、他の配信方法を選択してください。

Kaspersky Security Center を使用して、使用可能なライセンスをデバイスに配信できます。ここでは、3 個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**自動配信されるライセンス**］を 3 個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Linux）が、組織内のデバイスにインストールされているとします。ライセンスを配信する必要がある新しいデバイスが検出されます。リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である 2 個のライセンス情報ファイルが、そのデバイスに配信可能であると本製品が判断します。そのうち 1 個のライセンス情報ファイルが、デバイスに配信されます。この場合、どのライセンス情報ファイルがデバイスに適用されるかは予測ができません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

ライセンスが配信されると、そのライセンスを適用中のデバイスの台数が再度計上されます。ライセンスが適用可能な台数を超えないように、適用中のデバイスの台数を確認しておく必要があります。ライセンスを適用可能な台数の上限を超えると、ライセンスが適用されていないデバイスのステータスが「緊急」になります。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- ライセンスの管理サーバーリポジトリへの追加
- ライセンスの自動配信

次の場合、自動的に配布されたライセンスが仮想管理サーバーのリポジトリに表示されない場合があることに注意してください：

- ライセンスがアプリケーションに対して有効ではありません。
- 仮想管理サーバーには管理対象デバイスがありません。
- ライセンスは別の仮想管理サーバーによって管理されているデバイスに既に使用されており、デバイス数の制限に達しています。

## ライセンス情報ファイルまたはアクティベーションコードを管理対象アプリケーションのインストールパッケージに追加

セキュリティ上の理由から、このオプションの使用は推奨されません。インストールパッケージに追加したライセンス情報ファイルまたはアクティベーションコードは、漏洩などの危険にさらされる可能性があります。

インストールパッケージを使用して管理対象アプリケーションをインストールする場合、パッケージ内またはアプリケーションのポリシー内に含まれるアクティベーションコードまたはライセンス情報ファイルを指定できます。ライセンスが管理対象デバイスに配信されるのは、デバイスと管理サーバーの次回の同期時です。

実行手順の説明：インストールパッケージへのライセンスの追加

## 管理対象アプリケーションへのライセンスの追加タスクを使用して配信

管理対象アプリケーションへのライセンスの追加タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- ライセンスの管理サーバーリポジトリへの追加
- ライセンスのクライアントデバイスへの配信

アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

インストール済みのカスペルスキー製品を、製品インターフェイス内のツールを使用してローカルでアクティベーションできます。詳しくは、インストールされているアプリケーションのヘルプを参照してください。

# ライセンスの管理サーバーリポジトリへの追加

*ライセンスを管理サーバーリポジトリに追加するには：*

1. メインメニューで、［**操作**］→［**カスペルスキーのライセンス**］の順に選択します。




追加されたカスペルスキーのライセンスのリスト

2. ［**追加**］をクリックします。

3. 目的の対象を追加します：

- **ライセンス情報ファイルの追加**

  ［**ライセンス情報ファイルの選択**］をクリックし、追加するライセンス情報ファイルを指定します。




ライセンス情報ファイルを適用してライセンスを追加する

- **アクティベーションコードの入力**

  テキストフィールドにアクティベーションコードを入力し、［**送信**］をクリックします。

4. ［**閉じる**］をクリックします。

管理サーバーのリポジトリにライセンスが追加されます。

# ライセンスのクライアントデバイスへの配信

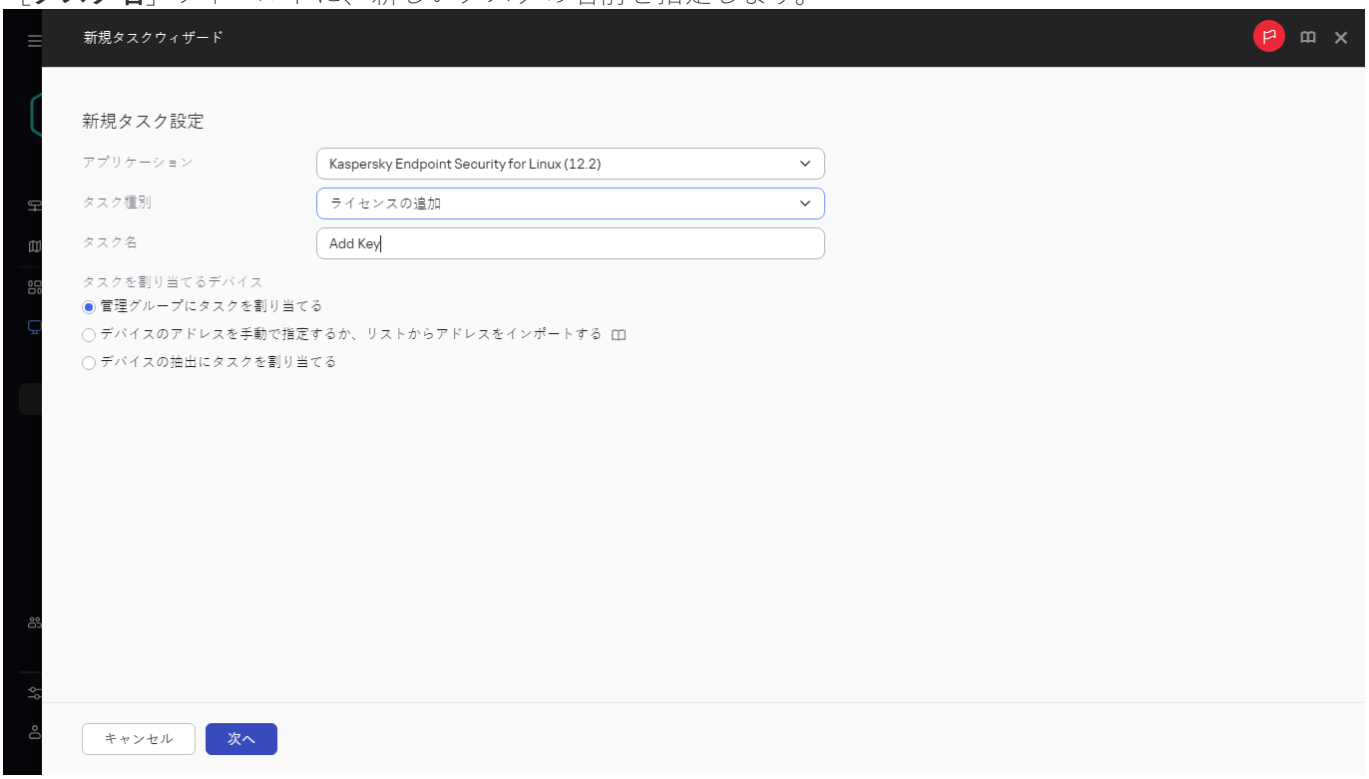
Kaspersky Security Center Web コンソールでは、ライセンスをクライアントデバイスに自動的に、または［**アプリケーションのアクティベーション**］タスクを通じて配信することができます。このタスクを使用して、特定のデバイスグループにライセンスを配信できます。タスク経由でライセンスが配信される際、デバイス数へのライセンスの制限が適用されません。自動ライセンス配信を使用すると、ライセンス制限に達した時にライセンスの配信を自動的に停止できます。

ライセンスの自動配信を有効にする場合は、そのライセンスをクライアントデバイスに配信するための［**アプリケーションのアクティベーション**］タスクを作成しないでください。そうしないと、頻繁な同期により管理サーバーの負荷が増加します。

配信前に、ライセンスを管理サーバーリポジトリに追加します。

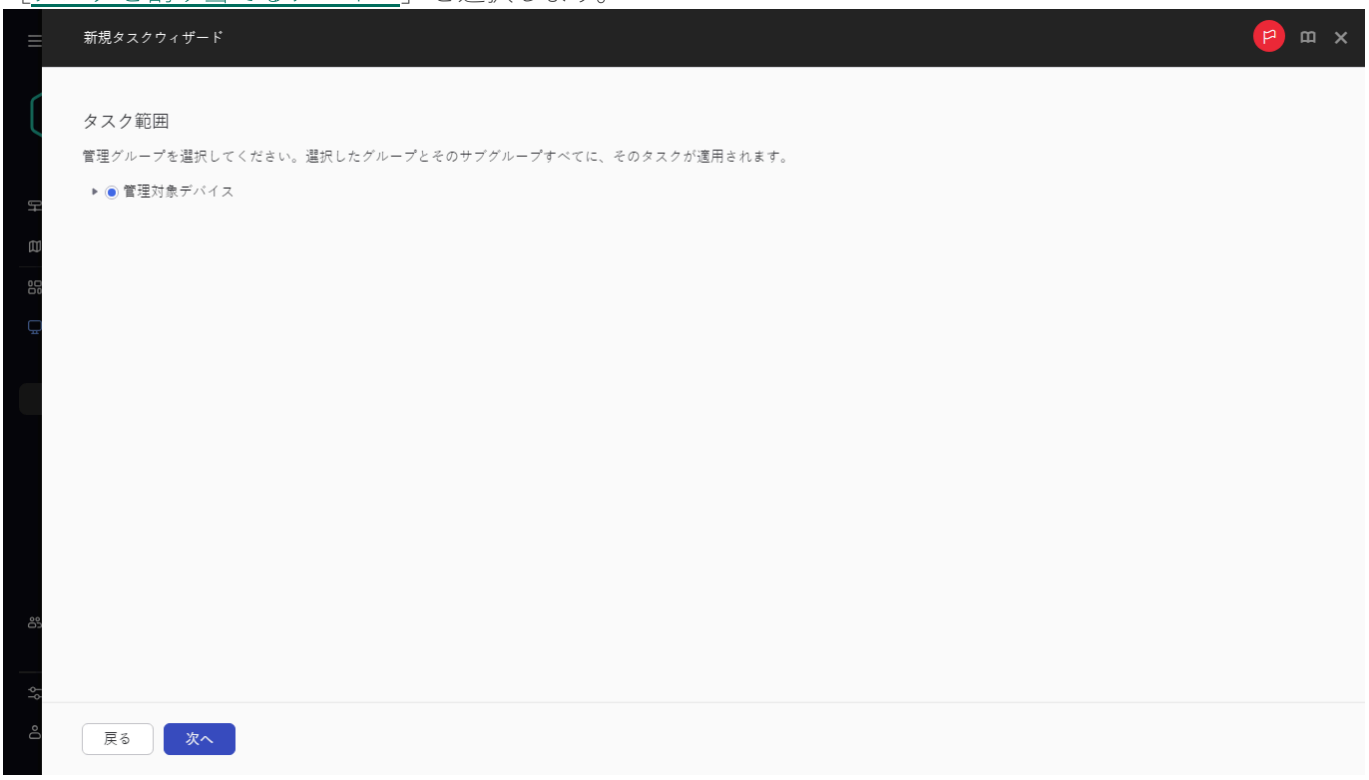
*［**アプリケーションのアクティベーション**］タスクを使用してクライアントデバイスにライセンスを配信するには、次の手順を実行します：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   **新規タスクウィザード**が起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、ライセンスを追加する製品を選択します。
4. ［**タスク種別**］リストから、［**アプリケーションのアクティベーション**］タスクを選択します。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。




ライセンスの追加タスクの作成

6. ［タスクを割り当てるデバイス］を選択します。




タスク範囲を指定します

7. ウィザードの［**ライセンス情報ファイルの選択**］手順で、［**ライセンスの追加**］リンクをクリックしてライセンスを追加します。

8. ［ライセンスの追加］ペインで、次のいずれかのオプションを使用してライセンスを追加します：

ライセンスを追加する必要があるのは、［**アプリケーションのアクティベーション**］タスクを作成する前にライセンスを管理サーバーのリポジトリに追加しなかった場合のみです。

- ［**アクティベーションコードの入力**］オプションを選択してアクティベーションコードを入力し、次の手順を実行します：

  a. アクティベーションコードを指定して［**送信**］ボタンをクリックしてください。

  ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

  b. ［**保存**］をクリックします。

  ライセンスを管理対象デバイスに自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

  ［ライセンスの追加］ペインが閉じます。

- ［**ライセンス情報ファイルの追加**］オプションを選択してライセンスファイルを追加し、次の操作を実行します：

  a. ［**ライセンス情報ファイルの選択**］ボタンをクリックします。

  b. ［ライセンス情報ファイルの選択］ウィンドウが開いたら、ライセンス情報ファイルを選択し、［**開く**］をクリックします。

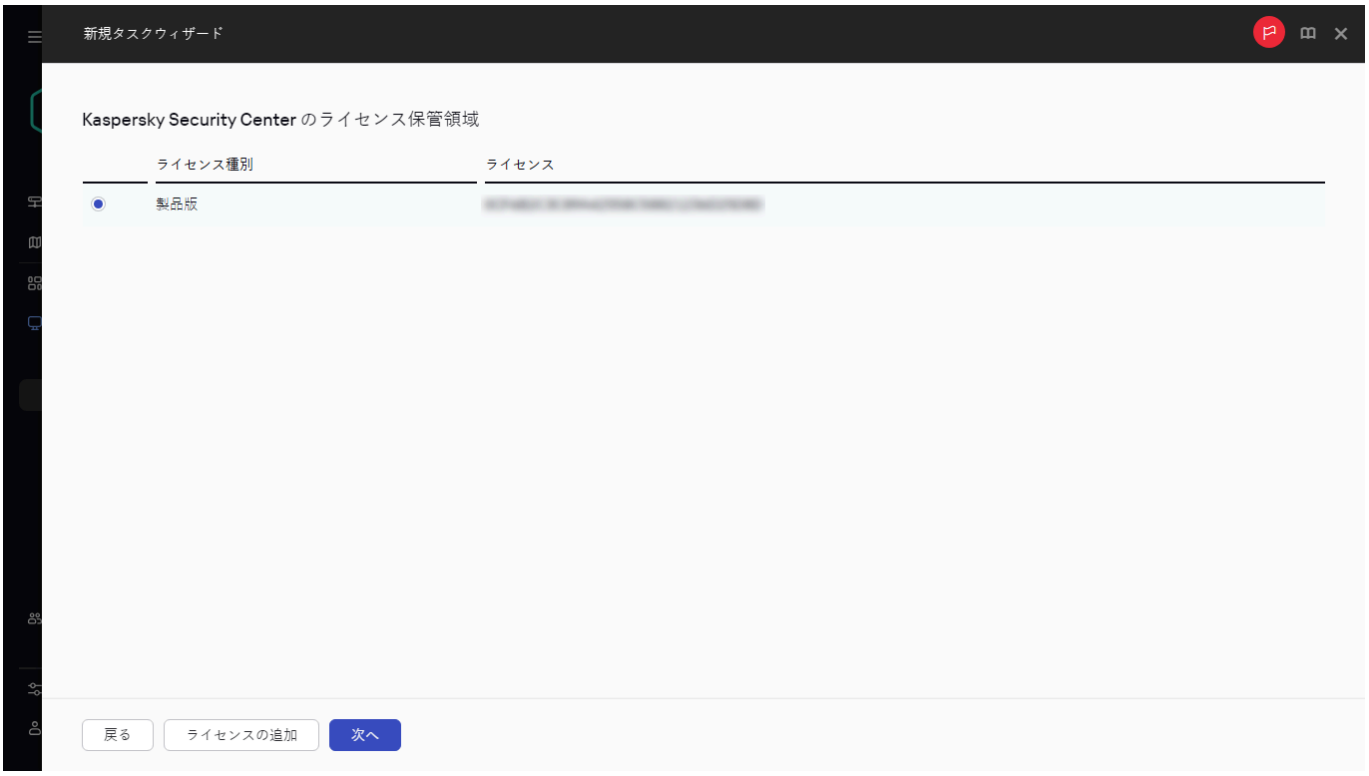
  ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

  c. ［**保存**］をクリックします。

  管理対象デバイスにライセンスを自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

  ［ライセンスの追加］ペインが閉じます。

9. ライセンスのテーブルで［ライセンス］を選択します。

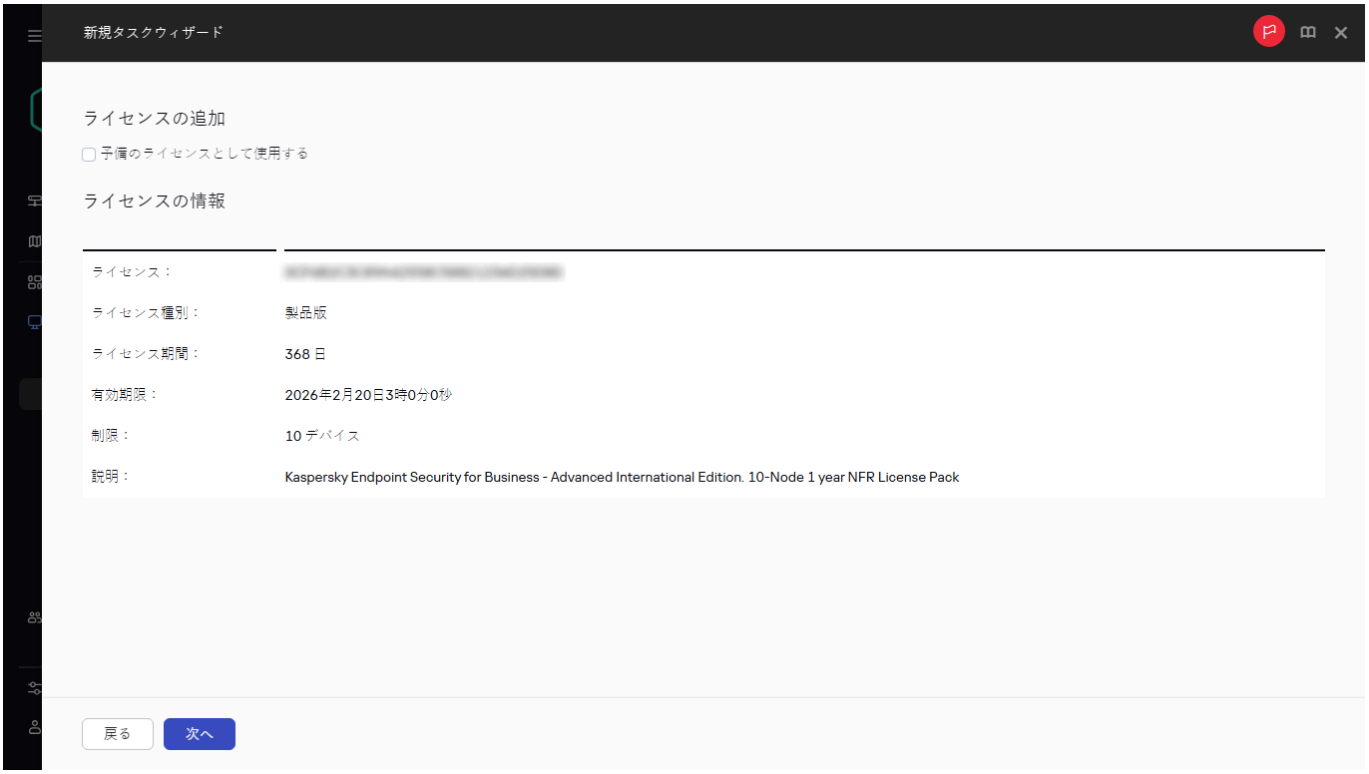



ライセンスの選択

10. ウィザードの［**ライセンス情報**］手順で、現在のライセンスを置き換える場合は、既定の［**予備のライセンスとして使用する**］をオフにします。

たとえば、組織が変更され、デバイスで別の組織のライセンスが必要な場合や、ライセンスが再発行され、新しいライセンスの有効期限が現在のライセンスよりも早く切れる場合に、これが必要になります。エラーを回避するには、［**予備のライセンスとして使用する**］をオフにする必要があります。

Kaspersky Security Center にライセンスを追加する際に発生する可能性のある問題とその解決方法の詳細については、Kaspersky Security Center ナレッジベースを参照してください。




予備のライセンスの指定

11. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。

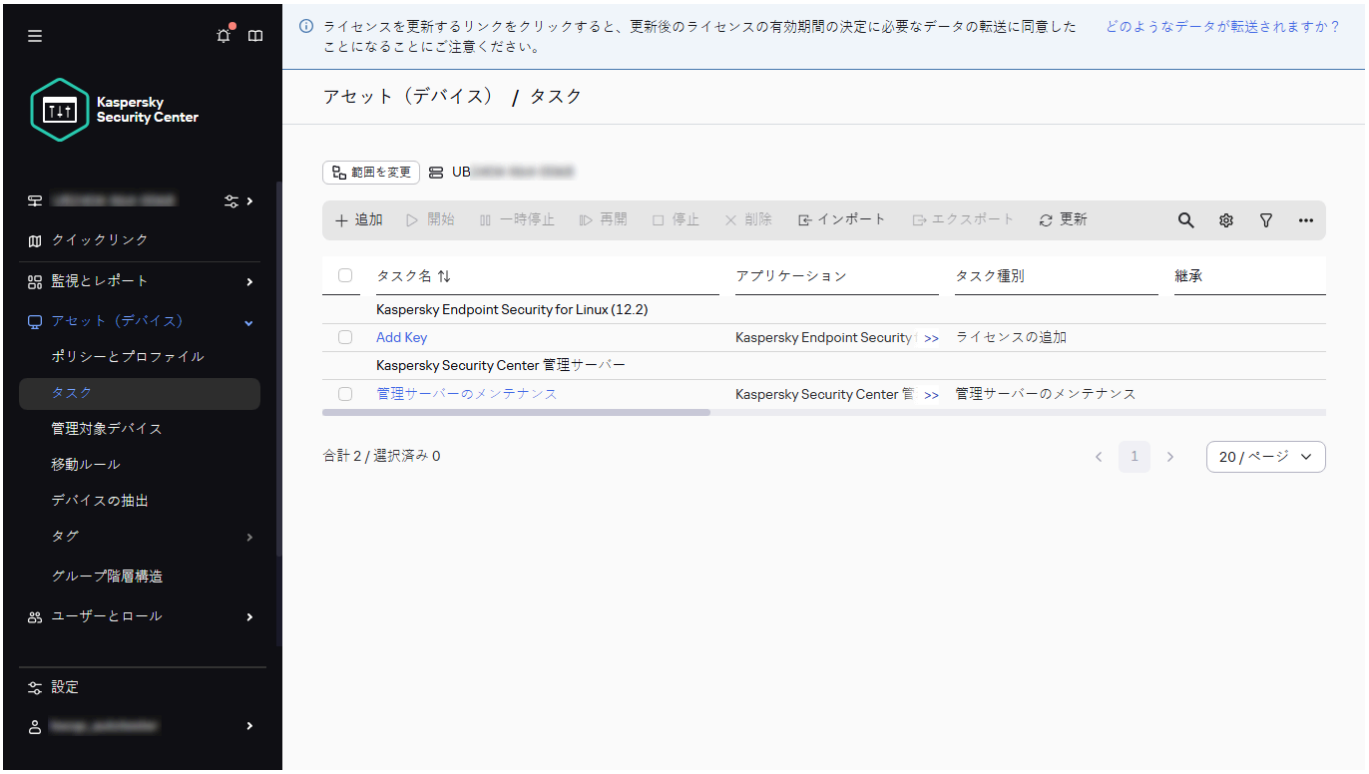
    このオプションをオンにしない場合、タスクは既定の設定で作成されます。既定の設定からの変更は、後からいつでも実行できます。

12. ［**終了**］をクリックします。

    ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

    > タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

    タスクが作成、設定され、タスクリストに表示されます。




タスクリスト

13. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。

    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、選択したデバイスにライセンスが導入されます。

# ライセンスの自動配信

Kaspersky Security Center Linux では、管理サーバーのライセンスリポジトリにあるライセンスを管理対象デバイスに自動配信できます。

*管理対象デバイスにライセンスを自動配信するには：*

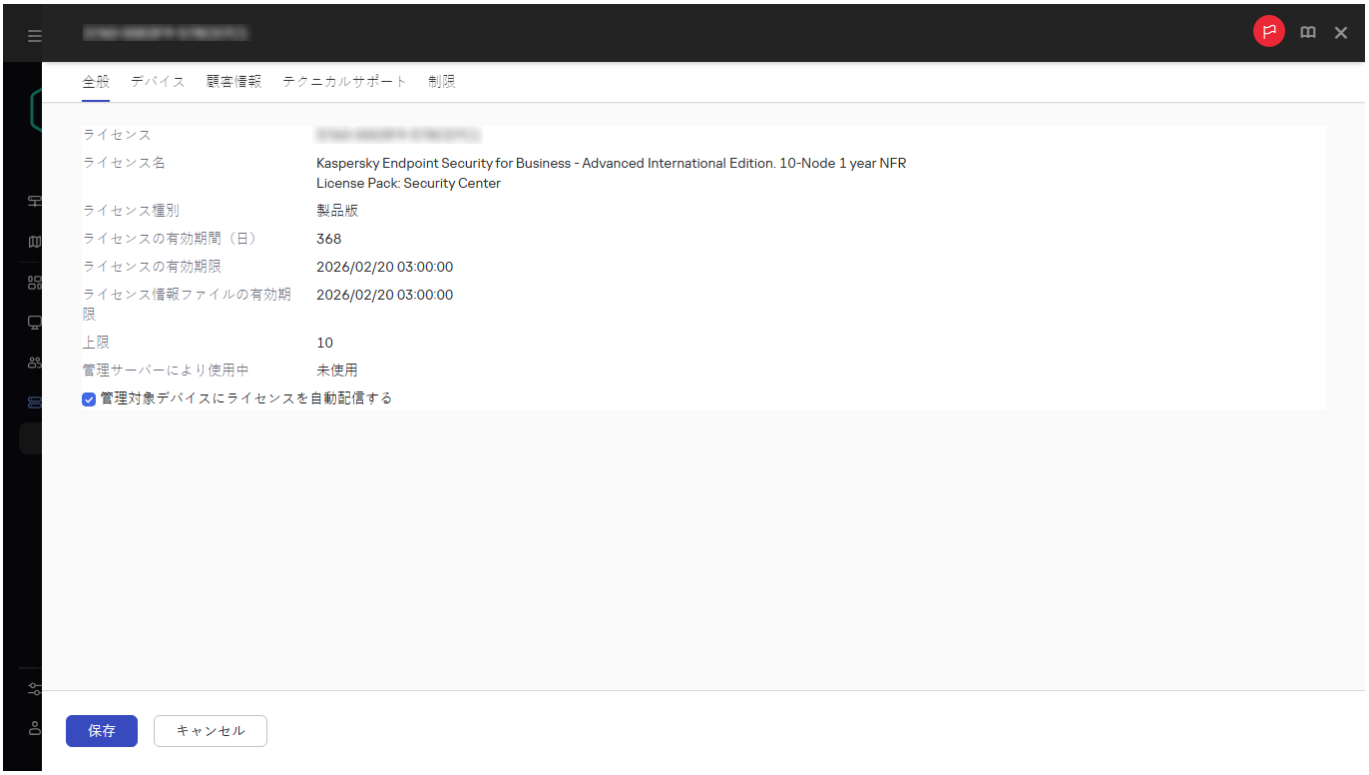
1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。




ライセンスリスト

2. デバイスに自動配信するライセンスをクリックします。

3. 表示されるライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］をオンにします。




ライセンスのプロパティウィンドウ

4. ［**保存**］をクリックします。

ライセンスは、互換性のあるすべてのデバイスに自動的に配信されます。

ライセンスはネットワークエージェント経由で配信されます。アプリケーションに対するライセンスの配信タスクは作成されません。

ライセンスが自動配信される際、デバイス数へのライセンスの制限が適用されます。ライセンスの制限は、ライセンスのプロパティで設定済みです。ライセンス数の上限に達した場合は、デバイスへの配信は自動的に停止します。

次の場合、自動的に配布されたライセンスが仮想管理サーバーのリポジトリに表示されない場合があることに注意してください：

- ライセンスがアプリケーションに対して有効ではありません。
- 仮想管理サーバーには管理対象デバイスがありません。
- ライセンスは別の仮想管理サーバーによって管理されているデバイスに既に使用されており、デバイス数の制限に達しています。

仮想管理サーバーは、そのリポジトリと管理サーバーのリポジトリからライセンスを自動的に配布します。以下を推奨します。

- *ライセンスの追加*タスクを使用して、デバイスに導入する必要があるライセンスを選択します。
- 仮想管理サーバーの設定で、［**この仮想管理サーバーからデバイスへのライセンスの自動配信を許可する**］をオフにしないでください。オフにした場合、仮想管理サーバーは、管理サーバーリポジトリからのライセンスを含め、ライセンスをデバイスに配布しません。

ライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］がオンになっている場合、ライセンスキーはネットワークにすぐに配布されます。このオプションを選択しない場合は、タスクを使用して後でライセンスを配信することができます。

プライマリ管理サーバー上で構成されたライセンスの自動配信は、非仮想セカンダリ管理サーバーによって管理されるデバイスには適用されません。

# 使用中のライセンスに関する情報の表示

*管理サーバーのリポジトリに追加されているライセンスのリストを表示するには：*

メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

管理サーバーのリポジトリに追加されているライセンス情報ファイルとアクティベーションコードのリストが表示されます。

*ライセンスの詳細情報を表示するには：*

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. 目的のライセンスの名前をクリックします。

ライセンスのプロパティウィンドウが表示され、次の情報を確認できます：

- ［**全般**］タブ：ライセンスに関する主要な情報

- ［**デバイス**］タブ：このライセンスが、インストールされているカスペルスキー製品のアクティベーションに使用されたクライアントデバイスのリスト

*特定のクライアントデバイスにどのライセンスが追加されたかを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］タブをクリックします。
4. ライセンスの情報を確認するアプリケーションの名前をクリックします。
5. 表示されるアプリケーションのプロパティウィンドウで、［**全般**］タブを選択し、［**ライセンス**］セクションを表示します。

現在のライセンスと予備のライセンスに関する主要な情報が表示されます。

仮想管理サーバーのライセンスの最新の設定を定義するため、管理サーバーはカスペルスキーのアクティベーションサーバーに少なくとも毎日1度はリクエストを送信します。システムDNSを使用したサーバーへのアクセスが不可能な場合は、パブリックDNSサーバーが使用されます。

# ライセンス制限超過のイベント

Kaspersky Security Center Linuxには、クライアントデバイスにインストールされたカスペルスキー製品がライセンスによる制限を超過した時のイベントに関する情報が表示されます。

ライセンス管理の制限を超過した時のイベントの重要度は、次のルールに従って決定されます：

- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の90～100%である場合、重要度が「**情報**」のイベントが発生します。
- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の100～110%である場合、重要度が「**警告**」のイベントが発生します。
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

# リポジトリからのライセンスの削除

管理対象デバイスに追加済みの現在のライセンスを管理サーバーのリポジトリから削除した場合、管理対象デバイスにインストールされている製品は動作を継続します。

*管理サーバーのリポジトリからライセンス情報ファイルまたはアクティベーションコードを削除するには：*

1. 削除するライセンス情報ファイルまたはアクティベーションコードが管理サーバーで使用されていないことを確認します。管理サーバーで使用されている場合、ライセンスを削除することはできません。チェックを実行するには：

   a. メインメニューで、管理サーバーの横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

   b. ［**全般**］タブで、［**ライセンス**］セクションを選択します。

   c. 開いたセクションに必要なライセンス情報ファイルまたはアクティベーションコードが表示されている場合は、［**現在のライセンスの削除**］をクリックし、処理内容を確定します。その後、削除されたライセンスが管理サーバーで使用されることはありませんが、ライセンスは管理サーバーのリポジトリに残ります。必要なライセンス情報ファイルまたはアクティベーションコードが表示されない場合、管理サーバーはこのライセンスを使用していません。

2. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

3. 必要なライセンス情報ファイルまたはアクティベーションコードを選択し、［**削除**］をクリックします。




ライセンスリスト

選択したライセンス情報ファイルまたはアクティベーションコードが削除されます。

削除されたライセンスの再追加や、新しいライセンスの追加も可能です。

# 使用許諾契約書による同意の取り消し

一部のクライアントデバイスの保護を停止する場合、任意の管理対象カスペルスキー製品の使用許諾契約書（EULA）への同意を取り消すことができます。EULA への同意を取り消す前に、選択したアプリケーションをアンインストールする必要があります。

*管理対象のカスペルスキー製品の EULA を取り消すには：*

1. 管理サーバーのプロパティウィンドウを開き、［**全般**］タブの［**使用許諾契約書**］セクションに移動します。

   インストールパッケージの作成時、アップデートのシームレスインストール時、または Kaspersky Security for Mobile の導入時に同意した EULA のリストが表示されます。




EULA のリスト

2. リストから、同意を取り消す EULA を選択します。

   EULA の以下のプロパティを確認できます：

   - EULA に同意した日付
   - EULA に同意したユーザーの名前

3. EULA に同意した日付のうち任意のものをクリックし、次のデータが表示されるプロパティウィンドウを開きます：

   - EULA に同意したユーザーの名前
   - EULA に同意した日付
   - EULA の一意な識別子（UID）
   - EULA のテキスト
   - EULA に関連するオブジェクト、および各オブジェクトの名前と種別のリスト（インストールパッケージ、シームレスアップデート、モバイルアプリ）

4. EULA のプロパティウィンドウの下部で、［**使用許諾契約書への同意を取り消す**］をクリックします。

EULA への同意の取り消しを妨げるオブジェクト（インストールパッケージ、およびそのパッケージを使用するタスク）が存在する場合、そのオブジェクトに関する通知が表示されます。これらのオブジェクトを削除するまで、取り消しの動作を続行できません。

表示されたウィンドウで、この EULA に対応するカスペルスキー製品を最初にアンインストールすることが必要であることが示されます。

5. ボタンをクリックして取り消しを確定します。

これで EULA が取り消されました。［**使用許諾契約書** ］セクションの使用許諾契約書のリストに表示されなくなります。EULA のプロパティウィンドウが閉じ、製品がインストールされなくなります。

# カスペルスキー製品のライセンスの更新

有効期間の終了した、または有効期間がまもなく終了する（残り 30 日以内）のカスペルスキー製品のライセンスを更新できます。

*有効期間が終了した、もしくは有効期間がまもなく終了するライセンスを更新するには：*

1. 次のいずれかの手順を実行します：

- メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
- ［**監視とレポート**］→［**ダッシュボード**］の順に移動し、通知に隣接する［**有効期間がまもなく終了するライセンスを表示**］をクリックします。

［**カスペルスキーのライセンス** ］ウィンドウが表示され、ライセンスを表示および更新できます。

2. 目的のライセンスに隣接する［**ライセンスの更新**］をクリックします。

ライセンスの更新リンクをクリックすることで、お客様は Kaspersky Security Center Linux に関する次の情報をカスペルスキーに送信することに同意したものとします：バージョン、使用している言語版、本ソフトウェアのライセンス識別子（更新中のライセンスの識別子）、および本製品を販売代理店経由でライセンスを購入したかどうかの情報。

3. 表示されるライセンス更新サービスのウィンドウで、ライセンスを更新する手順に従ってください。

ライセンスが更新されました。

Kaspersky Security Center Web コンソールでは、ライセンスの有効期間の終了間近になると次のスケジュールで通知が表示されます：

- 有効期限の 30 日前
- 有効期限の 7 日前
- 有効期限の 3 日前

- 有効期限の 24 時間前
- ライセンスの有効期間が終了した時

# マーケットプレイスを使用してカスペルスキーの法人向けソリューションを選択する

［**マーケットプレイス**］はカスペルスキーのビジネスソリューションを全体的に表示できるメインメニューのセクションです。必要なものを選択してカスペルスキーの Web サイトに移動して購入プロセスに進むことができます。フィルターを使用してお客様の組織や情報セキュリティシステムの要件に一致するソリューションのみを表示することが可能です。ソリューションを選択すると、Kaspersky Security Center Linux はそのソリューションの詳細について関連する Web ページにリダイレクトします。各 Web ページで、製品の購入に進んだり、購入に関する手順を確認したりできます。

［**マーケットプレイス**］セクションでは、次の条件を使用してカスペルスキー製品をフィルターすることができます：

- 保護対象のデバイスの数（エンドポイント、サーバー、その他の種別の資産）：
  - 50～250
  - 250～1000
  - 1000 以上
- 組織の情報セキュリティチームの成熟度：
  - **基本のセキュリティ**

    このレベルは IT チームを 1 つのみ持つ企業に典型的なレベルです。脅威は、自動的に可能な最大数ブロックされます。
  - **最適なセキュリティ**

    このレベルは IT チーム内に IT セキュリティ機能を持つ特定の IT チームを持つ企業に典型的なレベルです。このレベルでは、企業はコモディティ型の脅威や既存の防御メカニズムを回避する脅威などに対応するソリューションを必要とします。
  - **高度なセキュリティ**

    このレベルは複雑で分散化された IT 環境を持つ機能に典型的なレベルです。IT セキュリティチームの熟練度が高い、または企業が SOC（セキュリティオペレーションセンター）チームを持っているなどのレベルです。必要とされるソリューションは、複雑な脅威および標的型攻撃に対応するものです。
- 保護対象の資産の種別：
  - **エンドポイント**：物理および仮想マシン、埋め込みシステムなどの社員のワークステーション
  - **サーバー**：物理および仮想サーバー
  - **クラウド**：パブリック、プライベート、またはハイブリッドのクラウド環境およびクラウドサービス
  - **ネットワーク**：ローカルエリアネットワーク、IT インフラストラクチャ
  - **サービス**：カスペルスキーによって提供されるセキュリティ関連のサービス

*カスペルスキーのビジネスソリューションを検索および購入するには：*

1. メインメニューで、［**マーケットプレイス**］に移動します。

   既定では、セクションにはすべての使用可能なカスペルスキーのビジネスソリューションが表示されています。

2. 企業に合ったソリューションのみを表示するには、フィルターで必要な値を選択します。

3. 購入する、もしくは詳細を確認したいソリューションをクリックします。

   ソリューションの Web ページにリダイレクトされます。画面上の説明に従って、購入プロセスを進められます。

# カスペルスキー製品の設定

このセクションには、ポリシーとタスクの手動設定、ユーザーロール、管理グループの構造とタスクの階層構造の構築に関する情報を記載しています。

# シナリオ：ネットワーク保護の設定

クイックスタートウィザードにより、既定の設定でポリシーとタスクが作成されます。これらの設定は、組織のルールなどに照らして最適でない、または許容できない内容を含む可能性があります。したがって、これらのポリシーとタスクを微調整し、ネットワークに必要であれば他のポリシーとタスクを作成することを推奨します。

## 必須条件

導入を開始する前に、次が完了していることを確認してください：

- Kaspersky Security Center Linux 管理サーバーのインストール
- Kaspersky Security Center Web コンソールのインストール
- Kaspersky Security Center Linux の主要なインストールシナリオ
- クイックスタートウィザードを完了済みまたは［**管理対象デバイス**］管理グループで以下のポリシーとタスクを手動で作成済み：
  - Kaspersky Endpoint Security のポリシー
  - Kaspersky Endpoint Security をアップデートするグループタスク
  - ネットワークエージェントのポリシー
  - *脆弱性とアプリケーションのアップデートの検索タスク*

## 実行するステップ

ネットワーク保護の設定は、次の手順で進みます：

1. **カスペルスキー製品のポリシーとポリシーのプロファイルの設定と各デバイスへの反映**

   管理対象デバイスにインストールされているカスペルスキー製品のポリシーとポリシーのプロファイルを設定しデバイスに反映するには、デバイスベースとユーザーベースの 2 種類のセキュリティ管理方法を使用できます。これら 2 つの管理方法を組み合わせて使用できます。

2. **カスペルスキー製品のリモート管理用のタスクの設定**

   必要に応じて、クイックスタートウィザードを使用して作成したタスクを確認、調整します。

   手順：Kaspersky Endpoint Security をアップデートするためのグループタスクの設定、脆弱性とアプリケーションのアップデートの検索タスクの作成。

必要に応じて、クライアントデバイスにインストールされているカスペルスキー製品を管理するためのタスクを追加で作成します。

3. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中に発生したイベントに関する情報は、クライアントデバイスから送信され、管理サーバー定義データベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：イベントの最大数の設定

## 結果

この手順を完了すると、カスペルスキー製品、タスク、管理サーバーで取得されるイベントの設定によってネットワークの保護が機能するようになります。

- ポリシーとポリシーのプロファイルに従ってカスペルスキー製品が設定されます。
- 製品が一連のタスクによって管理されるようになります。
- データベースに保存されるイベント数の上限が設定されます。

ネットワーク保護の設定が完了すると、［定義データベースとカスペルスキー製品の定期アップデートの設定］手順に進むことができます。

# デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要

セキュリティ設定を、デバイスの仕様の観点やユーザーロールの観点から管理できます。1つ目のアプローチは*デバイスベースのセキュリティ管理*、2つ目のアプローチは*ユーザーベースのセキュリティ管理*と呼ばれます。異なるデバイスに異なるアプリケーション設定を適用するには、いずれかの管理方法あるいは両者を組み合わせた管理方法を使用できます。

デバイスベースのセキュリティ管理では、デバイスごとの状況などに合わせて、セキュリティ製品について複数の異なる設定を管理対象デバイスに適用できます。たとえば、異なる管理グループに属するデバイスに、異なる設定を適用できます。

ユーザーベースのセキュリティ管理を使用すると、ユーザーロールに応じて、異なるセキュリティ設定を適用できます。複数のユーザーロールを作成し、ユーザーごとに適切なユーザーロールを割り当てた上で、デバイスの所有者のユーザーロールに応じて、異なるセキュリティ設定をデバイスに適用できます。たとえば、経理部門の従業員と人事部門の従業員それぞれのデバイスに異なるアプリケーション設定を適用する場合などがありえます。これにより、ユーザーベースのセキュリティ管理を実施すると、経理部門の従業員と人事部門の従業員のカスペルスキー製品に対して、それぞれ独自の設定が適用されます。詳細設定により、製品設定のどの部分をユーザー側で設定でき、どの部分は管理者による設定が強制的に適用されるかを指定できます。

ユーザーベースのセキュリティ管理を使用すると、個々のユーザーに特定のアプリケーション設定を適用できます。該当する従業員が社内で固有のロールを担っていたり、特定のユーザーのデバイスに関連したセキュリティ問題を監視したい場合などに、こうした処理が必要になることがあります。社内でのこの従業員のロールに基づいて、ユーザーが製品設定を変更できる権限を拡張したり制限できます。たとえば、ローカルオフィスのクライアントデバイスを管理しているシステム管理者の権限を拡張する場合などです。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を組み合わせることもできます。たとえば、管理グループごとに製品ポリシーを設定した上で、企業内の1つ以上のユーザーロールを対象としたポリシープロファイルを作成するなどの方法を使用できます。この場合、ポリシーとポリシープロファイルは次の順序で適用されます。

1. デバイスベースのセキュリティ管理用に作成されたポリシーが適用されます。
2. ポリシーは、ポリシープロファイルの優先度に応じてポリシープロファイルで変更されます。
3. ポリシーは、ユーザーロールと関連付けられたポリシープロファイルで変更されます。

# ポリシーの設定と継承先への反映：デバイスベースの管理

この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

## 必須条件

手順を開始する前に、Kaspersky Security Center Linux 管理サーバーのインストールと Kaspersky Security Center Web コンソールのインストールが完了していることを確認してください。また、デバイスベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてユーザーベースのセキュリティ管理も検討すると有益な場合があります。2種類の管理方法について詳しくは、こちらのページを参照してください。

## 実行するステップ

カスペルスキー製品のデバイスベースの管理シナリオは、次の2つの手順からなります。

**1 製品ポリシーの設定**

管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center Linux は次のアプリケーションの既定のポリシーを作成します：

- Kaspersky Endpoint Security for Linux - Linux ベースのクライアントデバイス用
- Kaspersky Endpoint Security for Windows - Windows ベースのクライアントデバイス用

このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。

複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

実行手順の説明：ポリシーの作成

**2 ポリシーのプロファイルの作成（任意）**

同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合には、ポリシーのプロファイルを作成します。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。

プロファイルの有効化条件を使用することで、たとえば、特定のハードウェア設定のデバイス、特定のタグが付与されているデバイスなどの条件に応じて異なるポリシープロファイルを適用できます。タグを使用すると特定の基準を満たすデバイスをフィルタリングできます。たとえば、「*CentOS*」というタグを作成し、CentOS オペレーティングシステムを実行しているデバイスすべてにこのタグを付与し、ポリシープロファイルの有効化条件としてこのタグを指定します。これにより、CentOS を実行しているすべてのデバイスにインストールされているカスペルスキー製品は該当するポリシープロファイルで管理されます。

実行手順の説明：

- ポリシーのプロファイルの作成
- ポリシーのプロファイルの有効化ルールの作成

3. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

既定では、管理サーバーは 15 分ごとに管理対象デバイスと自動的に同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center Linux では、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：強制同期

## 結果

デバイスベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

管理グループに新しく追加されたデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

# ポリシーの設定と継承先への反映：ユーザーベースの管理

このセクションでは、管理対象デバイスにインストールされているカスペルスキー製品の設定をユーザーベースで一元的に行う手順について説明します。この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

## 必須条件

手順を開始する前に、Kaspersky Security Center Linux 管理サーバーのインストールと Kaspersky Security Center Web コンソールのインストールが正常に完了しており、さらに主要な導入シナリオが完了していることを確認してください。また、ユーザーベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法として デバイスベースのセキュリティ管理も検討すると有益な場合があります。2 種類の管理方法について詳しくは、こちらのページを参照してください。

## プロセス

カスペルスキー製品のユーザーベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center Linux は Kaspersky Endpoint Security の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。

   複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **デバイスの所有者の指定**

   管理対象デバイスを対応するユーザーに割り当てます。

   実行手順の説明：デバイスの所有者ユーザーの指定

3. **組織内の主なユーザーロールの定義**

   組織内の従業員が行う様々な業務の主要なものを検討します。すべての従業員がロールに従って振り分けられるようにする必要があります。たとえば、所属部門、職務内容、役職などで振り分けを行うことができます。この検討が完了したら、各グループに対応するユーザーロールを作成する必要があります。各ユーザーロールには、そのロールに固有の製品設定を含む独自のポリシープロファイルが割り当てられることを念頭において作業してください。

4. **ユーザーロールの作成**

   前の手順で定義した従業員のグループごとにユーザーロールの作成と設定を行うか、あるいは事前定義されたユーザーロールを使用します。ユーザーロールには製品の各機能に対するアクセス権限が組み合わされたかたちで付与されます。

   実行手順の説明：ユーザーロールの作成

5. **各ユーザーロールの対象範囲の指定**

   作成したユーザーロールごとに、ロールを割り当てるユーザーやセキュリティグループ、管理グループを指定します。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

   実行手順の説明：各ユーザーロールの対象範囲の編集

6. **ポリシーのプロファイルの作成**

   組織内のユーザーロールごとに、ポリシープロファイルを作成します。ポリシープロファイルによって、ユーザーのデバイスにインストールされている製品にユーザーロールに応じてどの設定が適用されるかが定義されます。

   実行手順の説明：ポリシープロファイルの作成

7. **ポリシープロファイルとユーザーロールの関連付け**

作成したポリシープロファイルをユーザーロールに関連付けます。完了すると、指定されたロールを割り当てられたユーザーに対してポリシープロファイルが有効になります。ユーザーのデバイスにインストールされているカスペルスキー製品に、ポリシープロファイルで指定した設定が適用されます。

実行手順の説明：ポリシーのプロファイルとロールの関連付け

8 **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

既定では、Kaspersky Security Center Linux 管理サーバーと管理対象デバイスは 15 分ごとに同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center Linux では、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：強制同期

## 結果

ユーザーベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

新規ユーザーに対しては、新しいアカウントを作成して作成済みのユーザーロールのいずれかを割り当て、デバイスをユーザーに割り当てる必要があります。このユーザーのデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

# ポリシーとポリシーのプロファイル

Kaspersky Security Center Web コンソールを使用して、カスペルスキー製品のポリシーを作成できます。このセクションでは、ポリシーおよびポリシーのプロファイルの概要、作成方法、編集方法を説明しています。

# ポリシーとポリシープロファイルについて

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに 1 つのポリシーを提供します。ポリシーは次のいずれかのステータスを持ちます：

ポリシーのステータス

| ステータス | 説明 |
| --- | --- |
| アクティブ | 現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは 1 つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。 |
| 非アクティブ | 現在デバイスに適用されていないポリシー。 |
| モバイルユーザー | このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。 |

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

# 「ロック」属性とロックされた設定の概要

各ポリシー設定には、ロックのアイコン（🔒）があります。次の表は、ロックのステータスを示しています。

ロックのステータス

| ステータス | 説明 |
| --- | --- |
| 編集を許可 | 設定の横に開いたロックが表示され、切り替えスイッチが無効になっている場合、その設定はポリシーで指定されていません。ユーザーは管理対象アプリケーションのインターフェイスを使用してこれらの設定を変更できます。このような設定を「*ロック解除*」と呼びます。 |
| 強制適用 | 設定の横に閉じたロックが表示され、切り替えスイッチが有効になっている場合、その設定はポリシーが適用されるデバイスに適用されます。ユーザーは、管理対象アプリケーションのインターフェイスでこれらの設定の値を変更することはできません。このような設定を「*ロック*」と呼びます。 |

管理対象デバイスに適用するポリシー設定のロックを閉じておくことを強く推奨します。ロックが解除されたポリシー設定は、管理対象デバイスのカスペルスキーのアプリケーション設定によって再度割り当てられます。

ロックを使用して、次の操作を実行します：

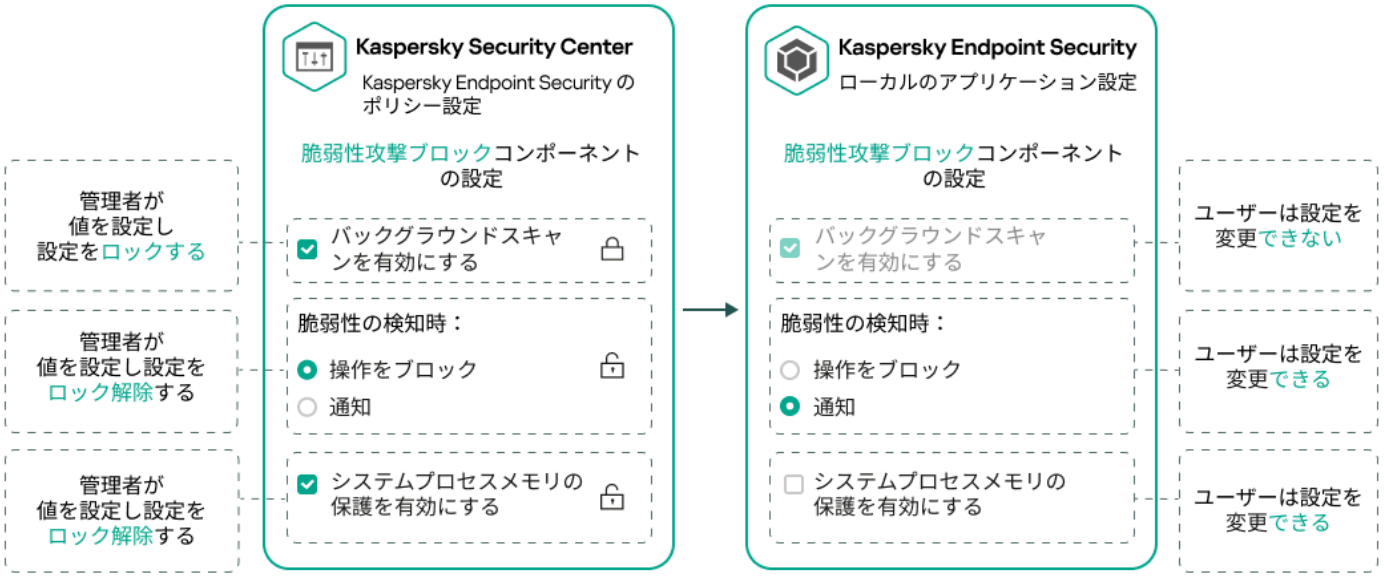
- 管理サブグループのポリシーの設定をロックする
- 管理対象デバイス上のカスペルスキー製品の設定をロックする

したがって、ロックされた設定は、有効な設定を管理対象デバイスに実装するために使用されます。

有効な設定の実装プロセスには、次の操作が含まれます：

- 管理対象デバイスが、カスペルスキー製品の設定値を適用する
- 管理対象デバイスが、ポリシーのロックされた設定の値を適用する

ポリシーおよび管理対象のカスペルスキー製品には、同じ設定内容が含まれています。ポリシー設定を構成すると、管理対象デバイスでカスペルスキー製品設定値が変更されます。管理対象デバイスのロックされた設定をユーザーが調整することはできません（下図を参照）：




ロックとカスペルスキー製品の設定

# ポリシーとポリシーのプロファイルの継承

このセクションでは、ポリシーとポリシープロファイルの階層と継承について説明します。

## ポリシーの階層

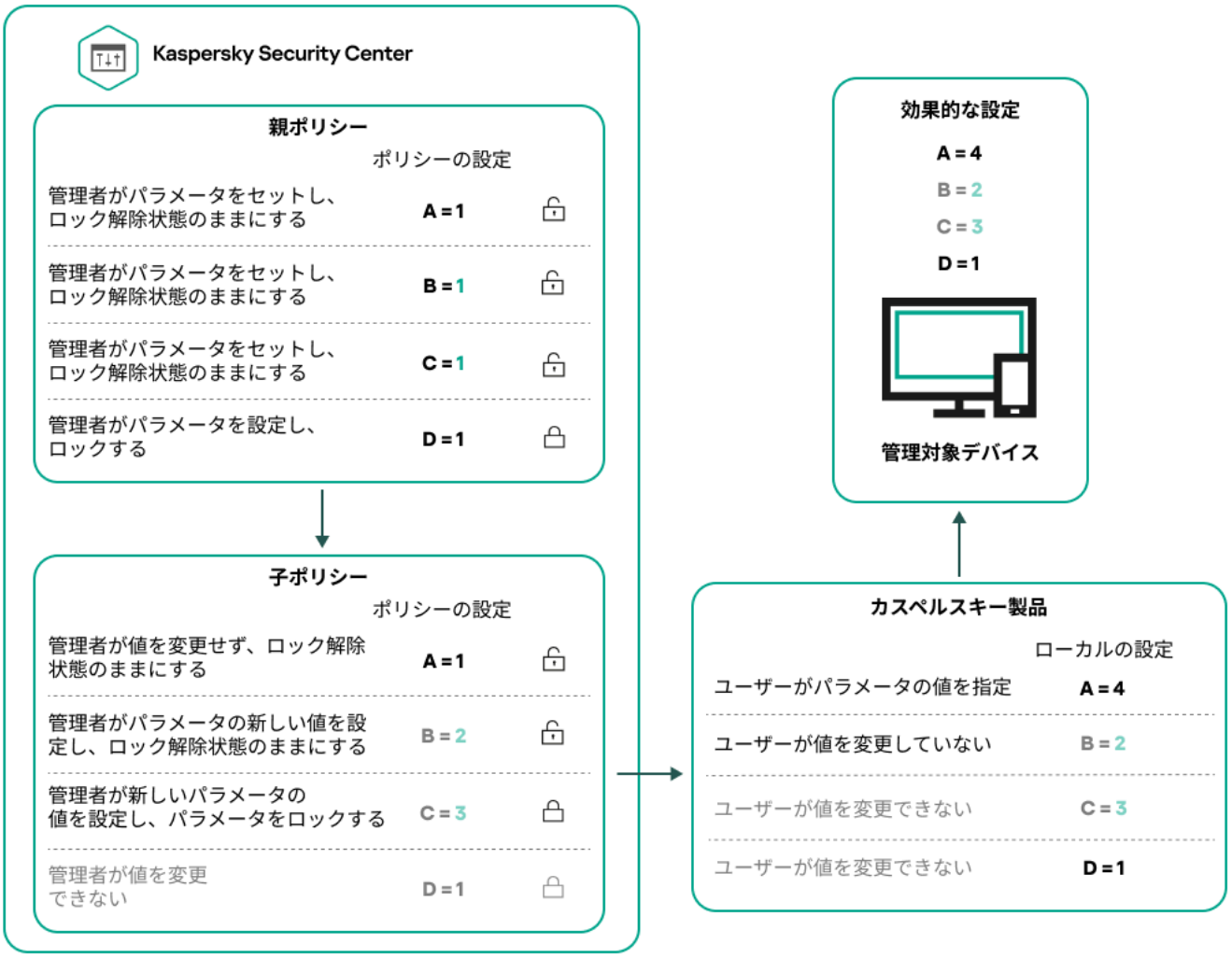
デバイスごとに異なる設定が必要な場合は、デバイスを管理グループに整理できます。

単一の管理グループにポリシーを1つ指定できます。ポリシー設定は*継承*できます。継承とは、上位（親）の管理グループのポリシーからサブグループ（子グループ）にポリシー設定値を受け取ることを意味します。

以降の説明では、親グループで設定されているポリシーを「*親ポリシー*」と表記する場合があります。サブグループ（子グループ）のポリシーを「*子ポリシー*」と表記する場合があります。

既定では、管理サーバーには少なくとも1つの管理対象デバイスグループが存在します。カスタムグループを作成する場合、それらは管理対象デバイスグループ内のサブグループ（子グループ）として作成されます。

同じアプリケーションのポリシーは、管理グループの階層に従って互いに影響を与えます。上位（親）管理グループのポリシーのロック済みの設定は、サブグループのポリシー設定値を再割り当てします（下の図を参照）。

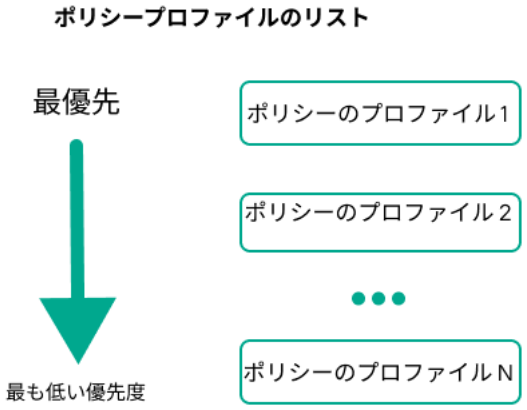



ポリシーの階層

# ポリシーの階層内のポリシープロファイル

ポリシープロファイルでの優先順位の割り当て条件は次の通りです：

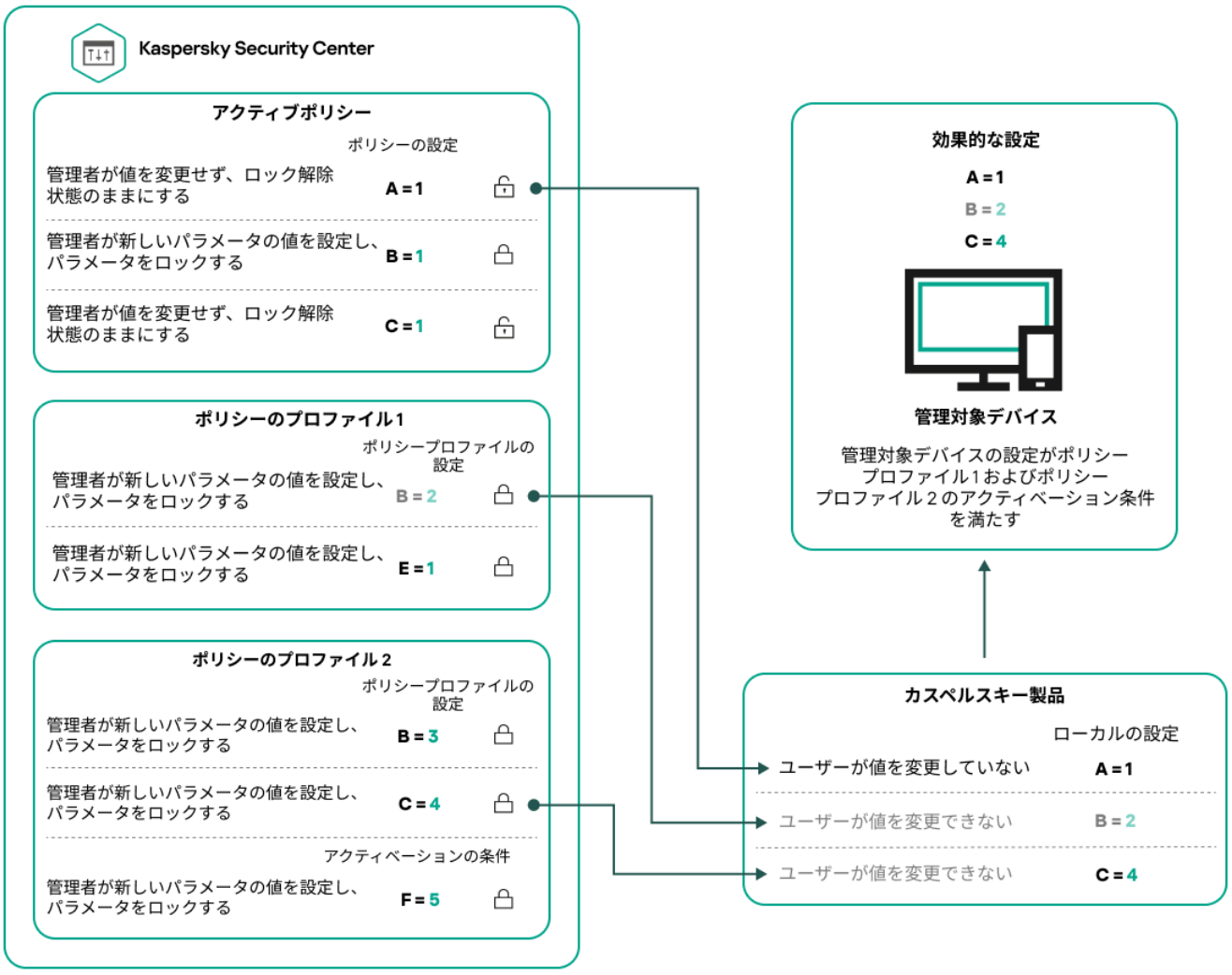
- ポリシープロファイルリスト内のプロファイルの位置は、そのプロファイルの優先度を示します。ポリシーのプロファイルの優先順位を変更できます。リストの一番上にある場合、優先順位が最も高くなります（下の図を参照）。




ポリシープロファイルの優先度の定義

- ポリシープロファイルの有効化条件は相互に依存しません。複数のポリシープロファイルを同時に有効化できます。複数のポリシープロファイルが同じ設定に影響を与える場合、デバイスは最も優先度の高いポリシ

ープロファイルから設定値を取得します（下の図を参照）。

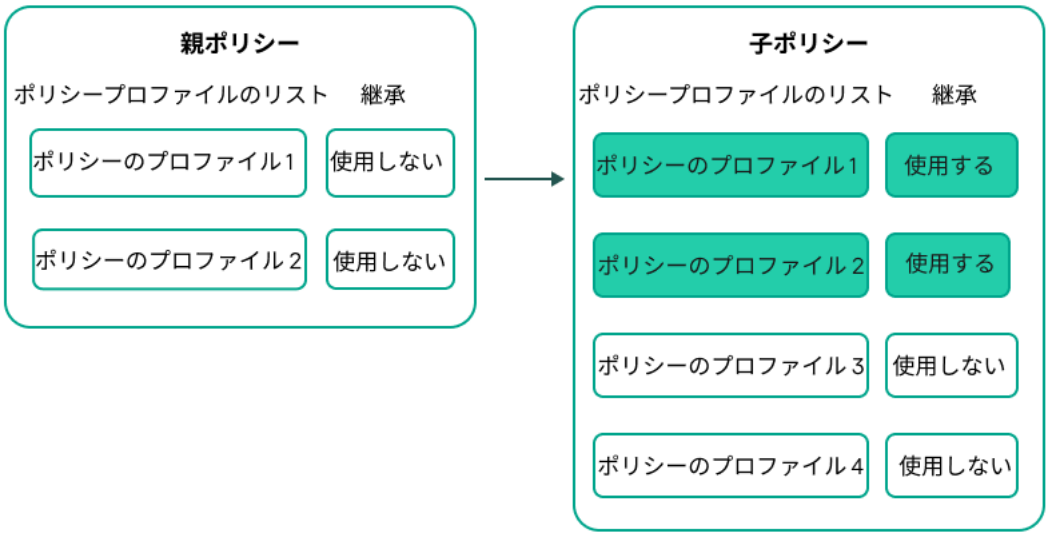



管理対象デバイスの構成が、複数のポリシープロファイルの有効化条件を満たしている

## 継承の階層におけるポリシープロファイル

様々な階層レベルにあるポリシーのポリシープロファイルは、次の条件を満たします：

- 下位のポリシーは、上位のポリシーからポリシープロファイルを継承します。上位のポリシーから継承されたポリシープロファイルは、元のポリシープロファイルのレベルよりも優先度が高くなります。
- 継承されたポリシープロファイルの優先度を変更することはできません（下の図を参照）。

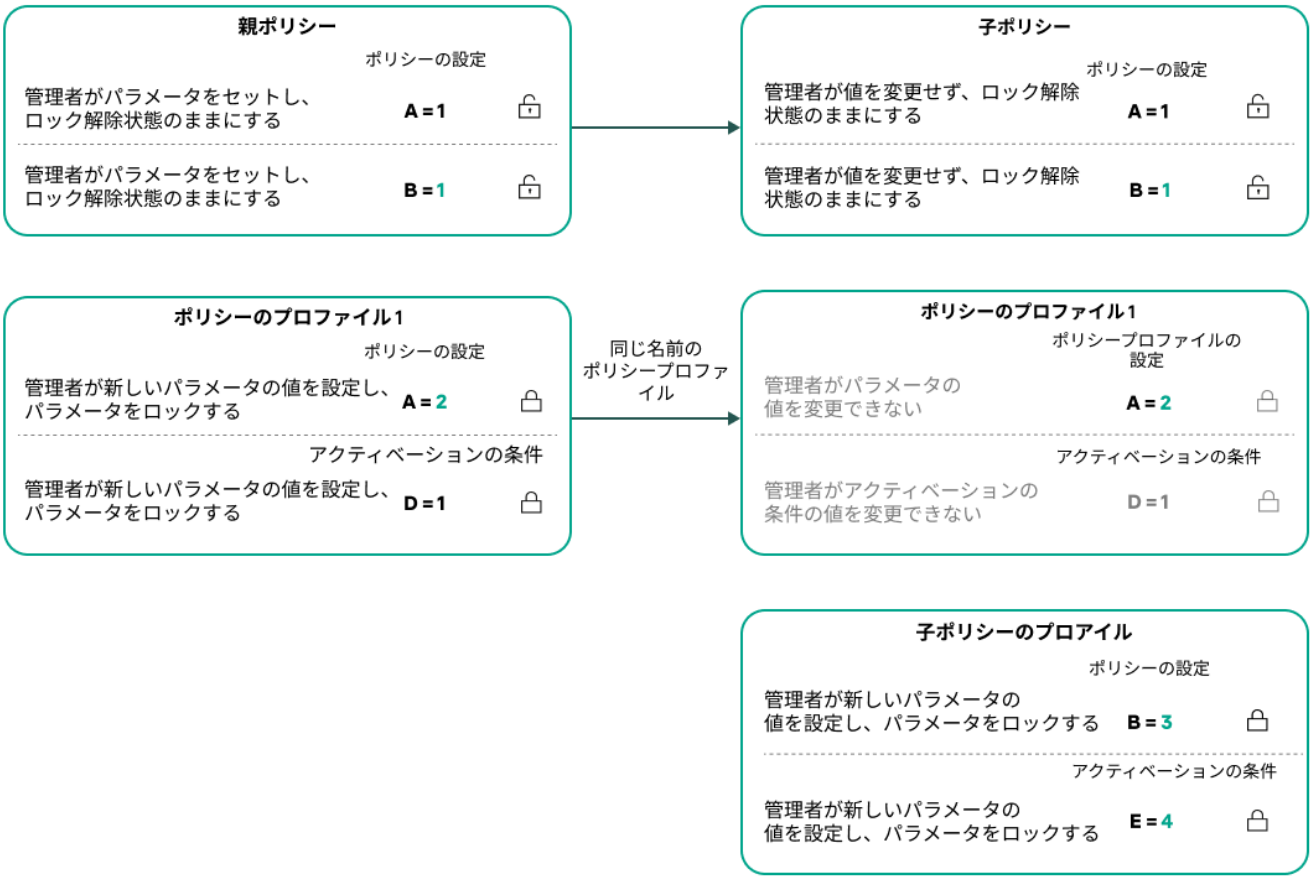



ポリシープロファイルの継承

### 同じ名前のポリシープロファイル

異なる階層レベルに、同じ名前の 2 つのポリシーがある場合、これらのポリシーは次のルールに従って機能します：

- ロックされた設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されます（下図を参照）。




子プロファイルは親ポリシープロファイルから設定値を継承する

- ロック解除された設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されません。

## 管理対象デバイスに設定が実装される方法

管理対象デバイスでの有効な設定の実装は、次のように説明できます：

- ロックされていないすべての設定の値は、有効なポリシーから取得されます。
- 次に、管理対象アプリケーション設定の値で上書きされます。
- 次に、有効なポリシーのロックされた設定値が適用されます。ロックされた設定値は、ロックされていない有効な設定値を変更します。

# ポリシーの管理

このセクションでは、ポリシーの管理について説明します。ポリシーのリストの表示、ポリシーの作成、ポリシーの変更、ポリシーのコピー、ポリシーの移動、強制同期、ポリシー導入ステータス図の表示、およびポリシーの削除に関する情報を提供します。

## ポリシーのリストの表示

管理サーバーまたは任意の管理グループを対象に作成されたポリシーのリストを表示できます。

*ポリシーのリストを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 管理グループのリストで、ポリシーのリストを表示する管理グループを選択します。

   ポリシーのリストが表形式で表示されます。ポリシーが存在しない場合、表は空です。表の列の表示と非表示の切り替え、列の順序の変更、指定した値を含む行のみの表示、検索の使用などを実行できます。

## ポリシーの作成

ポリシーの作成と、既存のポリシーの変更と削除を行うことができます。

*ポリシーを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ポリシーを作成する管理グループを選択します。

   - ルートグループ用。
     この場合は次のステップに進むことができます。
   - サブグループの場合：

     a. ページ上部の［**スコープの変更**］をクリックします。

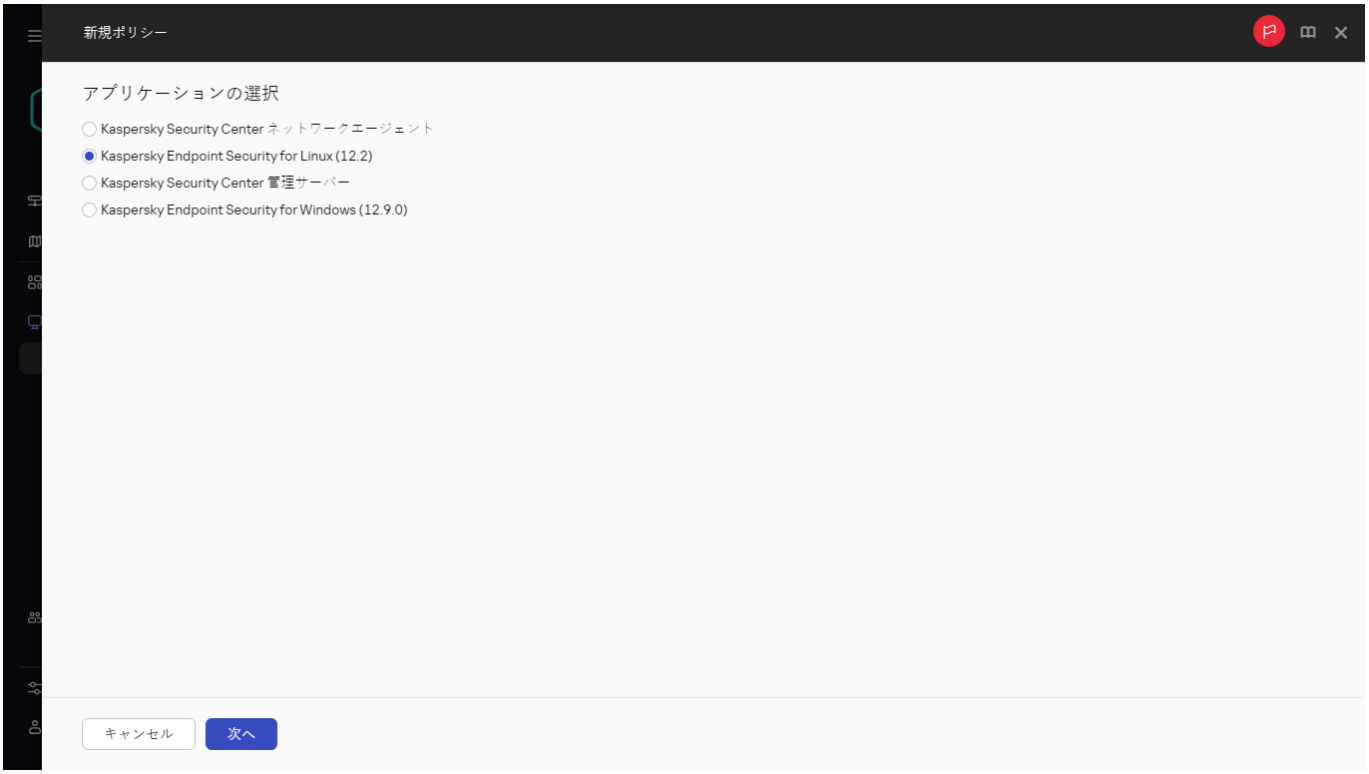
     b. 開いたウィンドウで、必要なサブグループの名前をクリックします。

   選択したグループへのパスがページの上部に表示されます。必要に応じて、管理グループ名のリンクをクリックしてグループに移動できます。既定では、パス内の最後のリンクは非アクティブです。




ポリシーのリスト

3. ［**追加**］をクリックします。
［**アプリケーションの選択**］ウィンドウが表示されます。




新しいポリシーの作成

4. ポリシーを作成するアプリケーションを選択します。

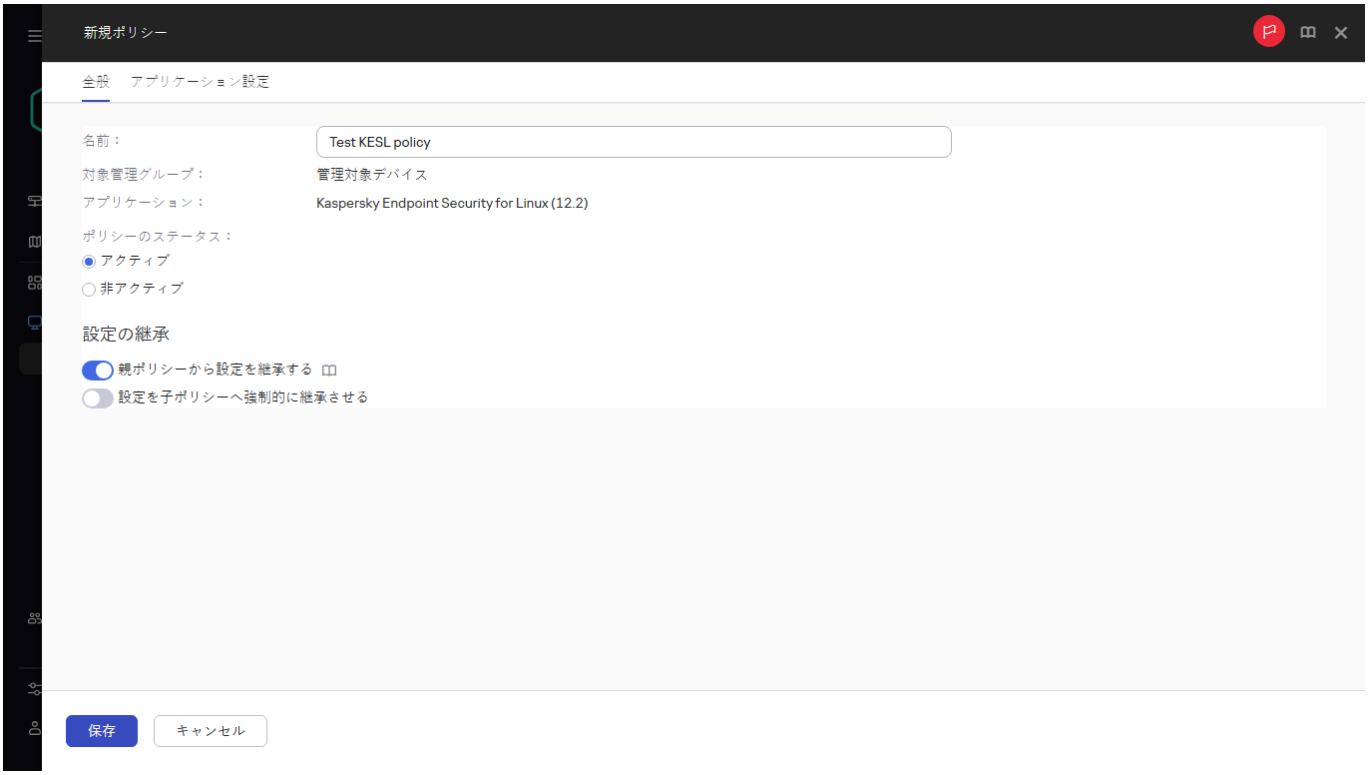
5. ポリシーを作成しているカスペルスキー製品で Kaspersky Security Network がサポートされている場合は、KSN 声明に同意するように要求されます。Kaspersky Security Network を使用する場合は、KSN 声明に同意してください。




KSN 声明の同意

6. ［**次へ**］をクリックします。

新規ポリシーの設定ウィンドウの［**全般**］タブが表示されます。必要に応じて、ポリシーの既定の名前、ステータス、継承設定を変更します。




新しいポリシー設定ウィンドウ

7. ［**アプリケーション設定**］タブを選択します。

あるいは、［**保存**］をクリックして作成を完了します。ポリシーのリストに新しいポリシーが表示されます。ポリシーの設定は後で編集できます。

8. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでポリシーの設定を編集します。ポリシーの各カテゴリ（セクション）の設定を編集できます。

設定内容は、作成するポリシーの対象となる製品に応じて異なります。詳細は、次を参照してください：

- 管理サーバーの設定
- ネットワークエージェントのポリシー設定
- Kaspersky Endpoint Security for Linux のヘルプ
- Kaspersky Endpoint Security for Windows のヘルプ

その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。

9. ［**保存**］をクリックしてポリシーを保存します。

ポリシーのリストに新しいポリシーが表示されます。

# ポリシーの全般的な設定

## 全般

［**全般**］タブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブ**

    このオプションをオンにすると、ポリシーがアクティブになります。

    既定では、このオプションがオンです。

  - **モバイルユーザー**

    このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

## イベントの設定

［**イベントの設定**］タブでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**
  ［**緊急**］セクションは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベントの種別をクリックすると、次の設定を指定できます：

- **イベント登録**
  イベントの保存日数を指定し、保存場所を選択できます：
  - **Syslog 経由で SIEM システムにエクスポートする**
  - **デバイスの OS イベントログに保存**
  - **管理サーバーの OS イベントログに保存**
- **イベント通知**
  次の通知方法ごとに、通知を受け取るかどうかを指定できます：
  - **メールで通知**
  - **SMS で通知**
  - **実行ファイルまたはスクリプトの実行で通知**
  - **SNMP 経由で通知**

  既定では、通知に利用する設定（受信アドレスなど）は、管理サーバーのプロパティで指定された設定を使用します。［**メール**］タブ、［**SMS**］タブ、［**実行ファイル**］タブで、必要に応じてそれぞれの設定を変更できます。

また、［**イベントの設定**］タブでは、新しいイベントタイプが追加されると（たとえば、製品の新しいバージョンで）通知が表示され、［**保存**］または［**保存して閉じる**］をクリックして新しい設定を適用することができます。

## 変更履歴

［**変更履歴**］タブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

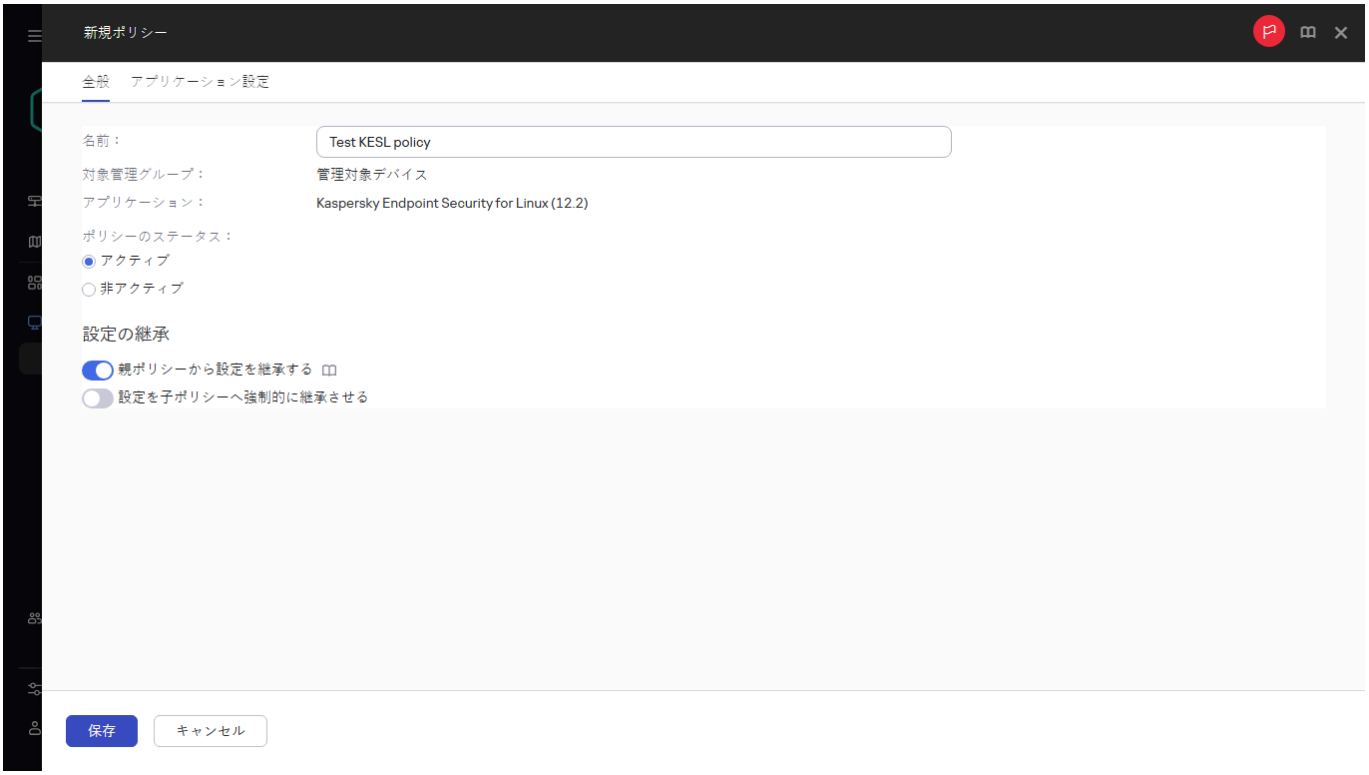
# ポリシーの変更

*ポリシーを変更するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。




2. 変更するポリシーを選択します：
   ポリシーの設定ウィンドウが表示されます。



3. 作成するポリシーの一般設定とアプリケーションの設定を指定します。詳細については、次を参照してください：

   - 管理サーバーの設定
   - ネットワークエージェントのポリシー設定
   - Kaspersky Endpoint Security for Linux のヘルプ
   - Kaspersky Endpoint Security for Windows のヘルプ

   その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

4. ［**保存**］をクリックします。

ポリシーに加えた変更は、ポリシーのプロパティに保存され、［**変更履歴**］セクションに表示されます。

# ポリシー継承オプションの有効化と無効化

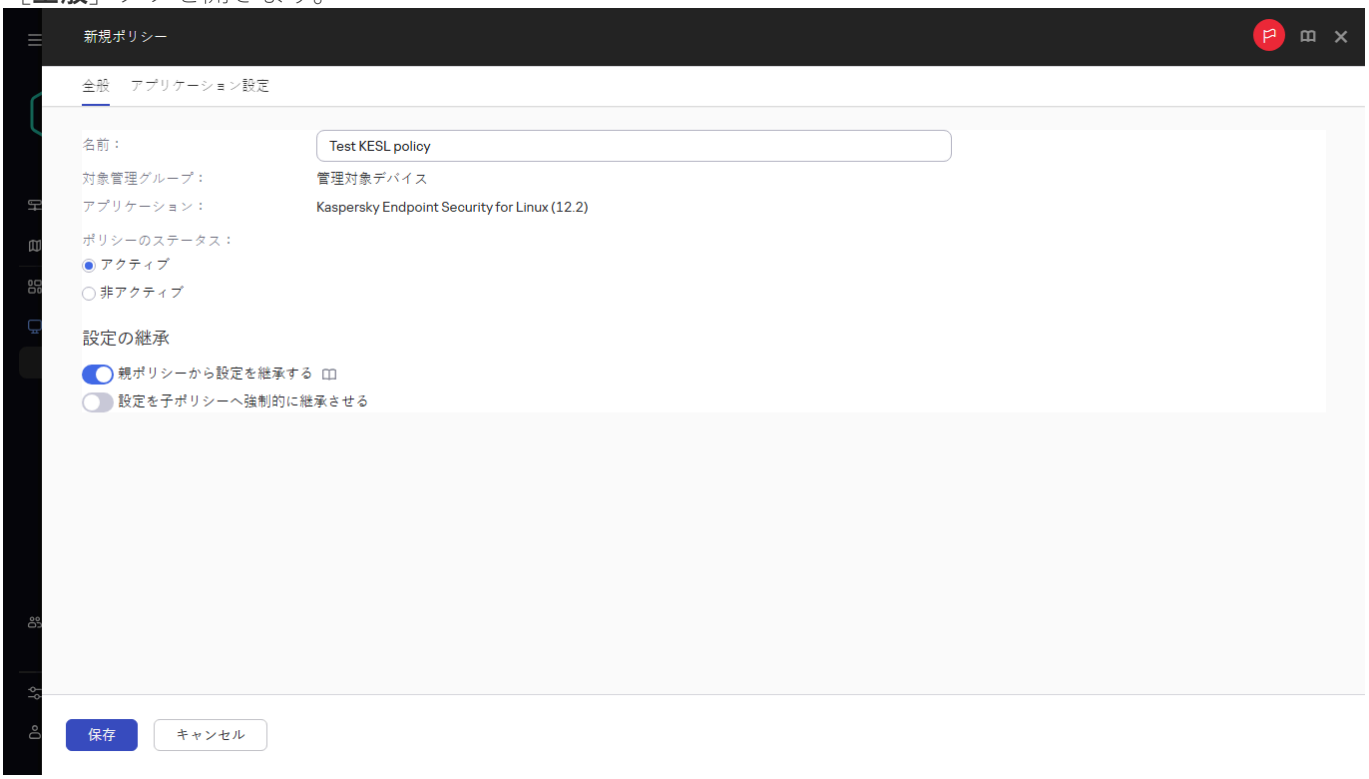
*ポリシーで継承オプションを有効または無効にするには：*

1. 必要なポリシーを開きます。




ポリシーのリスト

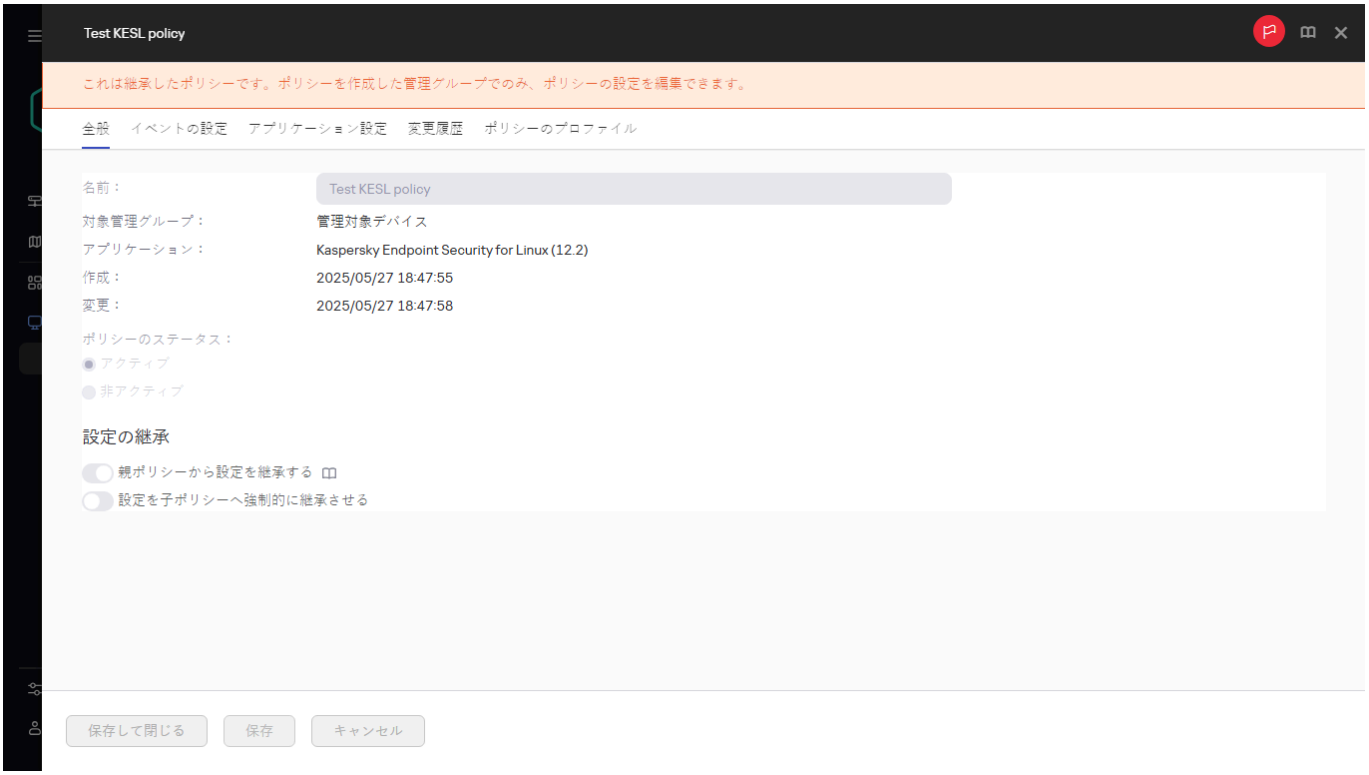
2. ［**全般**］タブを開きます。




新しいポリシーの作成

3. ポリシーの継承をオンまたはオフにします。

- 子ポリシーで［**親ポリシーから設定を継承する**］をオンにし、管理者が親ポリシーの設定の一部をロック状態にすると、子ポリシーでこれらの設定を変更することはできません。
- 子ポリシーで［**親ポリシーから設定を継承する**］をオフにすると、親ポリシーでロック状態の設定も含めて、子ポリシー側ですべての設定を変更できます。
- 親グループで［**設定を子ポリシーへ強制的に継承させる**］をオンにすると、各子ポリシーで［**親ポリシーから設定を継承する**］がオンになります。この場合、子ポリシーの側でこのオプションをオフにすることはできません。親ポリシーでロックされている設定はすべて強制的に子ポリシーに継承され、子グループ側でこれらの設定を変更することはできません。




ロックされたポリシーの設定

4. ［**保存**］ボタンをクリックして変更を保存するか、［**キャンセル**］ボタンをクリックして変更を破棄します。

既定では、新規に作成したポリシーでは［**親ポリシーから設定を継承する**］はオンです。

ポリシーにポリシープロファイルが存在する場合、子ポリシーでもこれらのプロファイルが継承されます。

## ポリシーのコピー

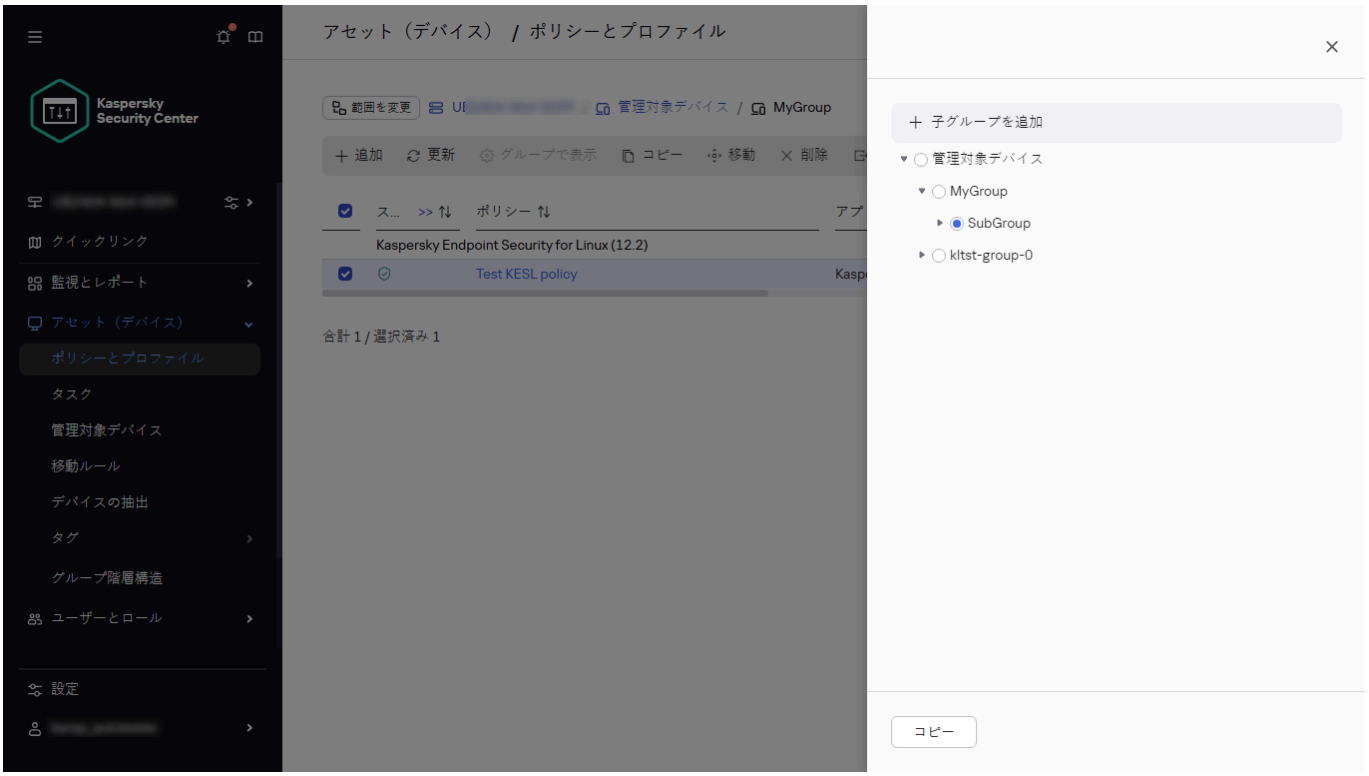
ポリシーを任意の管理グループから別の管理グループにコピーできます。

*ポリシーを別の管理グループにコピーするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. コピーするポリシーに隣接するチェックボックスをオンにします。




3. ［**コピー**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。




4. ツリーで、ポリシーのコピー先となるグループ（ターゲットグループ）を選択します。

5. ページの一番下にある［**コピー**］をクリックします。

6. ［OK］をクリックして処理内容を確定します。

すべてのプロファイルと合わせてターゲットグループにポリシーのコピーが作成されます。ターゲットグループにコピーして作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

## ポリシーの移動

ポリシーを任意の管理グループから別の管理グループに移動できます。たとえば、削除したいグループがあるが、そのグループのポリシーは別のグループで使用したいとします。その場合、グループを削除する前に、ポリシーを別のグループに移動できます。

*ポリシーを別の管理グループに移動するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. 移動するポリシーに隣接するチェックボックスをオンにします。



3. ［**移動**］をクリックします。

画面の右側に管理グループのツリーが表示されます。




4. ツリーで、ポリシーの移動先となるグループ（ターゲットグループ）を選択します。

5. ページの一番下にある［**移動**］をクリックします。

6. ［**OK**］をクリックして処理内容を確定します。

ポリシーがソースグループから継承されていない場合、ポリシーはすべてのプロファイルと合わせてターゲットグループに（コピーではなく）移動されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

ポリシーがソースグループから継承されている場合、ポリシーは元のグループにも残ります。そして、すべてのプロファイルと合わせてターゲットグループにコピーが作成されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

## ポリシーのエクスポート

Kaspersky Security Center Linux を使用すると、ポリシーとその設定、ポリシープロファイルを KLP ファイルに保存できます。この KLP ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したポリシーをインポートできます。

*ポリシーをエクスポートするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. エクスポートするポリシーの横のチェックボックスをオンにします。

   複数のポリシーを同時にエクスポートすることはできません。複数のポリシーを選択すると、［**エクスポート**］が無効になります。




エクスポートのポリシーの選択

3. ［**エクスポート**］をクリックします。
4. 表示される［**名前を付けて保存**］ウィンドウで、ポリシーファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、ポリシーファイルは自動的に［**Downloads**］フォルダーに保存されます。

## ポリシーのインポート

Kaspersky Security Center Linux を使用すると、KLP ファイルからポリシーをインポートできます。KLP ファイルには、エクスポートされたポリシー、その設定、およびポリシープロファイルが含まれています。

*ポリシーをインポートするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. ［**インポート**］をクリックします。
3. ［**参照**］をクリックして、インポートするポリシーファイルを選択します。

4. 表示されたウィンドウで、KLP ポリシーファイルのパスを指定し、［**開く**］をクリックします。選択できるポリシーファイルは 1 つだけです。

   ポリシーの処理が始まります。

5. ポリシーが正常に処理されたら、ポリシーを適用する管理グループを選択します。

6. ［**完了**］をクリックしてポリシーのインポートを完了します。

インポート結果の通知が表示されます。ポリシーが正常にインポートされた場合は、［**詳細**］をクリックして、ポリシーのプロパティを表示できます。

インポートが成功すると、ポリシーがポリシーリストに表示されます。ポリシーの設定とプロファイルもインポートされます。エクスポート中に選択されたポリシーステータスにかかわらず、インポートされたポリシーは非アクティブです。ポリシーのプロパティでポリシーステータスを変更できます。

新しくインポートされたポリシーと同じ名前のポリシーが既に存在している場合、インポートされたポリシーの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

# 強制同期

Kaspersky Security Center Linux では、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されます。定められた時点で、特定のデバイスで同期が実行されているかどうかを、管理者が正確に把握する必要がある場合があります。

## 単一デバイスの同期

*管理サーバーと管理対象デバイスの同期を強制的に実行するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。

2. 管理サーバーと同期させるデバイスの名前をクリックします。

   プロパティウィンドウの［**全般**］セクションが表示されます。

3. ［**強制同期**］をクリックします。

   指定したデバイスと管理サーバーの同期が実行されます。

## 複数デバイスの同期

*管理サーバーと複数の管理対象デバイスの同期を強制的に実行するには：*

1. 管理グループまたはデバイスの抽出からデバイスリストを開きます：

   - デバイスの抽出を実行してデバイスリストを表示します。
   - メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択して、同期するデバイスを含んだ管理グループを選択します：
     - ルートグループの場合は、次の手順に進むことができます。
     - サブグループの場合は、ページの上部にある［**スコープの変更**］をクリックし、開いたウィンドウでサブグループの名前をクリックします。

       選択したグループへのパスがページの上部に表示されます。必要に応じて、管理グループ名のリンクをクリックしてグループに移動できます。既定では、パス内の最後のリンクは非アクティブです。

2. 管理サーバーと同期するデバイスに隣接するチェックボックスをオンにします。
3. 管理対象デバイスのリストの上にある省略記号ボタン（**...**）、［**強制同期**］をクリックします。

   指定したデバイスと管理サーバーの同期が実行されます。
4. デバイスリストで、指定したデバイスでの前回の管理サーバーへの接続の時間が現在の時間に変更されていることが確認できます。時間が変更されていない場合は、［**更新**］をクリックしてページの内容を更新します。

選択したデバイスのデータが管理サーバーと同期します。

## ポリシーの配信時間の表示

管理サーバーでカスペルスキー製品のポリシーを変更した後、変更後のポリシーが特定の管理対象デバイスに配信されたかどうかを管理者は確認できます。ポリシーは、定期的な同期または強制的な同期によって配信されます。

*管理対象デバイスに製品ポリシーが配信された日時を表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。

   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**アプリケーション**］タブをクリックします。
4. ポリシーを同期した日時を表示する製品を選択します。

   製品ポリシーのプロパティウィンドウの［**全般**］セクションが表示され、ポリシーの配信日時を確認できます。

# ポリシー導入ステータス図の表示

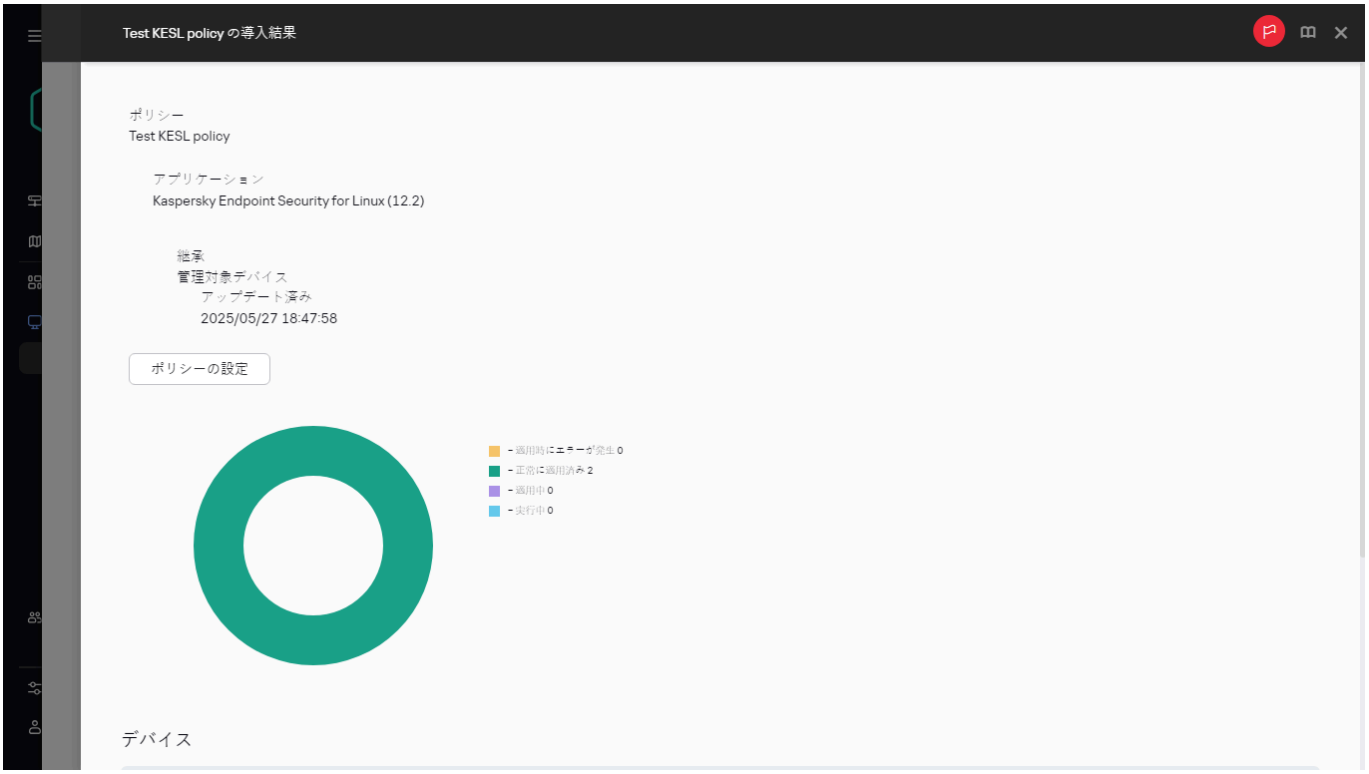
Kaspersky Security Center Linux では、各デバイスのポリシー適用のステータスをポリシー導入ステータス図で表示できます。

*各デバイスのポリシー導入ステータスを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. デバイスの導入ステータスを表示するポリシーの名前に隣接するチェックボックスをオンにします。



3. 表示されたメニューで、［**導入**］リンクを選択します。
［**<ポリシー名> 導入結果**］ウィンドウが開きます。




4. 開いた［**<ポリシー名> 導入結果**］ウィンドウに、ポリシーの**ステータスの説明**が表示されます。

ポリシーの導入結果のリストに表示されるデバイス数を変更できます。推奨されるデバイス数の上限は、100,000 台です。

*ポリシーの導入結果のリストに表示されるデバイスの数を変更するには：*

1. メインメニューで、［**設定**］→［**インターフェイスのオプション**］の順にクリックします。
2. ［**ポリシーの導入結果に表示するデバイス台数の上限**］に、デバイスの数（最大 100,000）を入力します。
既定では、この数は 5,000 です。
3. ［**保存**］をクリックします。
設定が保存され、適用されます。

# ［ウイルスアウトブレイク］イベント発生時におけるポリシーの自動アクティブ化

*［ウイルスアウトブレイク］イベント発生時にポリシーの自動アクティベーションを実行するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**ウイルスアウトブレイク**］セクションを選択します。
3. 右側のペインで、［**［ウイルスアウトブレイク］イベント発生時にアクティブ化するポリシーの設定**］をクリックします。
［**ポリシーのアクティブ化**］ウィンドウが表示されます。

4. ウイルスアウトブレイクを検知するコンポーネントの対象領域ごとに（ワークステーションおよびファイルサーバー向けアンチウイルス製品、メールサーバー向けアンチウイルス製品、境界防御向けアンチウイルス製品）、［**追加**］をクリックします。

   ［**管理対象デバイス**］管理グループウィンドウが表示されます。

5. ［**管理対象デバイス**］の横にあるアイコン（>）をクリックします。

   管理グループの階層とそれぞれの管理グループのポリシーが表示されます。

6. 管理グループの階層とポリシーから、ウイルスアウトブレイクの検知時にアクティブにするポリシーを選択します。

   1つのグループのすべてのポリシーを有効にする場合は、該当するグループ名の横のチェックボックスをオンにします。

7. ［**保存**］をクリックします。

   管理グループの階層とポリシーのウィンドウが閉じます。

選択したポリシーが、ウイルスアウトブレイクの検知時にアクティブ化されるポリシーのリストに追加されます。選択したポリシーは、その時点でアクティブか非アクティブかに関係なく、ウイルスアウトブレイクの発生時にアクティブになります。

［ウイルスアウトブレイク］イベントでポリシーがアクティブ化された場合は、手動モードを使用することによってのみ前のポリシーに戻ることができます。

## ポリシーの削除

必要ないポリシーは削除できます。ただし、削除できるのは上位のグループから継承されたのではないポリシーのみです。上位のグループから継承されたポリシーは、そのポリシーが作成された上位のグループでのみ削除できます。

*ポリシーを削除するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. 削除するポリシーの横のチェックボックスをオンにし、［**削除**］をクリックします。

   上位のポリシーから設定を継承したポリシーを選択した場合、［**削除**］はグレーアウトされ選択できなくなります。

3. ［**OK**］をクリックして処理内容を確定します。

ポリシーとそのすべてのプロファイルが削除されます。

# ポリシーのプロファイルの管理

このセクションでは、ポリシープロファイルの管理について説明します。ポリシーのプロファイルの表示、ポリシープロファイルの優先度の変更、ポリシープロファイルの作成、ポリシープロファイルのコピー、ポリシープロファイルの有効化ルールの作成、およびポリシープロファイルの削除に関する情報を提供します。

# ポリシーのプロファイルの表示

*ポリシーのプロファイルを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. プロファイルを表示するポリシーの名前をクリックします：
   ポリシーのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**ポリシーのプロファイル**］タブを開きます。

ポリシーのプロファイルのリストが表形式で表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。




ポリシーのプロファイルのリスト

# ポリシーのプロファイルの優先順位の変更

*ポリシーのプロファイルの優先順位を変更するには：*

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、優先度を変更するポリシープロファイルの横にあるチェックボックスをオンにします。

3. ［**優先度を高く設定**］または［**優先度を低く設定**］をクリックして、ポリシープロファイルの新しい位置を指定します。

   リスト内でポリシーの位置が上にあるほど、優先度も高くなります。




4. ［**保存**］をクリックします。

選択したポリシーのプロファイルの優先順位が変更され、適用されます。

## ポリシーのプロファイルの作成

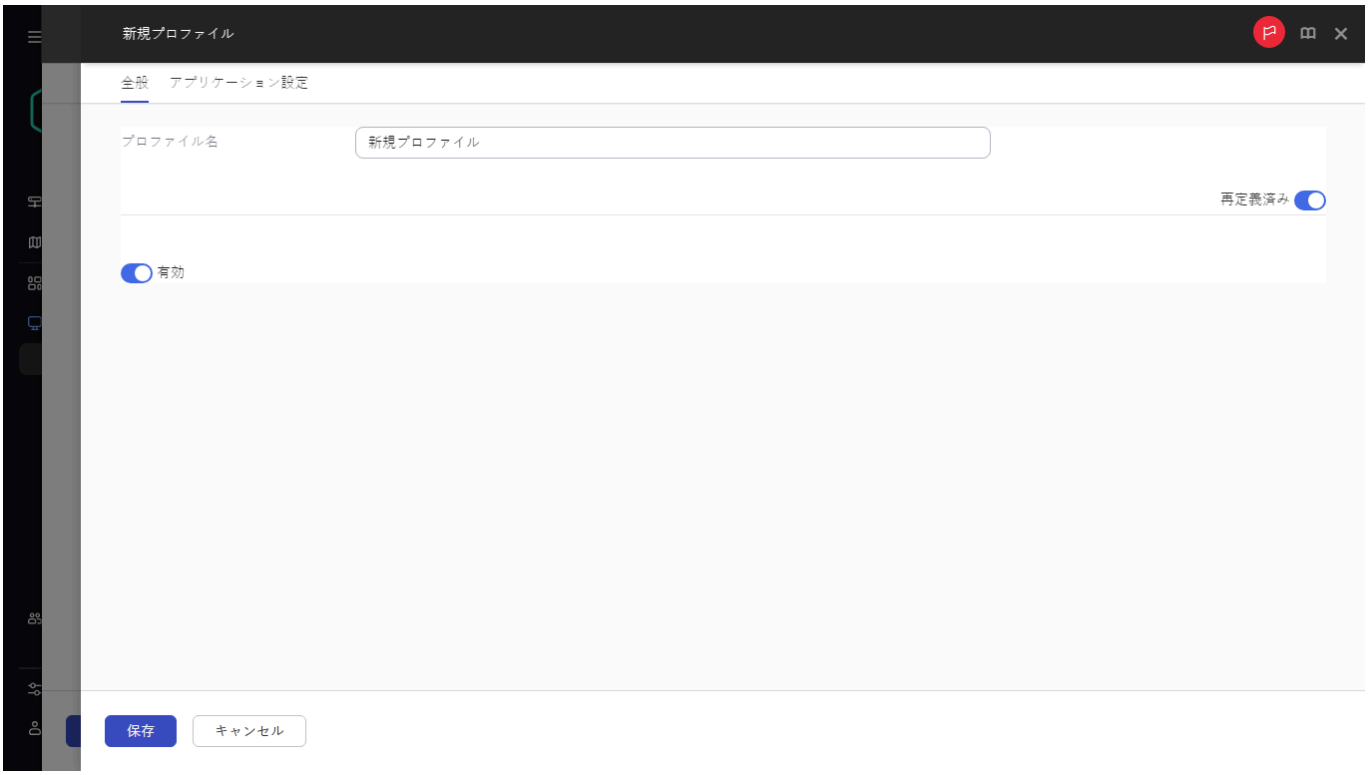
*ポリシーのプロファイルを作成するには：*

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**追加**］をクリックします。

3. 必要に応じて、プロファイルの既定の名前と継承設定を変更します。




新しいポリシーのプロファイルの作成

4. ［**アプリケーション設定**］タブを選択します。

   または、［**保存**］をクリックして完了します。ポリシープロファイルのリストに作成したプロファイルが表示されます。プロファイルの設定は後で編集できます。

5. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでプロファイルの設定を編集します。ポリシーのプロファイルの各カテゴリ（セクション）の設定を編集できます。

   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。




ポリシープロファイル設定の指定

6. ［**保存**］をクリックしてプロファイルを保存します。

   ポリシーのプロファイルのリストに新しいプロファイルが表示されます。

## ポリシーのプロファイルのコピー

ポリシーのプロファイルを現在の割り当て先のポリシーや別のポリシーにコピーして、同じポリシーを別のポリシーで使用できます。また、プロファイルのコピー機能は、一部の設定だけが異なる複数のプロファイルを作成する場合にも活用できます。

*ポリシーのプロファイルをコピーするには：*

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**ポリシーのプロファイル**］タブで、コピーするポリシープロファイルを選択します。

3. ［**コピー**］をクリックします。

4. 表示されるウィンドウで、プロファイルのコピー先にするポリシーを選択します。

   ポリシーのプロファイルを、現在割り当てられているのと同じポリシーまたは指定した別のポリシーにコピーできます。

5. ［**コピー**］をクリックします。

ポリシーのプロファイルが指定したポリシーにコピーされます。コピーして作成された新しいプロファイルには、最も低い優先度が設定されます。プロファイルを現在割り当てられているのと同じポリシーにコピーした場合、プロファイル名に (1)、(2) のようなインデックス「<数字>」が追加されます。

コピーの完了後、プロファイル名や優先度も含めてプロファイルの設定を変更できます。この変更によりコピー元のプロファイルが影響を受けることはありません。

## ポリシーのプロファイルの有効化ルールの作成

*ポリシーのプロファイルの有効化ルールを作成するには：*

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、有効化ルールを作成するポリシープロファイルをクリックします。
   ポリシープロファイルのリストが空の場合は、ポリシーのプロファイルを作成できます。
3. ［**有効化ルール**］タブで、［**追加**］をクリックします。
   ポリシーのプロファイルの有効化ルールのウィンドウが表示されます。
4. ルールの名前を入力します。

5. 作成しているポリシープロファイルの有効化に作用する条件の横にあるチェックボックスをオンにします：

- **ポリシープロファイルの有効化に対する全般ルール**

  このチェックボックスをオンにすると、デバイスのオフラインモードのステータス、管理サーバーへの接続ルール、デバイスに割り当てられているタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **デバイスのステータス**

    ネットワーク内にデバイスが存在するかどうかを指定します：

    - **オンライン** - デバイスはネットワーク内にあるため、管理サーバーを使用できます。
    - **オフライン** - デバイスは外部ネットワーク内にあるため、管理サーバーは使用できません。
    - **該当なし** - 基準は適用されません。

  - **管理サーバー接続のルールがこのデバイスでアクティブです**

    ポリシーのプロファイルを有効化する条件（ルールを実行する条件）を選択し、ルールの名前を指定します。

    ルールでは、管理サーバーへの接続に関するデバイスのネットワークロケーションを指定します。ポリシープロファイルを有効にするためにネットワークロケーションの説明の条件を満たす（または満たさない）必要があります。

    管理サーバーへの接続に関するデバイスのネットワークロケーションの説明は、ネットワークエージェント切り替えルールで作成または設定できます。

- **特定のデバイス所有者向けのルール**

  このオプションでは、次の項目を設定できます：

  - **デバイスの所有者**

    このオプションをオンにして、デバイスの所有者に応じたプロファイルの有効化ルールを設定を有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスが特定の所有者のものである（「=」記号）
    - デバイスが特定の所有者のものでない（「#」記号）

      このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。このオプションをオンにすると、デバイスの所有者を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **デバイスの所有者が属する内部セキュリティグループ**

このオプションをオンにして、デバイスの所有者の Kaspersky Security Center Linux の内部セキュリティグループの所属に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの所有者が特定のセキュリティグループのメンバーである（「=」記号）
- デバイスの所有者が特定のセキュリティグループのメンバーでない（「?」記号）

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。Kaspersky Security Center Linux のセキュリティグループを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ハードウェアの仕様のルール**

このチェックボックスをオンにすると、メモリサイズと論理プロセッサの数に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

このオプションでは、次の項目を設定できます：

- **RAM サイズ（MB）**

このオプションをオンにして、デバイスで使用可能な RAM サイズに応じたプロファイルの有効化のルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの RAM サイズは指定された値以下である（「<」記号）。
- デバイスの RAM サイズは指定された値以上である（「>」記号）。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイスの RAM ボリュームを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **論理プロセッサの数**

このオプションをオンにして、デバイスの論理プロセッサの数に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの論理プロセッサの数は指定された値以下である（「<」記号）。
- デバイスの論理プロセッサの数は指定された値以上である（「>」記号）。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイス上の論理プロセッサの数を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ロールの割り当てルール**

このオプションでは、次の項目を設定できます：

- **デバイス所有者のロールに応じてポリシープロファイルを有効化する**

このオプションをオンにすると、デバイスの所有者のロールに応じたプロファイルの有効化ルールを設定し、オンにすることができます。既存のロールのリストからロールを手動で選択して追加します。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。

- **タグの使用ルール**

  このチェックボックスをオンにすると、デバイスに割り当てられたタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。選択したタグが割り当てられているデバイスまたは割り当てられていないデバイスのいずれかで、ポリシーのプロファイルを有効にできます。

  このオプションでは、次の項目を設定できます：

  - **タグリスト**

    このタグのリストで、目的のタグのチェックボックスをオンにすると、ポリシーのプロファイルにデバイスを含めるためのルールを指定できます。

    リストの上のフィールドに新しいタグを入力して、[**追加**]をクリックすると、新しいタグをリストに追加できます。

    選択したタグのすべてを説明に含むデバイスがポリシーのプロファイルに含まれます。チェックボックスをオフにすると、基準は適用されません。既定では、これらのチェックボックスはオフです。

  - **指定したタグのないデバイスに適用する**

    タグの選択状態を反転させる必要がある場合は、このオプションをオンにします。

    このオプションをオンにすると、選択されたタグのいずれも説明に含まないデバイスがポリシープロファイルに含まれます。このオプションをオフにすると、基準が適用されません。

    既定では、このオプションはオフです。

- **Active Directory 使用のルール**

  このチェックボックスをオンにすると、Active Directory 組織単位（OU）内にデバイスが属しているか、または Active Directory セキュリティグループにデバイス（またはその所有者）が属しているかに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **Active Directory セキュリティグループのデバイス所有者メンバーシップ**

    このオプションを有効にすると、所有者が指定されたセキュリティグループに所属しているデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **デバイスが属している Active Directory セキュリティグループ**

このオプションを有効にすると、デバイスでポリシープロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスが割り当てられている Active Directory 組織単位**

  このオプションを有効にすると、指定された Active Directory 組織単位（OU）に属するデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。

  既定では、このオプションはオフです。

ウィザードで表示されるウィンドウ数は、最初のステップで選択した設定によります。ポリシープロファイルの有効化ルールは後で変更することができます。




ポリシーのプロファイルの有効化ルールの作成

6. 設定したパラメータのリストを確認します。リストのパラメータが正しいことが確認できたら、［**作成**］をクリックします。

プロファイルが保存されます。プロファイルは、有効化ルールが適合すると、デバイスで有効になります。

プロファイル用に作成したポリシープロファイルの有効化ルールが、［**有効化ルール**］タブのポリシープロファイルのプロパティに表示されます。ポリシープロファイルの有効化ルールはいずでも変更または削除することができます。

複数の有効化ルールを同時に適合させることができます。

## ポリシーのプロファイルの削除

*ポリシーのプロファイルを削除するには：*

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、削除するポリシープロファイルに隣接するチェックボックスをオンにし、［**削除**］をクリックします。

3. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

ポリシープロファイルが削除されます。下位のグループでこのポリシーが継承されている場合、該当する下位のグループでプロファイルが維持されますが、プロファイルの所属先がこの下位のグループのポリシーに変更されます。この処理は、下位グループのデバイスにインストールされている管理対象製品の設定が大幅に変更されてしまわないようにするために実装されています。

# ネットワークエージェントのポリシー設定

*ネットワークエージェントのポリシーを設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

2. ネットワークエージェントポリシーの名前をクリックします。

   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。プロパティウィンドウには、以下で説明するタブと設定が含まれています。

使用しているオペレーティングシステムの種類に応じて、以下の設定がどのように適用されるかを詳しく説明した比較表を参照してください。

## 全般

このタブでは、ポリシー名やポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**名前**］フィールドで、ポリシー名を変更できます。
- ［**ポリシーのステータス**］セクションで、次のポリシーのステータスを選択します：
  - **アクティブ**

    このオプションをオンにすると、ポリシーがアクティブになります。
    既定では、このオプションがオンです。

  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。
    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。
    既定では、このオプションはオフです。

## イベントの設定

このタブでは、イベントの記録と通知を設定できます。イベントは、次のセクションの重要度レベルに応じて分散されます。

- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の期間が表示されます。イベント種別をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベント種別で、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

たとえば、［**警告**］セクションでは、［**セキュリティ問題が発生しました**］イベント種別の設定を編集できます。このようなイベントは、たとえばディストリビューションポイントのディスク空き容量が 2 GB 未満の場合などに発生します（アプリケーションのインストール、アップデートのダウンロードをリモートで実行するには、少なくとも 4 GB が必要となります）。［**セキュリティ問題が発生しました**］イベントをクリックし、発生したイベントを保存する場所とその通知方法を指定します。

ネットワークエージェントがセキュリティ問題を検知した場合は、管理対象デバイスの設定を使用してこの問題を管理できます。

## アプリケーション設定

### 設定

［**設定**］セクションでは、ネットワークエージェントのポリシーを設定できます。

- **ディストリビューションポイント経由でのみファイルを配信する**

  このオプションをオンにすると、管理対象デバイスのネットワークエージェントはディストリビューションポイントからのみアップデートを取得します。

  このオプションをオフにすると、管理対象デバイス上のネットワークエージェント ディストリビューションポイントまたは管理サーバーからアップデートを取得します。

  管理対象デバイスのセキュリティ製品は、各セキュリティ製品のアップデートタスクで設定されたアップデート元からアップデートを取得することに注意してください。［**ディストリビューションポイント経由でのみファイルを配信する**］を有効にする場合、Kaspersky Security Center Linux がアップデートタスクのアップデート元に設定されていることを確認してください。

  既定では、このオプションはオフです。

- **イベントキューの最大サイズ（MB）**

  このフィールドでは、イベントキューが使用できるドライブの最大サイズを指定できます。

  既定値は 2 メガバイト（MB）です。

- **アプリケーションがポリシーの拡張データをデバイスから取得可能である**

  管理対象デバイスにインストールされたネットワークエージェントは、適用されたセキュリティ製品のポリシーに関する情報をセキュリティ製品（たとえば、Kaspersky Endpoint Security for Linux）に転送します。転送された情報は、セキュリティ製品のインターフェイスで表示できます。

  ネットワークエージェントは次の情報を転送します：

  - 管理対象デバイスへのポリシー導入の時間。
  - 管理対象デバイスにポリシーが配信された時点でのアクティブポリシーの名前。
  - 管理対象デバイスにポリシーが配信された時点のモバイルユーザーポリシーの名前（Linux 用ネットワークエージェントでは使用できません）。
  - 管理対象デバイスへポリシー導入の時点で管理対象デバイスが含まれていた管理グループの名前と完全パス。
  - 管理対象デバイスにポリシーが配信された時点でのアクティブポリシープロファイルとその名前および優先順位のリスト。

  情報を使用して、デバイスに正しいポリシーが適用されていることを確認し、トラブルシューティングを行うことができます。既定では、このオプションはオフです。

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックして、Windows ベースのデバイスで klmover ユーティリティおよびネットワークエージェントのリモートアンインストール時に使用するパスワードを指定できます。

  既定では、このオプションはオフです。

# リポジトリ

［**リポジトリ**］セクションでは、ネットワークエージェントから管理サーバーに詳細が送信されるオブジェクトの種別を選択できます：

- **インストール済みアプリケーションの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールされたアプリケーションに関する情報が管理サーバーに送信されます。

  既定では、このオプションはオンです。

- **パッチの情報を含める**

  クライアントデバイスにインストールされたアプリケーションのパッチに関する情報が管理サーバーに送信されます。このオプションをオンにすると、データベースに保存されるデータの容量が増えるとともに管理サーバーと DBMS での負荷が増大します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

- **Windows Update 更新プログラムの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールする必要のある Microsoft Windows アップデートの必須アップデートプログラムに関する情報が管理サーバーに送信されます。

  既定では、このオプションはオンです。Windows でのみ使用できます。

  オプションの Microsoft Windows アップデートに関する情報が管理サーバーに送信されていません。

- **ソフトウェアの脆弱性と対応するアップデートの詳細**

  このオプションをオンにすると、管理対象デバイスで検出されたサードパーティソフトウェア（Microsoft ソフトウェアを含む）の脆弱性に関する情報、およびサードパーティの脆弱性（Microsoft ソフトウェアを含まない）を修正するソフトウェアアップデートに関する情報が、管理サーバーに送信されます。

  このオプション（**ソフトウェアの脆弱性と対応するアップデートの詳細**）を選択すると、ネットワーク負荷、管理サーバーのディスク負荷、およびネットワークエージェントのリソース消費が増加します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

  Microsoft ソフトウェアのソフトウェアアップデートを管理するには、［**Windows Update 更新プログラムの詳細**］を使用します。

- **ハードウェアレジストリの詳細**

  デバイスにインストールされたネットワークエージェントから、そのデバイスのハードウェアに関する情報が管理サーバーに送信されます。ハードウェアの詳細は、デバイスのプロパティで確認できます。

  ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

このセクションの設定の一部を変更することがネットワークエージェントのポリシーで禁止されている場合、それらの設定を変更することはできません。

# ソフトウェアのアップデートと脆弱性

［**ソフトウェアのアップデートと脆弱性**］セクションでは、実行ファイルの脆弱性のスキャンをオンにすることができます：

- **実行ファイルの開始時に脆弱性をスキャンする**

  このオプションをオンにすると、実行ファイルが実行時にスキャンされ、脆弱性がないかチェックされます。

  既定では、このオプションはオンです。

# 再起動の設定

［**再起動の設定**］セクションでは、アプリケーションの正しい使用、インストール、またはアンインストールのために管理対象デバイスのオペレーティングシステムの再起動が必要な場合に行う動作を指定できます：

- **OS を再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **必要に応じて自動的に OS を再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **次の時間経過後に強制的に再起動する（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

  - **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

## パッチとアップデートの管理

［パッチとアップデートの管理］セクションでは、アップデートのダウンロードを設定できます。また、管理対象デバイスへのパッチの配信とインストールについても設定できます：

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

  このオプションをオンにすると、*承認*ステータスが「*未定義*」のカスペルスキー製品のパッチが、アップデートサーバーにダウンロードされるとすぐに、管理対象デバイスに自動インストールされます。

  このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

  既定では、このオプションはオンです。

- **アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**

  このオプションをオンにすると、オフライン方式でのアップデートのダウンロードが使用されます。管理サーバーは、アップデートの受信時に、管理対象アプリケーションに必要なアップデートを、該当するアプリケーションがインストールされたデバイス上のネットワークエージェントに通知します。ネットワークエージェントは、アップデートに関する情報を受け取ると、適切なファイルを管理サーバーからあらかじめダウンロードします。具体的には、管理サーバーは、ネットワークエージェントが次に接続された時にアップデートのダウンロードを開始します。ネットワークエージェントによってすべてのアップデートがクライアントデバイスにダウンロードされると、そのデバイスのアプリケーションでこれらのアップデートが利用可能になります。

  クライアントデバイス上の管理対象アプリケーションがアップデートのためにネットワークエージェントにアクセスしようとすると、ネットワークエージェントは必要なアップデートがあるかどうか確認します。管理対象アプリケーションから要求された時点で、管理サーバーからアップデートを受信してから経過した時間が 25 時間以内の場合、ネットワークエージェントは管理サーバーと接続せずに、ローカルキャッシュからアップデートを管理対象アプリケーションに渡します。ネットワークエージェントからクライアントデバイス上のアプリケーションへアップデートを配信する際には、アップデートのために管理サーバーへの接続を確立する必要はありません。

  このオプションをオフにすると、オフライン方式でのアップデートのダウンロードは使用されません。アップデートは、アップデートダウンロードタスクのスケジュールに従って配信されます。

  既定では、このオプションはオンです。

# 接続

［**接続**］セクションには 3 つのサブセクションが含まれます：

- **ネットワーク**
- **接続プロファイル**
- **接続スケジュール**

［**ネットワーク**］サブセクションでは、管理サーバーからクライアントコンピューターへの接続を設定したり、UDP ポートの使用を有効化したり、UDP ポート番号を定義したりできます。

- ［**管理サーバーに接続**］セクションでは、管理サーバーへの接続を設定し、クライアントデバイスと管理サーバーを同期する間隔を指定できます：

  - **同期間隔（分）**

    ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。同期間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

    同期間隔が 15 分以下に設定された場合、同期は 15 分ごとに実行されます。同期間隔が 15 分以上に設定されている場合は、指定された間隔で同期が実行されます。

  - **ネットワークトラフィックを圧縮する**

    このオプションをオンにすると、送信される情報量が減ることでネットワークエージェントによるデータ送信速度が向上し、これにより管理サーバーの負荷が軽減されます。

    クライアントコンピューターの CPU の負荷は増加する可能性があります。

    既定では、このチェックボックスはオンです。

  - **Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**

    このオプションをオンにすると、ネットワークエージェントの動作に必要なポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

    既定では、このオプションはオンです。

  - **SSL 接続を使用する**

    このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

    既定では、このオプションはオンです。

  - **既定の接続設定でディストリビューションポイントの接続ゲートウェイを使用する（使用可能な場合）**

    このオプションをオンにすると、ディストリビューションポイントの接続ゲートウェイが、管理グループのプロパティで指定された設定で使用されます。

    既定では、このオプションはオンです。

- **UDP ポートを使用する**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオフになっています。管理サーバーに接続するための既定の UDP ポートは 15000 です。

- **UDP ポート番号**

  このフィールドに、UDP ポート番号を入力できます。既定のポート番号は 15000 です。

  レコードには 10 進法が使用されます。

- **ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**

  ［**ディストリビューションポイントをプッシュサーバーとして使用する**］をディストリビューションポイントの設定ウィンドウでオンにする場合、このオプションをオンにします。オンにしないと、ディストリビューションポイントはプッシュサーバーとして動作しません。

［**接続プロファイル**］サブセクションで、ネットワークロケーションを設定したり、管理サーバーが使用できない際のモバイルユーザーモードをオンにしたりできます：

- **ネットワークロケーションの設定**

  ネットワークロケーションの設定では、クライアントデバイスが接続するネットワークの特性を定義し、ネットワークの特性が変更された時にネットワークエージェントが管理サーバーの接続プロファイルを切り替えるためのルールを指定します。

- **管理サーバー接続プロファイル**

  接続プロファイルは、Windows を実行しているデバイスでのみサポートされます。

  ネットワークエージェントから管理サーバーへの接続のプロファイルを表示して追加することができます。次のイベントの発生時、ネットワークエージェントから別の管理サーバーに切り替えるルールを作成することもできます：

  - クライアントデバイスが別のローカルネットワークに接続した場合
  - デバイスから組織のローカルネットワークへの接続が切断した場合
  - 接続ゲートウェイアドレスまたは DNS サーバーアドレスが変更された場合

- **管理サーバーが使用できない時にモバイルユーザーモードを有効にする**

  このオプションをオンにすると、このプロファイルで接続しているクライアントデバイスにインストールされているアプリケーションは、モバイルユーザーモードおよびモバイルユーザーポリシーを使用します。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

  このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

  既定では、このオプションはオフです。

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**

  このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

  既定では、このオプションがオンです。

- **指定の時間間隔で接続**

  このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

# ディストリビューションポイント別のネットワークポーリング

［**ディストリビューションポイント別のネットワークポーリング**］セクションでは、ネットワークの自動ポーリングを設定できます。次のオプションを使用してポーリングを有効にしたり、頻度を設定できます：

- **IP アドレス範囲**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって IP アドレス範囲が自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントは IP アドレス範囲をポーリングしません。

  ネットワークエージェントのバージョンが 10.2 より前の場合、IP アドレス範囲のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、オプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

- **Zeroconf**

  このオプションをオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索します。この場合、ディストリビューションポイントはネットワーク全体を検索するため、有効な IP 範囲の検索は無視されます。

  Zeroconf の使用を開始するには、次の条件が満たされている必要があります：

  - ディストリビューションポイントが Linux を実行している必要があります。
  - ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

  このオプションをオフにすると、ディストリビューションポイントは IPv6 デバイスを持つネットワークを検索しません。

  既定では、このオプションはオフです。

- **ドメインコントローラー**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによってアクティブディレクトリが自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントはドメインコントローラーをポーリングしません。

  10.2 より前のバージョンのネットワークエージェントドメインコントローラーのポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、このオプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

## ディストリビューションポイントのネットワーク設定

［**ディストリビューションポイントのネットワーク設定**］セクションで、インターネットアクセス設定を指定できます：

- **プロキシサーバーを使用する**
- **アドレス**
- **ポート番号**
- **ローカルアドレスにプロキシサーバーを使用しない**

  このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

  既定では、このオプションはオフです。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  既定では、このチェックボックスはオフです。

## KSN プロキシ（ディストリビューションポイント）

［**KSN プロキシ（ディストリビューションポイント）**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの Kaspersky Security Network（KSN）リクエストを転送するようにアプリケーションを設定できます：

- **ディストリビューションポイントで KSN プロキシを有効にする**

  ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

  ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。

  既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

  アクティブ / パッシブモードのクラスタのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

- **KSN リクエストを管理サーバーに転送する**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

  既定では、このオプションはオンです。

- **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

- **TCP ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポート**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオフになっています。管理サーバーに接続するための既定の UDP ポートは 15000 です。

- **HTTPS ポート**

  管理対象デバイスが HTTPS ポート経由で KSN プロキシサーバーに接続する必要がある場合は、［**HTTPS を使用する**］をオンにし、［**HTTPS ポート**］フィールドにポート番号を指定します。既定では、このオプションはオフです。HTTPS プロキシサーバーに接続する既定のポートは 17111 です。

## アップデート（ディストリビューションポイント）

［**アップデート（ディストリビューションポイント）**］セクションでは、差分ファイルのダウンロード機能を有効にすることができます。そのため、ディストリビューションポイントはカスペルスキーのアップデートサーバーから差分ファイルの形式でアップデートを取得します。

## ローカルアカウントの管理（Linux のみ）

［**ローカルアカウントの管理（Linux のみ）**］セクションには、次の 3 つのサブセクションが含まれます。

- **ユーザー証明書の管理**
- **適用可能なローカル管理者グループの追加または変更**
- **ユーザーのデバイス上で sudoers ファイルを変更から保護する参照ファイルのアップロード**

［**ユーザー証明書の管理**］サブセクションでは、インストールするルート証明書を指定できます。これらの証明書は、たとえば、Web サイトまたは Web サーバーの信頼性を検証するために使用できます。

- **ルート証明書のインストール**

  このオプションをオンにすると、テーブルに追加された証明書が指定されたデバイスにインストールされます。

  このオプションをオフにすると、指定されたデバイスに証明書はインストールされません。

  既定では、このオプションはオフです。

- **追加**

  このボタンをクリックすると、証明書を追加できるウィンドウが開きます。

  証明書は 10 MB 未満である必要があります。

  Kaspersky Security Center は、CER、CRT、CERT、PEM、および KEY 拡張子を持つ証明書をサポートしています。

［**適用可能なローカル管理者グループの追加または変更**］サブセクションでは、ローカル管理グループを管理できます。これらのグループは、たとえば、ローカル管理者権限を取り消す時に使用されます。**特権付きのデバイスのユーザーに関するレポート（Linux のみ）**を使用して、特権ユーザーアカウントのリストを確認することもできます。

- **追加**

  このボタンをクリックするとウィンドウが開き、ローカル管理グループを追加できます。

- **編集**

  このボタンをクリックするとウィンドウが開き、ローカル管理グループを編集できます。

  このボタンは、ローカル管理グループの横にあるチェックボックスがオンの場合に使用できます。

- **削除**

  このボタンをクリックすると、選択したローカル管理グループがテーブルから削除されます。

  このボタンは、ローカル管理グループの横にあるチェックボックスがオンの場合に使用できます。

［**ユーザーのデバイス上で sudoers ファイルを変更から保護する参照ファイルのアップロード**］サブセクションでは、ファイル sudoers の制御を設定できます。特権グループとデバイスユーザーは、デバイス上のファイル sudoers によって定義されます。ファイル sudoers は `/etc/sudoers` にあります。参照 sudoers ファイルをアップロードして、ファイル sudoers が変更されないように保護できます。これにより、ファイル sudoers への不要な変更が防止されます。

無効な参照 sudoers ファイルにより、ユーザーのデバイスが誤動作する可能性があります。

- **sudoers ファイルを管理する**

  このオプションをオンにすると、ファイル sudoers は現在の参照 sudoers ファイルに置き換えられます。

  このオプションをオフにすると、ファイル sudoers は変更されません。

  既定では、このオプションはオフです。

- **参照 sudoers ファイル**

  このフィールドには、アップロードされた参照 sudoers ファイルの名前が表示されます。

- **アップロード**

  このボタンをクリックするとウィンドウが開き、参照 sudoers ファイルをアップロードできます。

- **現在の参照 sudoers ファイル**

  このボタンをクリックすると、現在の sudoers ファイルの内容が表示されます。

### 変更履歴

［**変更履歴**］タブでは、次の操作を実行できます：

- ポリシーリビジョンの履歴の表示と保存
- ポリシーリビジョンへのロールバック
- ポリシーのリビジョンの説明を追加および編集

# Windows 用、Linux 用、macOS 用ネットワークエージェントの用途：比較

ネットワークエージェントの用途は、デバイスのオペレーティングシステムによって異なります。ネットワークエージェントのポリシーの設定とインストールパッケージの設定も、オペレーティングシステムによって異なります。次の表は、Windows、Linux、および macOS オペレーティングシステムで使用可能なネットワークエージェントの機能と使用シナリオを比較したものです。

| ネットワークエージェントの機能 | Windows | Linux | macOS |
|---|---|---|---|
| **インストール** | | | |
| サードパーティ製のツールを使用した、管理者のハードドライブのイメージの複製によるオペレーティングシステムとネットワークエージェントのインストール | ✓ | ✓ | ✓ |
| アプリケーションのリモートインストールにおけるサードパーティ製のツールを使用したインストール | ✓ | ✓ | ✓ |
| デバイスでアプリケーションインストーラーを実行しての手動インストール | ✓ | ✓ | ✓ |
| サイレントモードでのネットワークエージェントのインストール | ✓ | ✓ | ✓ |
| クライアントデバイスから管理サーバーへの手動接続：klmover ユーティリティ | ✓ | ✓ | ✓ |
| Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストール | ✓ | ✓ | – |
| ライセンスの自動配信 | ✓ | ✓ | ✓ |
| 強制同期 | ✓ | ✓ | ✓ |
| **ディストリビューションポイント** | | | |
| ディストリビューションポイントとして使用 | ✓ | ✓ | ✓ |
| ディストリビューションポイントの自動割り当て | ✓ | ✓<br>Network Location Awareness（NLA）を使用しない場合。 | ✓<br>Network Location Awareness（NLA）を使用しない場合。 |
| オフライン方式のアップデートのダウンロード | ✓ | ✓ | ✓ |
| ネットワークポーリング | ✓<br>• IP アドレス範囲のポーリング<br>• ドメインコントローラーのポーリング（Microsoft Active Directory） | ✓<br>• IP アドレス範囲のポーリング<br>• Zeroconf ポーリング<br>• ドメインコントローラーのポーリング（Microsoft Active Directory、Samba 4 Active Directory） | – |
| ディストリビューションポイントでの KSN プロキシサービスの実行 | ✓ | ✓ | – |
| 管理対象デバイスにアップデートを配布するディストリビューションポイントリポジトリに、カスペルスキーのアップデートサーバー経由でアップデートをダウンロードする | ✓ | ✓ | –<br>（[ディストリビューションポイントのリポジトリにアップデートをダウンロード] タスクの対象範囲に Linux または macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「失敗」ステータスが付与されます） |
| アプリケーションのプッシュインストール | ✓ | 制限あり：Linux ディストリビューションポイントを使用して Windows デバイスにプッシュ インストールを実行することはできません。 | 制限あり：macOS ディストリビューションポイントを使用して Windows デバイスにプッシュインストールを実行することはできません。 |

| ネットワークエージェントの機能 | Windows | Linux | macOS |
| --- | --- | --- | --- |
| プッシュサーバーとしての使用 | ✓ | ✓ | — |
| **サードパーティ製品の取り扱い** | | | |
| デバイスへのアプリケーションのリモートインストール | ✓ | ✓ | ✓<br>1. インストールパッケージと .sh インストールスクリプトで構成されるアーカイブを作成します。<br>2. ［**ダウンロード前に OS の種別を確認する**］をオフにします。<br>あるいは、［**スクリプトをリモートで実行**］タスクを使用することもできます。次の記事では、このタスクのファイルを構成する方法について説明します：［スクリプトをリモートで実行］タスクを使用してデバイスにアプリケーションをリモートでインストールします。 |
| ネットワークエージェントポリシーでのオペレーティングシステムのアップデートの設定 | ✓ | — | — |
| ソフトウェアの脆弱性に関する情報の表示 | ✓ | — | — |
| アプリケーションの脆弱性スキャン | ✓ | — | — |
| ソフトウェアのアップデート | ✓ | — | — |
| デバイスにインストールされたソフトウェアのインベントリ | ✓ | ✓ | — |
| **仮想マシン** | | | |
| 仮想マシンへのネットワークエージェントのインストール | ✓ | ✓ | ✓ |
| 仮想デスクトップインフラストラクチャ（VDI）に合わせた設定の最適化 | ✓ | ✓ | ✓ |
| 動的仮想マシンのサポート | ✓ | ✓ | ✓ |
| **その他** | | | |
| リモートクライアントデバイスでの Windows デスクトップ共有を使用した操作の監査 | ✓ | — | — |
| アンチウイルスによる保護のステータスの監視 | ✓ | ✓ | ✓ |
| デバイスの再起動の管理 | ✓ | — | — |
| ファイルシステムロールバックのサポート | ✓ | ✓ | ✓ |
| ネットワークエージェントを接続ゲートウェイとして使用する | ✓ | ✓ | ✓ |
| 接続マネージャー | ✓ | ✓ | ✓ |
| 別の管理サーバーへのネットワークエージェントの接続先の切り替え（ネットワーク上の位置により自動的に実行） | ✓ | — | ✓ |

| ネットワークエージェントの機能 | Windows | Linux | macOS |
|---|---|---|---|
| クライアントデバイスと管理サーバー間の接続の確認：klnagchk ユーティリティ | ✓ | ✓ | ✓ |
| クライアントデバイスのデスクトップへのリモート接続 | ✓ | ✓ | ✓<br>VNC（Virtual Network Computing）を使用 |
| 移行ウィザードを使用したスタンドアロンインストールパッケージのダウンロード | ✓ | ✓ | ✓ |
| クライアントデバイスのハードウェアに関する情報の表示 | ✓ | ✓<br>これらのデバイスにインストールされたネットワークエージェントによって管理サーバーに送信される Linux デバイスのハードウェアに関する情報は、管理対象デバイス設定の説明で指定された情報に限定されます。 | ✓<br>これらのデバイスにインストールされているネットワークエージェントによって管理サーバーに送信される macOS デバイスのハードウェアに関する情報は、管理対象デバイス設定の説明で指定された情報に限定されます。 |

# ネットワークエージェントの設定のオペレーティングシステム別の比較

次の表は、ネットワークエージェントがインストールされている管理対象デバイスのオペレーティングシステムに応じて、どのネットワークエージェントポリシー設定が使用できるかを示しています。

ネットワークエージェントの設定：オペレーティングシステムによる比較

| ［設定］セクション | Windows | Linux | macOS |
|---|---|---|---|
| **全般** | ✓ | ✓ | ✓ |
| **イベントの設定** | ✓ | ✓ | ✓ |
| **設定** | ✓ | ✓<br>次のオプションを使用できます：<br>• **ディストリビューションポイント経由でのみファイルを配信する**<br>• **イベントキューの最大サイズ（MB）**<br>• **アプリケーションがポリシーの拡張データをデバイスから取得可能である** | ✓ |
| **リポジトリ** | ✓ | ✓<br>次のオプションを使用できます：<br>• **インストール済みアプリケーションの詳細**<br>• **ハードウェアレジストリの詳細** | ✓<br>［**ハードウェアレジストリの詳細**］が使用可能です。 |
| ［**接続**］→［**ネットワーク**］ | ✓ | ✓<br>［**Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**］以外。 | ✓ |
| ［**接続**］→［**接続プロファイル**］ | ✓ | **ー** | ✓ |
| ［**接続**］→［**接続スケジュール**］ | ✓ | ✓ | ✓ |

| ［設定］セクション | Windows | Linux | macOS |
| --- | --- | --- | --- |
| **ディストリビューションポイント別のネットワークポーリング** | ✓<br>次のオプションを使用できます：<br>• **Windows ネットワーク**<br>• **IP アドレス範囲**<br>• **ドメインコントローラー** | ✓<br>次のオプションを使用できます：<br>• **Zeroconf**<br>• **IP アドレス範囲**<br>• **ドメインコントローラー** | – |
| **ディストリビューションポイントのネットワーク設定** | ✓ | ✓ | ✓ |
| **KSN プロキシ（ディストリビューションポイント）** | ✓ | ✓ | – |
| **アップデート（ディストリビューションポイント）** | ✓ | ✓ | – |
| **変更履歴** | ✓ | ✓ | ✓ |

# ネットワークエージェントの低リソース消費モードの有効化と無効化

低リソース消費モードでは、クライアントデバイスにインストールされているネットワークエージェントの RAM 使用量を制限できます。既定では、低リソース消費モードは無効になっています。

低リソース消費モードでは、次の機能は実行されません：

- ネットワークエージェントを（手動または自動で）ディストリビューションポイントとして割り当てることはできません。
- ネットワークエージェントは、ネットワークエージェントのステータスに関する情報を別のテキストファイルに記録しません。
- ネットワークエージェントは、アップデートダウンロードのオフラインモデルをサポートしていません。
- 次のコンポーネントとプロセスは無効になっています：
  - サードパーティのアップデートと脆弱性に関する情報の取得
  - ディストリビューションポイント側での KSN プロキシの実行
  - アップデートのディストリビューションポイントリポジトリへのアップロード
  - DNS サーバーブロックのバイパス
  - 空きディスク容量に関する情報を取得しています

低リソース消費モードを無効にすると、コンポーネントとプロセスは動作を再開します。

*低リソース消費モードを有効にするには：*

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：

   ```
   $ sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. 次のコマンドを使用してネットワークエージェントを再起動します：

   ```
   $ sudo service klnagent64 restart
   ```

3. オペレーティングシステムのログに、［**Kaspersky Security Center ネットワークエージェントは低リソース消費モードで動作しています**］というエントリが表示されているかどうかを確認します。

低リソース消費モードが有効になりました。

*低リソース消費モードを無効にするには：*

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：

   ```
   $ sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. 次のコマンドを使用してネットワークエージェントを再起動します：

   ```
   $ sudo service klnagent64 restart
   ```

低リソース消費モードが無効になりました。

*スクリプトをリモートで実行タスク*を使用して、低リソース消費モードをリモートで有効にすることもできます。

# Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、 Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項について説明します。ポリシーのプロパティウィンドウで設定を実行できます。設定を編集する際には、関連する設定グループの右側にあるロックアイコンをクリックして、指定した値をワークステーションに適用します。

## Kaspersky Security Network の設定

Kaspersky Security Network（KSN）は、ファイル、Web リソース、およびソフトウェアのレピュテーションに関する情報が含まれるクラウドサービスのインフラストラクチャです。Kaspersky Security Network を使用することで、 Kaspersky Endpoint Security for Windows はより迅速に様々な種類の脅威に対応し、保護コンポーネントのパフォーマンスを向上させ、誤検知の可能性を減らすことができます。Kaspersky Security Network の詳細は、Kaspersky Endpoint Security for Windows のヘルプ を参照してください。

*KSN について推奨される設定を指定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。
4. ［**Kaspersky Security Network**］がオンになっていることを確認します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。

   Managed Detection and Response を使用する場合、ディストリビューションポイントの［**Kaspersky Security Network**］をオンにし、拡張 KSN モードをオンにする必要があります。
5. KSN プロキシサービスが使用できない場合は、KSN サーバーの使用を有効にします。KSN サーバーは、カスペルスキー側に配置されている場合（KSN の使用時）とサードパーティ側に配置されている場合（KPSN の使用時）があります。
6. ［**OK**］をクリックします。

KSN について推奨される設定が指定されます。

# ファイアウォールで保護されているネットワークのリストの確認

Kaspersky Endpoint Security for Windows ファイアウォールがすべてのネットワークを保護していることを確認してください。既定では、ファイアウォールは次の種別の接続でネットワークを保護します：

- **パブリックネットワーク**。セキュリティ製品、ファイアウォール、またはフィルターは、このようなネットワーク内のデバイスを保護しません。
- **プライベートネットワーク**。このネットワーク内のデバイスは、ファイルとプリンターへのアクセスが制限されます。
- **信頼済みネットワーク**。このようなネットワーク内のデバイスは、ファイルやデータへの攻撃や不正アクセスから保護されます。

カスタムネットワークを設定している場合は、ファイアウォールがネットワークを保護していることを確認してください。このために、 Kaspersky Endpoint Security for Windows ポリシーのプロパティでネットワークのリストを確認します。このリストには、すべてのネットワークが含まれているとは限りません。

ファイアウォールの詳細は、 Kaspersky Endpoint Security for Windows のヘルプを参照してください。

*ネットワークのリストを確認するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］→［**脅威対策**］→［**ファイアウォール**］の順に選択します。

4. ［**使用可能なネットワーク**］で、［**ネットワーク設定**］をクリックします。

   ［**ネットワーク接続**］ウィンドウが表示されます。このウィンドウにはネットワークのリストが表示されます。

5. リストに欠落しているネットワークがある場合は、追加します。

# ネットワークドライブのスキャンをオフ

Kaspersky Endpoint Security for Windows がネットワークドライブをスキャンすると、ネットワークドライブに大きな負荷がかかる可能性があります。ファイルサーバーで間接スキャンを実行するのが有効です。

Kaspersky Endpoint Security for Windows ポリシーのプロパティで、ネットワークドライブのスキャンを無効にすることができます。ポリシーのプロパティの説明は、 Kaspersky Endpoint Security for Windows のヘルプ を参照してください。

*ネットワークドライブのスキャンを無効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。

   選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］-［**脅威対策**］-［**ファイル脅威対策**］の順に選択します。

4. ［**保護範囲**］セクションで、［**すべてのネットワークドライブ**］をオフにします。

5. ［**OK**］をクリックします。

ネットワークドライブのスキャンが無効になります。

# 管理サーバーのメモリからのソフトウェアの詳細情報の除外

ネットワークデバイスで起動されたソフトウェアモジュールに関する情報を管理サーバーに保存しないことを推奨します。その結果、管理サーバーのメモリがオーバーランすることはありません。

Kaspersky Endpoint Security for Windows ポリシーのプロパティで、この情報の保存を無効にすることができます。

*インストール済みのソフトウェアモジュールに関する情報の保存を無効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。

   選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］→［**全般設定**］→［**レポートと保管領域**］の順に選択します。

4. ［**管理サーバーへのデータ転送**］セクションで、［**起動されたアプリケーションの情報**］が上位のポリシーでオンになっている場合、これをオフにします。

   このチェックボックスをオンにすると、管理サーバーデータベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報が保存されます。この情報は、Kaspersky Security Center Linux データベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。

インストール済みのソフトウェアモジュールに関する情報が保存されなくなります。

# ワークステーションの Kaspersky Endpoint Security for Windows インターフェイスへのアクセスの設定

組織のネットワーク上の脅威対策による保護を Kaspersky Security Center Linux を介して集中モードで管理する必要がある場合は、以下の説明に従って、Kaspersky Endpoint Security for Windows ポリシーのプロパティでインターフェイス設定を指定します。その結果、ワークステーション上の Kaspersky Endpoint Security for Windows への不正アクセスと Kaspersky Endpoint Security for Windows 設定の変更を防ぐことができます。

ポリシーのプロパティの説明は、 Kaspersky Endpoint Security for Windows のヘルプ を参照してください。

*インターフェイスの推奨設定を指定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。

   選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］-［**全般設定**］-［**インターフェイス**］の順に選択します。

4. ［**ユーザーインターフェイス**］セクションで、［**表示しない**］をオンにします。これにより、ワークステーションで Kaspersky Endpoint Security for Windows のユーザーインターフェイスが表示されなくなり、ユーザーは Kaspersky Endpoint Security for Windows の設定を変更できなくなります。

5. ［**パスワードによる保護**］のスイッチをオンにします。これにより、ワークステーションで Kaspersky Endpoint Security for Windows の設定が不正に変更されたり、ユーザーが意図せずに変更してしまったりする危険性を低減できます。

以上の手順で、Kaspersky Endpoint Security for Windows のインターフェイスの推奨設定の指定が完了します。

# 管理サーバー定義データベースへのポリシーイベントの登録の設定

管理サーバー定義データベースのオーバーフローを回避するために、定義データベースには重要なイベントのみを保存することを推奨します。重要でないと思われるイベントについては、保存期間を短縮したり無効にしたりすることができます。

*イベントストレージ設定を構成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 必要なポリシー名をクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ［**イベントの設定**］タブに移動し、定義データベースへの登録を構成するイベントタイプの名前をクリックします。
4. 開いた右ペインで、次のいずれかを実行します：
   - イベントタイプの保存期間を変更する場合は、［**管理サーバーのデータベースに保存（日）**］がオンになっていることを確認し、イベントタイプを保存する日数を入力します。
   - イベントタイプを管理サーバー定義データベースに保存しない場合は、［**管理サーバーのデータベースに保存（日）**］をオフにします。
5. ［**OK**］をクリックし、右側のペインが閉じた後、［**保存**］ボタンをクリックします。

ポリシープロパティウィンドウが閉じ、構成した設定が適用されます。

# Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、Kaspersky Endpoint Security での最適かつ推奨されるスケジュールオプションは［**新しいアップデートがリポジトリにダウンロードされ次第**］です。

# Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ

クイックスタートウィザードにより、デバイススキャン用のグループタスクが作成されます。自動的に指定されたグループスキャンタスクのスケジュールが組織にとって適切でない場合は、組織で採用されている職場のルールに基づいて、このタスクに最も便利なスケジュールを手動で設定する必要があります。

たとえば、このタスクは**金曜日の午後 7 時に実行**するよう設定され、［**未実行のタスクを実行する**］がオフになっています。つまり、組織内のデバイスが、たとえば、金曜日の午後 6 時 30 分にシャットダウンされる場合、そのデバイスのスキャンタスクは一切実行されません。この場合、グループスキャンタスクを手動で設定する必要があります。

# Kaspersky Security Network（KSN）

このセクションでは、Kaspersky Security Network（KSN）というオンラインサービスのインフラストラクチャの使用方法を説明します。KSN の詳細、および KSN を有効にする方法、KSN へのアクセスの設定方法、KSN プロキシサーバーの使用の統計を表示する方法を説明します。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

## KSN について

Kaspersky Security Network（KSN）は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのナレッジベースへのオンラインアクセスを提供するオンラインサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護コンポーネントの効果が高まり、誤検知のリスクが低減されます。KSN によって、カスペルスキーの評価データベースを使用して、管理対象デバイスにインストールされたアプリケーションの情報を取得できます。

KSN への参加は、Kaspersky Security Center Linux によって管理されるクライアントデバイス上にインストールされたカスペルスキー製品の動作に関する情報を、自動的にカスペルスキーに送信することに同意したことを意味します。情報は、現在の KSN アクセス設定に従って転送されます。

Kaspersky Security Center Linux は、次の KSN インフラストラクチャソリューションをサポートしています：

- *Global KSN*：Kaspersky Security Network との情報交換を可能にするソリューションです。KSN に参加すると、Kaspersky Security Center Linux によって管理されるクライアントデバイス上にインストールされたカスペルスキー製品の動作に関する情報を、自動的にカスペルスキーに送信することに同意したことになります。情報は、現在の KSN アクセス設定に従って転送されます。カスペルスキーのアナリストは、受け取った情報をさらに分析し、Kaspersky Security Network の評価および統計データベースに追加します。Kaspersky Security Center Linux は既定でこのソリューションを使用します。

- *Kaspersky Private Security Network（KPSN）*は、カスペルスキー製品がインストールされたデバイスのユーザーが、自分のデバイスからグローバル KSN にデータを送信することなく、Kaspersky Security Network の定義データベースやその他の統計データにアクセスすることを可能にするソリューションです。KPSN は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

  - ユーザーデバイスがインターネットに接続されていない。

  - 国外や企業 LAN の外へのデータの送信が、法律で禁止されているか社内のセキュリティポリシーで制限されている。

  管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで、Kaspersky Private Security Network のアクセス設定をセットアップできます。

クイックスタートウィザードの実行時には、KSN に参加するよう促されます。アプリケーションの使用時であればいつでも、KSN の使用を開始または停止できます。

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合は、管理サーバーのバージョンをアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

KSN が有効になっている場合、Kaspersky Security Center Linux は、管理対象デバイスのセキュリティレベルが維持されていることを確認するために、KSN サーバーにアクセスできるかどうかを確認します。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。

管理サーバーが管理するクライアントデバイスは、KSN プロキシサーバーを使用して KSN と対話します。KSN プロキシサーバーは次の機能を提供します：

- クライアントデバイスは、インターネットに直接アクセスできない場合でも、KSN に要求を送信し、KSN から情報を取得し、KSN に情報を転送することができます。
- KSN プロキシサーバーでは処理データをキャッシュに保存するため、送信チャネルの負荷が軽減され、クライアントデバイスから要求された情報を待つ時間が短縮されます。

［管理サーバーのプロパティ］ウィンドウの［**KSN プロキシ**］セクションで、KSN プロキシサーバーを設定できます。

# KSN へのアクセスの設定

Kaspersky Security Network（KSN）へのアクセスを管理サーバーとディストリビューションポイントで設定できます。

*KSN への管理サーバーのアクセスを設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ**］セクションを選択します。

3. 切り替えスイッチを［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の位置まで移動します。

   このオプションをオンにすると、KSN プロキシサーバーはデータを KSN に送信し、Kaspersky Security Center コンポーネントの効率を高め、カスペルスキー製品のパフォーマンスを向上させます。クライアントデバイスでアクティブな Kaspersky Endpoint Security のポリシーに従って、クライアントデバイスから KSN にデータが送信されます。このスイッチをオフにすると、Kaspersky Security Center Linux を経由して、管理サーバーおよびクライアントデバイスから KSN にデータが送信されなくなります。しかし、クライアントデバイスが、個々の設定に従って KSN に直接（Kaspersky Security Center Linux を経由せずに）データを送信することがあります。クライアントデバイス上でアクティブな Kaspersky Endpoint Security ポリシーによって、それらのデバイスから直接（Kaspersky Security Center Linux を経由せずに）KSN に送信するデータが決定されます。

4. KSN インフラストラクチャソリューションを選択します。

［**KSN への参加**］サブセクションで、次のいずれかを実行します：

- グローバル KSN を使用している場合は、スイッチを［**Kaspersky Security Network の使用が［有効］です**］の位置まで移動します。

  このオプションをオンにする際には、必ず KSN 声明の条項を読み、それに同意する必要があります。

- KPSN を使用している場合、スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動し、［**KSN プロキシの設定ファイルを選択**］をクリックして、KPSN の設定をダウンロードします（拡張子 pkcs7、pem のファイル）。設定のダウンロード後、インターフェイスにはプロバイダー名と連絡先が表示されます。また、KPSN が設定されたファイルの作成日も表示されます。

スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動すると、KPSN に関する詳細のメッセージが表示されます。

以下のカスペルスキー製品が KPSN をサポートします：

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Kaspersky Security Center Linux KPSN をオンにすると、これらのカスペルスキー製品は KPSN の使用に関する通知を受け取ります。アプリケーション設定ウィンドウの［**先進の脅威対策**］セクションで、［**Kaspersky Security Network**］サブセクションに選択された KSN プロバイダーの情報が以下のように表示されています：KSN または KPSN。

> 管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで KPSN が設定されている場合、Kaspersky Security Center Linux は Kaspersky Security Network に統計データを送信しません。

5. 管理サーバーのプロパティでプロキシサーバー設定を構成済みだけれどもネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、［**KPSN への接続時にプロキシサーバーの設定を無視する**］をオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

6. 管理サーバーの KSN プロキシサービスへの接続を設定します：

- ［**接続設定**］の［**TCP ポート**］で、KSN プロキシサーバーへの接続に使用する TCP ポートの番号を指定します。KSN プロキシサーバーに接続する既定のポートは 13111 です。
- UDP ポートを経由して KSN プロキシサーバーと管理サーバーを接続する場合は、［**UDP ポートを使用する**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。
- 管理サーバーが HTTPS ポート経由で KSN プロキシサーバーに接続する場合は、［**HTTPS を使用する**］をオンにし、［**HTTPS ポート**］の番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。このオプションがオンの場合、KSN プロキシサーバーに接続する既定の HTTPS ポートは 17111 です。

7. トグルスイッチを［**プライマリ管理サーバー経由でのセカンダリ管理サーバーと KSN の接続が［有効］です**］の位置まで移動します。

   このオプションをオンにすると、セカンダリ管理サーバーはプライマリ管理サーバーを KSN プロキシサーバーとして使用します。このオプションをオフにすると、セカンダリ管理サーバーは直接 KSN に接続します。その場合、管理対象デバイスはセカンダリ管理サーバーを KSN プロキシサーバーとして使用します。

   セカンダリ管理サーバーのプロパティの［**KSN プロキシ**］セクションの右側で［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の切り替えスイッチが有効の位置にある場合、セカンダリ管理サーバーはプライマリ管理サーバーをプロキシサーバーとして使用します。

8. ［**保存**］をクリックします。

KSN のアクセス設定が保存されます。

管理サーバーの負荷を軽減したい場合などに、ディストリビューションポイントから KSN へのアクセスを設定できます。KSN プロキシサーバーとして動作しているディストリビューションポイントは、管理サーバーを使用せずに、管理対象デバイスからの KSN リクエストをカスペルスキーに直接送信します。

*Kaspersky Security Network（KSN）へのディストリビューションポイントのアクセスを設定するには：*

1. ディストリビューションポイントが手動で割り当てられていることを確認します。
2. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。
3. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
4. ディストリビューションポイントの名前をクリックし、プロパティウィンドウを開きます。
5. ［**KSN プロキシ**］のディストリビューションポイントのプロパティウィンドウで［**ディストリビューションポイントで KSN プロキシを有効にする**］をオンにしてから［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］をオンにします。
6. ［**OK**］をクリックします。

ディストリビューションポイントが KSN プロキシサーバーとして動作します。

ディストリビューションポイントは、NTLM プロトコルを使用した管理対象デバイスの認証をサポートしていないことに注意してください。

# KSN の使用の有効化と無効化

*KSN の使用を有効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ**］セクションを選択します。

3. 切り替えスイッチを［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の位置まで移動します。

KSN プロキシサーバーが有効になり、データを KSN に送信して、Kaspersky Security Center コンポーネントの効率を高め、カスペルスキー製品のパフォーマンスを向上させます。

1. 使用している KSN インフラストラクチャソリューションに応じて、対応するスイッチを有効にします。

   - グローバル KSN を使用している場合は、スイッチを［**Kaspersky Security Network の使用が［有効］です**］の位置まで移動します。

     KSN へのデータ送信が可能になりました。このオプションをオンにする際には、必ず KSN 声明の条項を読み、それに同意する必要があります。

   - KPSN を使用している場合、スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動し、［**KSN プロキシの設定ファイルを選択**］をクリックして、KPSN の設定をダウンロードします（拡張子 pkcs7、pem のファイル）。設定のダウンロード後、インターフェイスにはプロバイダー名と連絡先が表示されます。また、KPSN が設定されたファイルの作成日も表示されます。

     スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動すると、KPSN に関する詳細のメッセージが表示されます。

2. ［**保存**］をクリックします。

*KSN の使用を無効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ**］セクションを選択します。

3. KSN プロキシサービスを無効にするには、スイッチを［**KSN プロキシの管理サーバーでの有効化が［無効］です**］の位置に切り替えます。

4. ［**保存**］をクリックします。

# 同意した KSN に関する声明の表示

Kaspersky Security Network (KSN) を有効にする際には、KSN に関する声明を読み、同意する必要があります。同意した KSN に関する声明はいつでも表示できます。

*同意した KSN に関する声明を表示するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN プロキシ**］セクションを選択します。
3. ［**Kaspersky Security Network に関する声明を表示**］をクリックします。

表示されたウィンドウで、同意した KSN に関する声明の内容を表示できます。

# 更新された KSN に関する声明の同意

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合は、管理サーバーのバージョンをアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

管理サーバーのバージョンをアップグレードすると、更新された KSN 声明が自動的に表示されます。更新された KSN に関する声明を拒否した場合でも、後で表示して同意することができます。

*更新された KSN 声明を表示して同意するには：*

1. 製品のメインウィンドウの右上部にある[**通知の表示** ]をクリックします。
   ［**通知**］ウィンドウが開きます。
2. ［**更新された KSN 声明を表示**］をクリックします。
   ［**Kaspersky Security Network に関する声明の更新**］ウィンドウが開きます。
3. KSN に関する声明を読み、次のうち 1 つを選択して対応を判断します：
   - **更新された KSN 声明の内容に同意する**
   - **更新前の声明の内容に従って KSN を使用する**

選択に応じて、KSN は更新前の、もしくは更新された KSN 声明の規約に従い動作します。管理サーバーのプロパティからいつでも同意した KSN 声明の本文を表示できます。

# ディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかの確認

ディストリビューションポイントとして機能するように割り当てられた管理対象デバイスで、Kaspersky Security Network（KSN）プロキシを有効にできます。ksnproxy サービスがデバイスで実行されている場合、管理対象デバイスは KSN プロキシサーバーとして機能します。デバイスでこのサービスをローカルで確認し、オンまたはオフにできます。

Windows ベースまたは Linux ベースのデバイスをディストリビューションポイントとして割り当てることができます。ディストリビューションポイントのチェック方法は、このディストリビューションポイントのオペレーティングシステムによって異なります。

*Linux ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：*

1. ディストリビューションポイントのデバイスで `ps aux` コマンドを実行して、実行中のプロセスの一覧を表示します。
2. 実行中のプロセスのリストで、`/opt/kaspersky/klnagent64/sbin/ksnproxy` プロセスが実行されているかどうかを確認します。

`/opt/kaspersky/klnagent64/sbin/ksnproxy` プロセスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

*Windows ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：*

1. ディストリビューションポイントデバイスの Windows で、［**サービス**］（［**すべてのプログラム**］→［**管理ツール**］→［**サービス**］）を開きます。
2. サービスのリストで、ksnproxy サービスが実行されているかを確認します。

   ksnproxy サービスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

   必要に応じて ksnproxy サービスをオフにできます。この場合、ディストリビューションポイントのネットワークエージェントは Kaspersky Security Network への参加を停止します。この操作にはローカル管理者権限が必要です。

# KSN プロキシサーバーの統計を表示

Kaspersky Security Center Web コンソールを使用すると、KSN プロキシサーバーの使用統計を表示できます。

統計には次のパラメータが含まれます：

- KSN への接続ステータス
- キャッシュレコードの数
- キャッシュで処理されたパッケージの数
- 受け取ったパッケージの数

KPSN をインフラストラクチャソリューションとして使用する場合、KPSN の使用状況統計が表示されます。

*統計を表示するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで［**KSN プロキシ**］セクションを選択し、［**統計**］タブを開きます。

   このタブでは、KSN プロキシサーバーの使用に関する統計が表示されます。統計は 15 秒ごとに更新されます。

［**クリップボードへコピー**］をクリックすると、統計をコピーできます。

# タスクの管理

このセクションでは、Kaspersky Security Center Linux で使用できるタスクについて説明します。

## タスクの概要

Kaspersky Security Center Linux は、様々なタスクを作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

Kaspersky Security Center Web コンソールを使用してアプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインが Kaspersky Security Center Web コンソールサーバーにインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次の種別のタスクは管理サーバーで実行されます：

- レポートの自動配信
- リポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクの変更は、管理者が Kaspersky Security Center Web コンソールを使用して行うか、リモートデバイスのユーザーが行います（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、各デバイスのオペレーティングシステムのイベントログと管理サーバーのオペレーティングシステムのイベントログ、および管理データベースに保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

# タスクの対象範囲

*タスク範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。
- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている txt ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

# タスクの作成

*タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。表示される指示に従ってください。
3. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
4. ［**終了**］をクリックします。

タスクが作成され、タスクリストに表示されます。




タスク作成の終了

*選択したデバイスに割り当てる新しいタスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、デバイスの横にあるチェックボックスをオンにして、そのデバイスに対してタスクを実行します。対象のデバイスを見つけるには、検索機能とフィルター機能を使用できます。

3. ［**タスクの実行**］をクリックし、［**新規タスクの追加**］を選択します。

   新規タスクウィザードが起動します。

   ウィザードの最初の手順で、タスク範囲に含めるように選択したデバイスを削除できます。ウィザードの指示に従ってください。

4. ［**終了**］をクリックします。

選択したデバイスに対してタスクが作成されます。

# タスクの手動での開始

タスクは、各タスクのプロパティで指定されたスケジュール設定に従って、開始されます。タスクはタスクリストからいつでも手動で起動できます。あるいは、［**管理対象デバイス**］リストでデバイスを選択し、それらのデバイスに対する既存のタスクを開始することもできます。

*タスクを手動で開始するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. リスト内で、削除するタスクに隣接するチェックボックスをオンにします。

3. ［**開始**］をクリックします。




タスクリストからタスクを開始する

タスクが開始します。タスクのステータスは、［**ステータス**］列で、または［**結果**］をクリックして確認できます。

# 選択したデバイスでのタスクの開始

デバイスのリストで1つ以上のクライアントデバイスを選択して、それらに対して以前に作成したタスクを開始できます。これにより、特定のデバイスのセットに対して以前に作成したタスクを実行できるようになりました。

タスクが割り当てられたデバイスは、タスクの実行時に選択したデバイスのリストに変更されます。

*選択したデバイスに対するタスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、チェックボックスを使用して、タスクを実行するデバイスを選択します。対象のデバイスを見つけるには、検索機能とフィルター機能を使用できます。
3. ［**タスクの実行**］ボタンをクリックし、［**既存のタスクを適用する**］を選択します。

   既存のタスクのリストが表示されます。
4. 選択したデバイスがタスクリストの上に表示されます。必要に応じて、このリストからデバイスを削除できます。1つを除いてすべてのデバイスを削除できます。
5. リストから目的のタスクを選択します。リストの上にある検索ボックスを使用して、目的のタスクを名前で検索できます。選択できるタスクは1つだけです。
6. ［**保存してタスクを開始**］をクリックします。

   選択したタスクは、選択したデバイスに対してすぐに開始されます。タスクのスケジュール開始設定は変更されません。

# タスクリストの表示

Kaspersky Security Center Linux で作成されたタスクのリストを表示できます。

*タスクのリストを表示するには：*

メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

タスクのリストが表示されます。タスクは、関連するアプリケーションの名前でグループ化されます。たとえば、アプリケーションのリモートインストールタスクは管理サーバーに関連付けられ、アップデートタスクは Kaspersky Endpoint Security に関連付けられています。

*タスクのプロパティを表示するには：*

タスクの名前をクリックします。

タスクのプロパティウィンドウにいくつかの名前付きタブが表示されます。たとえば、［**タスク種別**］は［**全般**］タブに、タスクスケジュールは［**スケジュール**］タブに表示されます。

# タスクの全般的な設定

このセクションでは、ほとんどのタスクで表示および構成できる設定について説明します。使用可能な設定のリストは、構成しているタスクによって異なります。

## タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- OS の再起動設定：
  - **デバイスを再起動しない**

    操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

  - **デバイスを再起動する**

    インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

  - **セッションがブロックされたアプリケーションを強制終了する**

    アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

    このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

    このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

    既定では、このオプションはオフです。

- タスクスケジュールの設定：

  スケジュールの種類はタスクによって異なる場合があります。

  一部のタイプのスケジュールは、他のカスペルスキー製品では利用できない場合があります。

  - **タスク開始設定：**
    - **N 時間ごと**

      指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

    - **N 日ごと**

日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

既定では、現在のシステム日時から、1日ごとにタスクが実行されます。

- **N分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30分ごとにタスクが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後6時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、アップデートタスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、[**デバイスの電源をオンにする**]をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス([**正常終了**]または[**失敗**])を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、[**適用**]をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が[**手動**]、[**1回**]または[**即時**]に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

- タスクを割り当てるデバイス：
  - **ネットワークの管理サーバーによって検出されたデバイスを選択する**

    タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

    たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

  - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

    タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

    特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

  - **デバイスの抽出にタスクを割り当てる**

    デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

    たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

  - **管理グループにタスクを割り当てる**

    任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

    たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

    タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- アカウントの設定：
  - **既定のアカウント**

    タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

    既定では、このオプションがオンです。

  - **アカウントの指定**

    ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

## タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- グループタスクの設定：
  - **サブグループへ導入**

    このオプションはグループタスクの設定内でのみ使用可能です。

    このオプションをオンにすると、タスク範囲には次のものが含まれます：

    - タスクの作成中に選択した管理グループ。
    - 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

    このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

    既定では、このオプションはオンです。

  - **セカンダリまたは仮想管理サーバーに配信**

    このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

    このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

    既定では、このオプションはオフです。

- スケジュールの詳細設定
  - **Wake on LAN の機能を使用してタスク開始前にデバイスを起動する**

    タスク開始よりも指定した時間だけ前に、デバイス上のオペレーティングシステムが起動します。既定では、時間は 5 分です。

    タスクの開始予定時刻が近づいても電源がオフだったデバイスも含めて、タスク範囲に含まれるすべてのクライアントデバイスでタスクを実行するには、このオプションをオンにします。

    タスクの完了後にデバイスの電源を自動的にオフにする場合は、**タスク完了後にデバイスをシャットダウンする**を有効にします。このオプションは同じウィンドウ内にあります。

    既定では、このオプションはオフです。

  - **タスク完了後にデバイスをシャットダウンする**

    たとえば、毎週金曜日の業務時間終了後にクライアントデバイスへのアップデートのインストールを行い、その後デバイスの電源を切りたい時に、アップデートインストールタスクでこのオプションを使用できます。

    既定では、このオプションはオフです。

- **次の時間を超える場合はタスクを停止する**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。
  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。
  既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

- 通知の設定：
  - ［**タスク履歴の保存**］セクション：
    - **管理サーバーのデータベースに保存（日）**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、指定した日数の間、管理サーバーに保存されます。この期間が過ぎると、情報が管理サーバーから削除されます。

      既定では、このオプションはオンです。

    - **デバイスの OS イベントログに保存**

      タスク実行に関するアプリケーションイベントが、各クライアントデバイスの Syslog イベントログにローカルで保存されます。

      既定では、このオプションはオフです。

    - **管理サーバーの OS イベントログに保存**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、管理サーバーのオペレーティングシステムの Syslog イベントログに一元的に保存されます。

      既定では、このオプションはオフです。

    - **すべてのイベントを保存**

      このオプションをオンにすると、タスクに関するすべてのイベントがイベントログに保存されます。

    - **タスクの進捗に関連したイベントを保存**

      このオプションをオンにすると、タスク実行に関するイベントのみがイベントログに保存されます。

    - **タスク実行結果のみ保存**

      このオプションをオンにすると、タスクの実行結果に関するイベントのみがイベントログに保存されます。

  - **管理者にタスク実行結果を通知**

    管理者がタスク実行結果の通知を受け取る方法を、メール、SMS、実行ファイルの実行から選択できます。通知を設定するには、［**設定**］をクリックします。

    既定では、すべての通知方法がオフです。

  - **エラーのみ通知**

このオプションをオンにすると、管理者はタスクでエラーが発生して終了した場合にのみ通知を受け取ります。

このオプションをオフにすると、管理者はタスク終了時に常に通知を受け取ります。

既定では、このオプションはオンです。

- セキュリティ設定
- タスク範囲の設定

  タスク範囲の指定方法に応じて、次の設定が表示されます：

  - **デバイス**

    タスク範囲が管理グループを使用して指定されている場合、該当するグループを表示できます。ここでは、設定を変更することはできません。ただし、［**タスク範囲からの除外**］を設定できます。

    タスク範囲がデバイスのリストを使用して指定されている場合、デバイスを追加したり削除してこのリストを変更できます。

  - **デバイスの抽出**

    タスクが適用されるデバイスの抽出を変更できます。

  - **タスク範囲からの除外**

    タスクを適用しないデバイスのグループを指定できます。タスク範囲から除外できるのは、タスクが適用されない管理グループのサブグループのみです。

- **変更履歴**

# タスクのエクスポート

Kaspersky Security Center Linux を使用すると、タスクとその設定を KLT ファイルに保存できます。この KLT ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したタスクをインポートできます。

*タスクをエクスポートするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. エクスポートするタスクの横のチェックボックスをオンにします。

   複数のタスクを同時にエクスポートすることはできません。複数のタスクを選択すると、［**エクスポート**］が無効になります。管理サーバーのタスクもエクスポートできません。

3. ［**エクスポート**］をクリックします。

4. 表示される［**名前を付けて保存**］ウィンドウで、タスクファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、タスクファイルは自動的に［**Downloads**］フォルダーに保存されます。

# タスクのインポート

Kaspersky Security Center Linux を使用すると、KLT ファイルからタスクをインポートできます。KLT ファイルには、エクスポートされたタスクとその設定が含まれています。

> カスペルスキー製品タスクを正しくインポートするには、適切な管理プラグインをインストールする必要があります。

*タスクをインポートするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. ［**インポート**］をクリックします。

3. ［**参照**］をクリックして、インポートするタスクファイルを選択します。

4. 開いたウィンドウで、KLT タスクファイルへのパスを指定して、［**開く**］をクリックします。選択できるタスクファイルは 1 つだけです。

   タスクの処理が始まります。

5. タスクが正常に処理されたら、タスクを割り当てるデバイスを選択します。これには、次のいずれかのオプションを選択します：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

6. タスク範囲を指定します。

7. ［**完了**］をクリックしてタスクのインポートを完了します。

インポート結果の通知が表示されます。タスクが正常にインポートされた場合は、［**詳細**］をクリックして、タスクのプロパティを表示できます。

インポートが成功すると、タスクがタスクリストに表示されます。タスクの設定とスケジュールもインポートされます。タスクはスケジュールに従って開始されます。

新しくインポートされたタスクと同じ名前のタスクが既に存在している場合、インポートされたタスクの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

# タスクのパスワード変更ウィザードの起動

非ローカルタスクの場合、タスクを実行するアカウントを指定できます。アカウントは、タスクの作成時または既存のタスクのプロパティで指定できます。指定されたアカウントが組織のセキュリティ指示に従って使用されている場合、その指示によってアカウントパスワードの変更が必要になる場合があります。アカウントパスワードの有効期限が切れて新しいパスワードを設定すると、タスクプロパティで新しい有効なパスワードを指定するまで、タスクを開始しません。

タスクのパスワード変更ウィザードを使用すると、アカウントが指定されているすべてのタスクで、古いパスワードを新しいパスワードに自動的に置換できます。または、各タスクのプロパティで、このパスワードを手動で変更できます。

*タスクのパスワード変更ウィザードを起動するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**タスク開始に使用するアカウントの資格情報の管理**］をクリックします。

ウィザードの指示に従ってください。

## ステップ1：資格情報の指定

システムで現在有効な新しい証明書を指定します。ウィザードの次のステップに進むと、指定されたアカウント名が、非ローカルタスクそれぞれのプロパティのアカウント名と一致するかどうか確認されます。アカウント名が一致すると、タスクのプロパティのパスワードは自動的に新しいものに置換されます。

新しいアカウントを指定するには、オプションを選択します：

- **現在のアカウントを使用**

  ウィザードは、Kaspersky Security Center Web コンソールに現在サインインしているアカウントの名前を使用します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを手動で指定します。

- **別のアカウントを指定**

  タスクを起動する必要があるアカウントの名前を指定します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを指定します。

［**以前のパスワード（任意。現在のパスワードに置換したい場合に使用）**］フィールドに手動で入力した場合、アカウント名と古いパスワードの両方が見つかったタスクの、パスワードのみが置換されます。置換は自動で実行されます。その他の場合はすべて、ウィザードの次の手順で、実行する処理を選択する必要があります。

## ステップ2：実行する処理の選択

ウィザードの最初の手順で古いパスワードを指定しなかった場合、または指定した古いパスワードがタスクのプロパティのパスワードと一致しない場合、見つかったタスクに対して実行する処理を選択する必要があります。

*タスクに対する処理を選択するには：*

1. 処理を選択するタスクに隣接するチェックボックスをオンにします。
2. 次のいずれかを実行します：
   - タスクのプロパティのパスワードを削除するには、［**資格情報の削除**］をクリックします。
     タスクは既定のアカウントで実行されるように切り替わります。
   - パスワードを新しいパスワードに置換するには、［**古いパスワードが正しくないか未入力の場合でもパスワードの変更を強制する**］をクリックします。
   - パスワードの変更をキャンセルするには、［**処理が選択されていません**］をクリックします。

ウィザードの次のステップに移動すると、選択した処理が適用されます。

### ステップ 3：結果の表示

ウィザードの最後のステップで、見つかった各タスクの結果を表示します。ウィザードを終了するには、［**終了**］をクリックします。

## 管理サーバーに保存されているタスク実行結果の確認

Kaspersky Security Center Linux では、グループタスク、特定のデバイスに対するタスク、管理サーバータスクの実行結果を確認できます。

*タスク結果を表示するには：*

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。

*セカンダリ管理サーバーのタスク結果を表示するには：*

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。
3. ［**セカンダリサーバーからの統計**］をクリックします。
4. ［**タスク履歴**］ウィンドウを表示するセカンダリサーバーを選択します。

## アプリケーションタグ

このセクションでは、サードパーティ製品を対象としたアプリケーションタグの概要と、アプリケーションタグの作成、編集、製品への割り当てを行う方法を説明しています。

# アプリケーションタグ

Kaspersky Security Center Linux と、アプリケーションレジストリからアプリケーションにタグを付けることができます。タグとは、アプリケーションに割り当てるラベルで、アプリケーションのグループ化と検索に使用できます。アプリケーションに割り当てたタグは、デバイスの抽出の条件として使用できます。

たとえば、「**ブラウザー**」というタグを作成し、すべてのブラウザー（Microsoft Internet Explorer、Google Chrome、Mozilla Firefox など）に割り当てるなどの使い方ができます。

# アプリケーションタグの作成

*アプリケーションタグを作成するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. タグの名前を入力します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに新しいタグが表示されます。

# アプリケーションタグの名前変更

*アプリケーションタグの名前を変更するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. 名前を変更するタグの横のチェックボックスをオンにし、［**編集**］をクリックします。
   タグのプロパティウィンドウが表示されます。
3. タグの名前を変更します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに更新したタグが表示されます。

# アプリケーションへのタグの割り当て

*アプリケーションにタグを割り当てるには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを割り当てるアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。
   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 新たに割り当てるタグの［**タグの割り当て**］列のチェックボックスをオンにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションにタグが割り当てられます。

# アプリケーションに割り当てたタグの削除

*アプリケーションからタグを削除するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを削除するアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。
   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 削除するタグの［**タグの割り当て**］列のチェックボックスをオフにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションからタグが解除されます。

解除されたアプリケーションタグ自身は削除されません。必要に応じて、手動で削除できます。

# アプリケーションタグの削除

*アプリケーションタグを削除するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. リストから削除するアプリケーションタグを選択します。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

アプリケーションタグが削除されます。削除されたタグが割り当てられていたすべてのアプリケーションから、このタグが自動的に削除されます。

# デバイスコントロールでブロックされた外部デバイスへのオフラインモードでのアクセス権の付与

Kaspersky Endpoint Security のポリシーでのデバイスコントロール機能の設定により、クライアントデバイスに接続された外部デバイス（ハードディスク、カメラ、Wi-Fi モジュール）へのユーザーアクセスをコントロールできます。これにより、外部デバイスの接続によるクライアントデバイスへのマルウェアなどの感染を防止し、データの損失や流出などの被害を防ぐことができます。

デバイスコントロールでブロックされている外部デバイスへの一時的なアクセス権を付与する必要があるが、デバイスを信頼デバイスのリストに追加することは避けたい場合、外部デバイスへのオフラインモードでのアクセス権を付与することができます。オフラインモードでのアクセス権とは、クライアントデバイスがネットワークに接続されていない状態でのアクセス権です。

デバイスコントロールでブロックされている外部デバイスへのオフラインモードでのアクセス権を付与できるのは、Kaspersky Endpoint Security ポリシーの設定の［**アプリケーション設定**］→［**セキュリティコントロール**］→［**デバイスコントロール**］セクションで［**一時アクセスの要求を許可する**］がオンになっている場合のみです。

デバイスコントロールでブロックされた外部デバイスへのオフラインモードでのアクセス権の付与は、以下の手順で進みます：

1. クライアントデバイス上の Kaspersky Endpoint Security のウィンドウで、ブロックされている外部デバイスへのアクセス権を必要としているユーザーがアクセス要求ファイルを生成し、Kaspersky Security Center Linux の管理者に送信します。
2. この要求を受け取った Kaspersky Security Center Linux の管理者は、アクセスキーファイルを作成し、クライアントデバイスを使用しているユーザーに送信します。
3. クライアントデバイス上の Kaspersky Endpoint Security のウィンドウで、デバイスのユーザーはアクセスキーファイルを有効化し、外部デバイスへの一時的なアクセスを取得します。

*デバイスコントロールでブロックされた外部デバイスへの一時的なアクセス権を付与するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   管理対象デバイスのリストが表示されます。

2. このリストで、デバイスコントロールでブロックされている外部デバイスへのアクセス権を付与するクライアントデバイスを選択します。

   選択できるデバイスは1台のみです。

3. 管理対象デバイスのリストの上で省略記号（**...**）をクリックして、［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

4. 表示される［**アプリケーション設定**］ウィンドウの［**デバイスコントロール**］セクションで、［**参照**］をクリックします。

5. ユーザーから受け取ったアクセス要求ファイルを選択し、［**開く**］をクリックします。ファイルはAKEY形式である必要があります。

   現在ブロックされていて、ユーザーがアクセスを要求した外部デバイスの詳細情報が表示されます。

6. ［**アクセス期間**］設定の値を指定します。

   この設定では、ユーザーがブロックされたデバイスへのアクセスを許可される時間の長さを定義します。既定値は、アクセス要求ファイルの作成時にユーザーが希望して指定した値です。

7. デバイス上でアクセスキーをアクティベートできる期間を指定します。

   この設定では、ブロックされているデバイスへのアクセスを、ユーザーが受け取ったアクセスキーを使用して有効化できる期間を指定します。

8. ［**保存**］をクリックします。

9. 表示されるウィンドウで、ブロックされているデバイスへのアクセスキーを含んだファイルを保存する保存先フォルダーを選択します。

10. ［**保存**］をクリックします。

保存したアクセスキーをユーザーに送信し、ユーザーがKaspersky Endpoint Securityのウィンドウでこれを有効化すると、指定した期間、ブロックされているデバイスへのアクセス権がユーザーに付与されます。

# klscflagを使用したポート13291の開放

klakautユーティリティを使用して、Kaspersky Security Center Linuxの処理を自動化できます。klakautユーティリティとそのヘルプは、Kaspersky Security Center Linuxのインストールフォルダーにあります。klakautユーティリティを使用する場合は、klscflagユーティリティを使用して13291ポートを開きます。

klscflagユーティリティはKLSRV_SP_SERVER_SSL_PORT_GUI_OPENパラメータの値を変更します。

*ポート 13291 を開くには：*

1. コマンドラインで次のコマンドを実行します：
   ```
   $ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. 次のコマンドを実行して Kaspersky Security Center 管理サーバーサービスを再起動します：
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

   ポート 13291 が開きます。

*ポート 13291 が正常に開かれたことを確認するには：*

コマンドラインで次のコマンドを実行します：

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

このコマンドは次の結果を返します：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

値 `true` はポートが開かれていることを意味します。それ以外の場合は値 `false` が表示されます。

# Kaspersky Industrial CyberSecurity for Networks アプリケーションの Kaspersky Security Center Web コンソールでの登録

Kaspersky Security Center Web コンソールを使用して Kaspersky Industrial CyberSecurity for Networks アプリケーションの操作を開始するには、まず Kaspersky Security Center Web コンソールに登録する必要があります。

*Kaspersky Industrial CyberSecurity for Networks アプリケーションを登録するには：*

1. 次が完了していることを確認してください：

   - Kaspersky Industrial CyberSecurity for Networks Web プラグインのダウンロードとインストール。

     Kaspersky Industrial CyberSecurity for Networks サーバーと管理サーバーの同期の待機中、後で実行することも可能です。プラグインをダウンロードしてインストールすると、Kaspersky Security Center Web コンソールのメインメニューに［**KICS for Networks**］セクションが表示されます。

   - Kaspersky Industrial CyberSecurity for Networks Web インターフェイスでは、Kaspersky Security Center との対話が設定され、有効になります。詳細は、『Kaspersky Industrial CyberSecurity for Networks のオンラインヘルプ』を参照してください。

2. Kaspersky Industrial CyberSecurity for Networks サーバーがインストールされているデバイスを、未割り当てのデバイスグループから管理対象デバイスグループに移動します。

   a. メインメニューで、［**検索および導入**］→［**未割り当てデバイス**］の順に選択します。

   b. Kaspersky Industrial CyberSecurity for Networks サーバーがインストールされているデバイスに隣接するチェックボックスをオンにします。

   c. ［**グループに移動**］をクリックします。

   d. 管理グループの階層で、［**管理対象デバイス**］グループに隣接するチェックボックスをオンにします。

   e. ［**移動**］をクリックします。

3. Kaspersky Industrial CyberSecurity for Networks Server がインストールされているデバイスのプロパティウィンドウを開きます。

4. デバイスのプロパティページの［**全般**］セクションで［**管理サーバーから切断しない**］をオンにし、［**保存**］をクリックします。

5. デバイスのプロパティページで、［**アプリケーション**］セクションを選択します。

6. ［**アプリケーション**］セクションで、Kaspersky Security Center ネットワークエージェントを選択します。

7. 本製品の現在のステータスが「*停止中*」の場合、「*実行中*」に変更されるまで待機します。

   このプロセスには最大 15 分かかります。Kaspersky Industrial CyberSecurity for Networks の Web プラグインをまだインストールしていない場合は、今すぐインストールできます。

8. Kaspersky Industrial CyberSecurity for Networks の統計を表示したい場合は、ダッシュボードにウィジェットを追加できます。ウィジェットを追加するには、次の手順を実行します：

   a. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。

   b. ダッシュボードで、［**Web ウィジェットの追加または復元**］をクリックします。

   c. 開いたウィジェットメニューで、［**その他**］を選択します。

   d. 追加したいウィジェットを選択します：

      - KICS for Networks 導入マップ
      - ネットワークサーバー用 KICS に関する情報
      - KICS for Networks の最新イベント
      - KICS for Networks で問題のあるデバイス
      - KICS for Networks の重大なイベント
      - KICS for Networks のステータス

9. Kaspersky Industrial CyberSecurity for Networks Web インターフェイスに進むには、次の手順を実行します：

   a. メインメニューで、［**KICS for Networks**］→［**検索**］に移動します。

   b. ［**イベントまたはデバイスの検索**］をクリックします。

   c. 開いた［**クエリパラメータ**］ウィンドウで、［**サーバー**］フィールドをクリックします。

   d. Kaspersky Security Center と統合されているサーバーのドロップダウンリストから Kaspersky Industrial CyberSecurity for Networks サーバーを選択し、［**検索**］をクリックします。

   e. Kaspersky Industrial CyberSecurity for Networks Server の名前の横にある［**サーバーに移動**］をクリックします。

      Kaspersky Industrial CyberSecurity for Networks のサインインページが表示されます。

      Kaspersky Industrial CyberSecurity for Networks Web インターフェイスにログインするには、アプリケーションのユーザーアカウントの認証情報を提供する必要があります。

# ユーザーとユーザーロールの管理

このセクションでは、ユーザーとユーザーロールの概要および作成と編集の手順、ユーザーへのロールとグループの割り当て方法、ポリシーのプロファイルとロールの関連付けの方法について説明しています。

## ユーザーアカウントについて

Kaspersky Security Center Linux では、ユーザーアカウントとセキュリティグループを管理できます。アプリケーションは、次の 3 種類のアカウントをサポートしています：

- 組織の従業員のアカウント。管理サーバーは、組織のドメインコントローラーをポーリングする時に、ドメインユーザーのアカウントのデータを取得します。
- ローカルユーザーのアカウント管理対象デバイスのローカルアカウントと、管理サーバーがインストールされているデバイスのローカルアカウント。
- Kaspersky Security Center Linux の内部ユーザーのアカウント。内部ユーザーのアカウントを作成できます。これらのアカウントは、Kaspersky Security Center Linux 内でのみ使用されます。

kladmins グループを使用して、Kaspersky Security Center Linux の Kaspersky Security Center Web コンソールにアクセスすることはできません。kladmins グループには、Kaspersky Security Center Linux サービスを開始するために使用されるアカウントのみを含めることができます。

*ユーザーアカウントとセキュリティグループのテーブルを表示するには、次の手順を実行します：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動します。
2. ［**ユーザー**］タブまたは［**グループ**］タブを選択します。

ユーザーまたはセキュリティグループのテーブルが開きます。内部ユーザーまたはグループのみ、またはローカルユーザーまたはグループのみを含むテーブルを表示する場合は、［**サブタイプ**］フィルター条件をそれぞれ［**内部**］または［**ローカル**］に設定します。

## ユーザーロールの概要

*ユーザーロール*（省略して「*ロール*」とも表記）は、複数の権限をまとめたものと捉えることができます。ロールは、ユーザーのデバイスにインストールされているカスペルスキー製品の設定と関連付けることができます。ロールは、管理グループ、管理サーバー、または特定のオブジェクトのレベルのユーザーまたはセキュリティグループの階層構造の任意のレベルに位置する一連のユーザーまたは一連のセキュリティグループに割り当てることができます。

仮想管理サーバーを含む管理サーバーの階層を介してデバイスを管理する場合は、物理管理サーバーからのみユーザーロールを作成、変更、または削除できることに注意してください。次に、仮想サーバーを含むセカンダリ管理サーバーにユーザーロールを適用できます。

ユーザーロールはポリシーのプロファイルに関連付けることができます。ユーザーにロールを割り当てることで、このユーザーには、担当業務を実行する上で必要なセキュリティ設定が適用されます。

ユーザーロールは、特定の管理グループのデバイスのユーザーに関連付けることができます。

### ユーザーロールの対象範囲

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

### ロールを使用する利点

ロールを使用する利点として、管理対象デバイスごとあるいはユーザーごとに個別にセキュリティ設定を指定しなくて済む点があります。社内のユーザー数とデバイス数は組織の規模に応じて膨大になる場合がありますが、個別のセキュリティ設定を指定すべき担当業務の区分の数はそれほど多くはないはずです。

### ポリシーのプロファイルの使用との相違点と関連性

ポリシーのプロファイルは、各カスペルスキー製品に対して個別に作成されているポリシーのプロパティとして指定されています。ロールは、そうした様々なカスペルスキー製品に対して作成されている多数のプロファイルに 1 つのロールを関連付けることができます。つまり、ロールは、特定の種別のユーザーを対象とする複数の製品の設定を一元的に管理する目的で使用できます。

# 製品機能のアクセス権の設定：ロールベースのアクセス制御

Kaspersky Security Center Linux には、Kaspersky Security Center Linux と管理対象のカスペルスキー製品の機能へロールに基づくアクセスを提供する機能があります。

Kaspersky Security Center Linux ユーザーのアプリケーション機能へのアクセス権は、次のいずれかの方法で設定できます：

- 各ユーザーまたはユーザーグループに対する権限を個別に設定します。
- 事前定義された一連の権限を持つ標準のユーザーロールを作成し、職務の範囲に応じてそれらのロールをユーザーに割り当てる。

ユーザーロールの適用は、アプリケーション機能に対するユーザーのアクセス権を設定する定型的な手順を簡素化および短縮することを目的としています。ロール内のアクセス権は、標準タスクとユーザーの職務範囲に従って設定されます。

ユーザーロールには、それぞれの目的に対応する名前を割り当てることができます。作成できるロール数に制限はありません。

事前定義されたユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。

# 製品機能のアクセス権

次の表は、関連するタスク、レポート、設定を管理し、関連するユーザー操作を実行するためのアクセス権を備えた Kaspersky Security Center Linux の機能を示しています。

表に一覧表示されているユーザー操作を実行するには、ユーザーは操作内容の横に指定された権限を有している必要があります。

［**読み取り**］、［**書き込み**］、および［**実行**］の各権限は、あらゆるタスク、レポート、設定に適用されます。これらの権限に加えて、ユーザーは、デバイスの抽出でタスクとレポートおよび設定を管理するため、**デバイスの抽出操作を実行**する権限を持っている必要があります。

**一般的な機能**：**ACL に関係なくオブジェクトにアクセスする**機能領域は、監査を目的としています。この機能領域でユーザーに**読み取り**権限が付与されると、すべてのオブジェクトに対する完全な**読み取り**アクセス権が付与され、ローカル管理者権限（Linux の場合は root）を使用してネットワークエージェント経由で管理サーバーに接続されたデバイスの選択に対して作成されたタスクを実行できるようになります。これらの権限は、公務を遂行するために権限を必要とする限られたユーザーに慎重に付与することを推奨します。

表にないすべてのタスク、レポート、設定、およびインストールパッケージは、**一般的な機能：基本機能**にあります。

製品機能のアクセス権

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
|---|---|---|---|---|---|
| **一般的な機能**：**管理グループの管理** | **書き込み** | • デバイスを管理グループに追加：**書き込み**<br>• 管理グループからデバイスを削除：**書き込み**<br>• 管理グループを別の管理グループに追加：**書き込み**<br>• 別の管理グループから管理グループを削除：**書き込み** | なし | なし | なし |
| **一般的な機能**：**ACL にかかわらずオブジェクトにアクセスする** | **読み取り** | すべてのオブジェクトへの読み取り権限の取得：**読み取り** | なし | なし | 他の権限によって特定のオブジェクトへの読み取りアクセスが禁止されている場合でも、アクセスは許可されます。 |

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
| --- | --- | --- | --- | --- | --- |
| **一般的な機能：基本的な機能** | • **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | • 仮想サーバーのデバイス移動ルール（作成、変更、または削除）：**書き込み**、**デバイスの選択に対する操作を実行**<br>• モバイル（LWNGT）プロトコルのカスタム証明書の取得：**読み取り**<br>• モバイル（LWNGT）プロトコルのカスタム証明書の取得：**書き込み**<br>• NLA 定義のネットワークリストの取得：**読み取り**<br>• NLA 定義のネットワークリストの追加、変更、または削除：**書き込み**<br>• グループのアクセスコントロールリストの表示：**読み取り**<br>• オペレーティングシステムログの表示：**読み取り**<br>• BitLocker で暗号化されたハードドライブへのアクセスを復元するための回復キーを表示します：**実行** | • ［管理サーバーのリポジトリへのアップデートのダウンロード］<br>• ［レポートの配信］<br>• ［インストールパッケージの配布］<br>• ［セカンダリ管理サーバーへのアプリケーションのリモートインストール］ | • ［保護ステータスレポート］<br>• ［脅威レポート］<br>• ［感染が多いデバイスのレポート］<br>• ［定義データベースのステータスレポート］<br>• ［エラーレポート］<br>• ［ネットワーク攻撃のレポート］<br>• ［インストールされているメールシステム保護製品のサマリーレポート］<br>• 「インストールされているワークステーション保護および Windows サーバー保護製品のサマリーレポート」<br>• ［インストールされている境界防御製品のサマリーレポート］<br>• ［インストールされているアプリケーションの種別のサマリーレポート］<br>• ［感染したデバイスのユーザーに関するレポート］<br>• ［セキュリティ問題のレポート］<br>• ［イベントのレポート］<br>• ［ディストリビューションポイントのアクティビティレポート］<br>• 「セカンダリ管理サーバーのレポート」<br>• ［デバイスコントロールイベントのレポート］<br>• ［脆弱性レポート］<br>• ［ブロック対象アプリケーションのレポート］<br>• 「ウェブコントロールレポート」<br>• ［管理対象デバイスの暗号化ステータスレポート］<br>• ［大容量ストレージデバイスの暗号化ステータスレポート］<br>• ［暗号化されたドライブへのアクセス権に関するレポート］<br>• ［ファイル暗号化のエラーに関するレポート］<br>• ［暗号化されたファイルへのアクセスの | なし |

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
| --- | --- | --- | --- | --- | --- |
| | | | | ブロックに関するレポート］<br>• 「有効なユーザー権限のレポート」<br>• ［ユーザー権限のレポート］ | |
| **一般的な機能：削除されたオブジェクト** | • **読み取り**<br>• **書き込み** | • ごみ箱に削除されたオブジェクトの表示：**読み取り**<br>• ごみ箱からオブジェクトを削除：**書き込み** | なし | なし | なし |
| **一般的な機能：イベント処理** | • **イベントの削除**<br>• **イベント通知設定の編集**<br>• **イベントログ設定の編集**<br>• **書き込み** | • イベント登録設定の変更：**イベントログ設定の編集**<br>• イベント通知設定の変更：**イベント通知設定の編集**<br>• イベントの削除：**イベントの削除** | なし | なし | 設定：<br>• データベース内に保存されるイベント数の上限<br>• 削除されたデバイスからのイベントを保存する期間 |
| **一般的な機能：管理サーバー上での操作** | • **読み取り**<br>• **書き込み**<br>• **実行**<br>• **オブジェクト ACL の変更**<br>• **デバイスの抽出での操作の実行** | • ネットワークエージェント接続用の管理サーバーのポートを指定：**書き込み**<br>• 管理サーバーで起動した Activation Proxy のポートを指定：**書き込み**<br>• 管理サーバー上で開始したモバイル用の Activation Proxy のポートを指定：**書き込み**<br>• スタンドアロンパッケージの配布用の Web サーバーのポートを指定：**書き込み**<br>• MDM プロファイル配布用の Web サーバーのポートを指定：**書き込み**<br>• Web コンソール経由で接続するための管理サーバーの SSL ポートを指定：**書き込み**<br>• モバイル接続用の管理サーバーのポートを指定：**書き込み**<br>• 管理サーバーデータベースに記録するイベント数の上限を指定：**書き込み**<br>• 管理サーバーが送信可能なイベント数の上限を指定：**書き込み**<br>• 管理サーバーがイベントを送信できる期間を指定：**書き込み** | • ［管理サーバーデータのバックアップ］<br>• データベースのメンテナンス | なし | なし |

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
|---|---|---|---|---|---|
| **一般的な機能：カスペルスキー製品の導入** | • **カスペルスキー製品のパッチの管理**<br>• **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | パッチのインストールの承認または拒否：**カスペルスキー製品のパッチの管理** | なし | • ［仮想管理サーバーによるライセンス使用のレポート］<br>• ［カスペルスキー製品バージョンレポート］<br>• ［互換性のないアプリケーションのレポート］<br>• ［カスペルスキー製品のモジュールアップデートのバージョンに関するレポート］<br>• ［製品導入レポート］ | インストールパッケージ：<br>「カスペルスキー」 |
| **一般的な機能：ライセンス管理** | • **ライセンス情報ファイルのエクスポート**<br>• **書き込み** | • ライセンス情報ファイルのエクスポート：**ライセンス情報ファイルのエクスポート**<br>• 管理サーバーのライセンス設定を変更：**書き込み** | なし | なし | なし |
| **一般的な機能：適用されたレポートの管理** | • **読み取り**<br>• **書き込み** | • ACL にかかわらずレポートを作成：**書き込み**<br>• ACL にかかわらずレポートを実行：**読み取り** | なし | なし | なし |
| **一般的な機能：管理サーバーの階層構造** | **管理サーバー階層の設定** | • セカンダリ管理サーバーの登録、アップデート、または削除：**管理サーバー階層の設定** | なし | なし | なし |
| **一般的な機能：ユーザー権限** | **オブジェクト ACL の変更** | • 任意のオブジェクトのセキュリティプロパティの変更：**オブジェクト ACL の変更**<br>• ユーザーロールの管理：**オブジェクト ACL の変更**<br>• 内部ユーザーの管理：**オブジェクト ACL の変更**<br>• セキュリティグループの管理：**オブジェクト ACL の変更**<br>• エイリアスの管理：**オブジェクト ACL の変更** | なし | なし | なし |
| **一般的な機能：仮想管理サーバー** | • **仮想管理サーバーの管理**<br>• **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | • 仮想管理サーバーのリストの取得：**読み取り**<br>• 仮想管理サーバーに関する情報の取得：**読み取り**<br>• 仮想管理サーバーの作成、更新、または削除：**仮想管理サーバーの管理**<br>• 仮想管理サーバーの別のグループへの移動：**仮想管理サーバーの管理**<br>• 仮想管理サーバーの権限の設定：**仮想管理サーバーの管理** | なし | なし | なし |
| **全般的な機能：暗号化鍵の管理** | **書き込み** | 暗号化鍵をインポート：**書き込み** | なし | なし | なし |

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
| --- | --- | --- | --- | --- | --- |
| **モバイルデバイス管理**：**全般** | • **新しいデバイスの接続**<br>• **モバイルデバイスへの情報コマンドのみの送信**<br>• **モバイルデバイスへのコマンドの送信**<br>• **証明書の管理**<br>• **読み取り**<br>• **書き込み** | • ライセンス管理サービスの復元データの取得：**読み取り**<br>• ユーザー証明書の削除：**証明書の管理**<br>• ユーザー証明書の公開部分の取得：**読み取り**<br>• 公開鍵インフラストラクチャが有効になっているかどうかの確認：**読み取り**<br>• 公開鍵インフラストラクチャアカウントの確認：**読み取り**<br>• 公開鍵インフラストラクチャテンプレートの入手：**読み取り**<br>• 拡張キー使用証明書による公開キーインフラストラクチャテンプレートの取得：**読み取り**<br>• 公開鍵インフラストラクチャが取り消されているかどうかの確認：**読み取り**<br>• ユーザー証明書の発行設定の更新：**証明書の管理**<br>• ユーザー証明書の発行設定の取得：**読み取り**<br>• アプリケーション名とバージョンによるパッケージの取得：**読み取り**<br>• ユーザー証明書の設定またはキャンセル：**証明書の管理**<br>• ユーザー証明書の更新：**証明書の管理**<br>• ユーザー証明書タグの設定：**証明書の管理**<br>• MDM インストールパッケージ生成の実行、 MDM インストールパッケージ生成のキャンセル：**新しいデバイスの接続** | なし | なし | なし |
| **システム管理**：**接続性** | • **RDP セッションの開始**<br>• **既存の RDP セッションへの接続**<br>• **トンネリングの開始**<br>• **デバイスから管理者のワークステーションへのファイルの保存**<br>• **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | • デスクトップ共有セッションの作成：**デスクトップ共有セッションの作成権限**<br>• RDPセッションの作成：**既存の RDP セッションへの接続**<br>• トンネルの作成：**トンネリングの開始**<br>• コンテンツネットワークリストの保存：**デバイスから管理者のワークステーションへのファイルの保存** | なし | ［デバイスのユーザーに関するレポート］ | なし |

| 機能領域 | 権限 | ユーザー操作：操作を実行するために必要な権限 | タスク | レポート | その他 |
|---|---|---|---|---|---|
| **システム管理：脆弱性とパッチ管理** | • **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | • サードパーティのパッチプロパティの表示：**読み取り**<br>• サードパーティのパッチプロパティを変更：**書き込み** | • ［脆弱性の修正］<br>• ［アップデートのインストールと脆弱性の修正］ | ［ソフトウェアアップデートレポート］ | なし |
| **システム管理：スクリプトをリモートで実行** | • **読み取り**<br>• **書き込み**<br>• **実行**<br>• **デバイスの抽出での操作の実行** | ユーザーはタスクのプロパティを表示できます：**読み取り**<br>ユーザーはインストールパッケージを作成、削除、または変更できます：**書き込み**<br>ユーザーは［**書き込み**］タスクを実行できます。クライアント Linux デバイスでは、スクリプトはルート権限で実行されます。<br>ユーザーはタスクを実行したり、実行をスケジュールしたりできます：**実行**<br>ユーザーは選択したデバイスでタスクを実行できます：**デバイスの抽出操作を実行** | 「スクリプトをリモートで実行」 | なし | なし |

# 事前定義のユーザーロール

Kaspersky Security Center Linux のユーザーに割り当てられたユーザーロールによって、アプリケーション機能への一連のアクセス権がユーザーに付与されます。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

事前に定義されたユーザーロール（既に設定済みの権限セットを含む）を使用するか、新しいロールを作成できます。新しい役割を作成する際は、役割の範囲を設定し、Kaspersky Security Center Linux の機能へのアクセス権限を自分で割り当てる必要があります。Kaspersky Security Center Linux で使用可能な事前定義済みのユーザーロールの一部は、**監査**、**セキュリティ責任者**、**監督者**などの特定の役職に関連付けることができます。これらのロールのアクセス権は、関連する役職の標準タスクと職務の範囲に従って事前設定されています。次の表に、役割を特定の職位に関連付ける方法を示します。

特定の職位の役割の例

| ロール | コメント |
|---|---|
| 監査 | 削除されたオブジェクトの表示を含む、すべてのタイプのレポートでのすべての操作、すべての表示操作を許可します（［**削除されたオブジェクト**］領域で［**読み取り**］および［**書き込み**］の許可を付与します）。他の操作は許可されません。このロールは、組織の監査を実行する人に割り当てることができます。 |
| 上長・監督者 | すべての表示操作を許可します。他の操作は許可されません。組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。 |
| セキュリティ責任者 | すべての表示操作を許可し、レポート管理を許可します。**システム管理**：**接続**領域で制限付きのアクセス許可を付与します。組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。 |

次の表に、事前定義された各ユーザーロールに割り当てられているアクセス権を示します。

事前定義されたユーザーロールのアクセス権

| ロール | 説明 |
| --- | --- |
| 管理サーバーの管理者 | 次の機能領域でのすべての操作を許可します：<br>• **一般的な機能**：<br>  • **基本機能**<br>  • **暗号化鍵の管理**<br>  • **イベント処理**<br>  • **管理サーバーの階層構造**<br>  • **仮想管理サーバー**<br>• **システム管理**：<br>  • **接続**<br>  • **ハードウェアインベントリ**<br>  • **ソフトウェアインベントリ** |
| 管理サーバーのオペレーター | 次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します：<br>• **一般的な機能**：<br>  • **基本機能**<br>  • **暗号化鍵の管理**<br>  • **仮想管理サーバー**<br>• **システム管理**：<br>  • **接続**<br>  • **ハードウェアインベントリ**<br>  • **ソフトウェアインベントリ** |
| 監査 | ［**一般的な機能**］の次の機能領域におけるすべての操作を許可します：<br>• **ACL にかかわらずオブジェクトにアクセスする**<br>• **削除されたオブジェクト**<br>• **適用されたレポートの管理**<br>このロールは、組織の監査を実行する人に割り当てることができます。 |
| インストールの管理者 | 次の機能領域でのすべての操作を許可します：<br>• **一般的な機能：**<br>  • **基本機能**<br>  • **カスペルスキー製品の導入**<br>  • **ライセンス管理**<br>• **システム管理：**<br>  • **オペレーティングシステムの導入：**<br>  • **脆弱性とパッチ管理**<br>  • **リモートインストール**<br>  • **ソフトウェアインベントリ**<br>［**一般的な機能：仮想管理サーバー**］機能領域における**読み取り**と**実行**の権限を付与します。 |

| ロール | 説明 |
| --- | --- |
| インストールのオペレーター | 次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します：<br>• **一般的な機能：**<br>  • **基本機能**<br>  • **カスペルスキー製品の導入**（この領域で**カスペルスキー製品のパッチの管理**も許可されます）<br>  • **仮想管理サーバー**<br>• **システム管理：**<br>  • **オペレーティングシステムの導入：**<br>  • **脆弱性とパッチ管理**<br>  • **リモートインストール**<br>  • **ソフトウェアインベントリ** |
| Kaspersky Endpoint Security の管理者 | 次の機能領域でのすべての操作を許可します：<br>• **一般的な機能：基本的な機能**<br>• **一般的な機能：暗号化鍵の管理**<br>• **Kaspersky Endpoint Security** の領域（すべての機能を含む） |
| Kaspersky Endpoint Security オペレーター | 次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します：<br>• **一般的な機能：基本的な機能**<br>• **一般的な機能：暗号化鍵の管理**<br>• すべての機能を含む **Kaspersky Endpoint Security** のエリア |
| メインの管理者 | 次の領域を除く、**一般的な機能**の機能領域でのすべての操作を許可します。<br>• **ACL にかかわらずオブジェクトにアクセスする**<br>• **適用されたレポートの管理** |
| メインのオペレーター | 次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します：<br>• **一般的な機能**：<br>  • **基本機能**<br>  • **削除されたオブジェクト**<br>  • **暗号化鍵の管理**<br>  • **管理サーバー上での操作**<br>  • **デバイスのタグ**<br>  • **カスペルスキー製品の導入**<br>  • **製品統合**<br>  • **仮想管理サーバー**<br>• **モバイルデバイス管理**の領域（すべての機能を含む）<br>• **システム管理**の領域（すべての機能を含む）<br>• すべての機能を含む **Kaspersky Endpoint Security** のエリア |
| モバイルデバイス管理の管理者 | 次の機能領域でのすべての操作を許可します：<br>• **一般的な機能：基本的な機能**<br>• **モバイルデバイス管理**の領域（すべての機能を含む）<br>**一般的な機能：ライセンス管理**で**ライセンス情報ファイルのエクスポート**権限を付与します。<br>**システム管理：脆弱性とパッチ管理**で**読み取り**権限を付与します。 |
| モバイルデバイス管理のオペレーター | **一般的な機能：基本機能**で**読み取り**と**実行**の権限を付与します。<br>**モバイルデバイス管理**で、**読み取り**および**モバイルデバイスに情報コマンドのみを送信**の権限を付与します：<br>• **全般**<br>• **セルフサービスポータル** |

| ロール | 説明 |
| --- | --- |
| セキュリティ責任者 | ［**一般的な機能**］の次の機能領域におけるすべての操作を許可します：<br>• **ACL にかかわらずオブジェクトにアクセスする**<br>• **適用されたレポートの管理**<br>**システム管理：接続**機能領域で、**読み取り**、**書き込み**、**実行**、**デバイスから管理者のワークステーションへのファイルの保存**、**デバイスの抽出に関する操作の実行**権限を付与します。<br>組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。 |
| セルフサービスポータルのユーザー | ［**モバイルデバイス管理：セルフサービスポータル**］機能領域におけるすべての操作を許可します。 |
| 上長・監督者 | ［**一般的な機能**：**ACL に依存せずオブジェクトにアクセスする**］と［**一般的な機能**：**適用されたレポートの管理**］の機能領域における**読み取り**権限を付与します。<br>組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。 |
| 脆弱性とパッチ管理の管理者 | **一般的な機能**：**基本機能**および**システム管理**（**スクリプトをリモートで実行する機能**を除くすべての機能を含む）機能領域ですべての操作を許可します。 |
| 脆弱性とパッチ管理機能のオペレーター | **一般的な機能**：**基本機能**および**システム管理**（**スクリプトをリモートで実行**する機能を除くすべての機能を含む）の機能領域で、**読み取り**および**実行**（該当する場合）権限を付与します。 |

# 特定のオブジェクトへのアクセス権の割り当て

サーバーレベルでのアクセス権の割り当てに加えて、特定のオブジェクト（特定のタスクなど）へのアクセスを構成できます。本製品では、次のオブジェクトタイプへのアクセス権を指定できます：

- 管理グループ
- タスク
- レポート
- デバイスの抽出
- イベントの抽出

*特定のオブジェクトへのアクセス権を割り当てるには：*

1. オブジェクトタイプに応じて、メインメニューで、対応するセクションに移動します：
   - ［**アセット（デバイス）**］→［**グループ階層構造**］
   - ［**アセット（デバイス）**］→［**タスク**］
   - ［**監視とレポート**］→［**レポート**］
   - ［**アセット（デバイス）**］→［**デバイスの抽出**］
   - ［**監視とレポート**］→［**イベントの抽出**］
2. アクセス権を設定するオブジェクトのプロパティを開きます。
   管理グループまたはタスクのプロパティウィンドウを開くには、オブジェクト名をクリックします。ツールバーのボタンを使用して、他のオブジェクトのプロパティを開くことができます。

3. プロパティウィンドウで、［**アクセス権**］セクションを開きます。

   ユーザーリストが開きます。リストされたユーザーとセキュリティグループには、オブジェクトへのアクセス権があります。既定では、管理グループまたはサーバーの階層を使用する場合、リストとアクセス権は親管理グループまたはプライマリサーバーから継承されます。

4. リストを変更できるようにするには、［**カスタムの権限を使用する**］オプションを有効にします。

5. アクセス権を設定します：

   - リストを変更するには、［**追加**］と［**削除**］を使用します。
   - ユーザーまたはセキュリティグループのアクセス権を指定します。次のいずれかの手順を実行します：
     - アクセス権を手動で指定する場合は、ユーザーまたはセキュリティグループを選択し、［**アクセス権**］をクリックして、アクセス権を指定します。
     - ユーザーまたはセキュリティ グループにユーザーロールを割り当てる場合は、ユーザーまたはセキュリティグループを選択し、［**ロール**］をクリックして、割り当てるロールを選択します。

6. ［**保存**］をクリックします。

オブジェクトへのアクセス権が設定されます。

# ユーザーとセキュリティグループへのアクセス権の割り当て

ユーザーおよびセキュリティグループに、Kaspersky Endpoint Security for Linux などの管理サーバーの様々な機能を使用するためのアクセス権を付与できます。

*ユーザーまたはセキュリティグループへのアクセス権を割り当てるには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**アクセス権**］タブで、権限を割り当てるユーザーまたはセキュリティグループの名前の横にあるチェックボックスをオンにし、［**アクセス権**］をクリックします。

   複数のユーザーまたはセキュリティグループを同時に選択することはできません。複数のアイテムを選択すると、［**アクセス権**］がオフになります。

3. ユーザーまたはグループの権限セットを構成します：

   a. 管理サーバーまたは他のカスペルスキー製品の機能を含むノードを展開します。

   b. 必要な機能またはアクセス権の横にある［**許可**］または［**拒否**］をオンにします。

      *例 1：*［**製品統合**］ノードの横にある［**許可**］を選択して、アプリケーション統合機能（［**読み取り**］、［**書き込み**］、および［**実行**］）に対する使用可能なすべてのアクセス権をユーザーまたはグループに付与します。

      *例 2：*［**暗号化鍵の管理**］ノードを展開し、［**書き込み**］アクセス許可の横にある［**許可**］をオンにして、ユーザーまたはグループの暗号化鍵管理機能への［**書き込み**］アクセス権を付与します。

4. アクセス権のセットを構成した後、［OK］をクリックします。

ユーザーまたはユーザーグループに対する一連の権限が設定されます。

管理サーバー（または管理グループ）の権限は、次の領域から構成されます。

- 一般的な機能：
  - 管理グループの管理
  - ACL にかかわらずオブジェクトにアクセスする
  - 基本機能
  - 削除されたオブジェクト
  - 暗号化鍵の管理
  - イベント処理
  - 管理サーバー上での操作（管理サーバーのプロパティウィンドウのみ）
  - デバイスのタグ
  - カスペルスキー製品の導入
  - ライセンス管理
  - アプリケーションの統合
  - 適用されたレポートの管理
  - 管理サーバーの階層
  - ユーザーのアクセス許可
  - 仮想管理サーバー
- モバイルデバイス管理：
  - 全般
  - セルフサービスポータル
- システム管理：
  - 接続
  - スクリプトをリモートで実行
  - ハードウェアインベントリ
  - ネットワークアクセスコントロール
  - オペレーティングシステムの導入
  - 脆弱性とパッチ管理
  - リモートインストール

- ソフトウェアインベントリ

［**許可**］と［**拒否**］のどちらもオンになっていない場合、アクセス権は［*未定義*］とみなされ、ユーザーに対して明示的に許可ないし拒否されるまでは拒否されます。

ユーザーの権限は次から構成されます：

- ユーザー自身の権限
- ユーザーに割り当てられたすべてのロールの権限
- ユーザーが属するすべてのセキュリティグループの権限
- ユーザーが属するセキュリティグループに割り当てられたすべてのロールの権限

これらの権限のうち1つでも［**拒否**］として設定されている場合、他の権限が許可または未定義でも、ユーザーは該当する権限が拒否されます。

また、ユーザーロールのスコープにユーザーとセキュリティグループを追加して、管理サーバーのさまざまな機能を使用することもできます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

# 内部ユーザーのアカウントの追加

ユーザーアカウントを追加する場合は、アカウントに「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限があることを確認してください。

*Kaspersky Security Center Linux に新しい内部ユーザーアカウントを追加するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. ［**追加**］をクリックします。

3. ［**ユーザーを追加**］ウィンドウが開いたら、新しいユーザーアカウントの設定を指定します：

   - **名前**：
   - **パスワード**：Kaspersky Security Center Linux へのユーザーの接続用。
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 256 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
       - アルファベット大文字（A-Z）
       - アルファベット小文字（a-z）
       - 数字（0 - 9）
       - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
     - パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

     入力したパスワードを確認するには、をクリックしてください。
     ［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにすると、最初のユーザー認証時にパスワードの変更を強制できます。

4. 変更を保存して、新しいユーザーアカウントの作成を完了します。

新しいユーザーがユーザーリストに追加されます。

# セキュリティグループの作成

*セキュリティグループを作成するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. ［**追加**］をクリックします。
3. 開いた［**セキュリティグループの作成**］ウィンドウで、新しいセキュリティグループに次の設定を指定します：
   - **グループ名**
   - **説明**
4. ［**保存**］をクリックして変更内容を保存します。

新しいセキュリティグループがグループリストに追加されます。

# 内部ユーザーのアカウントの編集

ユーザーアカウントを編集する場合は、アカウントに「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限があることを確認してください。

*Kaspersky Security Center Linux で内部ユーザーアカウントを編集するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。

2. 編集するユーザーアカウントの名前をクリックします。

3. ユーザー設定ウィンドウが表示されるので、［**全般**］タブで、ユーザーアカウントの設定を変更します：

- **ユーザーアカウント**

  必要に応じて、スイッチを［**非アクティブ**］に切り替えることで、ユーザーの本製品への接続をブロックできます。たとえば、従業員が退職したあとなどにアカウントを無効化できます。

- 説明
- **完全名**
- **メールアドレス**
- **電話番号**
- **パスワード**

  必要に応じて、次のようにして Kaspersky Security Center Linux へのユーザー接続用の新しいパスワードを設定できます。

  a. ［**パスワードの変更**］をクリックし、ユーザーアカウントの新しいパスワードを設定します。
  パスワードは次のルールに従う必要があります：

  - パスワードは、8 文字以上 256 文字以下にしてください。
  - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
    - アルファベット大文字（A-Z）
    - アルファベット小文字（a-z）
    - 数字（0 - 9）
    - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
  - パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

  入力したパスワードを確認するには、をクリックしてください。

  b. 必要に応じて、［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにして、次回のユーザー認証時にパスワードの変更を強制します。

  c. ユーザーアカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。

4. ［**認証セキュリティ**］タブで、このアカウントに対するセキュリティ設定を指定できます。
5. ［**グループ**］タブで、セキュリティグループにユーザーを追加できます。
6. ［**デバイス**］タブで、ユーザーにデバイスを割り当てることができます。

7. ［**ロール**］タブで、ユーザーにロールを割り当てることができます。

8. 変更を保存して、ユーザーアカウントの編集を完了します。

ユーザーのリストにアップデートしたユーザーアカウントが表示されます。

# セキュリティグループの編集

*セキュリティグループを編集するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。

2. 編集するセキュリティグループの名前をクリックします。

3. 開いたグループ設定ウィンドウで、セキュリティグループの設定を変更します：

   - ［**全般**］タブでは、［**名前**］と［**説明**］設定を変更できます。これらの設定は、内部セキュリティグループのみが使用できます。

   - ［**ユーザー**］タブでは、ユーザーをセキュリティグループに追加できます。この設定は、内部ユーザーおよび内部セキュリティグループのみが使用できます。

   - ［**ロール**］タブで、セキュリティグループにロールを割り当てることができます。

4. ［**保存**］をクリックして変更内容を保存します。

変更はセキュリティグループに適用されます。

# ユーザーまたはセキュリティグループへのロールの割り当て

*ユーザーまたはセキュリティグループへロールを割り当てるには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。

2. ロールを割り当てるユーザーまたはセキュリティグループの名前を選択します。

   複数の名前を選択できます。

3. メニュー行で、［**ロールの割り当て**］をクリックします。

   ロールの割り当てウィザードが開始します。

4. ウィザードの手順に従います：選択したユーザーまたはセキュリティグループに割り当てるロールを選択し、ロールの範囲を選択します。

   *ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

管理サーバーを操作する一連の権限を持つロールは、ユーザー（または複数のユーザー、またはセキュリティグループ）に割り当てられます。ユーザーまたはセキュリティグループのリストで、［**ロール割り当て済み**］列にチェックボックスが表示されます。

# 内部セキュリティグループへのユーザーアカウントの追加

内部セキュリティグループに追加できるのは内部ユーザーのアカウントのみです。

*ユーザーアカウントを内部セキュリティグループに追加するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. セキュリティグループに追加するユーザーアカウントに隣接するチェックボックスをオンにします。
3. ［**グループの割り当て**］をクリックします。
4. 開いた［**グループの割り当て**］ウィンドウで、ユーザーアカウントを追加するセキュリティグループを選択します。
5. ［**保存**］をクリックします。

ユーザーアカウントがセキュリティグループに追加されます。グループ設定を使用して、内部ユーザーをセキュリティグループに追加することもできます。

# デバイスの所有者ユーザーの指定

ユーザーをモバイルデバイスの所有者として割り当てる方法の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

*デバイスの所有者ユーザーを指定するには：*

1. 仮想管理サーバーに接続されたデバイスの所有者を割り当てる場合は、まず仮想管理サーバーに切り替えます：

   a. メインメニューで、現在の管理サーバー名の右側にあるシェブロンアイコン（）をクリックします。

   b. 必要な管理サーバーを選択します。

2. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。

   ユーザーリストが開きます。現在、仮想管理サーバーに接続している場合、リストには現在の仮想管理サーバーとプライマリ管理サーバーのユーザーが含まれています。

3. デバイスの所有者に割り当てるユーザーアカウントの名前をクリックします。

4. ユーザー設定ウィンドウが表示されたら、［**デバイス**］を選択します。

5. ［**追加**］をクリックします。

6. デバイスリストから、ユーザーに割り当てるデバイスを選択します。

7. ［**OK**］をクリックします。

選択したデバイスが、ユーザーに割り当てられているデバイスのリストに追加されます。

［**アセット（デバイス）**］→［**管理対象デバイス**］で割り当てるデバイスをクリックし、［**デバイスの所有者の管理**］をクリックする方法でも、同じ処理を実行できます。

# ネットワークエージェントのインストール中にユーザーをデバイスの所有者として割り当てる

インストールパッケージ経由でネットワークエージェントをインストールする時にユーザーをデバイスの所有者として割り当てるには、以下の表に指定されている変数をネットワークエージェントのインストールパッケージ設定に追加します。

| 変数名 | 必須 | 説明 | 指定可能な値 |
|---|---|---|---|
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | いいえ | ネットワークエージェントのインストール後に、ユーザーをデバイスの所有者として登録するためのユーティリティを実行できるようにします。無効にすると、ユーザーはデバイスの所有者として登録できなくなります。 | 1—ネットワークエージェントのインストール後、ユーザーをデバイスの所有者として登録するためのユーティリティが起動します。<br>その他—ユーティリティは使用できません。 |
| KLNAGENT_DEVICEOWNER_LOGIN | いいえ<br>はい（パスワードを入力した場合） | デバイスの所有者として登録されるユーザーのログインが含まれます。 | Kaspersky Security Center Linux のユーザーリストに指定されているユーザーのログイン。 |
| KLNAGENT_DEVICEOWNER_PASSWORD | いいえ<br>はい（ログイン名を入力した場合） | デバイスの所有者として登録されるユーザーの暗号化されたパスワードが含まれます。 | ユーザーのパスワード。 |

ネットワークエージェントは、Kaspersky Security Center Linux のインストール中に指定されたログイン名とパスワードを復号し、ユーザーはデバイスの所有者として登録されます。

応答ファイルを使用してサイレントモードでネットワークエージェントをインストールする時に、ユーザーをデバイスの所有者として割り当てることもできます。

*応答ファイルを使用してサイレントモードでネットワークエージェントをインストールする時に、ユーザーをデバイスの所有者として割り当てるには：*

1. 応答ファイルに KLNAGENT_DEVICEOWNER_REGISTRATION_START パラメータを追加し、「1」に設定します。

   ネットワークエージェントのインストール後、ユーザーをデバイスの所有者として登録するためのユーティリティが起動します。

2. クライアントデバイスのコマンドラインにログイン名とパスワードを入力します。

   ユーザーはデバイスの所有者として割り当てられます。

ユーザーが内部セキュリティグループに含まれている場合、ログイン名にはユーザー名が含まれている必要があります。

ユーザーが Active Directory セキュリティグループに含まれている場合、ログイン名にはユーザー名とドメイン名が含まれている必要があります。

ユーザーに対して二段階認証が有効になっている場合は、アプリから時間に基づくワンタイムパスワード（TOTP）を入力する必要があります。

# ネットワークエージェントのインストール後にユーザーを Linux デバイスの所有者として割り当てる

*ユーザーが Linux デバイスの所有者として登録できるようにするには：*

1. Kaspersky Security Center Web コンソールで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］に移動します。

   インストールパッケージのリストが開きます。

2. ネットワークエージェントのインストールパッケージをクリックします。

   インストールパッケージのプロパティウィンドウが表示されます。

3. インストールパッケージのプロパティウィンドウで、［**設定**］→［**詳細**］をクリックします。

4. ［**デバイス所有者としてのユーザー登録（Linux のみ）**］セクションで、［**ネットワークエージェントのインストール後にユーザー登録ユーティリティの実行を許可する**］をオンにして、［**保存**］をクリックします。

ユーザーをデバイスの所有者として登録するためのユーティリティは、クライアントデバイスのコマンドラインから実行できます。

*クライアントデバイスでユーザーを Linux デバイスの所有者として登録するには：*

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. 要求された場合、ログイン名とパスワードを入力します。
   ログイン名とパスワードがネットワークエージェントの応答ファイルまたはインストールパッケージに含まれている場合は、クライアントデバイスのコマンドラインで次のコマンドを実行します：
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

ユーザーが内部セキュリティグループに含まれている場合、ログイン名にはユーザー名が含まれている必要があります。

ユーザーが Active Directory セキュリティグループに含まれている場合、ログイン名にはユーザー名とドメイン名が含まれている必要があります。

ユーザーに対して二段階認証が有効になっている場合は、アプリから時間に基づくワンタイムパスワード（TOTP）を入力する必要があります。

ユーザーはデバイスの所有者として登録されます。

# デバイスの所有者ユーザーの削除

*クライアントデバイスでデバイスの所有者としてのユーザーを削除するには：*

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：
   `$ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner`

2. ユーザー名とパスワードを入力します。

ユーザーが内部セキュリティグループに含まれている場合、ログイン名にはユーザー名が含まれている必要があります。

ユーザーが Active Directory セキュリティグループに含まれている場合、ログイン名にはユーザー名とドメイン名が含まれている必要があります。

ユーザーに対して二段階認証が有効になっている場合は、アプリから時間に基づくワンタイムパスワード（TOTP）を入力する必要があります。

ユーザーはデバイスの所有者から削除されます。

# 不正な変更からのユーザーアカウントの保護を有効にする

追加のオプションを有効にして不正な変更からのユーザーアカウントの保護を有効にすることができます。このオプションをオンにすると、ユーザーアカウントの編集にはユーザー認証が要求されます。

*不正な変更からのユーザーアカウントの保護を有効または無効にする*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 不正な変更からの保護を指定する内部ユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
4. ［**認証セキュリティ**］タブで、アカウント設定が変更または修正されるたびに認証情報を要求する場合は、［**認証を要求してこのユーザーアカウントの変更権限をチェックする**］をオンにします。そうでない場合は、［**追加の認証なしでのこのアカウントの変更をユーザーに対して許可する**］をオンにします。
5. ［**保存**］をクリックします。

# 二段階認証

このセクションでは、Kaspersky Security Center Web コンソールへの不正なアクセスのリスクを軽減するために二段階認証を使用する方法について説明します。

# シナリオ：すべてのユーザーに対して二段階認証を設定する

このシナリオでは、すべてのユーザーに対して二段階認証を有効にする方法と、二段階認証からユーザーアカウントを除外する方法について説明します。別のユーザーに対する二段階認証を有効にする前に自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初にお使いのアカウントの二段階認証を有効にするウィンドウを開きます。このシナリオでは、自分のアカウントに対して二段階認証を有効にする方法についても説明します。

自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にする手順に進んでください。

## 必須条件

開始する前に：

- ご自分のアカウントに、別のユーザーのアカウントのセキュリティ設定を変更するための［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があることを確認してください。
- 管理サーバーの他のユーザーがデバイス上に認証アプリをインストール済みであることを確認してください。

## 実行するステップ

すべてのユーザーに対して二段階認証を段階的に有効にするには：

1. **認証アプリをデバイスにインストールする**

時間ベースのワンタイムパスワードのアルゴリズム（TOTP）をサポートする任意のアプリケーションをインストールできます。たとえば：

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

Kaspersky Security Center Linux が使用する認証アプリケーションをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

手順の1つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center Linux は選択した認証システムをサポートします。

> 管理サーバーへの接続が確立されているデバイスと同じデバイスに認証アプリをインストールすることは強く推奨しません。

2. **管理サーバーがインストールされているデバイスの時刻と、認証アプリの時刻を同期する**

   外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。そうしないと、認証および二段階認証のアクティブ化中に失敗が発生する可能性があります。

3. **自分のアカウントの二段階認証を有効にし、アカウントの秘密鍵を受け取る**

   自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にできるようになります。

4. **すべてのユーザーに対して二段階認証を有効にする**

   二段階認証を有効にしたユーザーは、管理サーバーにログインする際に二段階認証を使用する必要があります。

5. **新規ユーザーが自分で二段階認証を設定することを禁止します**

   Kaspersky Security Center Web コンソールのアクセスセキュリティをさらに向上させるために、新しいユーザーが自分自身に二段階認証を設定することを禁止できます。

6. **セキュリティコードの発行元の名前を変更する**

   同じ名前の管理サーバーがある場合は、異なる管理サーバーとして認識できるように、セキュリティコードの発行元の名前を別のものに変更する必要があります。

7. **二段階認証を有効にする必要のないユーザーアカウントを除外する**

   必要に応じて、二段階認証からユーザーを除外することができます。アカウントが除外されたユーザーは管理サーバーへのログインの際に二段階認証が不要となります。

8. **自分のアカウントの二段階認証を設定します**

   ユーザーが二段階認証から除外されておらず、アカウントに二段階認証がまだ設定されていない場合は、Kaspersky Security Center Web コンソールにサインインする時に開くウィンドウで設定する必要があります。そうしないと、権限に従って管理サーバーにアクセスできなくなります。

### 結果

このシナリオの完了時には：

- 自分のアカウントの二段階認証が有効になります。
- 除外したユーザーアカウント以外の管理サーバーのすべてのユーザーアカウントに対して、二段階認証が有効になります。

## アカウントの二段階認証について

Kaspersky Security Center Linux では、 Kaspersky Security Center Web コンソールのユーザーに対して二段階認証をサポートしています。自分のアカウントに二段階認証が適用されると、Kaspersky Security Center Web コンソールにログインするたびに、ユーザー名、パスワードおよび追加で一回のみ使用するセキュリティコードを入力するようになります。このセキュリティコードを受け取るには、ご使用のコンピューターまたはモバイルデバイスなどに認証アプリがインストールされている必要があります。

セキュリティコードには、*発行元の名前*として参照される識別子があります。セキュリティコードの発行元の名前は、認証アプリの管理サーバーの識別子として使用されます。セキュリティコードの発行元の名前を変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。発行元の名前は、認証アプリの管理サーバーの識別子として使用されます。セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。セキュリティコードは1度のみ使用可能で、最大 90 秒間有効です（正確な時間は異なる場合があります）。

二段階認証が有効になっているユーザーは自分の秘密鍵を再発行できます。ユーザーが再発行された秘密鍵で認証しログインに使用した場合、管理サーバーはユーザーアカウントの新しい秘密鍵を保存します。ユーザーが新しい秘密鍵を誤って入力した場合、管理サーバーは新しい秘密鍵を保存せず、以降の認証は現在使用している秘密鍵を有効なままとします。

Google Authenticator など、Time-based One-time Password（時間に基づいて生成されるワンタイムパスワード）アルゴリズムをサポートする認証アプリを認証アプリケーションとして使用できます。セキュリティコードを生成するためには、認証アプリと管理サーバーの時刻を同期する必要があります。

Kaspersky Security Center Linux が使用する認証アプリケーションをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

手順の1つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center Linux は選択した認証システムをサポートします。

認証アプリは次のようにセキュリティコードを生成します：

1. 管理サーバーが特別な秘密鍵および QR コードを作成します。
2. 生成された秘密鍵または QR コードを認証アプリに入力します。
3. 認証アプリが、管理サーバーの認証ウィンドウに入力する、1度のみ使用するセキュリティコードを生成します。

秘密鍵（またはQRコード）を保存し、安全な場所に保管することを強くお勧めします。これにより、モバイルデバイスにアクセスできなかった際に Kaspersky Security Center Web コンソールへのアクセスを復元することができます。

Kaspersky Security Center Linux を安全に使用するため、自分のアカウントに対して二段階認証を設定し、すべてのユーザーに対して二段階認証を有効にできます。

二段階認証からアカウントを除外することができます。これは認証のためのセキュリティコードを受信できないサービスアカウントで必要となる場合があります。

二段階認証は次のルールに準拠して動作します：

- ［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持つユーザーアカウントのみがすべてのユーザーに対して二段階認証を有効にすることができます。
- 自分のアカウントに対して二段階認証を有効にしたユーザーのみが、すべてのユーザーに対する二段階認証を有効にできます。
- 自分のアカウントに対して二段階認証を有効にしたユーザーのみが、すべてのユーザーに対して有効にされた二段階認証からユーザーを除外できます。
- ユーザーは自分のアカウントに対してのみ二段階認証を有効にできます。
- ［一般的な機能：ユーザー権限］機能エリアの**オブジェクト ACL の変更**権限を持ち、二段階認証を使用して Kaspersky Security Center Web コンソールにログインしたユーザーアカウントが、次の両方の条件が一致する場合にすべてのユーザーに対して二段階認証を無効にすることができます：すべてのユーザーに対する二段階認証が無効になっているその他のユーザー、すべてのユーザーに対して有効にされた二段階認証のリストから除外されたユーザー。
- 二段階認証を使用して Kaspersky Security Center Web コンソールにログインしたすべてのユーザーは自分の秘密鍵を再発行できます。
- 現在作業中の管理サーバーに対してすべてのユーザーに対する二段階認証を有効にすることができます。管理サーバーのこのオプションをオンにすると、管理サーバーの仮想管理サーバーのユーザーアカウントに対してもこのオプションをオンにすることになり、セカンダリ管理サーバーのユーザーアカウントの二段階認証は有効にされません。

# 自分のアカウントの二段階認証を有効にする

自分のアカウントの二段階認証を有効にすることができます。

アカウントの二段階認証を有効にする前に、使用中のモバイルデバイスに認証アプリがインストールされていることを確認してください。認証アプリと管理サーバーがインストールされているデバイスの時刻が同期されていることを確認します。

*ユーザーアカウントの二段階認証を有効にするには：*

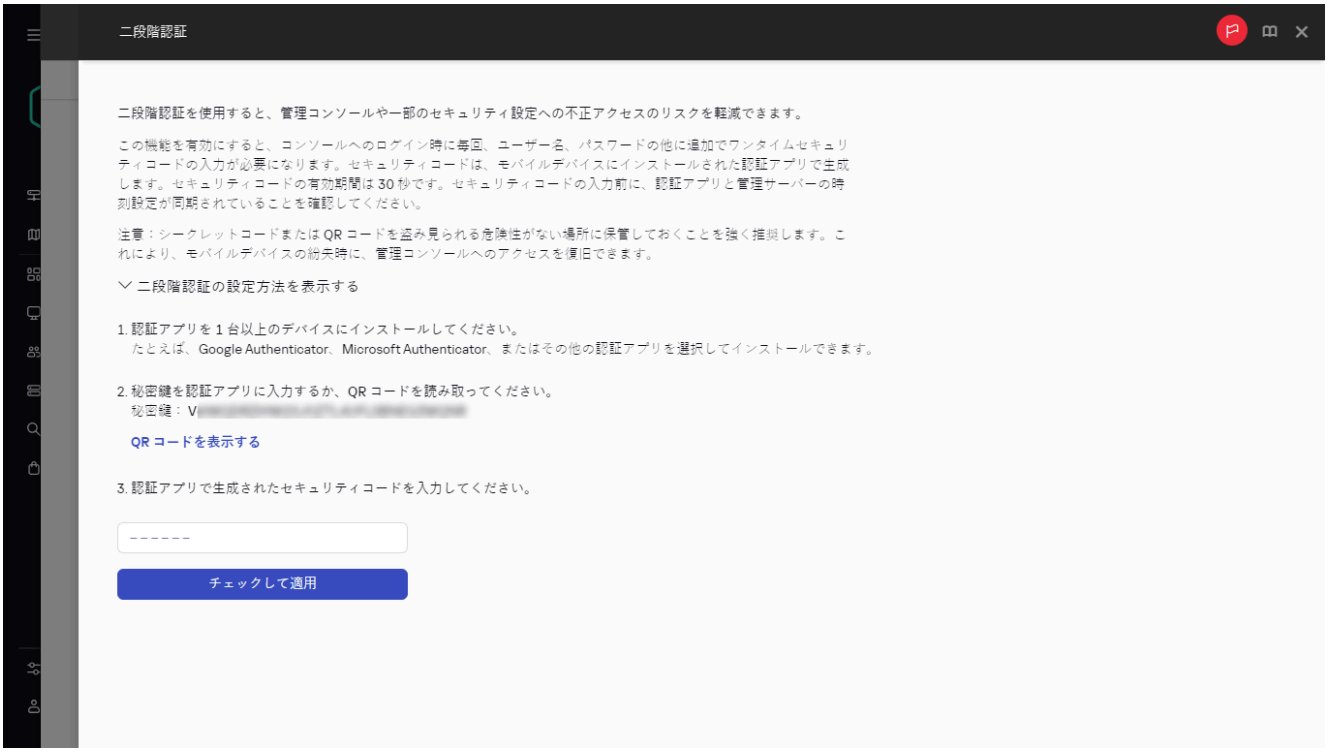
1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 自分のアカウントの名前をクリックします。

3. ユーザー設定ウィンドウが開いたら、［**認証セキュリティ**］タブを選択します。

a. ［**ユーザー名、パスワード、セキュリティコードを要求（二段階認証）**］をオンにします。［**保存**］をクリックします。

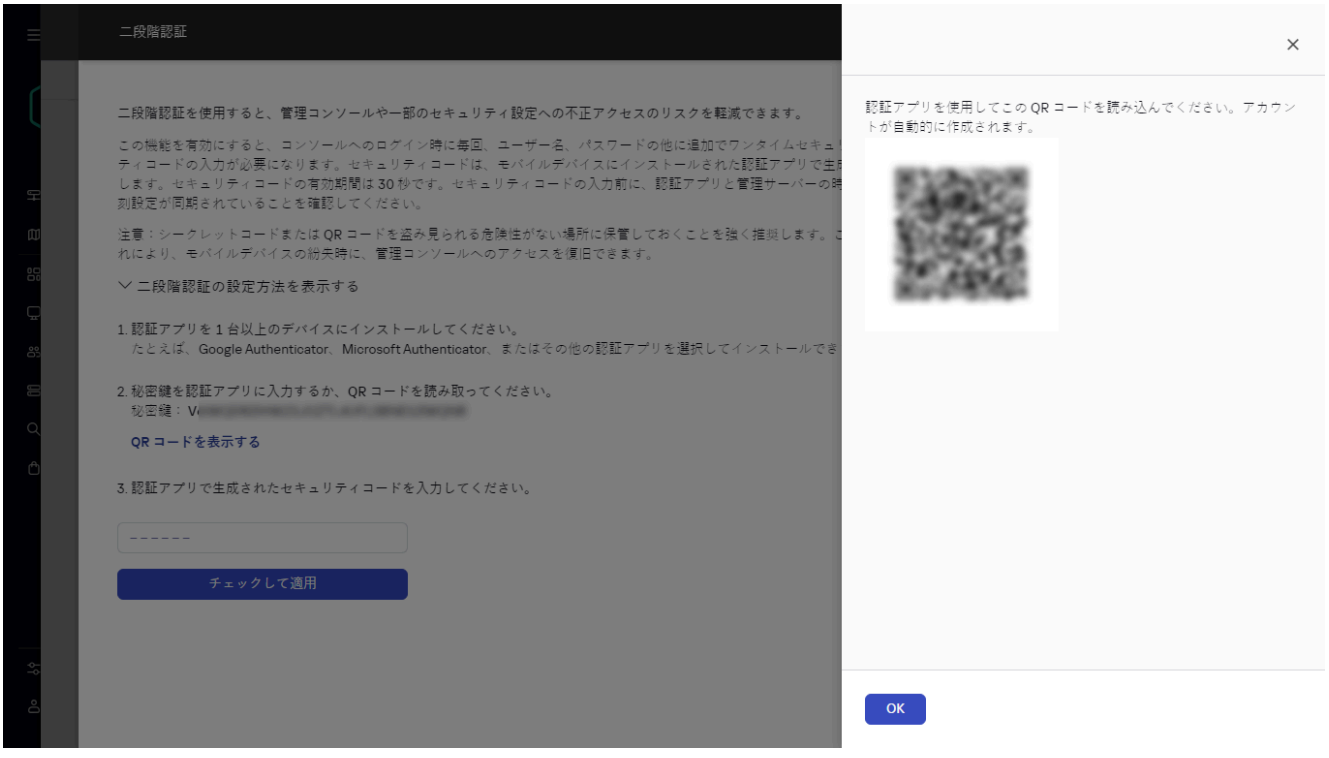
b. 開いた［二段階認証］ウィンドウで、［**二段階認証の設定方法を表示する**］をクリックします。

［**QR コードを表示する**］**をクリックします。**



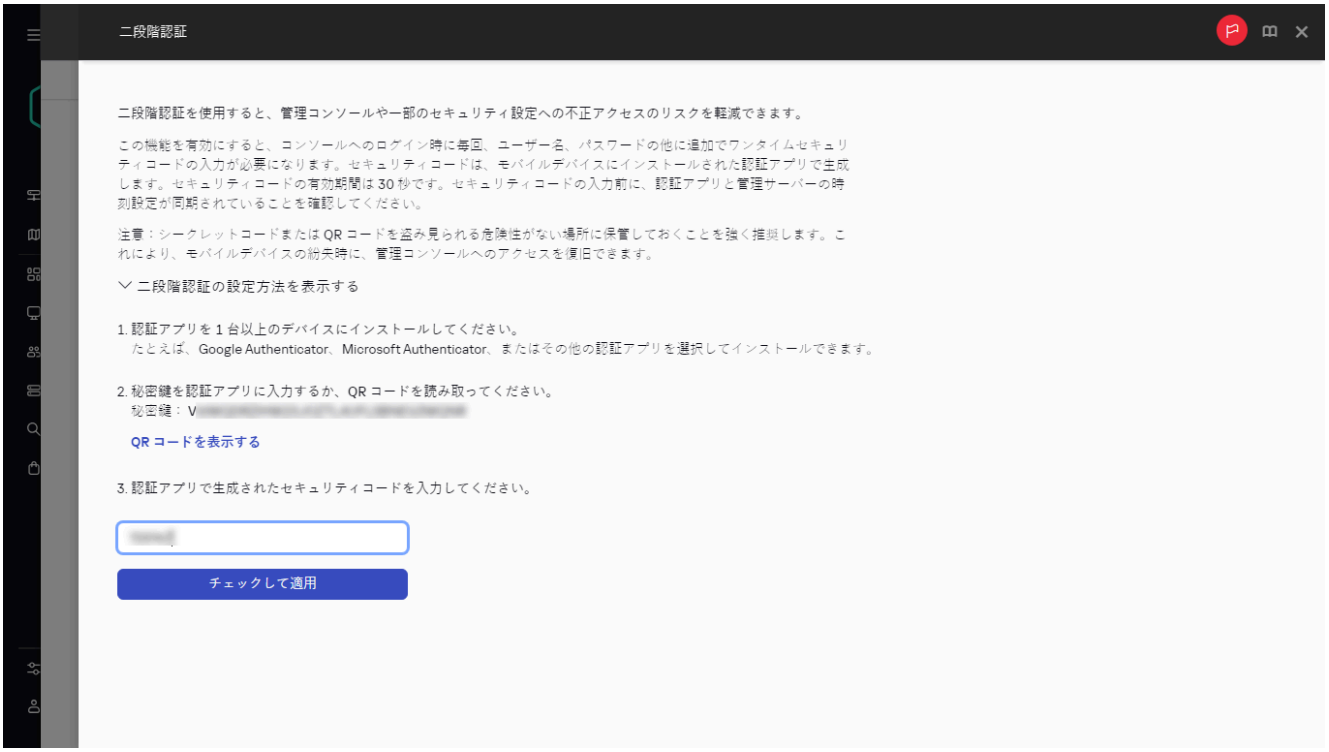

認証アプリ用の QR コードを生成する

a. モバイルデバイスの認証アプリに QR コードをスキャンして、ワンタイムセキュリティコードを受け取ります。




認証アプリの QR コード

a. 二段階認証のウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。




認証アプリからセキュリティコードを入力する

4. ［**保存**］をクリックします。

自分のアカウントの二段階認証が有効になります。

モバイルデバイスの認証アプリに QR コードをスキャンして、ワンタイムセキュリティコードを受け取ります。

# 全ユーザーに対して二段階認証の有効化

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、管理サーバーのすべてのユーザーに対して二段階認証を有効にすることができます。

*すべてのユーザーに対して二段階認証を有効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. プロパティウィンドウの［**認証セキュリティ**］タブで、**全ユーザーに対する二段階認証**の切り替えスイッチを有効の位置に移動します。

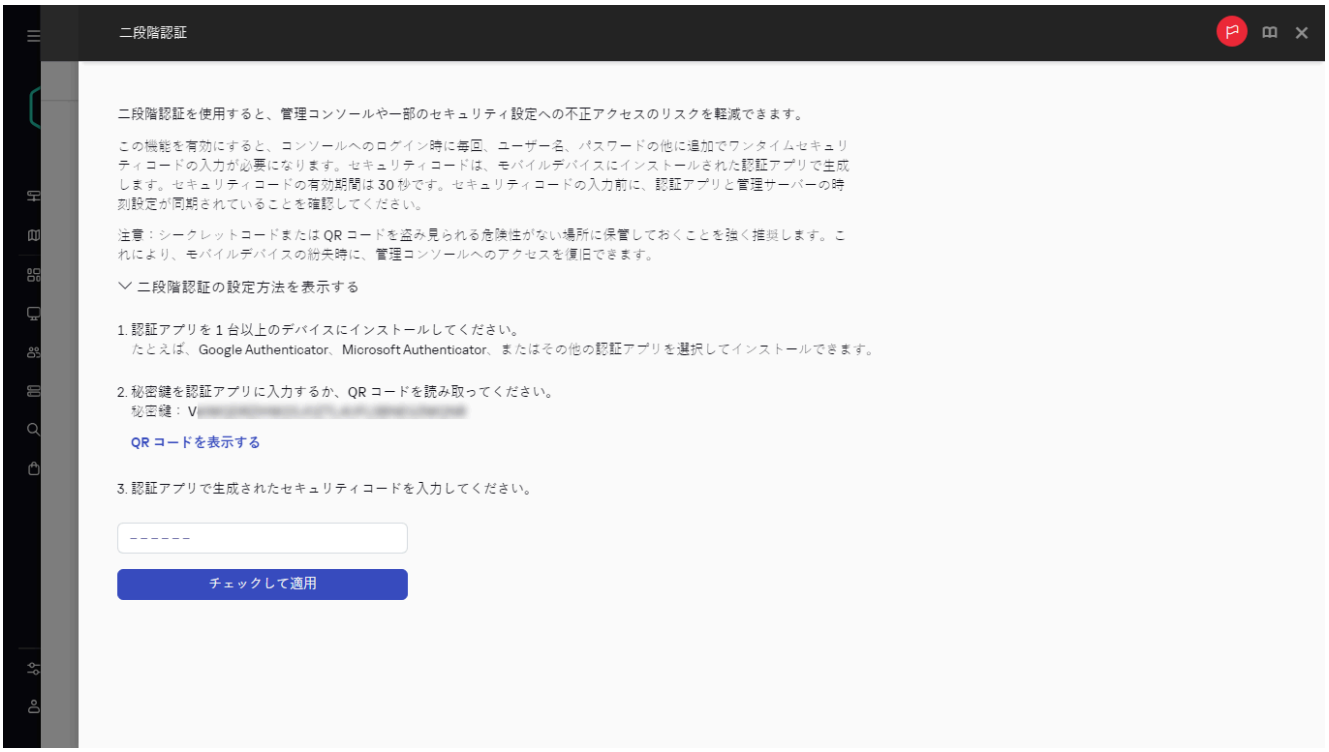



すべてのユーザーに対して二段階認証を有効にする

3. 自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初に自分のアカウントの二段階認証を有効にするウィンドウを開きます。

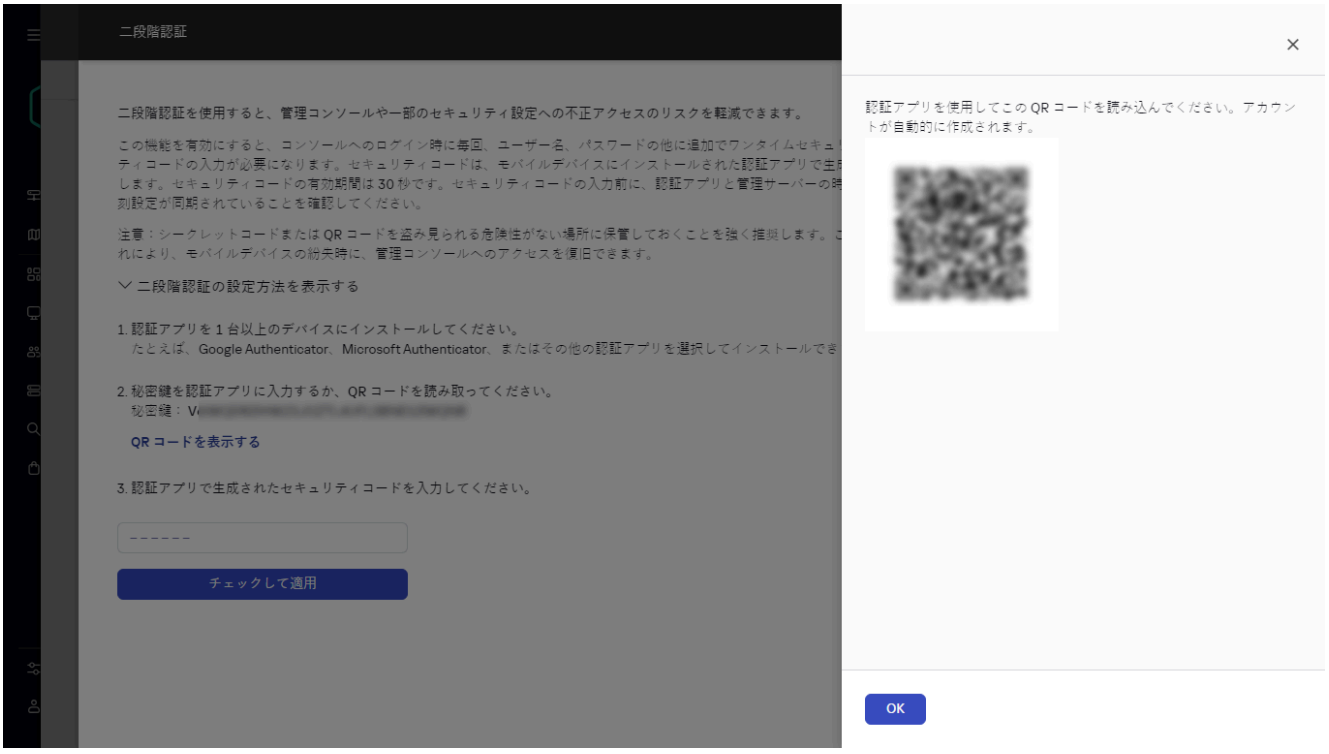
   a. ［二段階認証］ウィンドウで、［**二段階認証の設定方法を表示する**］をクリックします。

   b. ［**QR コードを表示する**］**をクリックします。**




認証アプリケーション用の QR コードを生成する

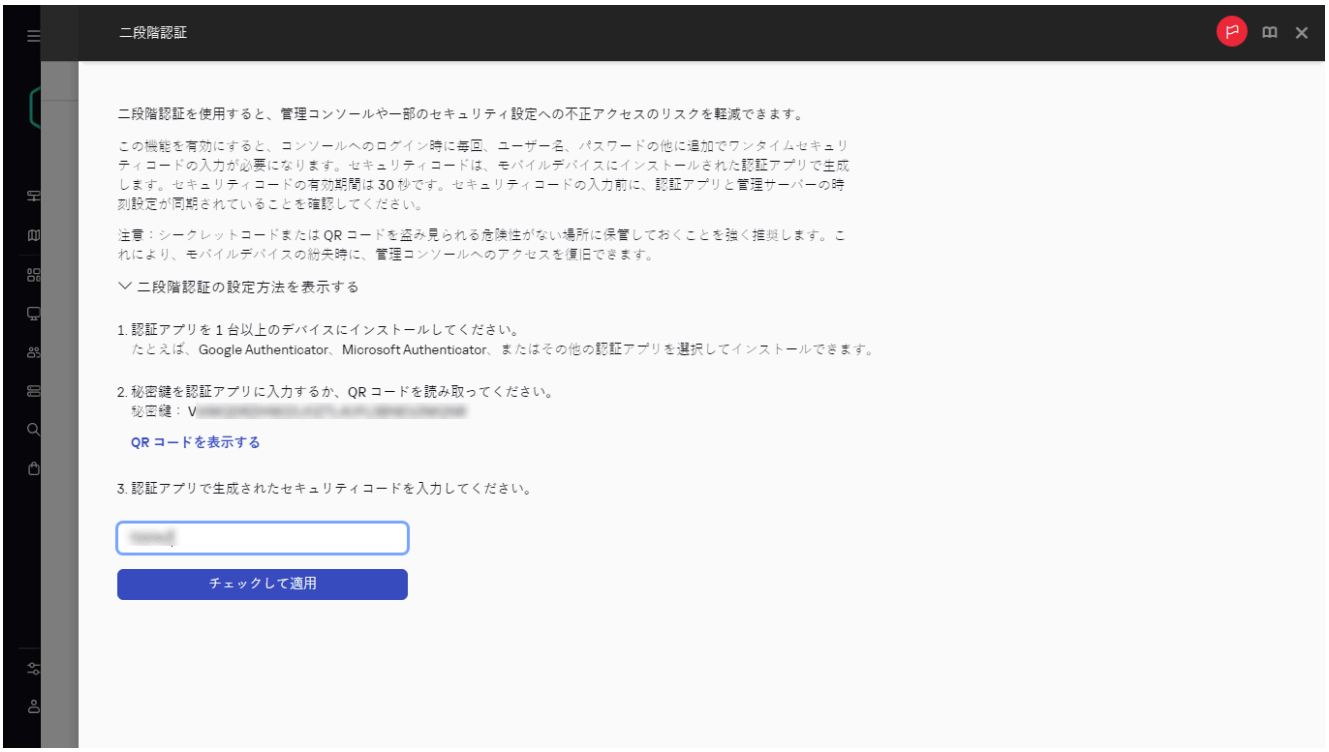
a. モバイルデバイスの認証アプリケーションで QR コードをスキャンして、ワンタイムセキュリティコードを受け取ります。




認証アプリケーション用の QR コード

または、認証アプリケーションに秘密鍵を手動で入力します。

a. 二段階認証のウィンドウで、認証アプリケーションが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。




認証アプリケーションからセキュリティコードを入力する

すべてのユーザーに対して二段階認証が有効になります。以降、すべてのユーザーに対する二段階認証を有効にする前に追加されたユーザーを含む管理サーバーのユーザーは、アカウントが二段階認証の対象から除外されたユーザー以外全員、アカウントに二段階認証を設定する必要があります。

# ユーザーアカウントの二段階認証を無効にする

ご自分のアカウント、または別のユーザーの二段階認証を無効にすることができます。

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、他のユーザーアカウントの二段階認証を無効にすることができます。

*ユーザーアカウントの二段階認証を無効にするには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 二段階認証を無効にする内部ユーザーアカウントの名前をクリックします。この名前は、ご自分のアカウントまたは別のユーザーのアカウントです。
3. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
4. ユーザーアカウントの二段階認証を無効にする場合は、［**ユーザー名とパスワードのみ要求**］をオンにします。
5. ［**保存**］をクリックします。

このユーザーアカウントの二段階認証が無効になります。

二段階認証を使用して Kaspersky Security Center Web コンソールにログインできないユーザーのアクセスを復元する場合は、このユーザーアカウントの二段階認証を無効にし、上記のように［**ユーザー名とパスワードのみ要求**］をオンにします。その後、二段階認証を無効にしたユーザーアカウントで Kaspersky Security Center Web コンソールにログインし、再度認証を有効にします。

# 全ユーザーに対して二段階認証の無効化

自分のアカウントで二段階認証が有効になっており、［**一般的な機能：ユーザー権限**］のオブジェクト ACL の変更権限がある場合にすべてのユーザーに対して必要な二段階認証を無効にすることができます。ご自身のアカウントで二段階認証が有効にされていない場合、すべてのユーザーに対して二段階認証を無効にする前にご自身のアカウントの二段階認証を有効にする必要があります。

*すべてのユーザーに対して二段階認証を無効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. プロパティウィンドウの[**認証セキュリティ**]タブで、**全ユーザーに対する二段階認証**オプションの切り替えスイッチを無効の位置に移動します。

すべてのユーザーに対して二段階認証が無効になります。全ユーザーに対して二段階認証を無効にしても、以前に二段階認証が個別に有効になっていた特定のアカウントには適用されません。

# 二段階認証からアカウントを除外する

使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合は、二段階認証からアカウントを除外することができます。

ユーザーアカウントがすべてのユーザーに対する二段階認証のリストから除外されている場合、このユーザーは二段階認証を使用する必要はありません。

認証中にセキュリティコードをパスできないサービスアカウントの場合、二段階認証からアカウントを除外する必要がある場合があります。

*二段階認証から複数のユーザーアカウントを除外する場合：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの［**認証セキュリティ**］タブで、二段階認証の除外のテーブルで［**追加**］をクリックします。
3. 表示されたウィンドウで以下を実行します：
   a. 除外するユーザーアカウントを選択します。
   b. ［**OK**］をクリックします。

選択したユーザーアカウントが二段階認証から除外されます。

# 自分のアカウントの二段階認証を設定します

二段階認証を有効にした後、初めて Kaspersky Security Center Linux にサインインすると、自分のアカウントの二段階認証を設定するためのウィンドウが開きます。

アカウントの二段階認証を設定する前に、使用中のモバイルデバイスに認証アプリがインストールされていることを確認してください。外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。

*アカウントの二段階認証を設定するには：*

1. モバイルデバイスの認証アプリを使用して、ワンタイムセキュリティコードを生成します。開くには、次のいずれかの操作を行います：
   - 認証アプリに秘密鍵を手動で入力します。
   - ［**QR コードを表示する**］をクリックし、認証アプリを使用して QR コードをスキャンします。

   モバイルデバイスにセキュリティコードが表示されます。
2. 二段階認証のウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。

アカウントには二段階認証が設定されています。自分の権利に従って管理サーバーにアクセスできます。

# 新規ユーザーが自分で二段階認証を設定することを禁止します

Kaspersky Security Center Web コンソールのアクセスセキュリティをさらに向上させるために、新しいユーザーが自分自身に二段階認証を設定することを禁止できます。

このオプションをオンにする場合、二段階認証が無効になっているユーザー（例：新しいドメイン管理者など）は、自分自身に二段階認証を設定できません。したがって、そのようなユーザーは管理サーバーで認証できず、既に二段階認証を有効にしている別の Kaspersky Security Center Linux 管理者の承認がなければ Kaspersky Security Center Web コンソールにサインインできません。

このオプションは、すべてのユーザーに対して二段階認証が有効になっている場合に使用できます。

*新しいユーザーが自分自身に二段階認証を設定することを禁止するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの［**認証セキュリティ**］タブで、［**新規ユーザーによる二段階認証の設定を禁止する**］スイッチをオンに切り替えます。

このオプションは、二段階認証の除外に追加されたユーザーアカウントには影響しません。

二段階認証が無効になっているユーザーに Kaspersky Security Center Web コンソールへのアクセスを許可するには、［**新規ユーザーによる二段階認証の設定を禁止する**］を一時的にオフにし、ユーザーに二段階認証をオンにするよう依頼してから、オプションをオンに戻します。

# 新しい秘密鍵の作成

使用するアカウントの二段階認証用の新しい秘密鍵は、二段階認証を使用してアカウントが認証された場合のみ生成できます。

*ユーザーアカウントに対する新しい秘密鍵を生成するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 二段階認証用の新しい秘密鍵を生成するユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
4. ［**認証セキュリティ**］タブで、［**新しい秘密鍵を生成**］をクリックします。
5. 表示された二段階認証ウィンドウで、認証アプリによって作成された新しい秘密鍵を指定します。
6. ［**チェックして適用**］をクリックします。

新しい秘密鍵が生成されました。

モバイルデバイスを紛失した場合は、別のモバイルデバイスに認証アプリをインストールし、新しい秘密鍵を生成して、Kaspersky Security Center Web コンソールへのアクセスを復元できます。

# セキュリティコードの発行元の名前を変更する

異なる管理サーバーに対して、複数の識別子（発行元）を設定することができます。別の管理サーバーに同じようなセキュリティコードの発行元の名前が使用されている場合などに、別のセキュリティコードの発行元の名前に変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。

セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。

*セキュリティコードの発行元の名前を指定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
3. ［**認証セキュリティ**］タブで、［**編集**］をクリックします。
   ［**セキュリティコード発行元の編集**］セクションが開きます。
4. 新しいセキュリティコードの発行元の名前を設定します。
5. ［**OK**］をクリックします。

管理サーバーに新しいセキュリティコードの発行元の名前が設定されます。

# 許可されるパスワード入力試行回数の変更

Kaspersky Security Center Linux のユーザーが無効なパスワードを入力できる回数には上限があります。入力回数が上限に達すると、ユーザーアカウントが 1 時間ブロックされます。

既定では、許可されるパスワードの入力試行回数の上限は 10 回です。このセクションの手順に従って、許可されるパスワード入力試行回数を変更できます。

*許可されるパスワード入力試行回数を変更するには：*

1. 管理サーバーデバイスで、Linux コマンドラインを実行します。
2. klscflag ユーティリティ用に、次のコマンドを実行します：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   N はパスワードの入力試行回数です。
3. 変更を適用するため、管理サーバーサービスを再起動します。

許可されるパスワードの入力試行回数の上限が変更されます。

# ユーザーとセキュリティグループの削除

削除できるのは内部ユーザーまたは内部セキュリティグループのみです。

*ユーザーまたはセキュリティグループを削除するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. 削除するユーザーまたはセキュリティグループの隣にあるチェックボックスをオンにします。

3. ［**削除**］をクリックします。

4. 表示されたウィンドウで［**OK**］をクリックします。

選択したユーザーまたはセキュリティグループが削除されます。

# ユーザーアカウントのパスワードを変更する

現在のパスワードの有効期限が近づいている場合、またはよりセキュアなパスワードに変更したい場合は、自分のアカウントまたは他のユーザーアカウントのパスワードを変更する必要がある場合があります。

パスワードは次のルールに従う必要があります：

- パスワードは、8 文字以上 256 文字以下にしてください。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

## 自分のアカウントのパスワードを変更する

*アカウントのパスワードを編集するには：*

1. メインメニューで、アカウント設定に移動して、［**パスワードの変更**］を選択します。
2. 現在のパスワードを入力し、Kaspersky Security Center Linux への接続用の新しいパスワードを指定します。

   入力したパスワードを確認するには、をクリックしてください。
3. アカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域で、自分のアカウントまたはオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。
4. 前の手順で使用したアカウントで二段階認証が有効になっている場合は、モバイルデバイスの認証アプリによって生成されたセキュリティコードを入力します。

## 内部ユーザーアカウントのパスワードの変更

*内部ユーザーアカウントのパスワードを編集するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 編集するユーザーアカウントの名前をクリックします。
3. 開いたユーザー設定ウィンドウの［**全般**］タブで、［**パスワードの変更**］をクリックします。
4. 新しいパスワードを設定します：Kaspersky Security Center Linux へのユーザー接続用。
   入力したパスワードを確認するには、をクリックしてください。
5. 必要に応じて、［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにして、次回のユーザー認証時にパスワードの変更を強制します。
6. ユーザーアカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。

## サーバーフラグを使用してパスワードを変更するためのオプションを構成します

次のコマンドを使用して、klscflag ユーティリティでパスワードの変更を設定できます：

- パスワードローテーション期間の設定（LP_SplPwdChangePeriodDays フラグ）

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <ローテーション期間>`

  **<ローテーション期間>** は、ユーザーパスワードの有効期限が切れるまでの日数です。可能な値：0～730。パラメータ値が 0 の場合、パスワードのローテーションは無効になります。

- パスワードを変更する必要があることを事前に警告する時間を設定する（LP_SplPwdChangeNotificationHours フラグ）

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <警告時間>`

  **<警告時間>** は、ユーザーパスワードの有効期限が切れるまでの時間です。この間、パスワード変更が必要であることを通知するメッセージが表示されます。可能な値：0～17520。パラメータ値が 0 の場合、警告時間はパスワードローテーション期間の 25% になります。

- 「**ユーザーは初回ログイン時にパスワードを変更する必要があります**」オプション（LP_SplPwdForceChange フラグ）の既定値を指定する

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <値>`

  **<値>** フラグに設定可能な値：

  `1`—［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］がオンになっています。

  `0`—［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］がオフになっています。

現在のフラグ値を表示するには、次のコマンドを実行します。

`klscflag -fget -pv .core/.independent -s KLLIM -n <フラグ> -t d`

< **フラグ** >は、 `LP_SplPwdChangePeriodDays`、 `LP_SplPwdChangeNotificationHours`、または `LP_SplPwdForceChange` フラグです。

# ユーザーロールの作成

*ユーザーロールを作成するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**新しいロール名**］ウィンドウが開いたら、新しいロールの名前を入力します。
4. ［**OK**］をクリックして変更を適用します。
5. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
6. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに新しいロールが表示されます。

# ユーザーロールの編集

*ユーザーロールを編集するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 編集するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
4. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに更新したロールが表示されます。

# 各ユーザーロールの対象範囲の編集

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

*ユーザーロールの対象範囲にユーザー、セキュリティグループ、管理グループを追加するには、次のいずれかの方法を使用できます：*

*方法 1：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。

2. ユーザーロールの対象範囲に追加するユーザーまたはセキュリティグループに隣接するチェックボックスをオンにします。

3. ［**ロールの割り当て**］をクリックします。

   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ［**ロールの選択**］ステップで、割り当てるユーザーロールを選択します。

5. ［**範囲の定義**］ステップで、ユーザーロールの対象範囲に追加する管理グループを選択します。

6. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

   選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

*方法 2：*

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。

2. 対象範囲を指定するロールの名前をクリックします。

3. ロールのプロパティウィンドウが開いたら、［**設定**］タブをクリックします。

4. ［**ロールの対象範囲**］セクションで、［**追加**］をクリックします。

   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

5. ［**範囲の定義**］ステップで、ユーザーロールの対象範囲に追加する管理グループを選択します。

6. ［**ユーザーを選択してください**］ステップで、ユーザーロールの対象範囲に追加するユーザーとセキュリティグループを選択します。

7. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

8. ［**閉じる**］ボタン（⨯）をクリックして、ロールのプロパティウィンドウを閉じます。

選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

*方法 3：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**アクセス権**］タブで、権限を割り当てるユーザーとロールスコープのユーザーまたはセキュリティグループの名前の横にあるチェックボックスをオンにし、［**ロール**]クリックします。

   複数のユーザーまたはセキュリティグループを同時に選択することはできません。複数のアイテムを選択すると、［**ロール**］ボタンがオフになります。

3. ［**ロール**］ウィンドウで、割り当てたいユーザーとロールを選択し、変更を適用して保存します。

   選択したユーザーまたはセキュリティグループが、ユーザーロールの対象範囲に追加されます。

# ユーザーロールの削除

*ユーザーロールを削除するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 削除するロールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

選択したユーザーロールが削除されます。

# ポリシーのプロファイルとロールの関連付け

ユーザーロールはポリシーのプロファイルに関連付けることができます。この場合、ポリシーのプロファイルの有効化ルールがベースにしているのはロールです：ポリシーのプロファイルは、指定したロールを持つユーザーに対してアクティブにされます。

たとえば、管理グループ内のすべてのデバイスに対して GPS ナビゲーションソフトウェアの使用を禁止するポリシーがあるとします。管理グループ「ユーザー」内に配達担当者が所有するデバイスが 1 台存在しており、そのデバイスでのみ GPS ナビゲーションソフトウェアを使用する必要があるとします。この場合、デバイスの所有者に「配達担当者」ロールを割り当てて、「配達担当者」ロールが割り当てられた所有者のデバイスでのみ使用できるように、GPS ナビゲーションソフトウェアを許可するポリシーのプロファイルを作成できます。その他のポリシー設定はいずれも変更されません。「配達担当者」ロールが割り当てられたユーザーのみが、GPS ナビゲーションソフトウェアを使用できるようになります。後で別の担当者に「配達担当者」ロールを割り当てた場合、その新規担当者も組織のデバイスでナビゲーションソフトウェアを使用できるようになります。同じ管理グループ内の他のデバイスでは、GPS ナビゲーションソフトウェアの使用は禁止されたままになります。

*ロールとポリシーのプロファイルを関連付けるには：*

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ポリシーのプロファイルと関連付けるロール名をクリックします。
   ロールのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**設定**］タブを選択して、［**ポリシーとプロファイル**］セクションまでスクロールします。
4. ［**編集**］をクリックします。
5. ロールを関連付けるには：
   - **既存のポリシーのプロファイル**– 該当するポリシー名の横にあるアイコン（›）をクリックして、ロールを関連付けるプロファイルの横にあるチェックボックスをオンにします。
   - **新しいポリシーのプロファイル**：
     a. プロファイルを作成するポリシーの横にあるチェックボックスをオンにします。
     b. ［**ポリシーのプロファイルの新規作成**］をクリックします。
     c. 新しいプロファイル名を指定して、プロファイルを設定します。
     d. ［**保存**］をクリックします。
     e. 新しいプロファイルの横にあるチェックボックスをオンにします。
6. ［**ロールへの割り当て**］をクリックします。

プロファイルがロールに関連付けられてロールのプロパティに表示されます。担当者が当該ロールに割り当てられているデバイスに対して、プロファイルが自動的に適用されます。

# セカンダリ管理サーバーにユーザーロールを反映させるには

既定では、プライマリ管理サーバーとセカンダリ管理サーバーのユーザーロールのリストは互いに独立しています。プライマリ管理サーバーで作成したユーザーロールをすべてのセカンダリ管理サーバーに自動的に反映するように、本製品を設定できます。任意のセカンダリ管理サーバーからその下位にあるセカンダリ管理サーバーにユーザーロールを反映できます。

*プライマリ管理サーバーからセカンダリ管理サーバーにユーザーロールを反映するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. **管理サーバーの階層**セクションに移動します。
3. **ロールのリストをセカンダリ管理サーバーに転送する**オプションを有効にし、**保存**ボタンをクリックします。

プライマリ管理サーバーからセカンダリ管理サーバーにユーザーロールがコピーされます。

**ロールのリストをセカンダリ管理サーバーに転送する**がオンでユーザーロールが反映されている場合、セカンダリ管理サーバーの側でこれらのユーザーロールを編集したり削除したりすることはできません。プライマリ管理サーバーで新しいロールを作成したり既存のロールを編集すると、これらの変更を自動的にセカンダリ管理サーバーに反映します。プライマリ管理サーバーでユーザーロールを削除した場合、該当するロールはセカンダリ管理サーバーにそのまま残りますが、このロールの編集や削除が可能になります。

プライマリ管理サーバーからセカンダリ管理サーバーに反映されたロールには緑色のチェックマーク（✓）が表示されます。これらのロールはセカンダリ管理サーバーでは編集できません。

プライマリ管理サーバーで作成したロールと同じ名前のロールがセカンダリ管理サーバーに存在した場合、新しいロールがセカンダリ管理サーバーにコピーされる時に「~~1」や「~~2」のような接尾辞が追加されます（接尾辞はランダムに生成されます）。

**ロールのリストをセカンダリ管理サーバーに転送する**を無効にすると、すべてのユーザーロールはセカンダリ管理サーバーにそのまま残りますが、プライマリ管理サーバーのユーザーロールとは互いに独立した状態になります。独立した状態になった後は、セカンダリ管理サーバーでユーザーロールを編集、削除できます。

# アカウントパスワードの変更

たとえば、ユーザーがローカルアカウントのパスワードを忘れた場合や、定期的なパスワードの変更を実行する場合に、ローカルアカウントのパスワードを変更できます。

ユーザーがアカウントにログインしていない場合でも、パスワードの変更は適用されます。ローカルルートアカウントのパスワードを変更することもできます。

> このタスクは Linux デバイスでのみ実行できます。

*特定のデバイスでローカルアカウントのパスワードを変更するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ［**タスク種別**］フィールドで、［**アカウントのパスワードの変更（Linux のみ）**］を選択します。

4. 次のいずれかのオプションをオンにします：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

指定されたデバイスに対して、*アカウントパスワードの変更（Linux のみ）*タスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ 1 になります。

5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

使用可能な設定は、前のステップでオンにしたオプションによって異なります。

6. **アカウント名と新しいパスワードの入力**ステップで、次の設定を指定します：

   - ［**アカウント名**］フィールドに、パスワードを変更するアカウントの名前を指定します。
   - ［**新しいパスワード**］フィールドに、前のフィールドで指定したアカウントに設定するパスワードを指定します。

     入力した文字を表示するには、［**表示**］を押し続けます。
   - 必要に応じて、［**ワンタイムパスワードとして設定（ユーザーは初回ログイン時にパスワードを変更する必要があります）**］をオンにします。
     - **ワンタイムパスワードとして設定（ユーザーは初回ログイン時にパスワードを変更する必要があります）**

       このチェックボックスをオンにすると、ユーザーは初回のログイン後に新しいパスワードを設定するよう要求されます。

       このチェックボックスをオフにすると、ユーザーは初回のログイン後に新しいパスワードを設定するように要求されません。

       既定では、このチェックボックスはオフです。

7. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

8. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

   または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

アカウントパスワードの変更タスクが完了すると、指定されたデバイス上の指定されたローカルアカウントのパスワードが変更されます。

アカウントパスワード変更タスクが正しく実行されるようにするには、ユーザーデバイスで SELinux を無効にする必要があります。

# ローカル管理者権限の取り消し

アカウントからローカル管理者権限を取り消すことができます。これにより、ユーザーアカウントをさらに細かく制御できるようになります。たとえば、1回限りの割り当ての完了後、ローカル管理者の権限を取り消すことができます。

このタスクを実行すると、指定されたローカルアカウントがローカル管理グループに属しているかどうかが確認されます。これらのグループは、ネットワークエージェントのポリシー設定で定義されます。ネットワークエージェントのポリシー設定で、ローカル管理グループのリストをカスタマイズできます。**特権付きのデバイスのユーザーに関するレポート（Linux のみ）**を使用して、特権ユーザーアカウントのリストを確認することもできます。

このタスクは Linux デバイスでのみ実行できます。

*特定のデバイスのローカル管理者権限を取り消すには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ［**タスク種別**］フィールドで、［**ローカル管理者権限の取り消し（Linux のみ）**］を選択します。
4. 次のいずれかのオプションをオンにします：

   - **管理グループにタスクを割り当てる**

     任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

     たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

     タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

   - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

     タスクを割り当てるデバイスの DNS 名、IP アドレス、IP サブネットを指定できます。

     特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

   - **デバイスの抽出にタスクを割り当てる**

     デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

     たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

   指定されたデバイスに対して、*ローカル管理者権限の取り消し（Linux のみ）*タスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ 1 になります。

5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。
   使用可能な設定は、前のステップでオンにしたオプションによって異なります。

6. ウィザードのこのステップでは、次の操作を指定します：

   - ［**動作モード**］設定グループで、動作モードを指定します：

     - **アカウントのリストからローカル管理者権限を取り消す**

       このオプションをオンにすると、指定されたローカルアカウントからローカル管理者権限が取り消されます。

       既定では、このオプションがオンです。

     - **アカウントのリストをローカル管理者権限の取り消し対象から除外する**

       このオプションをオンにすると、指定されたアカウントを除くすべてのローカルアカウントからローカル管理者権限が取り消されます。

       既定では、このオプションはオフです。

   - ローカルアカウントを指定します：

     - ［**追加**］をクリックします。

     - 開いたウインドウで以下の操作を行います：

       - ［**アカウント名**］フィールドに、ローカルアカウントの名前を指定します。

       - ［**アカウントの処理**］設定グループ（［**アカウントのリストからローカル管理者権限を取り消す**］がオンの場合のみ使用可能）で、操作を指定します。

       - **アカウントを保持する**

         このオプションをオンにすると、ローカル管理者権限が取り消された後もローカルアカウントは削除されません。

         既定では、このオプションがオンです。

       - **アカウントを削除する**

         このオプションをオンにすると、ローカル管理者権限があるかどうかに関係なく、ローカルアカウントが削除されます。

         既定では、このオプションはオフです。

7. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

8. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

   または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

ローカル管理者権限の取り消しタスクが完了すると、指定されたデバイス上の指定されたローカルアカウントからローカル管理者権限が取り消されます。

# 定義データベースとカスペルスキー製品のアップデート

このセクションでは、次の対象の定期的なアップデートに必要な手順について説明します。

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center Linux コンポーネントとセキュリティ製品を含む）

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

# シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート

このセクションでは、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを行う手順について説明します。ネットワーク保護の設定手順の完了後、管理サーバーと管理対象デバイスがウイルス、ネットワーク攻撃、フィッシング攻撃などの様々な脅威から常に保護されるよう、保護システムの信頼性を維持する必要があります。

ネットワーク保護を最新の状態に維持する定期的なアップデートは次の通りです：

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center Linux コンポーネントとセキュリティ製品を含む）

この手順を完了すると、次の状態を実現できます：

- ネットワークが最新のカスペルスキー製品（Kaspersky Security Center Linux コンポーネントとセキュリティ製品を含む）で保護されている。
- ネットワークのセキュリティレベルにとって重要な定義データベースとその他のカスペルスキーのデータベースが常に最新である。

## 必須条件

管理対象デバイスが管理サーバーに接続している必要があります。接続していない場合は、定義データベースとソフトウェアモジュールの手動アップデート、またはカスペルスキーのアップデートサーバーからの直接アップデートを検討してください。

管理サーバーはインターネットに接続している必要があります。

導入を開始する前に、次が完了していることを確認してください：

1. Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入手順に従って、カスペルスキーのセキュリティ製品を管理対象デバイスに導入した。
2. ネットワーク保護の設定手順に従って、必要なすべてのポリシー、ポリシーのプロファイル、タスクを作成して設定した。
3. 管理対象デバイスの数とネットワークトポロジーに従って、適切な数のディストリビューションポイントを割り当てた。

定義データベースとカスペルスキー製品のアップデート手順は次の通りです：

**1 アップデートスキームの選択**

セキュリティ製品のアップデートをインストールするために使用できるスキームがいくつかあります。ネットワークの要件に最も合致するスキームを選択してください（複数のスキームを組み合わせることもできます）。

**2 ［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成**

このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを作成してください。

カスペルスキーのアップデートサーバーから管理サーバーのリポジトリへのアップデートのダウンロード、および定義データベースと Kaspersky Security Center Linux のソフトウェアモジュールのアップデートには、このタスクが必要です。アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

ネットワークにディストリビューションポイントが割り当てられている場合、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。この場合、ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。

実行手順の説明：［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

**3 ［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成（オプション）**

既定では、管理サーバーからディストリビューションポイントにアップデートがダウンロードされます。カスペルスキーのアップデートサーバーからディストリビューションポイントにアップデートを直接ダウンロードするように Kaspersky Security Center Linux を設定できます。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。

ネットワークにディストリビューションポイントが割り当てられており、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクが作成されている場合、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

実行手順の説明：［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

**4 ディストリビューションポイントの設定**

ネットワークにディストリビューションポイントが割り当てられている場合、設定が必要なすべてのディストリビューションポイントのプロパティで［**アップデートの配信**］がオンになっていることを確認します。ディストリビューションポイントでこのオプションがオフになっていると、ディストリビューションポイントの範囲に含まれるデバイスは管理サーバーのリポジトリからアップデートをダウンロードします。

**5 差分ファイルの使用によるアップデート処理の最適化（省略可能）**

差分ファイルを使用することで管理サーバーと管理対象デバイス間のトラフィックを最適化することができます。この機能を有効にすると、管理サーバーまたはディストリビューションポイントは定義データベースまたはソフトウェアモジュールのファイル全体ではなく差分ファイルをダウンロードします。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。したがって、差分ファイルの方がファイル全体より容量が小さくなります。これにより、管理サーバーと管理対象デバイス間またはディストリビューションポイントと管理対象デバイス間のトラフィックを削減できます。この機能を使用するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクや、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク、またはその両方のプロパティで［**差分ファイルのダウンロード**］をオンにします。

実行手順の説明：カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

**6 セキュリティ製品のアップデートとパッチの自動インストールの設定**

管理対象の製品の*アップデート*タスクを作成して、ソフトウェアモジュール、および定義データベースをタイムリーにアップデートします。タイムリーにアップデートされるようにするため、タスクスケジュールの設定時に［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

ネットワークに IPv6 専用デバイスが含まれ、これらのデバイスにインストールされているセキュリティ製品を定期的にアップデート更新する場合は、管理対象デバイスに管理サーバーバージョン 13.2 またはそれ以降のバージョンとネットワークエージェントバージョン 13.2 またはそれ以降のバージョンがインストールされていることを確認してください。

使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。

**7 管理対象の Kaspersky アプリケーションのアップデートの承認と拒否**

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。ステータスは「*承認*」または「*拒否*」に変更できます。承認されたアップデートは常にインストールされます。管理対象の Kaspersky のアプリケーションのアップデートで、使用許諾契約書の条項を確認し、同意する必要がある場合は、最初にその条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。「*拒否*」のステータスを設定したアップデートはデバイスにインストールされません。拒否に設定した管理対象のアプリケーションのアップデートが以前にインストールされている場合、Kaspersky Security Center Linux はすべてのデバイスからのアップデートのアンインストールを試行します。

アップデートの承認と拒否は、Windows ベースおよび Linux ベースのクライアントデバイスにインストールされたネットワークエージェントおよび管理対象の Kaspersky アプリケーションでのみ使用できます。管理サーバー、Kaspersky Security Center Web コンソール、および管理 Web プラグインのシームレスなアップデートはサポートされていません。

実行手順の説明：ソフトウェアのアップデートの拒否と承認

ネットワークエージェントのアップデート後に、管理対象デバイスを再起動するように要求される場合があります。必要な再起動に関する通知が表示された場合、通知内の［**デバイスの表示**］をクリックし、再起動が必要なデバイスの横のチェックボックスを選択し、その後［**再起動**］をクリックしてネットワークエージェントのアップデートを完了してください。

## 結果

すべての手順を完了すると、管理サーバーのリポジトリにアップデートがダウンロードされた後で、カスペルスキーのデータベースをアップデートするように Kaspersky Security Center Linux が設定されます。続いて、ネットワークステータスの監視を設定できます。

# 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要

管理サーバーと管理対象デバイスの保護が最新の状態であるようにするには、次の項目のタイムリーなアップデートが必要です：

- 定義データベースとソフトウェアモジュール

  Kaspersky Security Center Linux は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、定義データベースを最新の状態に保ち、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

- インストール済みのカスペルスキー製品（Kaspersky Security Center Linux コンポーネントとセキュリティ製品を含む）

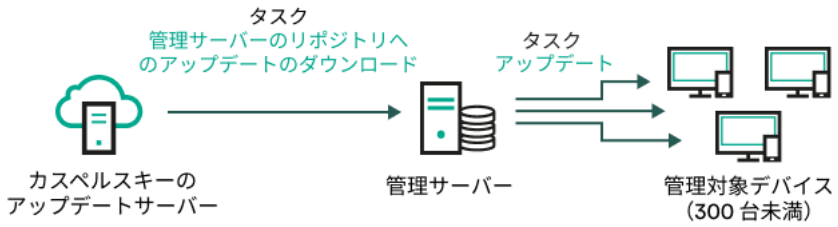
  Kaspersky Security Center Linux では、Windows ベースおよび Linux ベースのクライアントデバイスにインストールされているネットワークエージェントとカスペルスキー製品を自動的にアップデートできます。管理サーバー、Kaspersky Security Center Web コンソール、および管理 Web プラグインのシームレスなアップデートはサポートされていません。これらのコンポーネントをアップデートするには、カスペルスキーの Web サイトから最新バージョンをダウンロードし、手動でインストールしてください。

ネットワークの設定に応じて、管理対象デバイスへの必要なアップデートのダウンロードと配信に次のスキームを使用できます：

- 単一のタスク［*管理サーバーのリポジトリへのアップデートのダウンロード*］の使用
- 次の 2 つのタスクの使用：
  - *［管理サーバーのリポジトリへのアップデートのダウンロード］タスク*
  - *ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*
- ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行
- カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート
- 管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

## 管理サーバーのリポジトリへのアップデートのダウンロードタスクの使用

このスキームでは、Kaspersky Security Center Linux は［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用してアップデートをダウンロードします。単一のネットワークセグメントで構成され管理対象デバイスが 300 台未満、または複数のセグメントに分かれているが各ネットワークセグメントに含まれる管理対象デバイスが 10 台未満の小規模ネットワークでは、管理サーバーのリポジトリから管理対象デバイスにアップデートが直接配信されます（次の図を参照）。



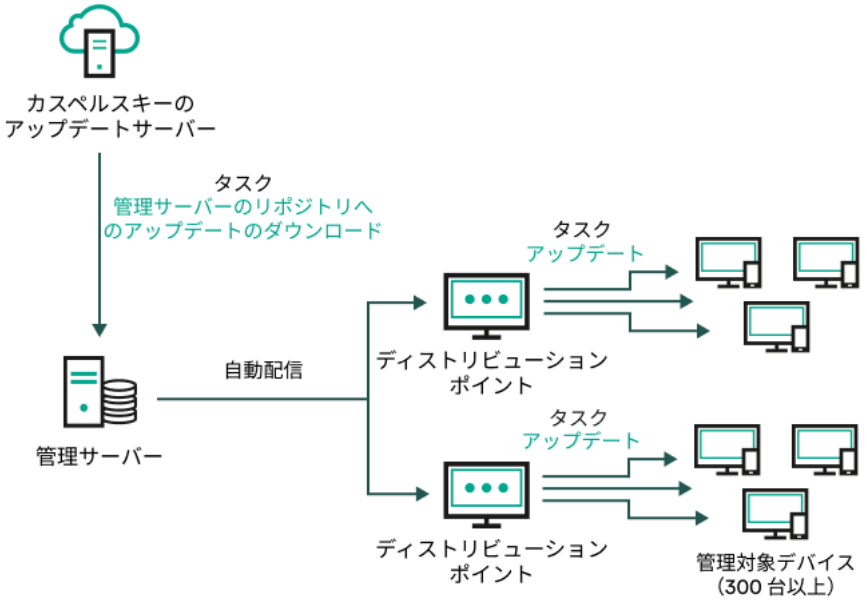

ディストリビューションポイントを使用しない、[*管理サーバーのリポジトリへのアップデートのダウンロード*] タスクによるアップデート

アップデート元として、カスペルスキーのアップデートサーバーだけでなく、ローカルまたはネットワークフォルダーを使用することもできます：

既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

単一のネットワークセグメントで構成され管理対象デバイスが 300 台以上、または複数のセグメントに分かれていて各ネットワークセグメントに含まれる管理対象デバイスが 9 台以上のネットワークの場合は、ディストリビューションポイントを使用して管理対象デバイスにアップデートを配信することを推奨します（次の図を参照）。ディストリビューションポイントは管理サーバーの負荷を低減し、管理サーバーと管理対象デバイス間のトラフィックを最適化します。ネットワークに必要なディストリビューションポイントの数と設定を計算できます。

このスキームでは、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。




ディストリビューションポイントを使用した、[*管理サーバーのリポジトリへのアップデートのダウンロード*] タスクによるアップデート

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクが完了すると、カスペルスキーのデータベースと Kaspersky Endpoint Security ソフトウェアモジュールのアップデートが管理サーバーのリポジトリにダウンロードされます。これらのアップデートは、Kaspersky Endpoint Security の *アップデート*タスクを使用してインストールされます。

仮想管理サーバーでは［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは利用できません。仮想管理サーバーのリポジトリには、プライマリ管理サーバーにダウンロードされたアップデートが表示されます。

テストデバイスを指定してアップデートの動作とエラーが検証されるように設定できます。検証に成功すると、アップデートが他の管理対象デバイスに配信されます。

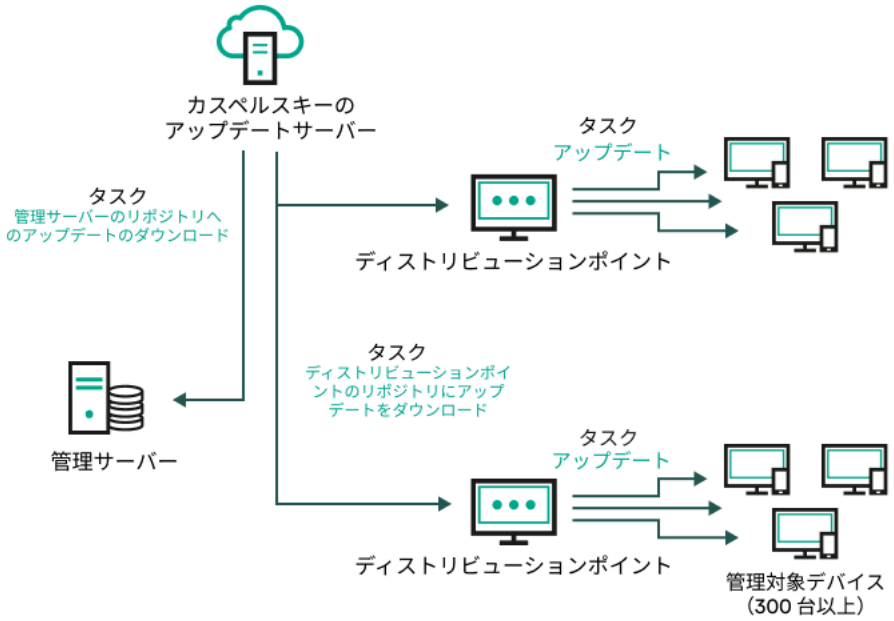
各カスペルスキー製品は、管理サーバーに必要なアップデートを要求します。管理サーバーはこれらの要求を集計した上で、いずれかの製品で要求されたアップデートのみをダウンロードします。これにより、同一のアップデートが複数回ダウンロードされたり、不必要なアップデートがダウンロードされることを防ぐことができます。［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行中、関連するバージョンの定義データベースとソフトウェアモジュールを確実にダウンロードする目的で、次の情報が管理サーバーからカスペルスキーのアップデートサーバーに自動的に送信されます：

- 製品 ID およびバージョン
- 製品セットアップ ID
- 現在のライセンス ID
- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの実行 ID

送信される情報には、個人データや機密データは含まれません。カスペルスキーでは、法律で定められた要件に従って情報を保護しています。

## 2 つのタスク（[管理サーバーのリポジトリへのアップデートのダウンロード］タスクおよび［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスク）の使用

管理サーバーのリポジトリを経由させずに、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートを直接ダウンロードして、管理対象デバイスにアップデートを配信できます（次の図を参照）。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。




*管理サーバーのリポジトリへのアップデートのダウンロードタスクおよびディストリビューションポイントのリポジトリにアップデートをダウンロードタスクによるアップデート*

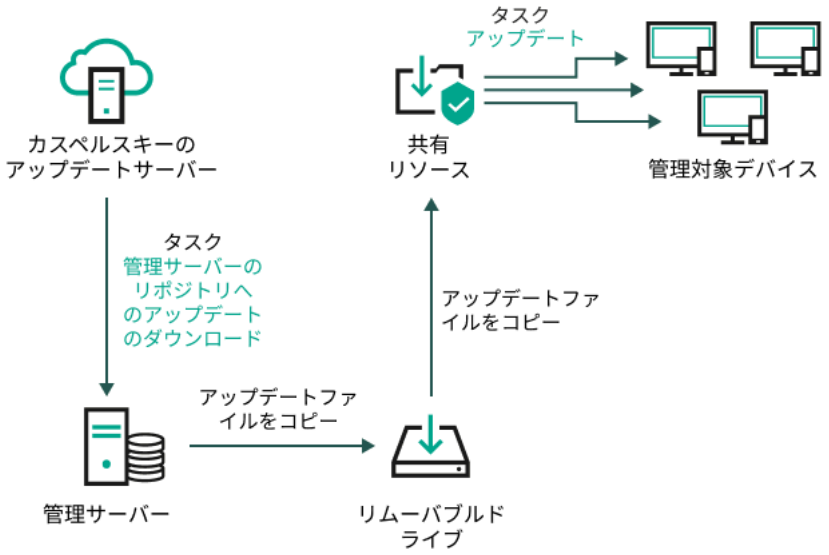
既定では、管理サーバーとディストリビューションポイントは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバー、ディストリビューションポイント、またはその両方で HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

このスキームを実装するには、*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクに加えて*［ディストリビューションポイントのリポジトリにアップデートをダウンロード］*タスクを作成します。その後、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

定義データベースと Kaspersky Security Center Linux のソフトウェアモジュールは［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用してダウンロードされるため、このスキームでもこのタスクが必要です。

## ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

クライアントデバイスが管理サーバーに接続できない場合、ローカルフォルダーまたは共有リソースを使用して定義データベース、ソフトウェアモジュール、カスペルスキー製品をアップデートできます。このスキームでは、管理サーバーのリポジトリからリムーバブルドライブに必要なアップデートをコピーして、Kaspersky Endpoint Security の設定でアップデート元として指定したローカルフォルダーまたは共有リソースにアップデートをコピーする必要があります（次の図を参照）。



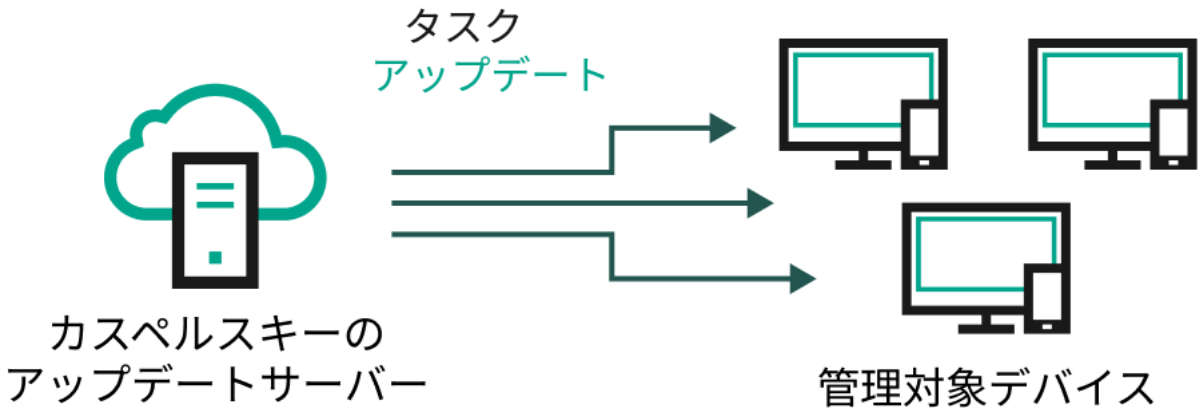

ローカルフォルダー、共有フォルダー、または FTP サーバーを使用したアップデート

Kaspersky Endpoint Security のアップデート元の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Linux のヘルプ
- Kaspersky Endpoint Security for Windows のヘルプ

## カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート

管理対象デバイスで、カスペルスキーのアップデートサーバーから直接アップデートを受信するように Kaspersky Endpoint Security を設定できます（次の図を参照）。




カスペルスキーのアップデートサーバーからセキュリティ製品を直接アップデート

このスキームでは、セキュリティ製品は Kaspersky Security Center Linux が提供するリポジトリを使用しません。カスペルスキーのアップデートサーバーからアップデートを直接受信するには、セキュリティ製品でカスペルスキーのアップデートサーバーをアップデート元として指定します。これらの設定の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Linux のヘルプ
- Kaspersky Endpoint Security for Windows のヘルプ

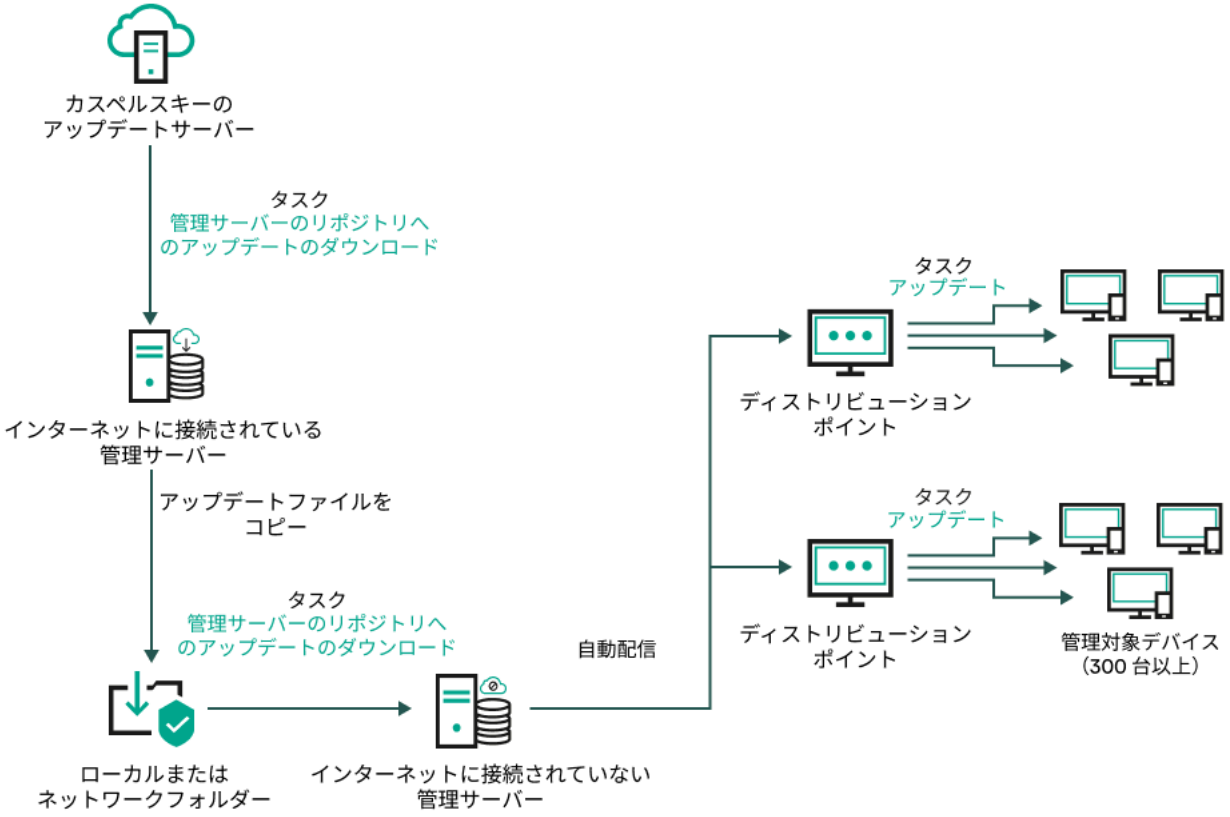
# 管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーがインターネットに接続されていない場合は、[*管理サーバーのリポジトリへのアップデートのダウンロード*] タスクを設定して、ローカルまたはネットワークフォルダーからアップデートをダウンロードできます。この場合、指定したフォルダーに必要なアップデートファイルを定期的にコピーする必要があります。たとえば、次のいずれかのソースから、必要なアップデートファイルをコピーできます：

- インターネットに接続されている管理サーバー（下図を参照）

  管理サーバーは、セキュリティ製品が要求したアップデートのみをダウンロードするため、管理サーバーによって管理されるセキュリティ製品のセット（インターネット接続があるものとないもの）が一致している必要があります。

  アップデートのダウンロードに使用する管理サーバーのバージョンが 13.2 以前の場合、[ *管理サーバーのリポジトリへのアップデートのダウンロード*] タスクのプロパティを開き、[**旧スキームを使用してアップデートをダウンロード**] オプションをオンにします。




管理サーバーがインターネットに接続されていない場合のローカルまたはネットワーク フォルダー経由のアップデート

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードするため、[*管理サーバーのリポジトリへのアップデートのダウンロード*] タスクのプロパティを開き、[*旧スキームを使用してアップデートをダウンロード*] オプションをオンにします。必要に応じて、Kaspersky Update Utility が必要なアップデートのみをダウンロードするように、[*アップデートリクエストファイルを自動的にダウンロードする*] をオンにすることもできます。

# ［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用すると、カスペルスキーのアップデートサーバーから管理サーバーのリポジトリに、カスペルスキーセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデートをダウンロードできます。

Kaspersky Security Center クイックスタートウィザードは、管理サーバーの［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを自動的に作成します。タスクリストには*管理サーバーのリポジトリへのアップデートのダウンロード*タスクが1つだけ表示されます。このタスクが管理サーバーのタスクリストから削除された場合、再度作成できます。

［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクが完了し、アップデートがダウンロードされたら、管理対象デバイスにこれらのアップデートを配信できます。

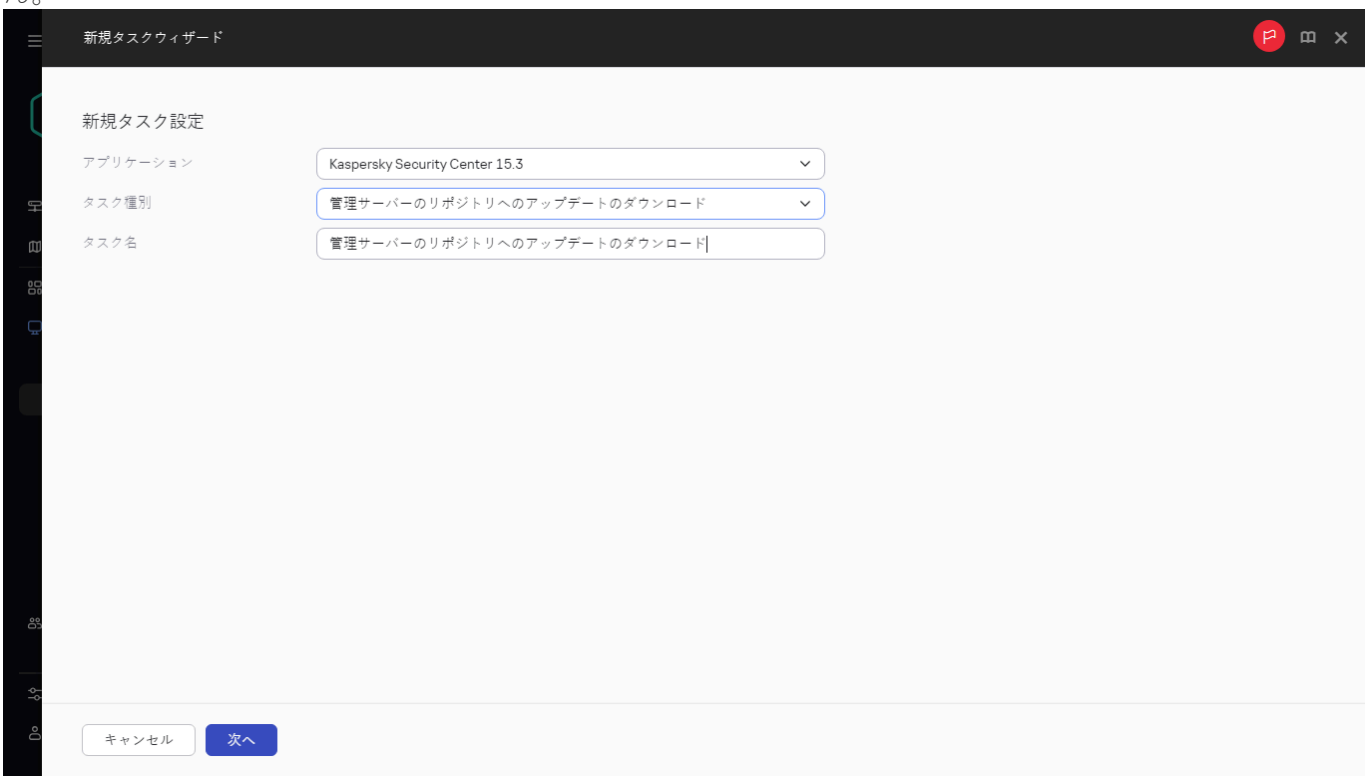
管理対象デバイスへのアップデートの配信前に、*アップデート検証*タスクを実行できます。これにより、管理サーバーが正しいアップデートをインストールし、アップデートによりセキュリティレベルが下がることがないことを確認できます。配信前に検証するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの設定で［**アップデートの検証の実行**］オプションをオンにします。

*［管理サーバーのリポジトリへのアップデートのダウンロード］タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスク種別を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。




［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

5. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにして、タスクのプロパティウィンドウを開き、既定のタスク設定を変更できます。変更しない場合、後でいつでもタスク設定を変更できます。




タスク作成の終了

6. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

7. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

8. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

- **アップデート元**

  アップデート元としては、 カスペルスキーのアップデートサーバー、ローカルフォルダーまたはネットワークフォルダー、プライマリ管理サーバーのいずれかを使用できます。

  ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center Linux は資格情報の入力を要求しません。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **セカンダリ管理サーバーの強制アップデート**

  このオプションをオンにすると、管理サーバーは、新しいアップデートがダウンロードされるとすぐに、セカンダリ管理サーバーのアップデートタスクを開始します。アップデートタスクは、セカンダリ管理サーバーのタスクプロパティで構成されているアップデートソースを使用して開始されます。

  このオプションをオフにすると、セカンダリ管理サーバーのアップデートタスクは、スケジュールに従って開始されます。

  既定では、このオプションはオフです。

- **ダウンロード済みのアップデートを追加のフォルダーにコピー**

  管理サーバーがアップデートを受信すると、指定されたフォルダーにコピーします。ネットワークでのアップデートの配信を手動で管理する場合は、このオプションをオンにします。

  このオプションの使用を検討する状況としては、たとえば、組織のネットワークが複数の独立したサブネットワークで構成され、各サブネットワークに属するデバイスは別のサブネットワークへのアクセス権を付与されていない場合があります。ただし、すべてのサブネットワークのデバイスは共通のネットワーク共有へのアクセス権は付与されています。この場合、いずれかのサブネットワークの管理サーバーでカスペルスキーのアップデートサーバーからアップデートをダウンロードするように設定した後、このオプションをオンにし、ネットワーク共有をコピー先に指定します。他の管理サーバーでは、リポジトリへのアップデートのダウンロードタスクのアップデート元として、このネットワーク共有を指定します。

  既定では、このオプションはオフです。

- **差分ファイルのダウンロード**

このオプションで差分ファイルのダウンロードを有効にすることができます。

既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

  Kaspersky Security Center Linux のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

  たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

  - Kaspersky Update Utility

    このユーティリティは旧スキームを使用してアップデートをダウンロードします。

  - Kaspersky Security Center 13 Linux

    例えば、管理サーバー 1 はインターネットに接続していないものとします。この場合、インターネットに接続できる管理サーバー 2 を使用してアップデートをダウンロードし、このアップデートを管理サーバー 1 のアップデート元として使用するために、ローカルまたはネットワークフォルダーに保存します。管理サーバー 2 に Kaspersky Security Center のバージョン 13 がインストールされていた場合、管理サーバー 1 向けのタスクでは［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

  既定では、このオプションはオフです。

- **アップデートの検証の実行**

  管理サーバーはアップデート元からアップデートをダウンロードし、それらを一時リポジトリに保存して、［**アップデート検証タスク**］で定義されたタスクを実行します。タスクが正常に終了すると、アップデートは一時保管領域から管理サーバーの共有フォルダーにコピーされ、この管理サーバーをアップデート元とするすべてのデバイスに配信されます（［**新しいアップデートがリポジトリにダウンロードされ次第**］のスケジュールが設定されたタスクが開始されます）。アップデートをリポジトリにダウンロードするタスクが完了するのは、*アップデートの検証*タスクの完了後のみです。

  既定では、このオプションはオフです。

- **アップデートリクエストファイルを自動的にダウンロードする**

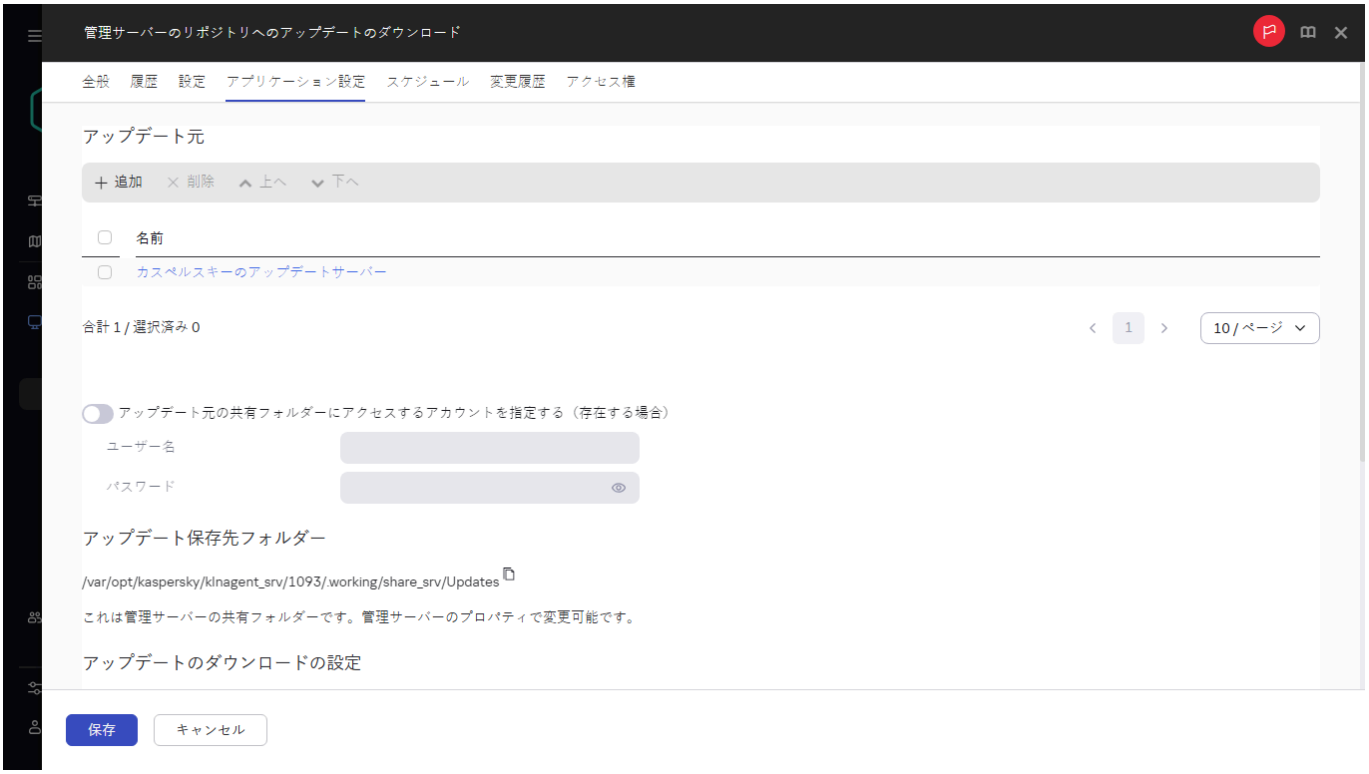
Kaspersky Update Utility が必要な場合、適切な設定で必要なアップデートのみをダウンロードするには、このオプションをオンにし、ダウンロードするアップデートに関する情報を含むアップデートリクエストファイルを Kaspersky Security Center Linux が作成するパスを指定します。アップデートリクエストファイルには、バージョン管理用のタイムスタンプと MD5 ハッシュが含まれています。

また、Kaspersky Update Utility でアップデートのダウンロードを設定する必要があります。

既定では、次のパスが指定されています：
var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml。必要に応じて、既定の名前（retranslation_request）とパスを変更できます。

リクエストファイルは、ローカルフォルダーまたは共有フォルダーに配置できます。共有フォルダーを使用する場合は、管理サーバーがインストールされているデバイスからこのフォルダーにアクセスできることを確認する必要があります。アクセスを確保する方法と使用するツールは、インフラストラクチャによって異なります。

*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを実行すると、Kaspersky Security Center Linux は指定したパスに .xml 形式のアップデートリクエストファイルを作成します。Kaspersky Update Utility はリクエストファイルから情報を自動的に取得し、必要なアップデートのみをダウンロードします。Kaspersky Update Utility が情報を自動的に取得できない場合（たとえば、Kaspersky Update Utility が Kaspersky Security Center Linux がリクエストファイルを作成したフォルダーにアクセスできない場合）、サードパーティのツールを使用してファイルを送信する必要があります。




管理サーバーのリポジトリへのアップデートのダウンロードタスクのプロパティの指定

9. タスクのプロパティウィンドウの［**スケジュール**］タブで、タスクの開始スケジュールを作成します。必要に応じて、次の設定を指定します：

- **タスク開始**：
  - **手動**（既定で選択）

    タスクは、自動的には実行されません。手動でのみ開始できます。

    既定では、このオプションがオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。
    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **曜日ごと**

    指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
    既定では、毎週金曜日の午後 6 時にタスクが実行されます。

  - **毎月**

    毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
    指定した日付が存在しない月には、月の最終日にタスクを実行します。
    既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

  - **毎月、選択した週の指定日**

    毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
    規定では、日付は選択されていません。規定の開始時間は 18:00 です。

  - **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、[**デバイスの電源をオンにする**]をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス([**正常終了**]または[**失敗**])を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、[**適用**]をクリックします。

- 追加タスクの設定:

  - **未実行のタスクを実行する**

    このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

    このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が[**手動**]、[**1回**]または[**即時**]に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

    このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

    既定では、このオプションはオフです。

  - **タスクの開始を自動的かつランダムに遅延させる**

    このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

    分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

    このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  - **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

- **次の時間を超える場合はタスクを停止する**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

  既定では、このオプションはオフです。既定のタスク実行時間は120分です。




管理サーバーのリポジトリへのアップデートのダウンロードタスクのスケジュールの指定

10. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。




タスクリスト

管理サーバーが［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行すると、アップデート元からデータベースとソフトウェアモジュールのアップデートがダウンロードされ、管理サーバーの共有フォルダーに保存されます。管理グループに対してこのタスクを作成すると、指定された管理グループにあるネットワークエージェントにのみ適用されます。

アップデートは管理サーバーの共有フォルダーからクライアントデバイスとセカンダリ管理サーバーに配信されます。

# ダウンロードされたアップデートの検証

管理対象デバイスにアップデートをインストールする前に、*アップデート検証*タスクを使用してアップデートの動作およびエラーがないかどうかを検証できます。*アップデート検証*タスクは、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの一部として自動的に実行されます。アップデート元からアップデートがダウンロードされて、一時リポジトリに保存された後、*アップデート検証*タスクが実行されます。タスクが正常に完了すると、一時リポジトリから管理サーバーの共有フォルダーにアップデートがコピーされます。アップデートのコピーは、管理サーバーがアップデート元として指定されているすべてのクライアントデバイスに配信されます。

*アップデート検証*タスクの結果、一時リポジトリにあるアップデートが正しくないことが判明した場合、または*アップデート検証*タスクがエラーで終了した場合、それらのアップデートは共有フォルダーにコピーされません。管理サーバーでは、以前のアップデートが維持されます。また、スケジュール種別として［**新しいアップデートがリポジトリにダウンロードされ次第**］が指定されたタスクも開始されません。新しいアップデートのスキャンが正常に完了した場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの次の開始時に、それらのタスクが実行されます。

少なくとも1台のテストデバイスで次のいずれかの条件が当てはまる場合、アップデートは正しくないと判断されます：

- アップデートタスクエラーが発生した
- セキュリティ製品のリアルタイム保護のステータスがアップデートの適用後に変更された
- オンデマンドスキャンタスクの実行中に、感染したオブジェクトが検知された
- カスペルスキー製品の実行時にエラーが発生した

すべてのテストデバイスの場合に挙げられた条件が当てはまらない場合、そのアップデートは正常とみなされ、*アップデート検証*タスクは正常に終了したと判断されます。

*アップデート検証*タスクを作成する前に、次の前提条件を実行してください：

1. 複数のテストデバイスで管理グループを作成する。このグループはアップデートの検証に必要になります。

   ネットワーク内で、最も信頼性の高い保護が適用されており、最も一般的なアプリケーション設定が行われているデバイスを使用してください。このアプローチにより、スキャン中のウイルス検知の精度が向上し、誤検知のリスクを最小限に抑えます。テストデバイスでウイルスが検知された場合、*アップデート検証*タスクは失敗と判断されます。

2. Kaspersky Endpoint Security for Linux など、Kaspersky Security Center Linux のサポート対象のアプリケーション向けにアップデートおよびマルウェアのスキャンタスクを作成します。アップデートおよびマルウェアスキャンタスクの作成時に、テストデバイスの管理グループを指定します。

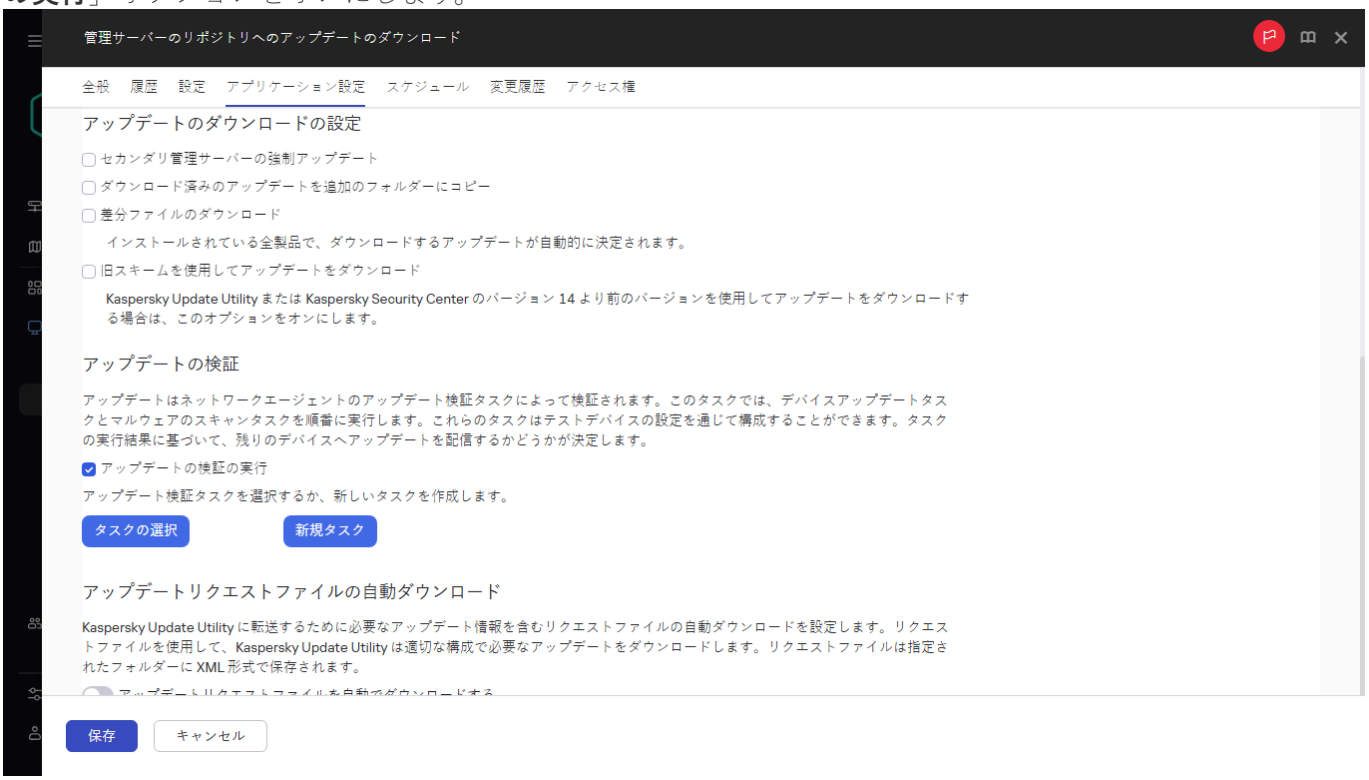
   *アップデート検証*タスクは、順次テストデバイスでアップデートとマルウェアスキャンタスクを実行し、すべてのアップデートが有効であることを確認します。また、*アップデート検証*タスクの作成中にアップデートおよびマルウェアスキャンタスクを指定する必要があります。

3. ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクをクリックします。

*ダウンロードしたアップデートを、クライアントデバイスに配信する前に Kaspersky Security Center Linux で検証するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスクをクリックします。

3. タスクのプロパティウィンドウが開いたら、［**アプリケーション設定**］タブに移動し、［**アップデートの検証の実行**］オプションをオンにします。



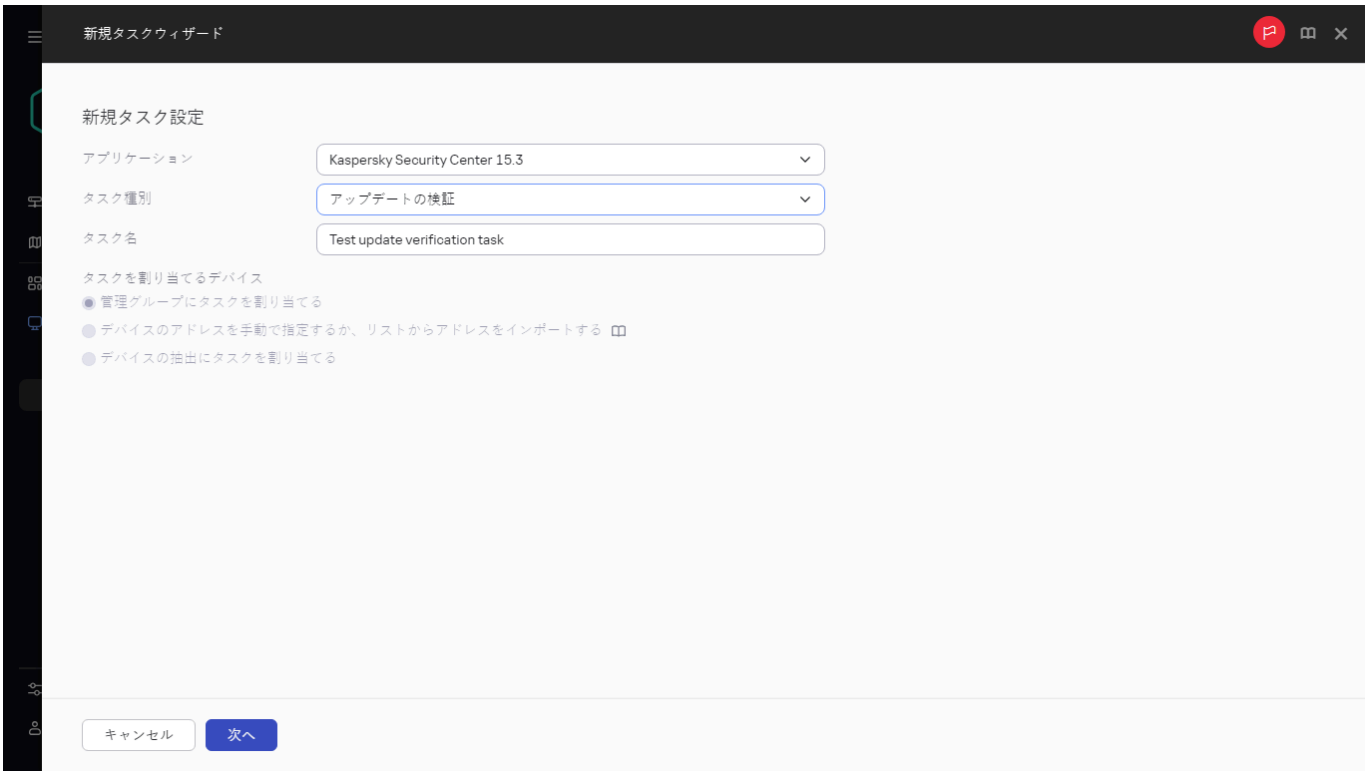

管理サーバーのリポジトリへのアップデートのダウンロードタスクのプロパティ

4. *アップデート検証*タスクがある場合は、［**タスクの選択**］をクリックします。表示されたウィンドウで、テストデバイスの管理グループで*アップデート検証*タスクを選択します。

5. 事前にアップデート検証タスクを作成していなかった場合は、次の操作を実行します：

   a. ［**新規タスク**］をクリックします。

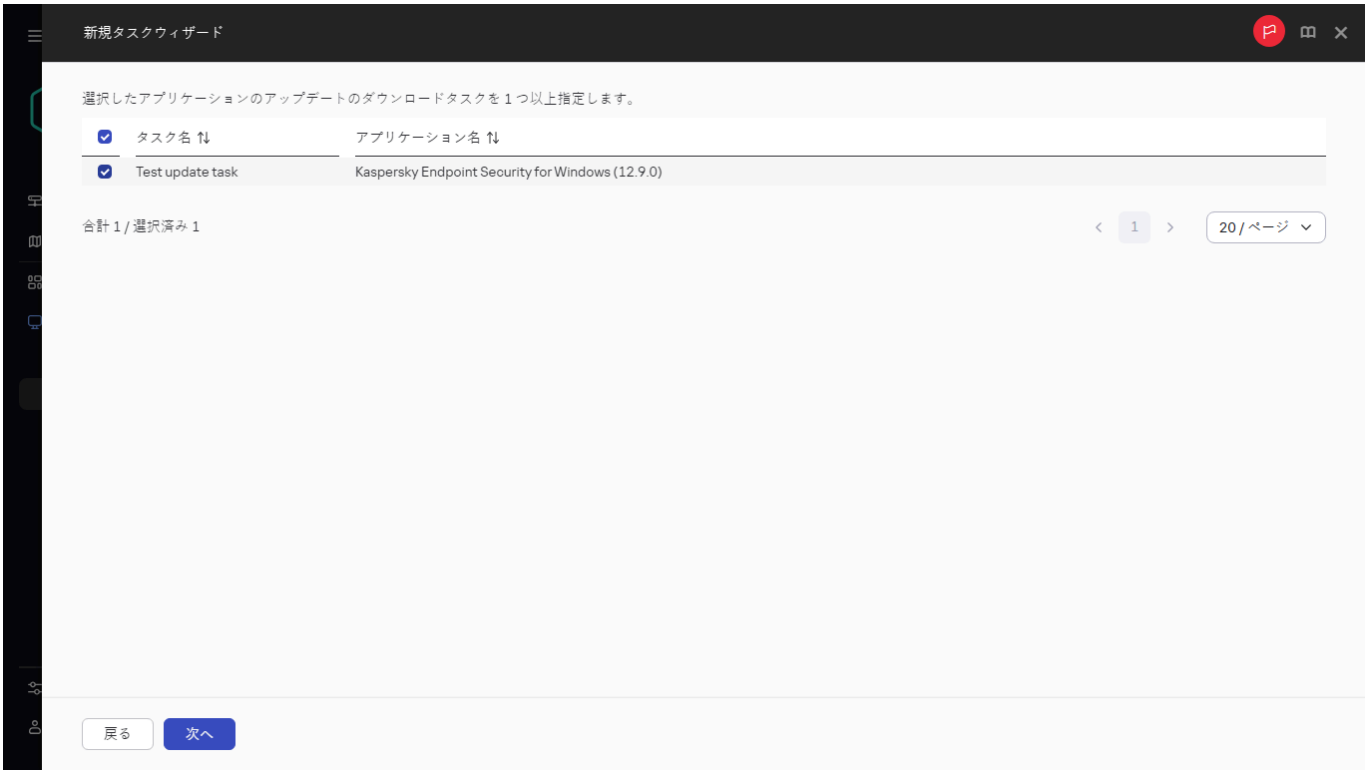
   b. タスクの追加ウィザードが表示されるので、事前設定されたタスク名を変更する場合は名前を指定します。




アップデート検証タスクの作成

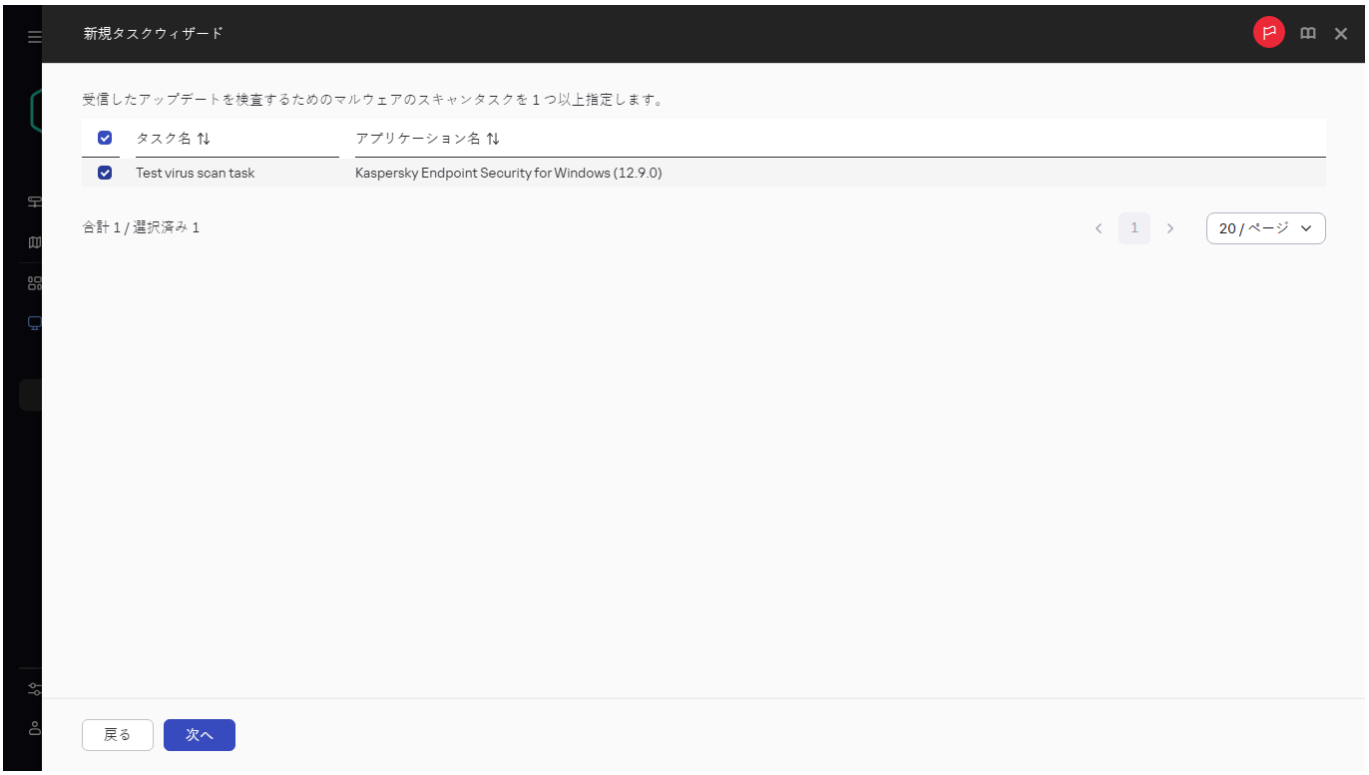
   a. 事前に作成しておいたテストデバイスの管理グループを選択します。

b. Kaspersky Security Center Linux でサポートされている必要なアプリケーションのアップデートタスクを選択します。




アプリケーションアップデートタスクの選択

a. Kaspersky Security Center Linux でサポートされている必要なアプリケーションのマルウェアのスキャンタスクを選択します。




マルウェアのスキャンタスクの選択

その後、次のオプションが表示されます。オプションはオンのままにしておくことを推奨します。

- **定義データベースのアップデート後にデバイスを再起動する**

デバイス上で定義データベースをアップデートした後には、デバイスの再起動を推奨します。

既定では、このオプションはオンです。

- **定義データベースのアップデートとデバイス再起動の後にリアルタイム保護のステータスを確認する**

  このオプションをオンにすると、*アップデート検証*タスクは、管理サーバーのリポジトリにダウンロードされたアップデートが有効であるかどうか、また定義データベースのアップデート後にデバイスが再起動された後に保護レベルが低下することがないかを確認します。

  既定では、このオプションはオンです。




タスク設定の指定

a. *アップデート検証タスク*を実行するアカウントを指定します。自身のアカウントの使用も可能で、[**既定のアカウント**]オプションをオンのままにします。または、必要なアクセス権を持つ別のアカウントを指定してタスクを実行することもできます。この場合は[**アカウントの指定**]をオンにしてそのアカウントの資格情報を入力してください。

6. [**保存**]をクリックして、[*管理サーバーのリポジトリへのアップデートのダウンロード*]タスクのプロパティウィンドウを閉じます。

アップデートの自動的な検証が有効になります。これで、[*管理サーバーのリポジトリへのアップデートのダウンロード*]タスクを実行できるようになりました。タスクはアップデートの検証から開始します。

# [ディストリビューションポイントのリポジトリにアップデートをダウンロード]タスクの作成

[*ディストリビューションポイントのリポジトリにアップデートをダウンロード*]タスクを管理グループに対して作成できます。このタスクは、指定の管理グループ内のディストリビューションポイントに対して実行されます。

このタスクの使用例としては、管理サーバーとディストリビューションポイント間の通信の方が、ディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などがあります。

このタスクは、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートをダウンロードするために必要です。アップデートのリストには次の内容が含まれます：

- カスペルスキーのセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデート
- Kaspersky Security Center コンポーネントのアップデート
- カスペルスキーのセキュリティ製品のアップデート

アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

***ディストリビューションポイントのリポジトリにアップデートをダウンロード**タスクを、特定の管理グループに対して作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。



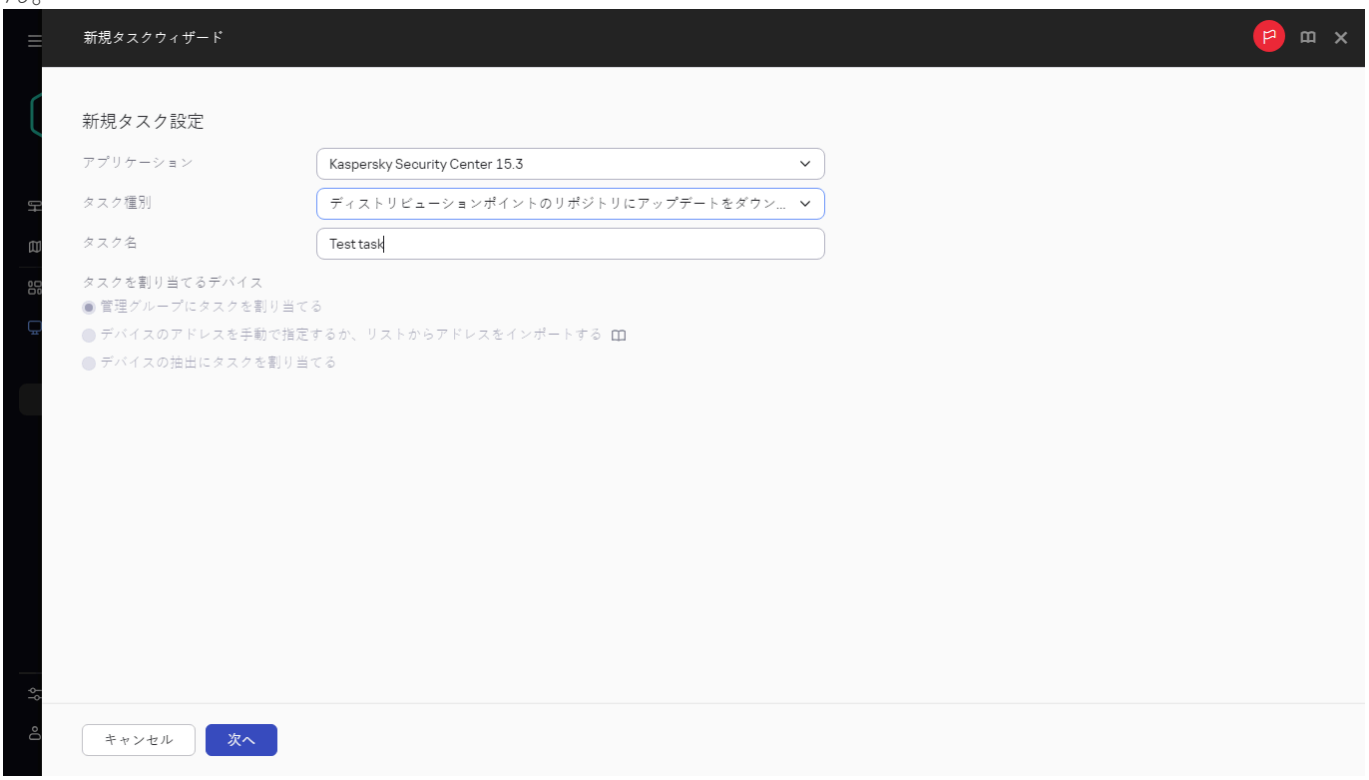

タスク セクション

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**タスク種別**］で［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。




［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

5. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。

6. ［**タスク作成の終了**］ステップで、既定のタスク設定を変更する場合、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

9. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

- **アップデート元**

  ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

  - カスペルスキーのアップデートサーバー

    カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

    既定ではこのオプションが選択されます。

  - プライマリ管理サーバー

    セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

  - ローカルまたはネットワークフォルダー

    最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：マウントされた SMB 共有のみ、ネットワークフォルダーとして使用できます。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

    ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center Linux は資格情報の入力を要求しません。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

Kaspersky Security Center Linux のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードします。

- Kaspersky Security Center 13 Linux

  たとえば、ディストリビューションポイントがローカルまたはネットワークフォルダーからアップデートを取得するように設定されているものとします。この場合、インターネットに接続できる管理サーバーを使用してアップデートをダウンロードし、このアップデートをディストリビューションポイントのローカルフォルダーに配置します。管理サーバーにバージョン 13 がインストールされている場合、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

既定では、このオプションはオフです。

10. タスクの開始スケジュール作成。必要に応じて、次の設定を指定します：

- **タスク開始**：
  - **手動**（既定で選択）

    タスクは、自動的には実行されません。手動でのみ開始できます。

    既定では、このオプションがオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。
    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **曜日ごと**

    指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
    既定では、毎週金曜日の午後 6 時にタスクが実行されます。

  - **毎月**

    毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
    指定した日付が存在しない月には、月の最終日にタスクを実行します。
    既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

  - **毎月、選択した週の指定日**

    毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
    規定では、日付は選択されていません。規定の開始時間は18:00 です。

  - **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行すると、定義データベースとソフトウェアモジュールのアップデートがアップデート元からダウンロードされ、共有フォルダーに保存されます。指定の管理グループに含まれていて、ディストリビューションポイントタスクが明示的に設定されていないディストリビューションポイントにしか、ダウンロードされたアップデートは使用されません。

# ［管理サーバーのリポジトリへのアップデートのダウンロード］タスクに対するアップデート元の追加

管理サーバーのリポジトリにアップデートをダウンロードするタスクを作成または使用する場合、次のアップデート元を選択することができます：

- カスペルスキーのアップデートサーバー
- プライマリ管理サーバー
  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。
- ローカルまたはネットワークフォルダー

> ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクおよび［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクで、パスワード保護されたローカルフォルダーまたはネットワークフォルダーをアップデート元として選択した場合はユーザー認証が動作しません。この問題を解決するには、最初にパスワード保護されたフォルダーをマウントしてから、オペレーティングシステムを使用するなどして必要な資格情報を指定します。この後、アップデートのダウンロードタスクでこのフォルダーをアップデート元として選択することができます。Kaspersky Security Center Linux は資格情報の入力を要求しません。

既定ではカスペルスキーのアップデートサーバーが使用されますが、ローカルまたはネットワークフォルダーにアップデートをダウンロードすることもできます。インターネットにアクセスできないネットワークを使用する場合にフォルダーを使用することがあります。この場合、カスペルスキーのアップデートサーバーから手動でアップデートをダウンロードして、フォルダーにダウンロードしたファイルを配置することができます。

ローカルまたはネットワークフォルダーに指定できるパスは1つのみです。ローカルフォルダーとして、管理サーバーがインストールされているデバイス上のフォルダーを指定する必要があります。ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。SMB 共有に認証が必要な場合は、事前に必要な資格情報を使用してシステムにマウントする必要があります。SMB1 プロトコルはセキュアではないため、使用しないことを推奨します。

*アップデート元を追加するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**管理サーバーのリポジトリへのアップデートのダウンロード**］をクリックします。
3. ［**アプリケーション設定**］タブに移動します。
4. ［**アップデート元**］テーブルで、［**追加**］をクリックします。
5. 開いたウィンドウで必要なソースを追加し、［**保存**］をクリックします。
   ［**ローカルまたはネットワークフォルダー**］を選択した場合は、フォルダーのパスを指定します。
6. タスクのウィンドウで［**保存**］をクリックします。

指定したアップデート元から管理サーバーのリポジトリにアップデートがダウンロードされるようになります。

カスペルスキーのアップデートサーバーとローカルフォルダーまたはネットワークフォルダーの両方を追加すると、アップデートの優先順位を設定できます。これを行うには、［**アップデート元**］テーブルで、優先度を変更する更新の横にあるチェックボックスをオンにし、［**上へ**］または［**下へ**］をクリックします。

# ソフトウェアアップデートの拒否と承認

アップデートのインストールタスクの設定によっては、インストールするアップデートの承認が必要な場合があります。インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへのこれらのアップデートのインストールを許可することができます。

アップデートの承認と拒否は、Windows ベースのクライアントデバイスにインストールされているネットワークエージェントと管理対象アプリケーションでのみ使用できます。管理サーバー、Kaspersky Security Center Web コンソール、および管理 Web プラグインのシームレスなアップデートはサポートされていません。これらのコンポーネントをアップデートするには、カスペルスキーの Web サイトから最新バージョンをダウンロードし、手動でインストールしてください。

*1 つ以上のアップデートを承認または拒否するには：*

1. メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**シームレスアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。

   管理対象の製品のアップデートには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。この最小バージョンが現在のバージョンよりも新しい場合、これらのアップデートは表示されますが、承認はできません。また、Kaspersky Security Center をアップグレードするまでは、このようなアップデートからインストールパッケージを作成することもできません。Kaspersky Security Center インスタンスを必要な最小バージョンにアップグレードするように要求されます。

2. 必要に応じて、［**使用許諾契約書の表示と同意**］をクリックして EULA に同意します。
3. 承認または拒否するアップデートを選択します。
4. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。
   既定値は［*未定義*］です。

   ［*承認*］ステータスを割り当てたアップデートは、インストールを待機するキューに置かれます。

［*拒否*］ステータスを割り当てたアップデートは、アップデートをインストール済みのすべてのデバイスからアンインストールされます（可能な場合）。また、今後これらのアップデートは他のデバイスに新規にインストールされません。

カスペルスキー製品の一部のアップデートはアンインストールできません。［*拒否*］ステータスを設定した場合、Kaspersky Security Center Linux はこれらのアップデートをインストール済みのデバイスからアンインストールしません。しかし、今後これらのアップデートが他のデバイスに新規にインストールされることはありません。

サードパーティ製のソフトウェアアップデートに［*拒否*］ステータスを設定すると、このアップデートは、アップデートのインストールを予定しているがまだ完了していないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

# Kaspersky Endpoint Security for Windows のアップデートの自動インストール

クライアントデバイスでの Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールの自動アップデートを設定できます。

*デバイスでの Kaspersky Endpoint Security for Windows のアップデートのダウンロードおよび自動インストールを設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Endpoint Security for Windows を対象アプリケーションとするタスクから、［**アップデート**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスク範囲を選択します。
6. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。
7. ［**タスク作成の終了**］ステップで、既定のタスク設定を変更する場合、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
8. ［**作成**］をクリックします。
   タスクが作成され、タスクリストに表示されます。
9. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

10. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、アップデートタスクの設定をローカルモードかモバイルモードで指定します：

    - **ローカルモード**：管理サーバーとデバイスの間で接続が確立されている場合。
    - **モバイルモード**：Kaspersky Security Center Linux とデバイスの間で接続が確立されていない場合（たとえば、デバイスがインターネットに接続されていない時）。

11. Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールのアップデートに使用するアップデート元を有効にします。必要に応じて、［**上へ**］と［**下へ**］を使用して、リスト内のアップデート元の順序を変更できます。複数のアップデート元が有効な場合は、リスト上位のリソースから次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。

12. ［**承認されたソフトウェアモジュールのアップデートのインストール**］をオンにすると、定義データベースとともに、ソフトウェアモジュールのアップデートをダウンロードしてインストールできます。

    このオプションをオンにすると、Kaspersky Endpoint Security for Windows によって適用可能なソフトウェアモジュールのアップデートについてユーザーに通知され、アップデートタスクの実行時に、アップデートパッケージにソフトウェアモジュールのアップデートが追加されます。Kaspersky Endpoint Security for Windows では、*承認*ステータスが付与されたアップデートのみがインストールされます。ローカルへのインストールは、製品インターフェイスまたは Kaspersky Security Center Linux を経由して実行されます。

    ［**ソフトウェアモジュールの重要なアップデートを自動的にインストール**］をオンにすることもできます。ソフトウェアモジュールのアップデートが使用可能な時、Kaspersky Endpoint Security for Windows は「*緊急*」ステータスのアップデートのみを自動的にインストールし、残りのアップデートは承認後にインストールします。

    ソフトウェアモジュールのアップデートで使用許諾契約書とプライバシーポリシーの条項を確認して同意する必要がある場合、カスペルスキー製品では、使用許諾契約書とプライバシーポリシーの条項をユーザーが同意した後にアップデートがインストールされます。

13. フォルダーへダウンロード済みのアップデートを保存するには［**アップデートをフォルダーにコピー**］をオンにし、保存先のフォルダーのパスを指定します。

14. タスクのスケジュールを設定します。確実にタイムリーにアップデートされるようにするため、［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

15. ［**保存**］をクリックします。

［**アップデート**］タスクの実行時、製品からカスペルスキーのアップデートサーバーにリクエストが送信されます。

アップデートによっては、最新バージョンの管理プラグインをインストールする必要があります。

# カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

Kaspersky Security Center Linux がカスペルスキーのアップデートサーバーからアップデートをダウンロードする時、差分ファイルを使用することでトラフィックが最適化されます。また、ネットワーク内の他のデバイスからアップデートを取得するデバイス（管理サーバー、ディストリビューションポイント、クライアントデバイス）についても、差分ファイルの使用を有効化できます。

### 差分ファイルのダウンロード機能の概要

差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を軽減できます。管理サーバーまたはディストリビューションポイントで［*差分ファイルのダウンロード*］機能が有効になっている場合、該当する管理サーバーまたはディストリビューションポイントに差分ファイルが保存されます。これにより、この管理サーバーまたはディストリビューションポイントからアップデートを取得するデバイスでは、保存されている差分ファイルを使用して定義データベースとソフトウェアモジュールのアップデートを実行できます。

差分ファイルをより効果的に使用するには、デバイス側でのアップデートスケジュールを、アップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデートスケジュールと同期することを推奨します。ただし、このような設定を行わなくても、デバイス側のアップデート頻度がアップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデート頻度より低いだけでもトラフィックの軽減につながります。

ディストリビューションポイントは差分ファイルの自動配信に IP マルチキャストを使用しません。

# 差分ファイルのダウンロード機能の有効化

### 実行するステップ

1. **管理サーバーでこの機能を有効にする**

   *管理サーバーのリポジトリへのアップデートのダウンロード*タスクの設定でこの機能を有効にします。

2. **ディストリビューションポイントでこの機能を有効にする**

   ［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを使用してアップデートを取得するディストリビューションポイントでこの機能を有効にします。

   管理サーバーからアップデートを受け取るディストリビューションポイントのネットワークエージェントのポリシー設定でこの機能を有効にします。

   管理サーバーからアップデートを取得するディストリビューションポイントでこの機能を有効にします。

   ネットワークエージェントのポリシー設定と（ディストリビューションポイントを手動で割り当てていてポリシー設定を上書きしたい場合）管理サーバーのプロパティの［**ディストリビューションポイント**］セクションで機能を有効にできます。

［差分ファイルのダウンロード］機能が有効になっているかどうかを確認する方法としては、これらの手順を実行する前後での内部トラフィックを測定することができます。

# ディストリビューションポイントによるアップデートのダウンロード

Kaspersky Security Center Linux では、ディストリビューションポイントはアップデートを管理サーバー、カスペルスキーのサーバー、ローカルまたはネットワークフォルダーから取得できます。

*ディストリビューションポイントによるアップデートのダウンロードを設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. このグループのクライアントデバイスにアップデートを配信するディストリビューションポイントの名前をクリックします。
4. ディストリビューションポイントのプロパティウィンドウで、［**アップデート元**］セクションを選択します。
5. ディストリビューションポイントのアップデート元を選択します：

   - **アップデート元**

     ディストリビューションポイントのアップデート元を選択します：
     - ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
     - タスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートのダウンロードタスクを使用**］をオンにして、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを指定します：
       - そのようなタスクが既にデバイスにある場合は、リストからタスクを選択します。
       - タスクがデバイスに存在しない場合、［**タスクの作成**］をクリックし、タスクを作成します。新規タスクウィザードが起動します。ウィザードの指示に従ってください。

   - **差分ファイルのダウンロード**

     このオプションで差分ファイルのダウンロードを有効にすることができます。

     既定では、このオプションはオンです。

ディストリビューションポイントは指定されたアップデート元からアップデートを取得します。

# オフラインデバイスの定義データベースとソフトウェアモジュールのアップデート

管理対象デバイスの定義データベースとソフトウェアモジュールのアップデートは、ウイルスやその他の脅威からデバイスを継続して保護するために重要なタスクです。通常、管理者は管理サーバーのリポジトリを使用するように指定して、定期的なアップデートを設定します。

管理サーバー（プライマリまたはセカンダリ）、ディストリビューションポイント、インターネットのいずれにも接続されていないデバイス（またはデバイスのグループ）のデータベースとソフトウェアモジュールをアップデートする必要がある場合は、FTP サーバーまたはローカルフォルダーなどの代替のアップデート元を使用する必要があります。この場合、フラッシュドライブまたは外付けハードディスクなどの大容量ストレージデバイスを使用して必要なアップデートのファイルを受け渡しする必要があります。

必要なアップデートは次からコピーできます：

- 管理サーバー：

  オフラインデバイスにインストールされているセキュリティ製品に必要なアップデートが管理サーバーのリポジトリに含まれるようにするには、少なくとも1台のオンラインの管理対象デバイスに同じセキュリティ製品がインストールされている必要があります。また、この製品が［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを使用して管理サーバーのリポジトリからアップデートを受信するように設定されている必要があります。

- 同じセキュリティ製品がインストールされていて、管理サーバーのリポジトリやディストリビューションポイントのリポジトリからアップデートを受信するか、カスペルスキーのアップデートサーバーからアップデートを直接受信するように設定されている任意のデバイス

管理サーバーのリポジトリからアップデートをコピーして、データベースおよびソフトウェアモジュールのアップデートを設定する例を次に示します。

*オフラインデバイスの定義データベースとソフトウェアモジュールをアップデートするには：*

1. 管理サーバーがインストールされているデバイスにリムーバブルドライブを接続します。

2. アップデートファイルをリムーバブルドライブにコピーします。

   既定では、アップデートは次の場所にあります：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/

   または、選択したフォルダーにアップデートを定期的にコピーするように Kaspersky Security Center Linux を設定できます。これには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティにある［**ダウンロード済みのアップデートを追加のフォルダーにコピー**］を使用します。フラッシュドライブまたは外付けハードディスクのフォルダーをこのオプションのターゲットフォルダーに指定した場合、この大容量ストレージデバイスには常にアップデートの最新バージョンが含まれることになります。

3. オフラインデバイスで、ローカルフォルダーまたは FTP サーバーや共有フォルダーなどの共有リソースからアップデートを受信するように Kaspersky Endpoint Security を設定します。

   実行手順の説明：

   - Kaspersky Endpoint Security for Linux のヘルプ
   - Kaspersky Endpoint Security for Windows のヘルプ

4. リムーバブルドライブからローカルフォルダーまたはアップデート元として使用する共有リソースにアップデートファイルをコピーします。

5. アップデートのインストールが必要なオフラインデバイスで、オフラインデバイスのオペレーティングシステムに応じて、Kaspersky Endpoint Security for Linux または Kaspersky Endpoint Security for Windows のアップデートタスクを開始します。

アップデートタスクが完了すると、デバイスの定義データベースとソフトウェアモジュールが最新の状態になります。

# Web プラグインのバックアップと復元

Kaspersky Security Center Web コンソールを使用すると、Web プラグインの現在の状態をバックアップして、後から保存した状態を復元できるようになります。たとえば、新しいバージョンへのアップデート前に Web プラグインをバックアップできます。アップデート後、新しいバージョンが要件や期待にそぐわない場合に、バックアップから以前のバージョンの Web プラグインを復元できます。

*Web プラグインをバックアップするには：*

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に移動します。
2. ［**Web プラグイン**］セクションで、バックアップする Web プラグインを選択して、［**バックアップの作成**］をクリックします。

   選択した Web プラグインがバックアップされます。作成したバックアップは、［**バックアップ**］セクションで表示できます。

*バックアップから Web プラグインを復元するには：*

1. メインメニューで、［**設定**］→［**バックアップ**］の順にクリックします。
2. ［**バックアップ**］セクションで、復元する Web プラグインを選択して、［**バックアップから復元**］をクリックします。

   選択したバックアップから Web プラグインが復元されます。

# 監視、レポート、監査

このセクションでは Kaspersky Security Center Linux の監視機能とレポート機能について説明しています。これらの機能を使用して、インフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center Linux の導入後または運用中に、必要に応じて監視とレポート機能の設定を最適な状態に編集できます。

# シナリオ：監視とレポート

このセクションでは、Kaspersky Security Center Linux の監視機能とレポート機能を設定する手順を説明しています。

## 必須条件

組織のネットワークへの Kaspersky Security Center Linux の導入後、監視を開始し、動作状況のレポートを生成できます。

組織のネットワークにおける監視の実施とレポートの利用は、以下の手順で進みます：

1. **デバイスのステータスの切り替えの設定**

   特定の条件に応じたデバイスのステータスの設定方法を確認します。各種設定を変更することで、重要度レベルが「*緊急*」または「*警告*」のイベントの数を変えることができます。デバイスのステータスの切り替えを設定する時には、次の点に注意してください：

   - 新しい設定が組織の情報セキュリティポリシーと矛盾しない。
   - 組織のネットワークにおける重要なセキュリティイベントに迅速に対応できる。

2. **クライアントデバイスで発生したイベントに関する通知の設定**

   実行手順の説明：

   **クライアントのデバイス上でイベントの通知（メール、SMS、ファイルの実行）を設定します。**

3. **緊急および警告の通知について推奨される処理の実行**

   実行手順の説明：

   **組織のネットワークに応じて、推奨される処理を実行する**

4. **組織のネットワークのセキュリティステータスの確認**

   実行手順の説明：

   - ［保護ステータス］ウィジェットを確認する
   - ［保護ステータスレポート］を生成し確認する
   - ［エラーに関するレポート］を生成し確認する

5. **保護されていないクライアントデバイスの検出**

   実行手順の説明：

- ［新しいデバイス］ウィジェットを確認する
- ［製品導入レポート］を生成し確認する

6. **クライアントデバイスの保護状態の確認**

   実行手順の説明：

   - ［保護ステータス］および［脅威の統計］カテゴリからレポートを生成して確認する
   - ［緊急］についてのイベント抽出を開始して確認する

7. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中に発生したイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：

   - イベント数の上限の設定

8. **ライセンス情報の確認**

   実行手順の説明：

   - ［ライセンス使用状況］ウィジェットをダッシュボードに追加して確認をする
   - ［ライセンス使用レポート］を生成し確認する

### 結果

これらの手順が完了すると、組織のネットワークの保護に関する情報を確認できるようになり、今後のセキュリティ対策の計画や脅威への対応に役立てることができます。

# 監視機能とレポート機能の種別の概要

組織ネットワーク内のセキュリティ関連のイベントに関する情報は管理サーバーデータベースに保存されます。イベントの情報に基づいて、Kaspersky Security Center Web コンソールでは、組織ネットワークを対象とした次の種別の監視機能とレポート機能を使用できます。

- ダッシュボード
- レポート
- イベントの抽出
- 通知

### ダッシュボード

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

### レポート

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

### イベントの抽出

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

### 通知

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。

## スマートトレーニングモードでのルールの適用条件

このセクションでは、クライアントデバイス上の Kaspersky Endpoint Security for Windows によるアダプティブアノマリーコントロールルールを使用した検知結果について説明します。

ルールは、クライアントデバイス上の通常と異なるふるまいを検知し、ブロックできます。ルールをスマートトレーニングモードで動作させている場合は、ルールによって異常なふるまいが検知されると、すべての検知について管理サーバーにレポートが送信されます。検知された異常な動作に関するレポートは、［**操作**］→［**リポジトリ**］→［**「スマートトレーニング」ステータスのルール適用条件**］で確認できます。検知結果を適切だとして確認することも、同種のふるまいが異常なふるまいとみなされないように除外として追加することもできます。

検知結果に関する情報は、管理サーバーでイベントログ（他のイベントと同様）と［アダプティブアノマリーコントロール］レポートに保存されます。

アダプティブアノマリーコントロールルールおよびルールのモードとステータスの詳細は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# アダプティブアノマリーコントロールルールを使用して実行された検知の表示と確認

*アダプティブアノマリーコントロールルールを使用した検知のリストを表示するには：*

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**「スマートトレーニング」ステータスのルール適用条件**］の順に移動します。

   リストには、アダプティブアノマリーコントロールルールを使用した検知結果について次の情報が表示されます：

   - **管理グループ**

     デバイスが属する管理グループの名前

   - **仮想管理サーバー**

     デバイスを管理する仮想管理サーバー。

   - **デバイス名**

     ルールが適用されたクライアントデバイスの名前

   - **名前**

     適用されたルールの名前

   - **ステータス**

     **除外済み、同期待ち** - 管理者がこの項目を処理してルールの除外対象として追加した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

     **確認済み、同期待ち** - 管理者がこの項目を処理して確認した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

     （空白） - 管理者が項目を処理していない場合。

   - **検知数**

     ヒューリスティックルール1件、プロセス1回、クライアントデバイス1台での検知数。この数は、Kaspersky Endpoint Security によってカウントされます。

   - **ユーザー名**

     検知が発生したプロセスを実行したクライアントデバイスユーザー名

- **ソースプロセスのパス**

  処理を実行したプロセスであるソースプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースプロセスのハッシュ**

  ソースプロセスファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのパス**

  プロセスを開始したオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのハッシュ**

  ソースファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのパス**

  ターゲットプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのハッシュ**

  ターゲットファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのパス**

  ターゲットオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのハッシュ**

  ターゲットファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **処理日**

  異常が検知された日付。

*検知のプロパティを表示するには：*

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**「スマートトレーニング」ステータスのルール適用条件**］の順に移動します。
2. 次のいずれかの手順を実行します：
   - ［**名前**］列で、表示する検知の名前のリンクをクリックします。
   - 検知のリストで、修正する検知の横にあるチェックボックスをオンにして、［**プロパティ**］をクリックします。

   選択した検知のプロパティウィンドウが開き、その検知に関する情報が表示されます。

アダプティブアノマリーコントロールルールの検知リスト、または選択した検知のプロパティウィンドウから、検知を確認できます。

*検知を確認するには：*

- 検知結果のリストで任意の検知（または複数の検知）を選択して、［**確認**］をクリックします。
- 選択した検知のプロパティウィンドウを開き、［**確認**］をクリックします。

  対象の検知のステータスが［**確認中**］に変更されます。この検知は、クライアントデバイスと管理サーバーの次回の同期後に検知リストから消えます。

  あなたの確認は、ルールで使用される統計に貢献します。詳細については、Kaspersky Endpoint Security for Windows ヘルプを参照してください。

# アダプティブアノマリーコントロールルールから除外に追加

アダプティブアノマリーコントロールへの除外の追加ウィザードを使用して、Kaspersky Endpoint Security のアダプティブアノマリーコントロールルールに除外を追加できます。

*ウィザードを使用して、アダプティブアノマリーコントロールルールから除外を追加するには：*

1. 次のいずれかの方法で、ウィザードを開始します：

   - メインメニューで、［**操作**］→［**リポジトリ**］→［**「スマートトレーニング」ステータスのルール適用条件**］に移動し、1つまたは複数の検知を選択して、［**除外**］ボタンをクリックします。

     1回につき最大1000個の除外を追加できます。

     検知を除外に追加する前に、検知名または［**プロパティ**］をクリックして、検知のプロパティを表示できます。開いた検知プロパティウィンドウで、［**除外**］ボタンをクリックすることもできます。

   - メインメニューで［**監視とレポート**］→［**イベントの抽出**］に移動し、必要なイベントの抽出のリンクをクリックし、除外する検知の横にあるチェックボックスをオンにして、［**アダプティブアノマリーコントロールから除外**］ボタンをクリックします。

   アダプティブアノマリーコントロール除外への追加ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. 除外項目を追加するポリシーとプロファイルを選択します。

   継承したポリシーの内容は更新できません。自分が変更権限を持っていないポリシーの内容はアップデートできません。

3. ［**完了**］をクリックしてウィザードを終了します。

   対象の検知のステータスが［**除外中**］に変更されます。この検知は、クライアントデバイスと管理サーバーの次回の同期後に検知リストから消えます。アダプティブアノマリーコントロールルールからの除外が構成され、適用されます。

# ダッシュボードとウィジェット

このセクションでは、ダッシュボードとダッシュボードで利用できるウィジェットについて説明します。このセクションでは、ウィジェットを管理する方法と、ウィジェットの設定について説明します。

# ダッシュボードの使用

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**ダッシュボード**］をクリックすると、ダッシュボードが表示されます。




ウィジェット付きダッシュボード

ダッシュボードでは、カスタマイズ可能なウィジェットを利用できます。円グラフや表、棒グラフ、リストなどの各種形式で表示できる様々なウィジェットを選択できます。ウィジェットに表示される情報は自動的に更新されます。更新には1～2分かかります。更新の間隔はウィジェットごとに異なります。設定メニューを使用して、任意のタイミングで手動でウィジェットを更新できます。

既定では、ウィジェットには管理サーバーのデータベースに保存されているイベントの情報が含まれています。

Kaspersky Security Center Web コンソールには、次のカテゴリのウィジェットが既定のウィジェットのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

一部のウィジェットのテキスト情報にはリンクが含まれている場合があります。リンクをクリックすると詳細情報を確認できます。

ダッシュボードの設定では、必要に応じて、ウィジェットの追加、非表示への変更、サイズや表示の変更、移動、設定の変更を行うことができます。

# ダッシュボードへのウィジェットの追加

*ダッシュボードにウィジェットを追加するには：*

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。




ウィジェット付きダッシュボード

2. ［**Web ウィジェットを追加または復元**］をクリックします。




ウィジェットの追加

3. 使用可能なウィジェットのリストから、ダッシュボードに追加するウィジェットを選択します。

ウィジェットはカテゴリ別にグループ化されています。カテゴリに含まれるウィジェットのリストを表示するには、カテゴリ名の横にあるアイコン（›）をクリックします。




ウィジェット種別の選択

4. ［**追加**］をクリックします。

選択したウィジェットがダッシュボードの一番下に追加されます。

追加したウィジェットの表示と設定を変更できます。

# ダッシュボードでウィジェットを非表示にする操作

*ダッシュボードで表示中のウィジェットを非表示にするには：*

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 非表示にするウィジェットに隣接する設定アイコン（⚙）をクリックします。




ウィジェットメニュー

3. ［**Web ウィジェットを非表示にする**］を選択します。
4. ［**警告**］ウィンドウが表示されたら、［**OK**］をクリックします。

選択したウィジェットが表示されなくなります。いつでも、このウィジェットをもう一度ダッシュボードに追加できます。

# ダッシュボードでのウィジェットの移動

*ダッシュボードでウィジェットを移動するには：*

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**移動**］を選択します。
4. ウィジェットを移動する場所をクリックします。選択できるのは別のウィジェットの表示位置のみです。

選択したウィジェットの表示位置が入れ替わります。

# ウィジェットのサイズと表示形式の変更

グラフを表示するウィジェットでは、グラフの形式（棒グラフまたは折れ線グラフ）を変更できます。一部のウィジェットではウィジェットのサイズを「コンパクト」「中サイズ」「最大」に変更できます。

*ウィジェットの表示形式を変更するには：*

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 編集するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. 次のいずれかの手順を実行します：
   - ウィジェットを棒グラフとして表示するには、［**グラフの種別：棒**］をオンにします。
   - ウィジェットを折れ線グラフとして表示するには、［**グラフの種別：折れ線**］をオンにします。
   - ウィジェットの表示領域を変更するには、次の値のうちの1つを選択してください：
     - **コンパクト**
     - **コンパクト（棒グラフのみ）**
     - **中サイズ（円グラフ）**
     - **中サイズ（棒グラフ）**
     - **最大**

選択したウィジェットの表示形式が変更されます。

# ウィジェットの設定の変更

*ウィジェットの設定を変更するには：*

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 変更するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**設定を表示する**］を選択します。
4. ウィジェットの設定ウィンドウが表示されるので、必要に応じてウィジェットの設定を変更します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したウィジェットの設定が変更されます。

どのような設定項目が存在するかは、ウィジェットごとに異なります。一般的な設定項目としてはたとえば次のような設定があります：

- **Web ウィジェットの範囲**（管理グループやデバイスの抽出など、ウィジェットが情報を表示する対象オブジェクトの範囲）。
- **タスクの選択**（ウィジェットが情報を表示する対象タスクの範囲）。
- **時間**（[開始日から終了日まで]、[開始日から現在まで]、[今日から指定した日数だけ過去にさかのぼった範囲を対象] のいずれかの形式で指定できる、ウィジェットが情報を表示する対象期間）。
- **ステータスを「緊急」にする条件**および**ステータスを「警告」にする条件**（ステータス信号の色を決定するルール）。

ウィジェットの設定を変更した後、ウィジェット上のデータを手動で更新できます。

*ウィジェットのデータを更新するには：*

1. メインメニューで、[**監視とレポート**] → [**ダッシュボード**] に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. [**更新**] を選択します。

   ウィジェットのデータが更新されました。

# ダッシュボードのみモードについて

幹部社員など、ネットワークを管理してはいないが、Kaspersky Security Center Linux でネットワークの保護ステータスを表示する必要がある社員に対して[［ダッシュボードのみモード］を設定](#)することができます。ユーザーがこのモードを有効にすると、事前設定されたウィジェットのあるダッシュボードのみが表示されます。このように、すべての管理対象デバイスの保護ステータスや、最近検知された脅威数、またはネットワーク内で頻繁に検知される脅威など、ウィジェットで指定された統計情報を管理できます。

ユーザーがダッシュボードのみモードで作業する場合、次の制限事項が適用されます：

- ユーザーにはメインメニューは表示されません。そのためネットワーク保護の設定などを変更することはできません。
- ユーザーはウィジェットに対して表示もしくは非表示にするなどの操作を行うことはできません。そのため、オブジェクトの計算ルールや時間間隔の指定など、ユーザーに必要なすべてのウィジェットをダッシュボードに表示できるように設定する必要があります。

自分自身にダッシュボードのみモードを割り当てることはできません。このモードで作業したい時は、システム管理者、マネージドサービスプロバイダー（MSP）、または［**一般的な機能：ユーザー権限**］機能領域の**[オブジェクト ACL の変更](#)**権限を持つユーザーに問い合わせてください。

# ダッシュボードのみモードの設定

ダッシュボードのみモードの設定を始める前に、次の要件を満たしていることを確認してください：

- ［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持っている。この権限を持っていない場合、モードの設定用タブは表示されません。
- ［**一般的な機能:：基本機能**］の機能領域の**読み取り**権限を持っている。

ネットワークで管理サーバーの階層が配置されている場合、ダッシュボードのみモードを設定するには［**ユーザーとロール**］→［**ユーザーとグループ**］セクションの［**ユーザー**］タブでユーザーアカウントが使用できるサーバーに移動します。プライマリサーバーまたは物理セカンダリサーバーを選択できます。仮想サーバーでモードを調整することはできません。

*ダッシュボードのみモードを設定するには：*

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. ダッシュボードのウィジェットを調整するユーザーアカウント名をクリックします。
3. アカウント設定ウィンドウが表示されたら、［**ダッシュボード**］を選択します。

   表示されたタブに、ユーザーに表示されるものと同じダッシュボードが表示されます。
4. ［**ダッシュボードのみモードでコンソールを表示**］オプションがオンになっている場合は切り替えスイッチをオフにします。

   このオプションがオンになっていると、自身もダッシュボードを変更することができません。このオプションをオフにした後、ウィジェットを管理できるようになります。
5. ダッシュボードの表示を設定します。カスタマイズ可能なアカウントを持つユーザー向けに、［**ダッシュボード**］タブで事前設定されたウィジェットのセットが使用可能です。ユーザーはウィジェットのサイズや設定を変更したり、ダッシュボードからウィジェットを追加したり削除したりすることはできません。そのため、ユーザーに対してネットワーク保護の統計が表示されるようにウィジェットを調整します。［**監視とレポート**］→［**ダッシュボード**］セクションで行うのと同様の操作を［**ダッシュボード**］タブで実行します：
   - ダッシュボードに新しいウィジェットを追加します。
   - ユーザーに必要ないウィジェットを非表示にします。
   - 必要な順番にウィジェットを移動します。
   - ウィジェットの表示方法やサイズを変更します。
   - ウィジェットの設定を変更します。

6. ［**ダッシュボードのみモードでコンソールを表示**］オプションの切り替えスイッチをオンにします。

   その後、ユーザーはダッシュボードのみを使用できるようになります。ユーザーは統計情報を監視できますが、ネットワーク保護の設定やダッシュボードの表示を変更することはできません。ユーザーとお客様ご自身にも同じダッシュボードが表示され、お客様もダッシュボードを変更することはできません。

   このオプションをオフにしておくと、ユーザーにはメインメニューが表示され、ユーザーは Kaspersky Security Center Linux でセキュリティ設定やウィジェットの変更を含む、様々な操作を実行することができます。

7. ダッシュボードのみモードの設定を完了したら、［**保存**］をクリックします。この後、準備したダッシュボードがユーザーに表示されます。

8. ユーザーが、サポートされるカスペルスキー製品の統計を表示するアクセス権を必要とする場合は、ユーザーの権限を設定します。設定すると、カスペルスキー製品のデータがユーザーのこれらのアプリケーションのウィジェットに表示されるようになります。

ユーザーはカスタマイズされたアカウントで Kaspersky Security Center Linux にログインし、ダッシュボードのみモードでネットワーク保護の統計を監視できるようになりました。

# レポート

このセクションでは、レポートの使用、カスタムレポートテンプレートの管理、レポートテンプレートを使用した新規レポートの作成、レポートの配信タスクの作成について説明します。

# レポートの使用

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**レポート**］をクリックすると、レポートが表示されます。

既定では、レポートには過去 30 日の情報が含まれます。

Kaspersky Security Center Linux には、次のカテゴリのレポートが既定のレポートのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

カスタムレポートテンプレートの作成、レポートテンプレートの編集、レポートテンプレートの削除を行うことができます。

既存のテンプレートに基づくレポートの作成、ファイルへのレポートのエクスポート、レポートの配信タスクの作成を行うことができます。

# レポートテンプレートの作成

*レポートテンプレートを作成するには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. ［**追加**］をクリックします。
   新規レポートテンプレートウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. レポート名を入力し、レポートの種類を選択します。




レポート名の指定とレポートの種類の選択

4. ウィザードの［**範囲**］ステップで、このレポートテンプレートに基づいたレポートでデータの表示対象にするクライアントデバイス（管理グループ、デバイスの抽出、指定したデバイス、ネットワーク内のすべてのデバイス）を指定します。




レポートの範囲の指定

5. ウィザードの［**レポート期間**］ステップで、レポートの対象期間を指定します。次の値を設定できます：

- 指定した 2 つの日付の間の期間
- 指定日からレポート作成日までの期間
- レポート作成日から指定した日数だけ過去にさかのぼった期間

一部のレポートではこのページが表示されない場合もあります。




レポート期間の指定

6. ［**OK**］をクリックしてウィザードを終了します。

7. 次のいずれかの手順を実行します：

- ［**保存して実行**］をクリックすると、新しいレポートテンプレートを保存して、テンプレートに基づくレポートを実行できます。

  レポートテンプレートが保存されます。レポートが生成されます。

- ［**保存**］をクリックすると、新しいレポートテンプレートを保存できます。

  レポートテンプレートが保存されます。

新しいテンプレートを使用して、レポートの作成と表示ができます。




レポートのリスト

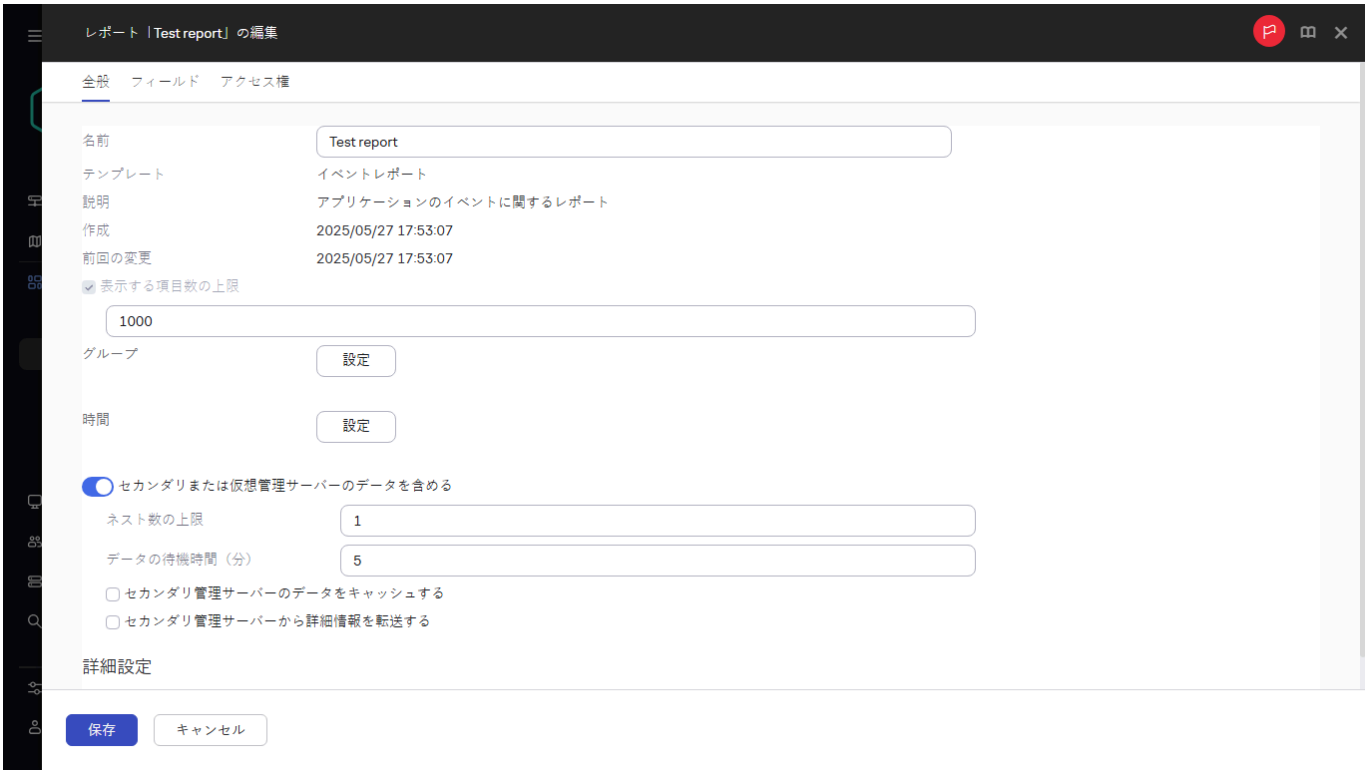
# レポートテンプレートのプロパティの表示と編集

レポートテンプレートについて、レポートテンプレートの名前やレポートに表示されるフィールドなどの基本的なプロパティを表示し、編集できます。

*レポートテンプレートのプロパティを表示したり編集するには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. プロパティの表示と編集を行うレポートテンプレートに隣接するチェックボックスを選択します。
   あるいは、まずレポートを生成して、次に［**編集**］をクリックします。

3. ［**レポートテンプレートのプロパティを開く**］をクリックします。
   ［**レポート「<レポート名>」の編集**］ウィンドウの［**全般**］タブが表示されます。




レポートテンプレートのプロパティ

4. レポートテンプレートのプロパティを編集します。

- ［**全般**］タブ：
  - レポートテンプレート名
  - **表示する項目数の上限**

    このオプションをオンにすると、詳細なレポートデータの表に表示されるエントリ数に、指定した上限値が設定されます。このオプションは、レポートをファイルにエクスポートする時にレポートに含めることができるイベントの最大数には影響しません。

    レポートのエントリは、レポートテンプレートの［**フィールド**］→［**詳細フィールド**］セクションで指定したルールに従って並べ替えられ、合致するエントリのうち表示順が上のエントリだけが維持されます。詳細レポートのタイトルには、レポートテンプレートで設定したその他の条件に合致するエントリの合計数と表示されている数が表示されます。

    このオプションをオフにすると、詳細なレポートデータの表にはすべての使用可能なエントリが表示されますこのオプションをオフにすることは推奨されません。表示されるレポートエントリの数を制限することにより、DBMS（データベース管理システム）の負荷を減らし、レポートの生成とエクスポートの所要時間を削減できます。一部のレポートではエントリ数が多すぎる場合があります。このような場合、すべてのエントリに目を通し分析することは困難です。また、こうしたレポートの生成中にデバイスのメモリ不足が発生し、レポート自体を表示できない可能性もあります。

    既定では、このオプションはオンです。既定値は 1000 です。

  - **グループ**

    レポートの作成対象にするクライアントデバイスを変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。実際の設定は、レポートテンプレートの作成時に指定した設定によって異なります。

  - **時間**

    レポートの対象期間を変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。次の値を設定できます：

    - 指定した 2 つの日付の間の期間
    - 指定日からレポート作成日までの期間
    - レポート作成日から指定した日数だけ過去にさかのぼった期間

  - **セカンダリまたは仮想管理サーバーのデータを含める**

    このオプションをオンにすると、レポートテンプレートを作成する管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーからの情報をレポートに含めます。

    現在の管理サーバーのデータのみを表示する場合は、このオプションをオフにします。

    既定では、このオプションはオンです。

  - **ネスト数の上限**

対象の管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーのうち、指定したネスト数以内のサーバーのデータをレポートに含めます。

既定値は1です。ツリー内でより下位に位置するセカンダリ管理サーバーの情報を取得する必要がある場合、この値を変更することができます。

- **データの待機時間（分）**

  レポートを生成する前に、レポートテンプレートを作成する管理サーバーは、セカンダリ管理サーバーからデータが送信されるのを、指定した分数だけ待機します。指定した時間が経過してもセカンダリ管理サーバーからデータを取得できなかった場合は、これらのデータを除外してレポートが実行されます。［**セカンダリ管理サーバーのデータをキャッシュする**］を有効にすると、実際のデータの代わりにキャッシュデータがレポートに表示されます。無効にすると、［**該当なし**］と表示されます。

  既定値は5分です。

- **セカンダリ管理サーバーのデータをキャッシュする**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。送信されたデータはキャッシュに保存されます。

  レポートの生成時に現在の管理サーバーがセカンダリ管理サーバーからデータを取得できなかった場合、キャッシュから取得したデータがレポートに表示されます。データがキャッシュに送信された日付も合わせて表示されます。

  このオプションをオンにすると、最新のデータを取得できなかった場合でもセカンダリ管理サーバーの情報を表示できます。ただし、表示されるデータが最新のものではない場合があります。

  既定では、このオプションはオフです。

- **キャッシュの更新頻度（時間）**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。この期間は時間単位で指定できます。0時間を指定すると、レポートの生成時にのみデータが送信されます。

  既定値は0です。

- **セカンダリ管理サーバーから詳細情報を転送する**

  生成されたレポートの詳細なレポートデータの表に、レポートテンプレートを作成する管理サーバーのセカンダリ管理サーバーから取得したデータを含めます。

  このオプションをオンにすると、レポートの生成にかかる時間が長くなり、管理サーバー間のトラフィックも増大します。ただし、1つのレポートですべてのデータを表示できるメリットもあります。

  このオプションをオンにする他に、先に詳細なレポートデータを分析してエラーが発生しているセカンダリ管理サーバーを特定した上で、エラーが発生している管理サーバーのみを対象にレポートを生成するという方法も活用できます。

  既定では、このオプションはオフです。

- ［**フィールド**］タブ

レポートで表示されるフィールドを選択し、［**上へ**］と［**下へ**］を使用して、フィールドの順序を変更します。［**追加**］または［**編集**］をクリックすると、該当するフィールドに基づいて情報の並べ替えとフィルター処理を行えるかどうかを設定できます。

［**詳細フィールドのフィルター**］で、［**フィルターの変換**］をクリックすることでも拡張フィルタリング形式の使用を開始できます。この形式は、論理演算子「OR」を使用することで様々なフィールドに指定された条件を結合できます。ボタンをクリックした後、［**フィルターの変換**］パネルが右側に開きます。［**フィルターの変換**］をクリックして変換を確定します。［**詳細フィールド**］セクションで論理演算子「OR」を使用することで適用される条件付きの変換されたフィルターを定義できるようになります。

複雑なフィルタリング条件をサポートする形式にレポートを変換すると、以前の Kaspersky Security Center (11 より前のバージョン) でレポートを使用できなくなることがあります。また、このような互換性のないバージョンの製品を実行しているセカンダリの管理サーバーからのデータは、変換されたレポートに含めることができません。

5. ［**保存**］をクリックして変更内容を保存します。
6. ［**レポート <レポート名> の編集**］ウィンドウを閉じます。

レポートテンプレートのリストに更新したレポートテンプレートが表示されます。

# レポートのファイルへのエクスポート

1 つまたは複数のレポートを XML、HTML、または 1 つの PDF として保存できます。Kaspersky Security Center Linux では、同時に最大 10 個のレポートを指定した形式のファイルにエクスポートできます。

*レポートをファイルにエクスポートするには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. エクスポートするレポートを選択します。
   10 件を超えるレポートを選択すると、［**レポートのエクスポート**］ボタンが無効になります。




レポートのリスト

3. ［**レポートのエクスポート**］をクリックします。

4. 表示されたウィンドウで、次のエクスポートパラメータを指定します：

- **ファイル名**。

  エクスポートするレポートを 1 つ選択する場合は、レポートファイル名を指定します。

  複数のレポートを選択した場合、レポートファイル名は、選択したレポートテンプレートの名前と一致します。

- **エントリの最大数**。

  レポートファイルに含まれるエントリの最大数を指定します。既定値は 10,000 です。

  エントリ数に制限のないレポートをエクスポートできます。レポートに多数のエントリが含まれている場合、レポートの生成とエクスポートにかかる時間が長くなります。

- **ファイル形式**。

  レポートのファイル形式（XML、HTML、PDF）を選択します。複数のレポートをエクスポートする場合、選択したすべてのレポートが指定された形式で個別のファイルとして保存されます。

  > wkhtmltopdf ツールはレポートを PDF に変換するために必要です。PDF を選択すると、管理サーバーはデバイスに wkhtmltopdf ツールがインストールされているかどうか確認します。ツールがインストールされていない場合は、管理サーバーデバイスにツールをインストールする必要があることに関するメッセージが表示されます。手動でツールをインストールして次の手順に進みます。




レポートのエクスポート設定の指定

5. ［**レポートのエクスポート**］をクリックします。

レポートは、指定した形式でファイルに保存されます。

# レポートの生成と表示

*レポートを作成および表示するには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポートの作成に使用するレポートテンプレートの名前をクリックします。

   選択したテンプレートを使用してレポートが作成され、表示されます。

レポートデータは、管理サーバーのローカリゼーションセットに従って表示されます。

作成されたレポートの図で、一部のフォントが正しく表示されない場合があります。この問題を解決するには、fontconfig ライブラリをインストールします。また、オペレーティングシステムのロケールに対応するフォントがオペレーティングシステムにインストールされていることを確認してください。

レポートには次のデータが表示されます：

- ［**サマリー**］タブ：
  - レポート名とレポート種別、概要説明、レポート期間、レポートが作成されたデバイスグループに関する情報。
  - 代表的なレポートのデータを示している図表。
  - 計算されたレポートの指標を含む表。
- **[詳細]**タブで、詳細レポートデータの表が表示されます。

# レポート配信タスクの作成

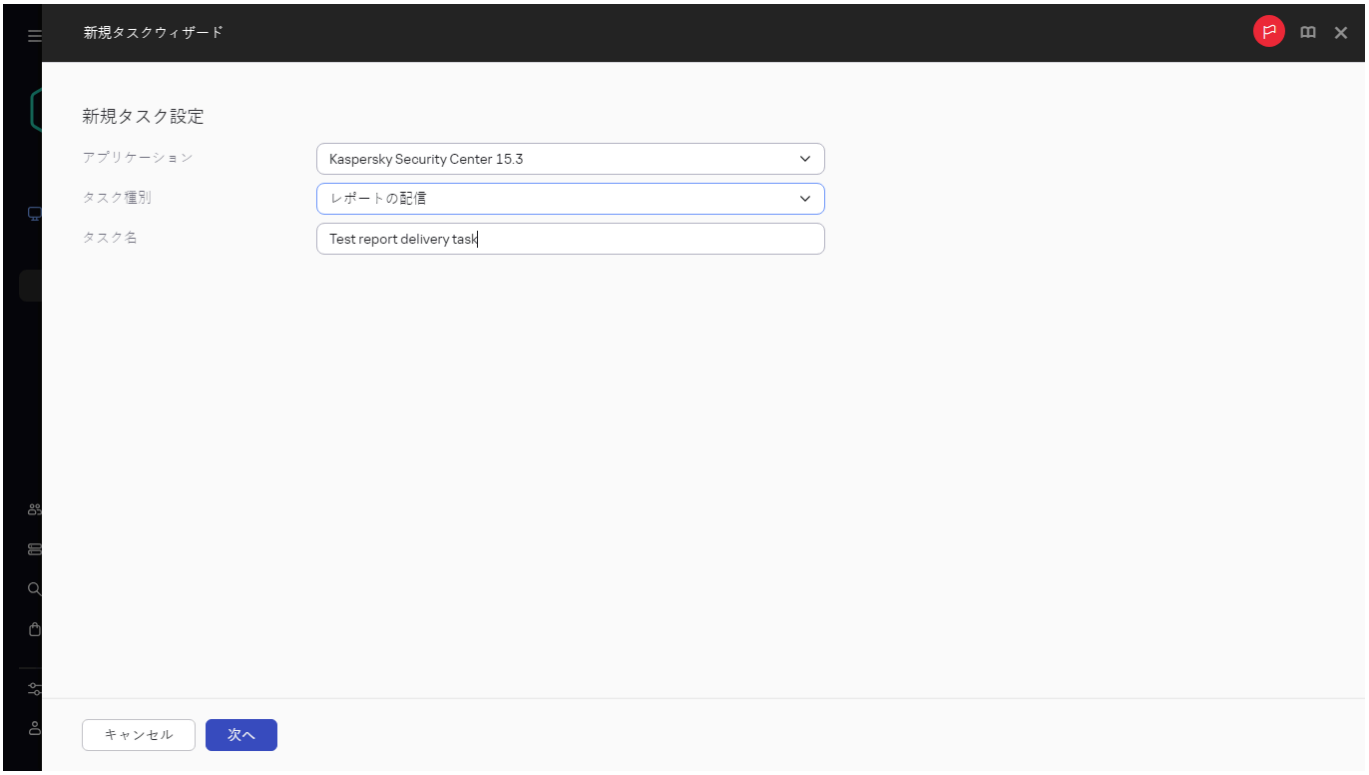
選択したレポートを配信するタスクを作成できます。

*レポート配信タスクを作成するには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポート配信タスクを作成するレポートテンプレートの横にあるチェックボックスをオンにします。
3. ［**配信タスクを作成**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードの**新規タスク設定**ステップで、タスク名を入力します。

   既定の名前は「**レポートの配信**」です。この名前のタスクが既に存在する場合は、タスク名にシーケンス番号（<N>）が追加されます。




レポート配信タスクの作成

5. ウィザードの**レポート設定**ステップで、次の設定を指定します：

a. タスクでレポートを配信するレポートテンプレート。

b. レポート形式（HTML、XLS、PDF）。

wkhtmltopdf ツールはレポートを PDF に変換するために必要です。PDF を選択すると、管理サーバーはデバイスに wkhtmltopdf ツールがインストールされているかどうか確認します。ツールがインストールされていない場合は、管理サーバーデバイスにツールをインストールする必要があることに関するメッセージが表示されます。手動でツールをインストールして次の手順に進みます。

c. レポートをメールで送信するかどうかと、送信する場合のメール通知設定。

最大 20 個のメールアドレスを指定できます。メールアドレスを区切るには、**Enter** キーを押します。カンマで区切られたメールアドレスのリストを貼り付けて、**Enter** キーを押すこともできます。

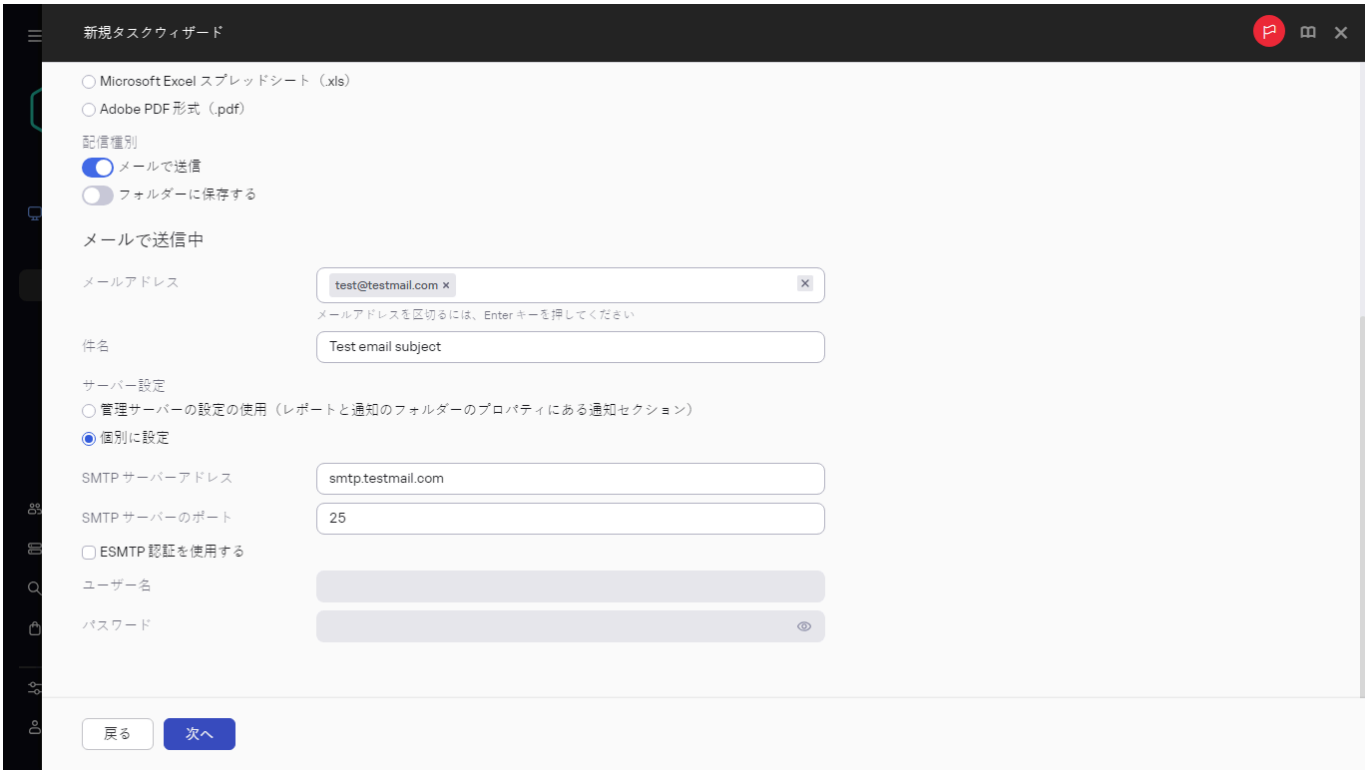
d. レポートを対応する設定とともにフォルダーに保存するかどうか。

［**フォルダーに保存する**］をオンにした場合、フォルダーへの POSIX パスを指定する必要があります。レポートを共有フォルダーに保存する場合は、［**共有フォルダーにアクセスするアカウントを指定する**］もオンにし、このフォルダーにアクセスするためのユーザーアカウントとパスワードを指定する必要があります。

> レポートを共有フォルダーに保存することを選択した場合は、管理サーバーがインストールされているデバイスからこのフォルダーにアクセスできることを確認する必要があります。アクセスを確保する方法と使用するツールは、インフラストラクチャによって異なります。

レポートをローカルフォルダーに保存する場合、管理サーバーを実行しているアカウントにはこのフォルダーへのアクセス権があるため、通常は資格情報は必要ありません。必要に応じて、ウィザードの［**タスクを実行するアカウントの選択**］ステップでユーザー資格情報を指定できます。

フォルダーの選択に関係なく、新しいレポートファイルで前回のタスクの起動時にレポートフォルダーに保存されたファイルを上書きする場合は、［**同じ種別の古いレポートを上書きする**］をオンにすることもできます。




タスク設定の指定

6. ウィザードの**タスクスケジュールの設定**ステップで、タスクの開始スケジュールを選択します。
以下のタスクスケジュールオプションが使用可能です：

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。
  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。
  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **N 週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、金曜日の現在のシステム時刻にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **指定した日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

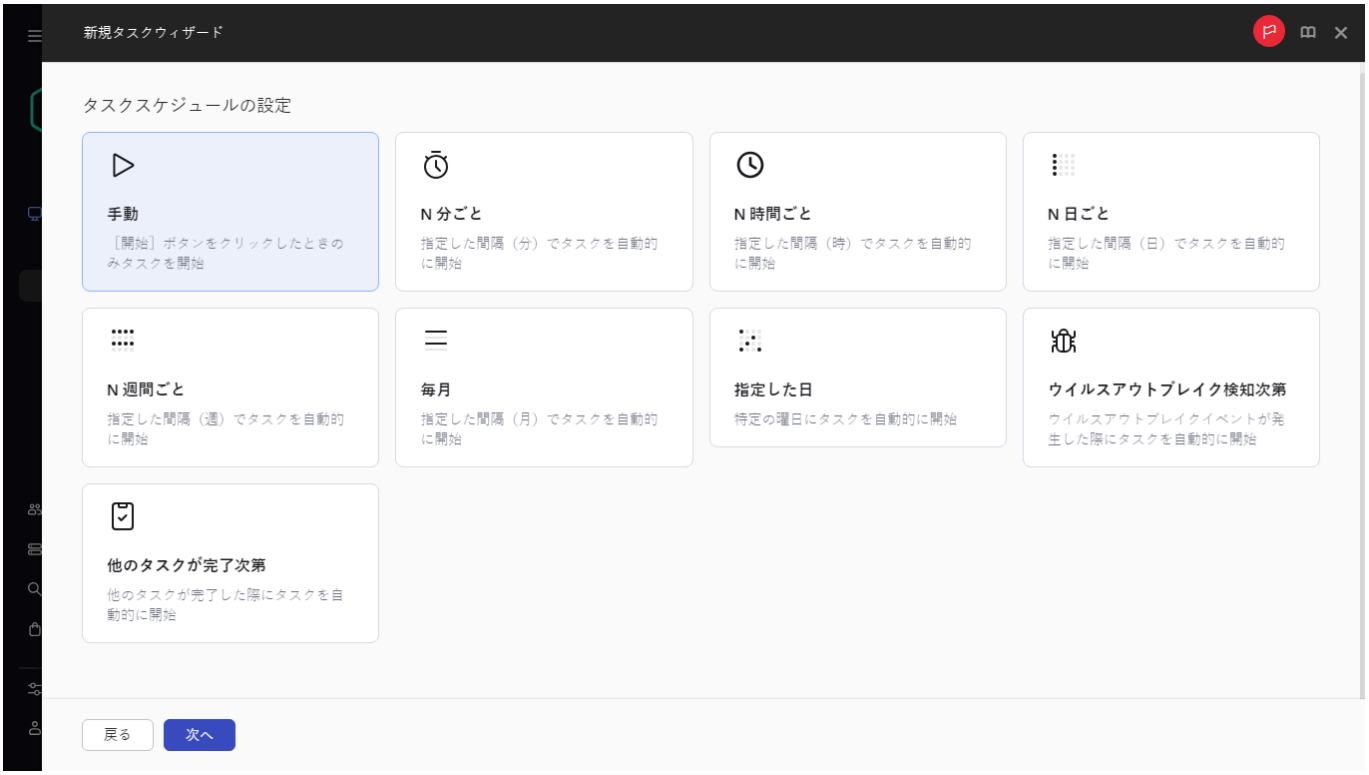
他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。




タスク開始スケジュールの選択

7. ウィザードのこのステップでは、その他のタスクスケジュール設定を指定します：

- ［**タスクのスケジュール**］セクションで、以前に選択したスケジュールをチェックまたは再設定し、時間間隔、日付または曜日を設定し、ウイルスアウトブレイク条件を設定するか、タスクを開始するトリガーとして別のタスクを完了します。該当するスケジュールを選択した場合は、このセクションで開始時間を指定することもできます。

- ［**追加設定**］セクションで、次の設定を指定します：

  - **未実行のタスクを実行する**

    このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

    このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

    このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

    既定では、このオプションはオフです。

  - **タスクの開始を自動的かつランダムに遅延させる**

    このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

    分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

    このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  - **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

    このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

    このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

    既定では、このオプションはオフです。既定の時間は1分です。

  - **次の時間を超える場合はタスクを停止する**

指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

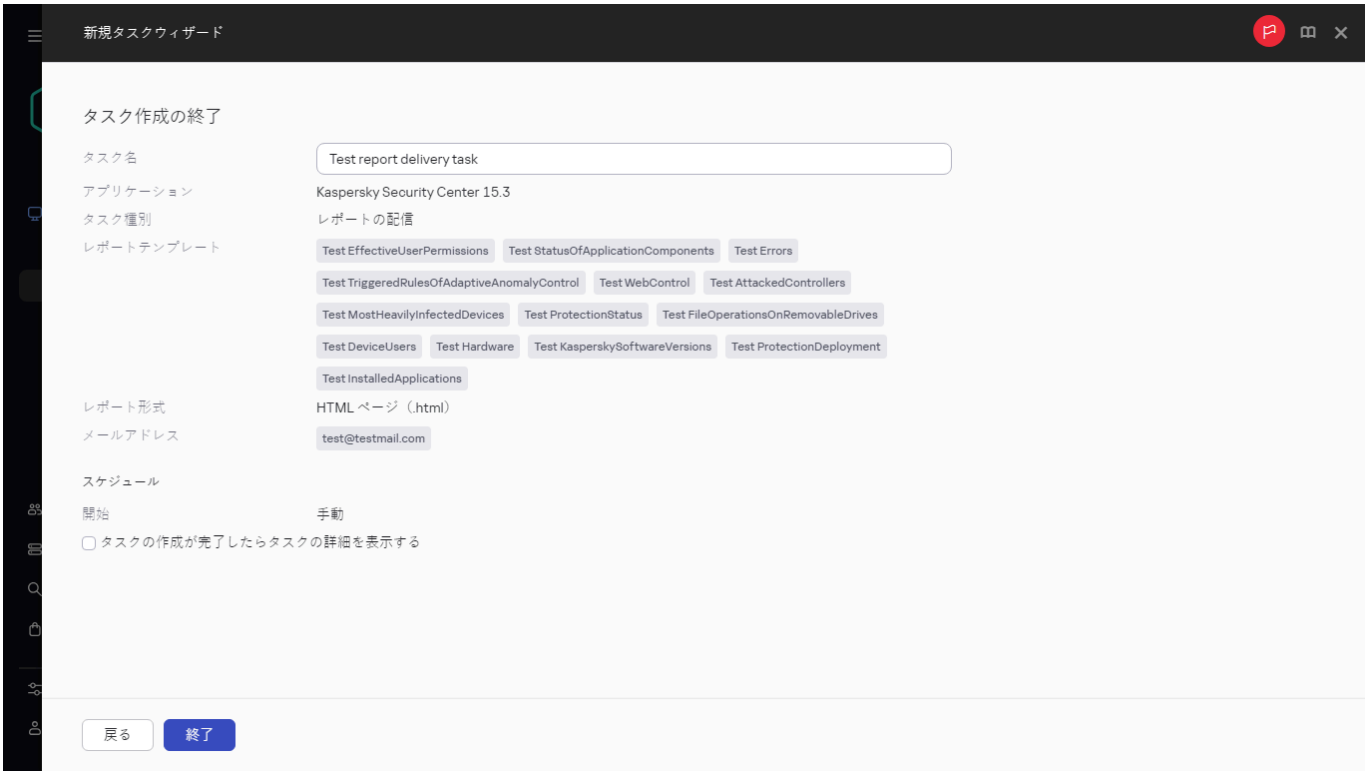



タスクスケジュール設定の指定

8. ウィザードの**タスクを実行するアカウントの選択**ステップで、タスクの実行に使用するユーザーアカウントの資格情報を指定します。

9. タスク作成後に他のタスク設定を変更したい場合は、ウィザードの**タスク作成の終了**ステップで、［**タスクの作成が完了したらタスクの詳細を表示する**］オプションをオンにします（既定でオンになっています）。

10. タスクを作成しウィザードを終了するには、［**終了**］をクリックします。




タスク作成の完了

レポート配信タスクが作成されます。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。

# レポートテンプレートの削除

*レポートのテンプレートを削除するには：*

1. メインメニューで、［**監視とレポート**］→［**レポート**］の順に選択します。
2. 削除するレポートテンプレートの隣にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで、［**OK**］をクリックして処理を確定します。

選択したレポートテンプレートが削除されます。これらのレポートテンプレートがレポートの配信タスクに含まれていた場合、タスクからも該当するレポートテンプレートが削除されます。

# イベントとイベントの抽出

このセクションでは、イベントとイベントの抽出、Kaspersky Security Center Linux コンポーネントで発生するイベントの種別、頻出イベントのブロック管理について説明します。

# Kaspersky Security Center Linux のイベントについて

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。

## 種別ごとのイベント

Kaspersky Security Center Linux には、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。
- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

## ソース別イベント

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center Linux のコンポーネント：
  - 管理サーバー
  - ネットワークエージェント
- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

## 重要度別イベント

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。
- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。

- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。

- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center Linux でイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

# Kaspersky Security Center Linux のコンポーネントでのイベント

Kaspersky Security Center Linux の各コンポーネントには、独自のイベント種別のセットがあります。このセクションでは、Kaspersky Security Center 管理サーバーとネットワークエージェントで発生するイベントの種別について説明します。カスペルスキー製品で発生する可能性のあるイベントの種別は、このセクションの説明には含まれていません。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

## イベント種別のデータ構造の説明

イベント種別ごとに、表示名、識別子（ID）、英字コード、内容の説明、既定の保管期間を記載しています。

- **イベント種別の表示名**：イベントを設定してそれが発生すると、この列のテキストが Kaspersky Security Center Linux で表示されます。

- **イベント種別の ID**：イベント解析用のサードパーティ製品を使用してイベントを処理すると、この列の数字コードが使用されます。

- **イベント種別**（英字コード）：Kaspersky Security Center Linux データベースで提供されるパブリックビューを使用してイベントの参照と処理を行う場合とイベントを SIEM システムにエクスポートする場合に、この列のコードが使用されます。

- **説明**：この列では、イベントが発生する状況と可能な対応が説明されています。

- **既定の保管期間**：この列には、イベントが管理サーバーデータベースに保管され、管理サーバーのイベントリストに表示される日数が記載されています。この期間が過ぎると、イベントが削除されます。イベントの保管期間の値が「0」の場合、これらのイベントについては検知のみが行われ、管理サーバーのイベントリストへの表示は行われません。こうしたイベントをオペレーティングシステムのイベントログに保存するように設定した場合、それらの保存先でイベントを確認できます。

  イベントの保管期間を変更できます：イベントの保管期間の設定

# 管理サーバーのイベント

このセクションには、管理サーバーに関するイベントの情報が記載されています。

## 管理サーバーの緊急イベント

次の表は、重要度が「**緊急**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの緊急イベント

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **ライセンス数の上限を超えました** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | 1 日に 1 回、Kaspersky Security Center Linux はライセンス管理の上限の超過が発生していないかどうかを確認します。<br>この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンスの上限の超過を管理サーバーが検出しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 110% を超えている場合に記録されます。<br>このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。<br>このイベントには、次の方法で対応できます：<br>• 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。<br>• 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。<br>Kaspersky Security Center Linux では、ライセンス管理の上限を超過した時にイベントを生成するルールを指定できます。 | 180 日間 |
| **デバイスが管理対象外になりました** | 4111 | KLSRV_HOST_OUT_CONTROL | この種別のイベントは、デバイスはネットワーク上で可視だが管理サーバーに接続していない状態が指定期間を超えて継続すると記録されます。<br>デバイス上でネットワークエージェントの正常な動作を妨げている要素を特定します。原因としては、ネットワークの問題や、ネットワークエージェントがデバイスから削除された状況などが考えられます。 | 180 日間 |
| **デバイスのステータスが「緊急」です** | 4113 | KLSRV_HOST_STATUS_CRITICAL | この種別のイベントは、管理対象デバイスに「緊急」ステータスが割り当てられると記録されます。デバイスのステータスが「緊急」に切り替わる条件を設定できます。 | 180 日間 |
| **このライセンス情報ファイルは拒否リストに追加されています** | 4124 | KLSRV_LICENSE_BLACKLISTED | この種別のイベントは、使用しているアクティベーションコードまたはライセンス情報ファイルがカスペルスキーで拒否リストに登録されると記録されます。<br>詳細は、テクニカルサポートに問い合わせてください。 | 180 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **ライセンスの有効期間がまもなく終了します** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | この種別のイベントは、製品版ライセンスの有効期限が近づいている時に発生します。<br>1日に1回、Kaspersky Security Center Linux はライセンス有効期間の終了日が近づいているかどうかを確認します。この種別のイベントは、ライセンスの有効期限まで残り 30 日、15 日、5 日および1日となった時に発生します。この日数は変更できません。管理サーバーがライセンスの有効期限より前に指定された日にオフになった場合は翌日までイベントは発生しません。<br>製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center Linux は基本機能のみを提供します。<br>このイベントには、次の方法で対応できます：<br>• 予備のライセンスが管理サーバーに追加されていることを確認します。<br>• 定額制サービスをご利用の場合は、必ず更新してください。支払い期日までに決済された場合、無制限の定額制サービスは自動的に更新されます。 | 180 日間 |
| **MDM 証明書の有効期間が終了しています** | 4132 | KLSRV_CERTIFICATE_EXPIRED | このタイプのイベントは、モバイルデバイスのクライアント証明書の有効期限が切れた時に発生します。 | 180 日間 |
| **管理サーバー証明書の有効期間が終了しています。** | 6129 | KLSRV_EV_SRV_CERT_EXPIRED_DN | このタイプのイベントは、モバイルデバイスと UEFI デバイスの管理用の管理サーバー証明書の有効期間が切れた時に発生します。<br>期限切れの証明書をアップデートする必要があります。 | 180 日間 |
| **監査：SIEM へエクスポートできませんでした** | 5130 | KLAUD_EV_SIEM_EXPORT_ERROR | このタイプのイベントは、SIEM システムとの接続エラーが原因で SIEM システムへのイベントのエクスポートが失敗した場合に発生します。 | 180 日間 |
| **機能が制限されています** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | この種別のイベントは、Kaspersky Security Center Linux の動作モードが変更されて基本機能のみが使用可能になり、脆弱性とパッチの管理機能およびモバイルデバイス管理機能が使用できない時に記録されます。<br>イベントが発生する理由と対応は次の通りです：<br>• ライセンスの有効期限が終了している：Kaspersky Security Center Linux の全機能を使用できるモードで必要なライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。<br>• ライセンスの上限で指定された台数を超過して管理サーバーでデバイスを管理している：管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動します（移動先の管理サーバーのライセンスの上限内で）。 | 180 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **カスペルスキー製品モジュールのアップデートが取り消されました** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | この種別のイベントは、カスペルスキーのテクニカルスペシャリストにより、より新しいバージョンの製品にアップデートする必要があるなどの理由でシームレスアップデートの利用が拒否された場合（アップデートのステータスとして「*取り消し*」が表示）に記録されます。このイベントは、Kaspersky Security Center Linux のアップデートパッチを対象としており、管理対象のカスペルスキー製品モジュールとの関連はありません。イベントでは、シームレスアップデートがインストールされなかった理由に関する情報が提供されます。 | 180 日間 |
| **ウイルスアウトブレイク** | • 26（ファイル脅威対策の場合）<br>• 27（メール脅威対策の場合）<br>• 28（ファイアウォールの場合） | GNRL_EV_VIRUS_OUTBREAK | この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。<br>このイベントには、次の方法で対応できます：<br>• 対象となるしきい値を管理サーバーのプロパティで編集します。<br>• このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。 | |

## 管理サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **指定フォルダーにアップデートをコピーできませんでした** | 4123 | KLSRV_UPD_REPL_FAIL | この種別のイベントは、ソフトウェアアップデートが指定したフォルダーでなく共有フォルダーにコピーされた場合に記録されます。<br>このイベントには、次の方法で対応できます：<br>• 指定したフォルダーへのアクセスに使用されたユーザーアカウントに、書き込み権限があるかどうかを確認します。<br>• フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。<br>• インターネット接続がイベント発生の原因の可能性もあるので、これをチェックします。定義データベースとソフトウェアモジュールのアップデート手順に従って操作します。 | 180 日間 |
| **クラウドセグメントのポーリングに失敗しました** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | この種別のイベントは、管理サーバーがクラウド環境でネットワークセグメントのポーリングに失敗した時に発生します。イベントの説明に記載されている詳細情報を読み、適宜対応します。 | 保管されません |
| **インストール数の上限を超えたライセンス認証済みアプリケーショングループがあります** | 4126 | KLSRV_INVLICPROD_EXCEDED | この種別のイベントは、管理サーバーによって 1 時間ごとに生成されます。この種別のイベントは、Kaspersky Security Center Liux でサードパーティ製品を管理していて、サードパーティ製品のライセンスで設定された上限を超えると記録されます。<br>このイベントには、次の方法で対応できます：<br>• 管理対象デバイスのリストを確認します。該当するサードパーティ製品が使用されていないデバイスからサードパーティ製品を削除します。<br>• 製品を使用できるデバイス数の上限が増えるように、サードパーティ製品のライセンスを追加します。<br>ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすサードパーティ製品が含まれます。 | 180 日間 |
| **ディスクに空き容量がありません** | 4107 | KLSRV_DISK_FULL | この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスクの空き容量が不足すると発生します。<br>デバイスのディスク領域を解放します。 | 180 日間 |
| **管理サーバーデータベースに空き容量がありません** | 4110 | KLSRV_DATABASE_FULL | この種別のイベントは、管理サーバーのデータベースに空き容量がないと記録されます。<br>管理サーバーのデータベースが容量の上限に達してデータベースへの情報の記録ができなくなると、管理サーバーが正常に機能しなくなります。<br>このイベントが発生する主な原因は使用中の DBMS の種別に応じて 2 つあり、それぞれ適切な対応方法が異なります：<br>• 管理サーバーデータベースに保存されるイベントの数を制限してください。<br>• 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security ポリシーの設定を変更することで対応できます。<br>DBMS の選定に関する情報を確認します。 | 180 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **実行時エラー** | 4125 | KLSRV_RUNTIME_ERROR | この種別のイベントは、不明な問題が生じた時に記録されます。<br>ほとんどの場合、問題は DBMS の問題、ネットワークの問題、またはソフトウェアやハードウェアの問題から発生しています。<br>エラー情報の詳細は、イベントの説明で参照できます。 | 180 日間 |
| **共有フォルダーが使用できません** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | この種別のイベントは、管理サーバーの共有フォルダーが利用できない場合に記録されます。<br>このイベントには、次の方法で対応できます：<br>• （共有フォルダーのある）管理サーバーが起動されていて利用可能な状態であることを確認します。<br>• フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。<br>• ネットワーク接続の問題がないか確認します。 | 180 日間 |
| **管理サーバーデータベースが使用できません** | 4109 | KLSRV_DATABASE_UNAVAILABLE | この種別のイベントは、管理サーバーのデータベースが利用できなくなっている場合に記録されます。<br>このイベントには、次の方法で対応できます：<br>• DBMS がインストールされているリモートサーバーが使用できる状態になっているかを確認します。<br>• DBMS ログを確認し、管理サーバーデータベースを使用できなくなっている理由を特定します。 | 180 日間 |

## 管理サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **頻出イベントが検出されました** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | このタイプのイベントは、管理サーバーが管理対象デバイスで頻出イベントを検知した時に発生します。詳細については、次のセクションを参照してください：「頻出イベントのブロック」。 | 90 日間 |
| **ライセンス数の上限を超えました** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | 1 日に 1 回、Kaspersky Security Center Linux はライセンス管理の上限の超過が発生していないかどうかを確認します。<br>この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品でライセンスの上限の超過が発生していることを管理サーバーが検知し、なおかつ単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 100% から 110% の範囲内の場合に記録されます。<br>このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。<br>このイベントには、次の方法で対応できます：<br>• 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。<br>• 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。<br>Kaspersky Security Center Linux では、ライセンス管理の上限を超過した時にイベントを生成するルールを指定できます。 | 90 日間 |
| **デバイスがネットワーク上で長期間アクティブになっていません** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | この種別のイベントは、管理対象デバイスが一定時間休止状態である場合に発生します。<br>このイベントが最も高頻度で発生するのは、管理対象デバイスが廃止された場合です。<br>このイベントには、次の方法で対応できます：<br>• 管理対象デバイスのリストからデバイスを手動で削除します。<br>Kaspersky Security Center Web コンソールを使用して［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定します。<br>• Kaspersky Security Center Web コンソールを使用して、デバイスがグループから自動的に削除されるまでの期間を指定します。 | 90 日間 |
| **デバイスの名前が競合しています** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | この種別のイベントは、管理サーバーが 2 つ以上の管理対象デバイスを単一のデバイスと判断した場合に発生します。<br>このイベントが最も高頻度で発生するのは、クローンされたハードディスクが管理対象デバイスでのソフトウェアの導入に使用され、ネットワークエージェントを参照デバイスの専用ディスククローンモードに切り替えなかった場合です。<br>この問題を回避するには、このデバイスのハードディスクを複製する前に、参照デバイスでネットワークエージェントをディスククローンモードに切り替えます。 | 90 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **デバイスのステータスが「警告」です** | 4114 | KLSRV_HOST_STATUS_WARNING | この種別のイベントは、管理対象デバイスに「警告」ステータスが割り当てられると記録されます。デバイスのステータスが「警告」に切り替わる条件を設定できます。 | 90 日間 |
| **インストール数が上限に近づいているライセンス認証済みアプリケーショングループがあります** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | このタイプのイベントは、ライセンス認証済みアプリケーショングループに含まれるサードパーティアプリケーションのライセンスの1つが期限切れになる時に発生します。その結果、いずれかのグループのインストール制限が削減されます。<br>このイベントには、次の方法で対応できます：<br>• 一部の管理対象デバイスでサードパーティ製品を使用していない場合は、これらのデバイスからアプリケーションを削除します。<br>• サードパーティ製品のインストール数が近い将来に許可される最大数を超えることが予想される場合は、事前にサードパーティのライセンスを取得する対象デバイスの数を増やすことを検討してください。<br>ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。 | 90 日間 |
| **証明書が要求されました** | 4133 | KLSRV_CERTIFICATE_REQUESTED | この種別のイベントは、モバイルデバイス管理用の証明書を自動的に再発行できない場合に発生します。<br>考えられるイベントの原因と適切な対応について以下に示します。<br>• ［**可能であれば証明書を自動で再発行**］がオフにされている証明書に対して自動再発行が開始された。これは、証明書の作成中に発生したエラーが原因であると考えられます。証明書の手動再発行が必要になる場合があります。<br>• 公開鍵インフラストラクチャと統合している場合、PKI との統合および証明書の発行に使用されるアカウントの SAM-Account-Name 属性の欠落が原因であると考えられます。アカウントのプロパティを確認します。 | 90 日間 |
| **証明書が削除されました** | 4134 | KLSRV_CERTIFICATE_REMOVED | この種別のイベントは、管理者がモバイルデバイス管理用の任意の種別の証明書（一般、メール、VPN）を削除した場合に発生します。<br>証明書を削除すると、この証明書を介して接続されたモバイルデバイスは、管理サーバーへの接続に失敗します。<br>このイベントは、モバイルデバイスの管理に関連した誤動作を調査する際に有用な場合があります。 | 90 日間 |
| **証明書の有効期間がまもなく終了します** | 6128 | KLSRV_EV_SRV_CERT_EXPIRES_SOON | このタイプのイベントは、モバイルデバイスと UEFI デバイスの管理用の管理サーバー証明書の有効期間が切れた時に発生します。<br>期限切れの証明書をアップデートする必要があります。 | 90 日間 |
| **APNs 証明書の有効期間が終了しています** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | この種別のイベントは、APNs証明書の有効期限が切れた場合に発生します。<br>手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。 | 保管されません |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **APNs 証明書の有効期間がまもなく終了します** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | この種別のイベントは、APNs 証明書の有効期限が切れるまでの残日数が 14日未満の場合に発生します。<br>APNs 証明書の有効期限が切れた場合は、手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。<br>有効期限に達する前に APNs 証明書の更新スケジュールを設定することを推奨します。 | 保管されません |
| **モバイルデバイスに FCM メッセージを送信できませんでした** | 4138 | KLSRV_GCM_DEVICE_ERROR | この種別のイベントは、Android オペレーティングシステムを搭載した管理対象のモバイルデバイスに接続するために Google Firebase Cloud Messaging（FCM）を使用するようにモバイルデバイス管理が設定されており、FCM サーバーが管理サーバーから受信したリクエストの一部を処理できない場合に発生します。これは、一部の管理対象モバイルデバイスがプッシュ通知を受信しないことを意味します。<br>イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Google Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。 | 90 日間 |
| **FCM メッセージを FCM サーバーに送信している時に HTTP エラーが発生しました** | 4139 | KLSRV_GCM_HTTP_ERROR | この種別のイベントは、モバイルデバイス管理が Android オペレーティングシステムを搭載した管理対象モバイルデバイスに接続するために Google Firebase Cloud Messaging （FCM）を使用するように設定されており、FCM サーバーが 200（OK）以外の HTTP コードで管理サーバーのリクエストに応答する場合に発生します。<br>考えられるイベントの原因と適切な対応について以下に示します。<br>• FCM サーバー側の問題。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Google Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。<br>• プロキシサーバー側の問題（プロキシサーバーを使用している場合）。イベントの詳細で HTTP コードを読み取り、適宜対応します。 | 90 日間 |
| **FCM メッセージを FCM サーバーに送信できませんでした** | 4140 | KLSRV_GCM_GENERAL_ERROR | この種別のイベントは、Google Firebase Cloud Messaging HTTP プロトコルを使用する際の管理サーバー側での予期しないエラーが原因で発生します。<br>イベントの説明に記載されている詳細情報を読み、適宜対応します。<br>ご自分で問題の解決方法を見つけられない場合は、カスペルスキーのテクニカルサポートへのお問い合わせを推奨します。 | 90 日間 |
| **ハードディスクの空き容量が残りわずかです** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスク容量が不足した場合に発生します。<br>デバイスのディスク領域を解放します。 | 90 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **管理サーバーデータベースに空き容量がありません** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | この種別のイベントは、管理サーバーのデータベースの空き容量が非常に少なくなっている場合に記録されます。状況を修正しないと、すぐに管理サーバーデータベースの容量が上限に達し、管理サーバーが正常に動作しなくなります。<br>使用されている DBMS の種別に応じた、このイベントが発生する原因と適切な対応方法を次に示します。<br>• 管理サーバーのデータベースに保存されるイベントの数を制限しないでください<br>• 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください<br>DBMS の選定に関する情報を確認します。 | 90 日間 |
| **セカンダリ管理サーバーとの接続が中断されました** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | この種別のイベントは、セカンダリ管理サーバーへの接続が中断された場合に発生します。<br>セカンダリ管理サーバーがインストールされているデバイスのオペレーティングシステムログを読み、適宜対応します。 | 90 日間 |
| **プライマリ管理サーバーとの接続が中断されました** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | この種別のイベントは、プライマリ管理サーバーへの接続が中断された場合に発生します。<br>プライマリ管理サーバーがインストールされているデバイスのオペレーティングシステムログを読み、適宜対応します。 | 90 日間 |
| **カスペルスキー製品モジュールの新しいアップデートが登録されました** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | この種別のイベントは、インストールの承認が必要な管理対象デバイスにインストールされているカスペルスキーソフトウェアの新しいアップデートを管理サーバーが登録する場合に発生します。<br>Kaspersky Security Center Web コンソールを使用して、アップデートを承認または拒否します。 | 90 日間 |
| **データベースのイベントの上限数を超えました。イベントの削除が開始されました** | 4145 | KLSRV_EVP_DB_TRUNCATING | この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントの削除が開始された時に記録されます。<br>このイベントには、次の方法で対応できます：<br>• 管理サーバーデータベースに保管されるイベント数の上限を変更してください<br>• 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください | 保管されません |
| **データベースのイベントの上限数を超えました。このイベントは削除されました** | 4146 | KLSRV_EVP_DB_TRUNCATED | この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントが削除された時に記録されます。<br>このイベントには、次の方法で対応できます：<br>• 管理サーバーデータベースに保管できるイベント数の上限を変更してください<br>• 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください | 保管されません |
| **デバイスにファイルをダウンロードできません** | 4165 | KLSRV_FILE_DOWNLOAD_FAILED | このイベントは次の場合に発生します：<br>• セッション中にファイルをデバイスにダウンロードできなかった場合。<br>• 管理サーバーからファイルをダウンロードできなかった場合。 | 90 日間 |
| **監査：SIEM サーバーへの接続テストが失敗しました** | 5120 | KLAUD_EV_SIEM_TEST_FAILED | このタイプのイベントは、SIEM サーバーへの自動接続テストが失敗した時に発生します。 | 90 日間 |

# 管理サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの情報イベント

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **モバイルデバイス用の予備の管理サーバーの証明書が更新されています** | 6127 | KLSRV_EV_SRV_CERT_RENEWED | このイベントは、管理サーバー証明書が更新された場合に発生します。 | 30 日間 |
| **監査：管理サーバーへの接続が切断されました** | 4151 | KLAUD_EV_SERVERDISCONNECT | | 30 日間 |
| **監査：管理サーバーとの接続が確立されました** | 4147 | KLAUD_EV_SERVERCONNECT | このタイプのイベントは、ユーザーが Kaspersky Security Center Web コンソールを使用して管理サーバーに接続した時に発生します。これらのイベントには、Kaspersky Security Center Web コンソールサーバーがインストールされているデバイスの IP アドレスが含まれます。 | 30 日間 |
| **監査：暗号化の鍵がインポートまたはエクスポートされました** | 5100 | KLAUD_EV_DPEKEYSEXPORT | たとえば、このイベントは移行中に発生します。 | 30 日間 |
| **監査：グループ設定が変更されました** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | このタイプのイベントは、セキュリティグループが編集された時に発生します。 | 30 日間 |
| **監査：オブジェクトが変更されました** | 4148 | KLAUD_EV_OBJECTMODIFY | このイベントは次のオブジェクトの変更を追跡します：<br>• 管理グループ<br>• セキュリティグループ<br>• ユーザー<br>• パッケージ<br>• タスク<br>• ポリシー<br>• サーバー<br>• 仮想サーバー | 30 日間 |
| **監査：オブジェクトのプロパティが変更されました** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | このイベントは、次のプロパティの変更を追跡します：<br>• ユーザー<br>• ライセンス<br>• サーバー<br>• 仮想サーバー | 30 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **監査：オブジェクトのステータスが変更されました** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | たとえば、このイベントはタスクがエラーで失敗した時に発生します。 | 30 日間 |
| **監査：SIEM サーバーへの接続テストが成功しました** | 5110 | KLAUD_EV_SIEM_TEST_SUCCESS | このイベントは、SIEM サーバーへのテスト接続が成功した時に発生します。 | 30 日間 |
| **監査：ユーザーの権限が変更されました** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | このイベントは、ユーザー権限が変更された時に発生します | 30 日間 |
| **プライマリ管理サーバーとの接続が確立されました** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | | 30 日間 |
| **セカンダリ管理サーバーとの接続が確立されました** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 詳細については、次のトピックを参照してください管理サーバーの階層の作成：セカンダリ管理サーバーの追加。 | 30 日間 |
| **定義データベースがアップデートされました** | 4144 | KLSRV_UPD_BASES_UPDATED | このタイプのイベントは、**「管理サーバーのリポジトリへのアップデートのダウンロード」**タスクが定義データベースのアップデートを完了した時に発生します。 | 30 日間 |
| **デバイスが自動的にグループに追加されました** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | この種別のイベントは、デバイス移動ルールに従ってデバイスがグループに割り当てられた場合に発生します。 | 30 日間 |
| **デバイスがルールに従って自動的に移動されました** | 1074 | KLSRV_HOST_MOVED_WITH_RULE_EX | この種別のイベントは、デバイス移動ルールに従ってデバイスが管理グループに移動された場合に発生します。 | 30 日間 |
| **デバイスがグループから削除されました：ネットワーク上で長期間アクティブになっていません** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | このタイプのイベントは、デバイスが非アクティブのためにグループから自動的に削除された時に発生します。 | 30 日間 |
| **このモバイルデバイス上で FCM 送信者 ID が変更されました** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | このタイプのイベントは、デバイス上で Firebase Cloud Messaging トークンが変更された時に発生します。<br>FCM トークンのローテーションの詳細については、「Firebase サービスのドキュメント」を参照してください。 | 30 日間 |
| **管理サーバーからファイルが削除されました** | 4163 | KLSRV_FILE_REMOVED | このイベントは、管理サーバーからファイルが削除された場合に発生します。 | 30 日間 |
| **ファイルがデバイスにダウンロードされました** | 4164 | KLSRV_FILE_DOWNLOADED | このイベントは次の場合に発生します：<br>• セッション中にファイルがデバイスにダウンロードされた場合。<br>• 管理サーバーからファイルがダウンロードされた場合。 | 30 日間 |
| **カスペルスキーへ分析のために送付するファイルが見つかりました** | 4131 | KLSRV_APS_FILE_APPEARED | | 30 日間 |
| **管理サーバーにファイルがアップロードされました** | 4162 | KLSRV_FILE_UPLOADED | このイベントは、ファイルが管理サーバーにアップロードされた場合に発生します。 | 30 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループがあります** | 4127 | KLSRV_INVLICPROD_FILLED | この種別のイベントは、ライセンス認証済みアプリケーショングループに含まれるサードパーティ製品のインストール数が、ライセンスのプロパティで指定された最大許容値の 90% に達すると発生します。<br>このイベントには、次の方法で対応できます：<br>• 一部の管理対象デバイスでサードパーティ製品を使用していない場合は、これらのデバイスからアプリケーションを削除します。<br>• サードパーティ製品のインストール数が近い将来に許可される最大数を超えることが予想される場合は、事前にサードパーティのライセンスを取得する対象デバイスの数を増やすことを検討してください。<br>ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。 | 30 日間 |
| **新しいデバイスが検出されました** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | この種別のイベントは、新しいネットワークデバイスが検出された場合に発生します。 | 30 日間 |
| **ライセンス使用率が 90% を超えています** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンス管理の上限の超過を管理サーバーが検知しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 90% を超えている場合に記録されます。<br>ライセンス管理の上限を超えた場合でも、クライアントデバイスは保護されます。<br>このイベントには、次の方法で対応できます：<br>• 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。<br>• 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。<br>Kaspersky Security Center Linux では、ライセンス管理の上限を超過した時にイベントを生成するルールを指定できます。 | 30 日間 |
| **モバイルデバイス用の予備の管理サーバーの証明書が作成されました** | 6126 | KLSRV_EV_SRV_CERT_RESERVE_CREATED | このイベントは、管理サーバー証明書が作成された場合に発生します。 | 30 日間 |
| **指定のフォルダーにアップデートがコピーされました** | 4122 | KLSRV_UPD_REPL_OK | このタイプのイベントは、**「管理サーバーのリポジトリへのアップデートのダウンロード」タスク**が指定されたフォルダーへのファイルのコピーを完了した時に発生します。 | 30 日間 |

［**予備の証明書が作成されました**］および［**証明書を更新中です**］というイベントは、モバイルデバイス用および UEFI デバイス用の管理サーバー証明書に対してこれらのイベントに対応する操作が行われた場合にのみ、管理サーバーから自動的に公開され、管理コンソールに表示されます。

## ネットワークエージェントのイベント

このセクションには、ネットワークエージェントに関するイベントの情報が記載されています。

## ネットワークエージェントの機能エラーイベント

次の表は、深刻度が［**機能エラー**］に分類される Kaspersky Security Center Linux ネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの機能エラーイベント

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **ルート証明書をインストールできませんでした** | 7728 | KLNAG_EV_ROOT_CERT_INSTALL_ERR | イベントには、証明書のインストールエラーの説明が含まれます。 | 30 日間 |
| **サードパーティ製品のアップデートをインストールできませんでした** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | この種別のイベントは、脆弱性とパッチ管理機能とモバイルデバイス管理を使用していて、サードパーティ製品のアップデートに失敗した時に記録されます。<br>サードパーティ製品へのリンクが有効かどうかを確認します。イベントの説明を確認します。 | 30 日間 |
| **Windows Update 更新プログラムをインストールできませんでした** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | この種別のイベントは、Windows の更新プログラムの適用に失敗した時に記録されます。<br>イベントの説明を確認します。該当するエラーに関する説明がマイクロソフト サポート技術情報で提供されていないかを検索してください。問題の解決が困難な場合は、マイクロソフトのテクニカルサポートにお問い合わせください。 | 30 日間 |
| **ルート証明書を削除できません** | 7730 | KLNAG_EV_ROOT_CERT_REMOVE_ERR | イベントには、証明書削除エラーの説明が含まれます。 | 30 日間 |
| **sudoers ファイルを参照値に復元できませんでした** | 7726 | KLNAG_EV_SUDOER_RESTORED_ERR | イベントには、ファイル sudoers の置換エラーの説明が含まれています。 | 30 日間 |
| **アップデートのインストールエラー** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | この種別のイベントは、Kaspersky Security Center Linux コンポーネントの自動アップデートおよびパッチ適用に失敗した時に記録されます。このイベントは、管理対象のカスペルスキー製品のアップデートとの関連はありません。<br>イベントの説明を確認します。管理サーバーで Windows 関連の問題がこのイベントの原因となっている可能性があります。イベントの説明で Windows の設定に関する問題が言及されている場合、その問題を解決してください。 | 30 日間 |
| **ユーザー管理：エラー** | 7723 | KLNAG_EV_USR_MNG_ERR | 一般警告イベント。 | 30 日間 |

## ネットワークエージェントの警告イベント

次の表は、重要度が［**警告**］深刻度に分類されるネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの警告イベント

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 説明 | 既定の保管期間 |
|---|---|---|---|---|
| **KSN プロキシサーバーが起動しました。KSN 可用性をチェックできませんでした** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | このタイプのイベントは、構成された KSN プロキシ接続のテスト接続が失敗した時に発生します。 | 30 日間 |
| **セキュリティ問題が発生しました** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | このタイプのイベントは、デバイス上でインシデントが見つかった場合に発生します。たとえば、このイベントはデバイスのディスク容量が少ない場合に発生します。 | 30 日間 |
| **検出された sudoers ファイルは参照値と一致しません** | 7724 | KLNAG_EV_SUDOER_DIFFERENT | このタイプのイベントは、sudoers ファイルと参照ファイルの間に不一致がある場合に発生します。 | 30 日間 |
| **サードパーティ製品のアップデートのインストールが延期されました** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | たとえば、このタイプのイベントは、サードパーティのアップデートプログラムのインストールに関する EULA が拒否された場合に発生します。 | 30 日間 |
| **サードパーティ製品のアップデートのインストールが警告を出力して完了しました** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 詳細については、トレースファイルをダウンロードし、［KLRI_PATCH_RES_DESC］フィールドの値を確認してください。 | 30 日間 |
| **ユーザー管理：警告** | 7722 | KLNAG_EV_USR_MNG_WRN | 一般警告イベント。 | 30 日間 |
| **ソフトウェアモジュールのアップデートのインストール中に警告が発生しました** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 詳細については、トレースファイルをダウンロードし、［KLRI_PATCH_RES_DESC］フィールドの値を確認してください。 | 30 日間 |

## ネットワークエージェントの情報イベント

次の表は、重要度が［**情報**］深刻度に分類されるネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの情報イベント

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 既定の保管期間 |
|---|---|---|---|
| **アプリケーションがインストールされました** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 日間 |
| **アプリケーションがアンインストールされました** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 日間 |
| **Web サーバーの HTTPS ポート用の証明書を受け取りました** | — | WEB_SERVER_CERTIFICATE_RENEWED | 30 日間 |
| **デバイスが認証されました** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 日間 |
| **新しいデバイスが検出されました** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 日間 |
| **デバイスが削除されました** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 日間 |
| **ソフトウェアモジュールのアップデートのインストールを開始しました** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 日間 |
| **KSN プロキシサーバーが起動しました。KSN 可用性チェックが完了しました** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 日間 |
| **KSN プロキシが停止しました** | 7720 | KSNPROXY_STOPPED | 30 日間 |

| イベント種別の表示名 | イベント種別の ID | イベント種別 | 既定の保管期間 |
|---|---|---|---|
| **監視対象アプリケーションがインストールされました** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 日間 |
| **監視対象アプリケーションがアンインストールされました** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 日間 |
| **新しいデバイスが追加されました** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 日間 |
| **ルート証明書がインストールされました** | 7727 | KLNAG_EV_ROOT_CERT_INSTALLED | 30 日間 |
| **ルート証明書が削除されました** | 7729 | KLNAG_EV_ROOT_CERT_REMOVED | 30 日間 |
| **sudoers ファイルが正常に参照値に復元されました** | 7725 | KLNAG_EV_SUDOER_RESTORED | 30 日間 |
| **サードパーティ製品がインストールされました** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 日間 |
| **サードパーティ製品のアップデートがインストールされました** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 日間 |
| **サードパーティ製品のアップデートのインストールを開始しました** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 日間 |
| **ソフトウェアモジュールのアップデートがインストールされました** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 日間 |
| **ユーザー管理：情報** | 7721 | KLNAG_EV_USR_MNG_INF | 30 日間 |
| **ホストで Web サーバーが開始されました** | — | WEB_SERVER_STARTED | 30 日間 |
| **ホストで Web サーバーが停止されました** | — | WEB_SERVER_STOPPED | 30 日間 |
| **Windows デスクトップ共有：アプリケーションが起動しました** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 日間 |
| **Windows デスクトップ共有：ファイルが変更されました** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 日間 |
| **Windows デスクトップ共有：ファイルが読み取られました** | 7712 | KLUSRLOG_EV_FILE_READ | 30 日間 |
| **Windows デスクトップ共有：開始しました** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 日間 |
| **Windows デスクトップ共有：停止しました** | 7716 | KLUSRLOG_EV_WDS_END | 30 日間 |

# イベントの抽出の使用

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**イベントの抽出**］をクリックすると、イベントの抽出が表示されます。




イベントの抽出リスト

既定では、イベントの抽出には過去 7 日の情報が含まれます。

Kaspersky Security Center Linux には、事前定義された次の既定のイベントの抽出のセットが用意されています：

- 重要度別のイベント：
  - **緊急イベント**
  - **機能エラー**
  - **警告**
  - **情報イベント**
- **ユーザー要求**（管理対象製品のイベント）
- **最近のイベント**（過去 1 週間を対象）
- **監査イベント**

ユーザー定義の抽出を追加で作成し設定できます。ユーザー定義の抽出では、イベントが発生したデバイスの属性（デバイス名、IP アドレスの範囲、管理グループ）、イベントの種別と重要度、製品名とコンポーネント名、および対象期間によってイベントをフィルターできます。検索対象に、タスクの実行結果を含めることもできます。また、1 つ以上の単語を入力して検索する、シンプルな検索フィールドも使用できます。この場合、入力した単語のいずれかが、いずれかの属性（イベント名、説明、コンポーネント名など）に含まれるイベントがすべて一致対象として表示されます。

事前定義の抽出とユーザー定義の抽出の両方で、表示するイベント数と検索対象にするレコード数を制限できます。両方のオプションの値が、Kaspersky Security Center Linux でイベントの抽出が表示されるまでの所要時間に影響します。データベースのサイズが大きいほど、プロセスの所要時間が長くなります。

次のことができます：

- イベントの抽出のプロパティの編集
- イベントの抽出の生成
- イベントの抽出の詳細の表示
- イベントの抽出の削除
- 管理サーバーのデータベースからのイベントの削除

# イベントの抽出の作成

*イベントの抽出を作成するには：*

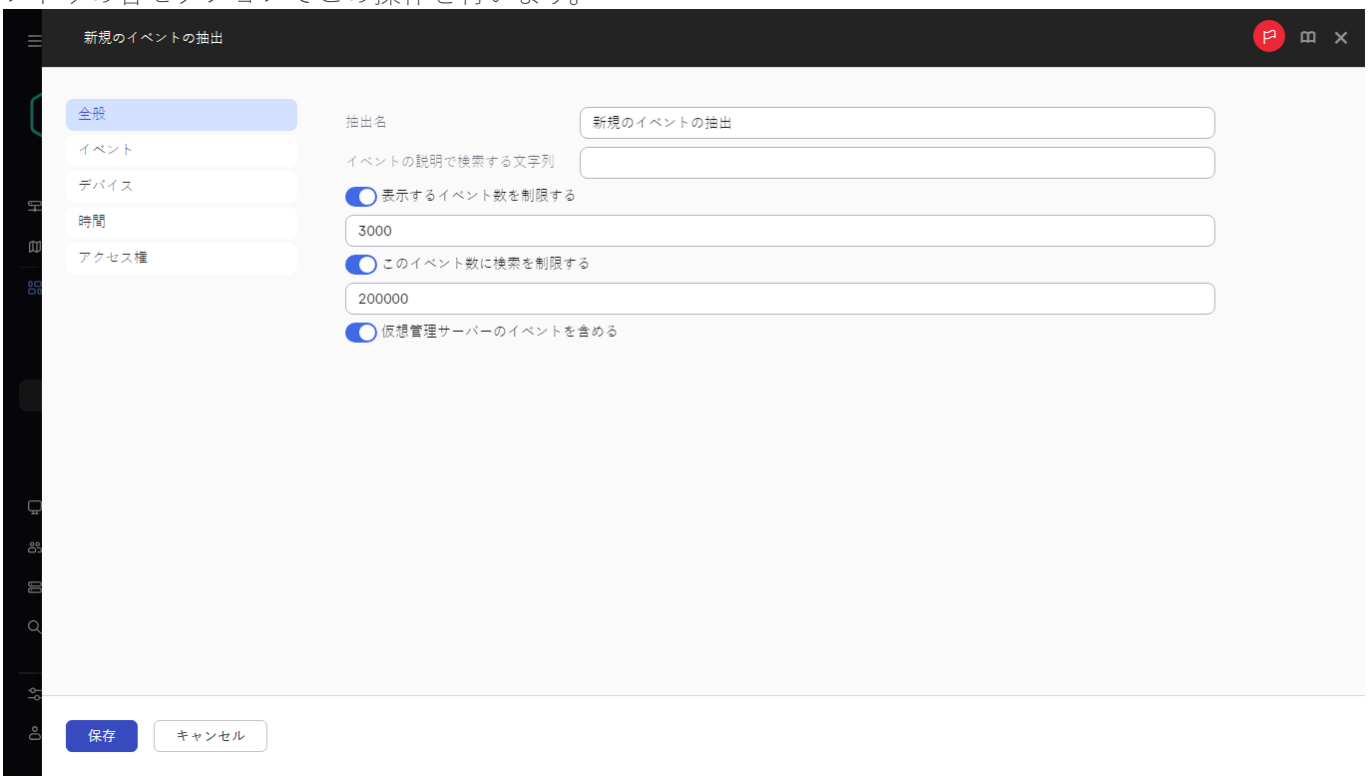
1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に移動します。




イベントの抽出リスト

2. ［**追加**］をクリックします。

3. ［**新規のイベントの抽出**］ウィンドウで、新しいイベントの抽出の設定を指定します。必要に応じて、ウィンドウの各セクションでこの操作を行います。




新しいイベントの抽出の作成

4. ［**保存**］をクリックして変更内容を保存します。

   確認ウィンドウが開きます。

5. イベントの抽出の結果を表示するには、［**抽出の結果に移動**］をオンにしたままにします。

6. ［**保存**］を選択して、イベントの抽出の作成を確定させます。

   ［**抽出の結果に移動**］をオンにしたままの場合、イベントの抽出結果が表示されます。オフにした場合、新しいイベントの抽出が追加されたイベントの抽出のリストが表示されます。

# イベントの抽出の編集

*イベントの抽出を編集するには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 編集するイベントの抽出に隣接するチェックボックスをオンにします。




イベントの抽出リスト

3. ［**プロパティ**］をクリックします。
   イベントの抽出の設定ウィンドウが表示されます。
4. イベントの抽出のプロパティを編集します。

   製品導入時から利用できる定義済みのイベントの抽出では、［**全般**］タブ（抽出の名前以外）、［**時間**］タブ、［**アクセス権**］タブのプロパティのみを編集できます。

   ユーザー定義の抽出では、すべてのプロパティを編集できます。
5. ［**保存**］をクリックして変更内容を保存します。

編集したイベントの抽出がリストに表示されます。

# イベントの抽出のリストの表示

*イベントの抽出を表示するには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 開始するイベントの抽出に隣接するチェックボックスをオンにします。



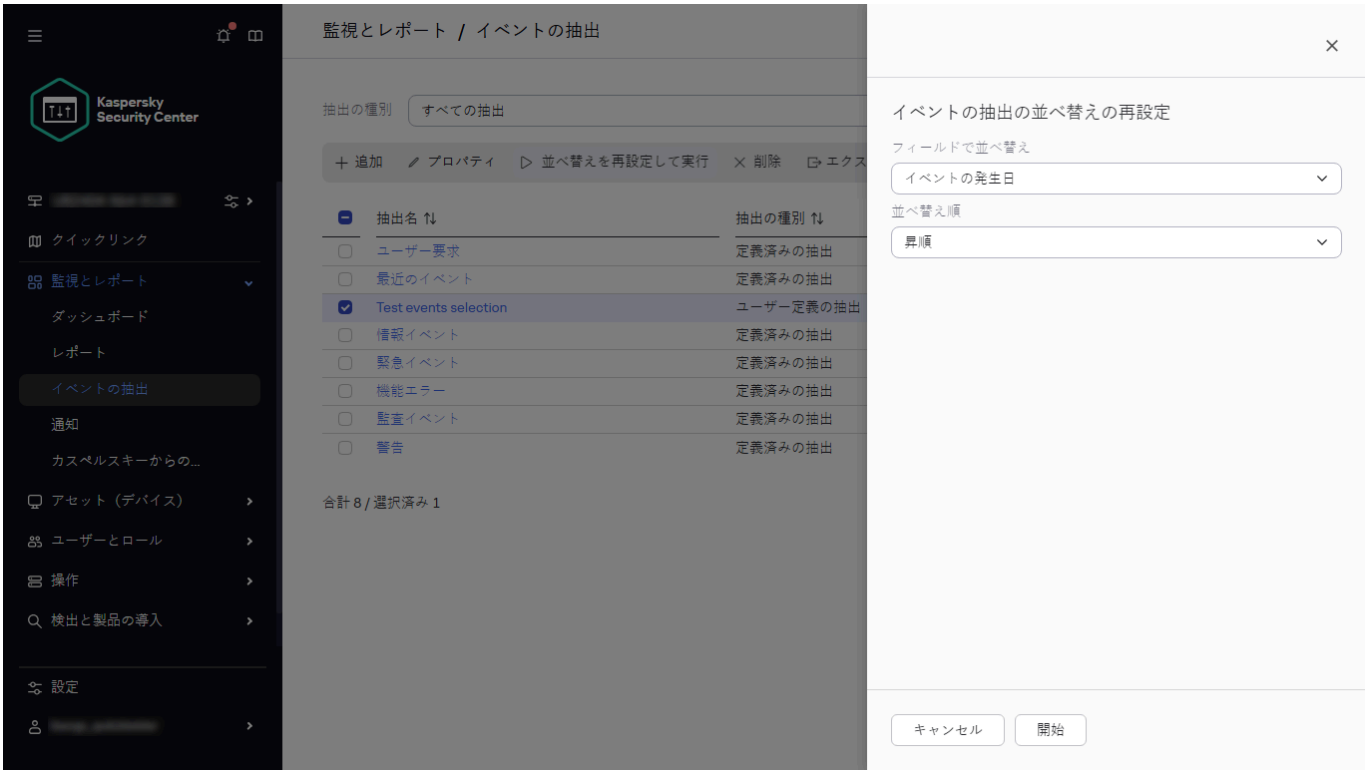

イベントの抽出リスト

3. 次のいずれかの手順を実行します：

- イベントの抽出結果の表示で並べ替えを設定したい場合は、次の操作を実行します：

  a. ［**並べ替えを再設定して実行**］をクリックします。

b. ［**イベントの抽出の並べ替えの再設定**］ウィンドウが表示されるので、並べ替えの設定を指定します。

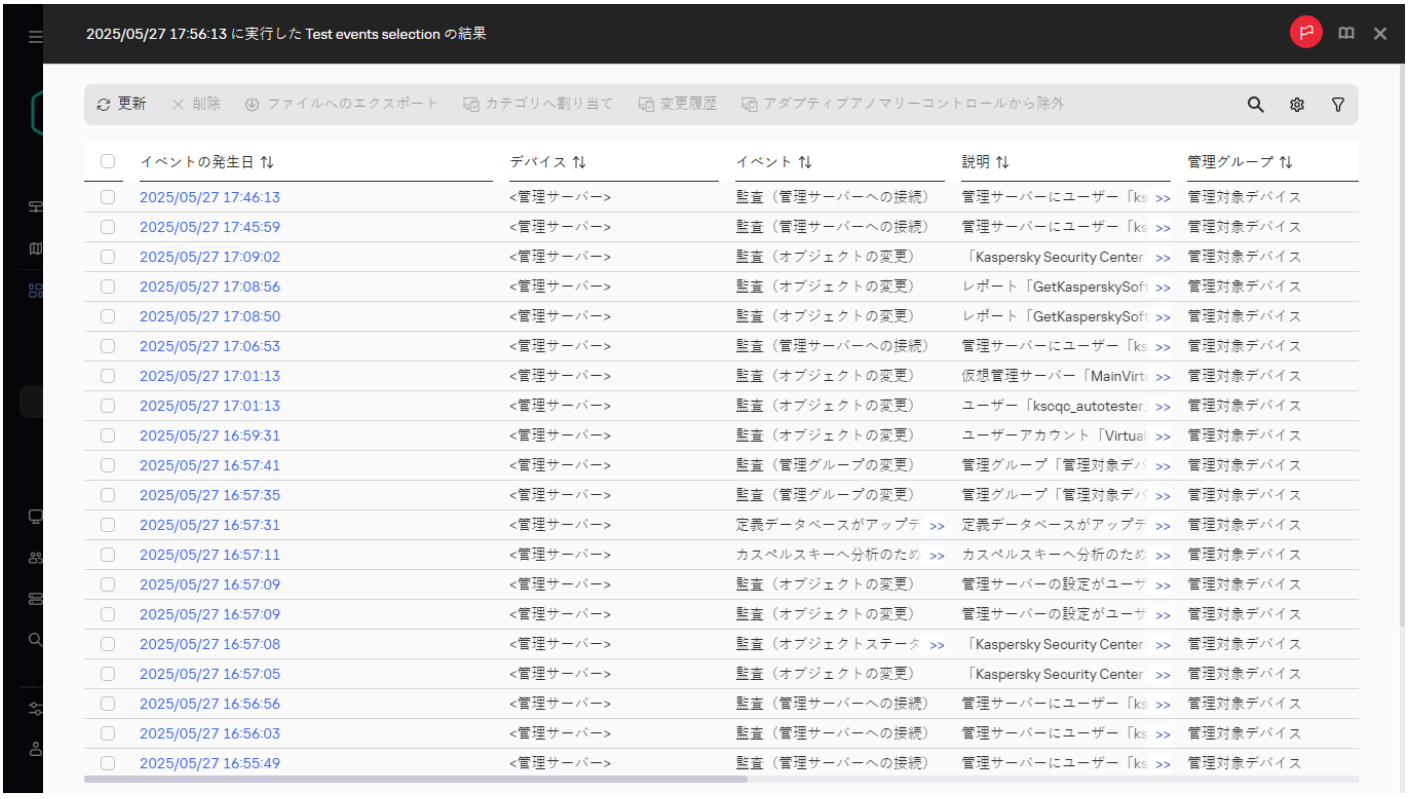



イベントの抽出の並べ替え設定の指定

a. 抽出名をクリックします。

- 管理サーバーでの並べ替え順序を変更せずにイベントのリストを表示する場合は、抽出名をクリックします。

イベントの抽出結果が表示されます。




イベントの抽出結果が表示されます。

# イベントの抽出のエクスポート

Kaspersky Security Center Linux では、イベントの抽出とその設定を KLO ファイルに保存できます。この KLO ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したイベントの抽出をインポートできます。

エクスポートできるのは、ユーザー定義のイベントの抽出のみであることに注意してください。既定の Kaspersky Security Center Cloud Linux コンソールセットからのイベントの抽出（事前定義された抽出）は、ファイルに保存できません。

*イベントの抽出をエクスポートするには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. エクスポートするイベントの抽出に隣接するチェックボックスをオンにします。

   複数のイベントの抽出を同時にエクスポートすることはできません。複数の抽出を選択すると、［**エクスポート**］が無効になります。
3. ［**エクスポート**］をクリックします。
4. 開いた［**名前を付けて保存**］ウィンドウで、イベントの抽出ファイル名とパスを指定し、［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、イベントの抽出ファイルは自動的に［**Downloads**］フォルダーに保存されます。

# イベントの抽出のインポート

Kaspersky Security Center Linux では、KLO ファイルからイベントの抽出をインポートできます。KLO ファイルには、エクスポートされたイベントの抽出とその設定が含まれています。

*イベントの抽出をインポートするには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. ［**インポート**］をクリックし、インポートするイベントの抽出ファイルを選択します。
3. 表示されたウィンドウで、KLO ファイルのパスを指定し、［**開く**］をクリックします。選択できるイベントの抽出イベントの抽出ファイルは 1 つだけです。

   イベントの抽出処理が開始されます。

インポート結果の通知が表示されます。イベントの抽出が正常にインポートされた場合は、［**インポートの詳細を表示**］をクリックしてイベントの抽出のプロパティを表示できます。

インポートが成功すると、イベントの抽出が抽出リストに表示されます。イベントの抽出の設定もインポートされます。

新しくインポートされたイベントの抽出と同じ名前のイベントの抽出が既に存在している場合、インポートされたイベントの抽出の名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

# イベントの詳細の表示

*イベントの詳細を表示するには：*

1. イベントの抽出を開始します。
2. 目的のイベントの時刻をクリックします。
   ［**イベントのプロパティ**］ウィンドウが開きます。




イベントのプロパティウィンドウ

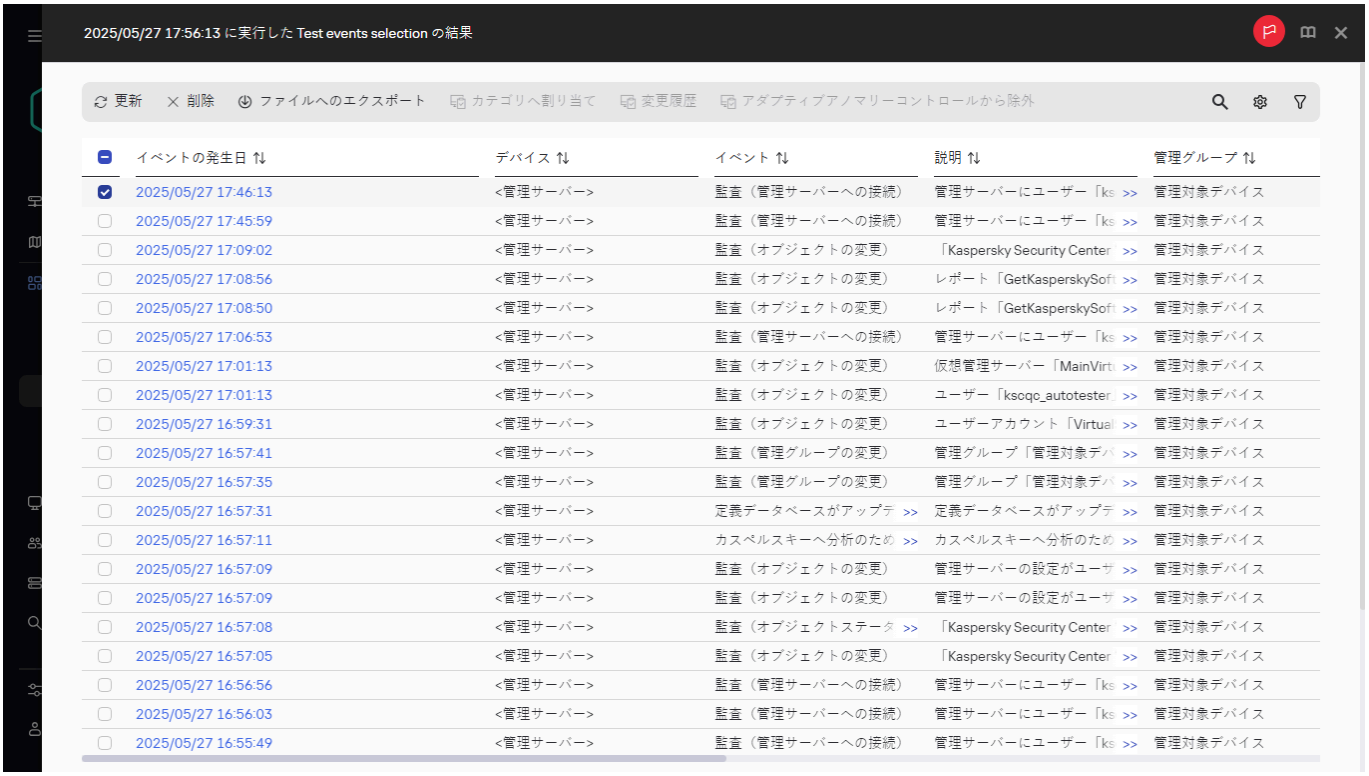
3. 表示されたウィンドウでは、次の操作を実行できます：
   - 選択したイベントの情報の表示
   - イベントが発生したデバイスの情報への移動
   - イベントが発生したデバイスが属する管理グループへの移動
   - （タスクに関係しているイベントの場合）該当タスクへの移動

# イベントのファイルへのエクスポート

Kaspersky Security Center Linux では、イベントの抽出からイベントを TXT ファイルに保存することができます。

*イベントをファイルにエクスポートするには：*

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
   複数のイベントまたはイベント全体を抽出することもできます。




イベントの抽出結果が表示されます。

3. ［**ファイルへのエクスポート**］をクリックします。

   抽出したイベントが TXT ファイルにエクスポートされます。

# イベントに含まれるオブジェクトの履歴の表示

リビジョン管理をサポートするオブジェクトの作成イベントまたは変更イベントからは、オブジェクトの履歴画面に移動することができます。

*イベントからオブジェクトの履歴を表示するには：*

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**変更履歴**］をクリックします。

   オブジェクトの変更履歴が表示されます。

# イベントの削除

*イベントを削除するには：*

1. イベントの抽出を開始します。
2. 目的のイベントの横にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。

   選択したイベントは削除され、このイベントは復元できません。

# イベントの抽出の削除

削除できるのはユーザー定義のイベントの抽出のみです。製品組み込みで定義済みのイベントの抽出は削除できません。

*イベントの抽出を削除するには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 削除するイベントの抽出に隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

   イベントの抽出が削除されます。

# イベントの保管期間の設定

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。一部のイベントを既定値の期間より長くまたは短く保管することが必要な場合があります。イベントの既定の保管期間を変更できます。

管理サーバーのデータベースに保存しなくてよいイベントがある場合は、管理サーバーポリシーとカスペルスキー製品ポリシー、または管理サーバーのプロパティ（管理サーバーのイベントのみ）で適切な設定を無効にできます。これにより、データベースに保存されるイベント種別の数を減らすことができます。

イベントの保管期間が長いほど、データベースが容量の上限に達するのが早くなります。一方で、イベントの保存期間を長くすることで、監視や レポートのタスクをより長い期間実行することができます。

*管理サーバーデータベースへのイベントの保管期間を指定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 必要なポリシー名をクリックします。

   管理対象のカスペルスキー製品、ネットワークエージェント、または管理サーバーのポリシーを選択できます。管理サーバーでは、必要な管理サーバーの名前の横にある設定アイコン（）をクリックして、イベントの保存期間を構成することもできます。
3. ［**イベントの設定**］タブを選択します。

   ［**緊急**］セクションのイベント種別のリストが表示されます。必要に応じて、［**機能エラー**］、［**警告**］、または［**情報**］セクションに移動できます。
4. 右側のペインのイベント種別のリストで、保存期間を変更するイベントのリンクをクリックします。

   表示されるウィンドウの［**イベント登録**］セクションで、［**管理サーバーのデータベースに保存（日）**］がオンになっています。
5. このスイッチの下に、イベントを保存する日数を入力します。
6. 管理サーバーのデータベースにイベントを保存しない場合は、［**管理サーバーのデータベースに保存（日）**］を無効にします。

   管理サーバーのプロパティウィンドウで管理サーバーのイベントを設定し、Kaspersky Security Center 管理サーバーのポリシーでイベントの設定がロックされている場合、この画面でイベントの保管期間を編集することはできません。
7. ［**OK**］をクリックし、右側のペインが閉じた後、［**保存**］をクリックします。

   ポリシーのプロパティウィンドウが閉じます。

以降、選択した種別のイベントを管理サーバーが受け取ったイベントの保存期間は、変更した期間保存されるようになります。管理サーバーが以前受け取ったイベントの保存期間は変更されません。

# 頻出イベントのブロック

このセクションでは、頻出イベントのブロックの管理および頻出イベントのブロックの解除について説明します。

# 頻出イベントのブロックについて

単一または複数の管理対象デバイスにインストールされた Kaspersky Endpoint Security for Linux などの管理対象アプリケーションは、管理サーバーに対して同様の種別のイベントを大量に送信することがあります。頻出イベントを受信すると、管理サーバーのデータベース高負荷がかかり、他のイベントが上書きされる場合があります。管理サーバーは、受信したイベントの総量がデータベースで指定した制限を超えた場合、頻出イベントをブロックします。

管理サーバーは頻出イベントの受信を自動的にブロックします。ユーザー自身による頻出イベントのブロックや、ブロックするイベントの選択はできません。

イベントがブロックされているかどうかを確認したい場合、通知リストを表示するか、そのイベントが管理サーバーのプロパティの［**頻出イベントのブロック**］セクションに存在するかどうかで確認できます。イベントがブロックされている場合、次を実行します：

- データベースの上書きを防止したい場合、このような種別のイベントの受信のブロックを継続できます。
- たとえば、管理サーバーに頻出イベントが送信される原因を見つける場合などには、頻出イベントのブロックを解除してこの種別のイベントの受信を継続できます。
- 頻出イベントの受信が再度ブロックされるまで受信を継続する場合は、頻出イベントのブロック対象から削除することができます。

# 頻出イベントのブロックの管理

管理サーバーは頻出イベントの自動受信をブロックしますが、ブロックを解除してイベントの受信を継続することができます。また、以前にブロック解除したイベントを再度ブロックすることもできます。

*頻出イベントのブロックを管理するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで次を実行します：
   - 頻出イベントの受信のブロックを解除する場合：
     a. ブロック解除する頻出イベントを選択し、［**除外**］をクリックします。
     b. ［**保存**］をクリックします。
   - 頻出イベントをブロックする場合は：
     a. ブロックする頻出イベントを選択し、［**ブロック**］をクリックします。
     b. ［**保存**］をクリックします。

管理サーバーはブロック解除された頻出イベントを受け取り、ブロック対象の頻出イベントは受け取りません。

## 頻出イベントのブロックの解除

頻出イベントのブロックを解除して、管理サーバーが再度ブロックするまでこれらの頻出イベントを受信できます。

*頻出イベントのブロックを解除するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで、ブロックを解除したいイベントの行をクリックします。
4. ［**ブロック解除**］をクリックします。

イベントは頻出イベントのリストから削除されます。管理サーバーはこの種別のイベントを受信します。

# 管理サーバーでのイベントの処理と保管

アプリケーションの動作および管理対象デバイスでのイベントに関する情報は、管理サーバー定義データベースに保存されます。イベントにはそれぞれ種別と重要度（*緊急イベント*、*機能エラー*、*警告*、*情報*）という属性があります。イベントが発生した条件に応じて、同じ種別のイベントに異なる重要度を割り当てることができます。

イベントに割り当てられた種別および重要度は、管理サーバーのプロパティウィンドウの［**イベントの設定**］セクションに表示されます。［**イベントの設定**］セクションでは、管理サーバーによる各イベントの処理を設定することもできます。

- 管理サーバーにおけるイベントの登録、およびデバイスと管理サーバーのオペレーティングシステムのイベントログにおけるイベントの登録
- 管理者へのイベントの通知方法（例：SMS、メール）

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

アプリケーションは 10 分ごとにデータベースをチェックします。イベント数が指定された最大値に 10,000 を加えた値に達すると、アプリケーションは最も古いイベントを削除し、指定された最大数のイベントのみが残ります。

管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報はオペレーティングシステムログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。既定では、イベントキューは 20,000 イベントに制限されます。KLEVP_MAX_POSTPONED_CNT フラグ値を編集することで、キュー制限をカスタマイズできます。

# 通知とデバイスのステータス

このセクションでは、通知の表示、通知の配信の設定、デバイスのステータスの使用、デバイスのステータス変更を有効にする方法について説明します。

## 通知機能の使用

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。




通知リスト

次の種別の通知を、通知方法の選択に応じて使用できます：

- 画面表示による通知
- SMS 通知
- メール通知
- 実行ファイルまたはスクリプトの実行で通知

### 画面表示による通知

画面表示による通知では、重要度別にアラート通知を確認できます（*緊急*、*警告*、*情報*）。

画面表示による通知には 2 種類のステータスがあります：

- *確認済み*：推奨される処理として記載されている処理を行ったか、通知に手動でこのステータスを割り当てた場合に、このステータスが付与されます。
- *未確認*：推奨される処理として記載されている処理を未実行か、通知に「確認済み」のステータスを手動で割り当てていない場合に、このステータスが付与されます。

既定では、通知リストには「*未確認*」ステータスの通知が表示されます。

画面表示される通知を確認し、リアルタイムでの対応を行うことで、組織ネットワークの監視業務を実行できます。

### メール、SMS、または実行ファイルやスクリプトの実行による通知

Kaspersky Security Center Linux では、必要に応じて、重要だと考えられる任意のイベントに対して通知の送信を設定し、組織ネットワークの監視に役立てることができます。任意のイベントで、メール、SMS、または実行ファイルやスクリプトの実行による通知を設定できます。

メールまたは SMS で通知を受け取った場合、イベント内容を確認して必要な対応を決定できます。この対応は組織のネットワークに対して最も適切なものである必要があります。実行ファイルまたはスクリプトの実行を設定する場合は、イベントに対する対応を事前に指定できます。また、実行ファイルまたはスクリプトの実行による対応を、イベントに対する初期対応として考えることもできます。この場合、実行ファイルの実行後に、イベントに対して必要な追加対応を担当者自身が実施できます。

## 画面表示による通知の確認

通知は次の 3 通りの方法で画面表示できます：

- ［**監視とレポート**］→［**通知**］セクション。ここで定義済みのカテゴリに関連する通知を確認できます。
- どのセクションからもメニュー上部のアイコンを使用して開くことができる別のウィンドウ。この方法を使用すると、通知を確認済みとしてマークできます。
- ［**監視とレポート**］→［**ダッシュボード**］セクションの［**選択した深刻度別の通知**］ウィジェット。ウィジェットで、重要度が*緊急*と*警告*のイベントの通知のみ確認できます。

イベントに応答するなど、処理を実行できます。

*定義済みのカテゴリから通知を確認するには：*

1. メインメニューで、［**監視とレポート**］→［**通知**］に移動します。

   ［**すべての通知**］カテゴリが左側のペインで選択されており、右側のペインですべての通知が表示されます。




通知リスト

2. 左側のペインで、次のカテゴリのいずれかを選択します：

   - **製品の導入**
   - **デバイス**
   - **プロテクション**
   - **アップデート**（ダウンロード可能なカスペルスキー製品に関する通知、ダウンロードされたウイルス対策定義データベースのアップデートに関する通知、およびネットワークエージェントのアップデート後に再起動が必要なデバイス（ある場合）に関する通知が含まれます）
   - **脆弱性攻撃ブロック**
   - **管理サーバー**（管理サーバーのみに関するイベントが含まれます）
   - **参考リンク**（カスペルスキーのリソース（たとえば、カスペルスキーのテクニカルサポート、カスペルスキーのコミュニティ、販売代理店リストのページ、ウイルス百科事典など）へのリンクが含まれます）
   - **カスペルスキーニュース**（カスペルスキー製品のリリースに関する情報が含まれます）

選択したカテゴリの通知のリストが表示されます。リストには次が含まれます：

- 情報の内容に関連するアイコン：導入 (  )、保護 (  )、アップデート(  )、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
- 通知の重要度：重要度が、**緊急の通知**（）、**警告の通知**（）、**情報の通知**の通知が表示されます。リスト内の通知は重要度に応じてグループ化されています。
- **通知**：通知の説明が含まれます。
- **処理**：コンソールで実行可能な、推奨される処理へのリンクが含まれます。それぞれのリンクをクリックすると、たとえば、リポジトリに移動してデバイスにセキュリティ製品をインストールしたり、デバイスまたはイベントのリストを確認できます。通知に推奨される処理を実行すると、この通知に*確認済み*のステータスが割り当てられます。
- **ステータス登録後の時間**：通知が管理サーバーに登録された時点から経過した日数または時間数が含まれます。

*別のウィンドウで、画面表示による通知を重要度別に確認するには：*

1. Kaspersky Security Center Web コンソールの右上端で、フラグアイコン（  ）をクリックします。

   フラグアイコンに赤い丸印が表示されている場合は、確認されていない通知があります。

   通知のリストを含むウィンドウが開きます。既定では、［**すべての通知**］タブが選択されており、*緊急*、*警告*、*情報*の重要度別に通知がグループ化されています。

2. ［**システム**］タブを選択します。

   重要度が*緊急*（  ）と*警告*（）の通知のリストが表示されます。通知のリストには以下が含まれます：

   - カラーマーカー：緊急の通知には赤色のマーカーが使用されます。警告の通知には黄色のマーカーが使用されます。
   - 情報の内容を示すアイコン：導入 (  )、保護 (  )、アップデート(  )、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
   - 通知の説明。
   - フラグアイコン：通知に*未確認*のステータスが割り当てられている場合、［フラグ］アイコンは灰色です。灰色の［フラグ］アイコンを選択して通知に*確認済み*のステータスを割り当てると、アイコンは白色に変更されます。
   - 推奨される処理へのリンク：リンクをクリックした後で推奨される処理を実行すると、通知は*確認済み*のステータスになります。
   - 通知が管理サーバーに登録された時点から経過した日数または時間数。

3. ［**詳細**］タブを選択します。

   重要度が*情報*の通知のリストが表示されます。

   リストの各項目の構成は、［**システム**］タブのリスト（前述の説明を参照）と同じです。カラーマーカーが使用されない点のみ異なります。

通知が管理サーバーに登録された期間で通知をフィルタリングできます。フィルターを管理するには、［**フィルターの表示**］をオンにします。

*ウィジェットで画面表示による通知を確認するには：*

1. ［**ダッシュボード**］セクションで、［**Web ウィジェットを追加または復元**］を選択します。
2. 表示されたウィンドウで、［**その他**］のカテゴリをクリックし、［**選択した深刻度別の通知**］ウィジェットを選択して、［追加］をクリックします。

   これによりウィジェットが［**ダッシュボード**］タブに表示されます。既定では、重要度が*緊急*の通知がウィジェットに表示されます。

   ウィジェットの［**設定**］をクリックしてウィジェットの設定を変更すると、重要度が*警告*の通知を表示できます。または、*警告*の重要度を指定して［**選択した深刻度別の通知**］ウィジェットを追加できます。

   通知リストのウィジェットには表示領域のサイズの制限があるため、表示される通知は 2 つまでです。これらの 2 つの通知は最新のイベントに関連します。

通知リストのウィジェットには以下が含まれます：

- 情報の内容に関連するアイコン：導入 ()、保護 ()、アップデート()、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
- 推奨される処理へのリンクを含む通知の説明：リンクをクリックした後で推奨される処理を実行すると、通知は「*確認済み*」のステータスになります。
- 通知が管理サーバーに登録された時点から経過した日数または時間数。
- その他の通知へのリンク：このリンクをクリックすると、［**監視とレポート**］セクションの［**通知**］セクションに表示される通知リストの画面に移動します。

# デバイスのステータスの概要

Kaspersky Security Center Linux は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center Linux はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center Linux が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK* または *OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

| 条件 | 条件の説明 | 設定可能な値 |
| --- | --- | --- |
| セキュリティ製品がインストールされていません | デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。 | • 切り替えスイッチをオン<br>• 切り替えスイッチをオフ |
| ウイルスが多数検知されました | マルウェアスキャンタスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。 | 0 より大きい値 |
| リアルタイム保護レベルが管理者の設定と異なります | デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。 | • 停止<br>• 一時停止<br>• 実行中 |
| マルウェアのスキャンが長期間実行されていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャンタスク*もローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。 | 1日より大きい値 |
| 定義データベースがアップデートされていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。 | 1日より大きい値 |
| 長期間接続されていません | デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。 | 1日より大きい値 |
| アクティブな脅威を検知しました | ［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。 | 0 項目より大きい値 |
| 再起動が必要です | デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。 | 0 分より大きい値 |
| 競合アプリケーションがインストールされています | デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| ソフトウェアの脆弱性が検知されました | デバイスはネットワーク上で可視でネットワークエージェントもインストールされていますが、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された重要度の脆弱性を検知しました。 | • 緊急<br>• 高<br>• 中<br>• 脆弱性を修正できない場合は無視する<br>• 修正プログラムがインストール用に割り当てられている場合は無視する |
| ライセンスの有効期間が終了しました | デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| ライセンスの有効期間がまもなく終了します | デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。 | 0 日より大きい値 |
| Windows Update 更新プログラムのチェックが長期間実行されていません | デバイスはネットワーク上で可視ですが、*Windows Update の同期の実行*タスクが実行されていない状態が指定期間を越えて続いています。 | 1日より大きい値 |

| 条件 | 条件の説明 | 設定可能な値 |
| --- | --- | --- |
| 暗号化ステータスが無効です | デバイスにネットワークエージェントはインストールされていますが、デバイスの暗号化結果が割り当て条件として指定されているものと合致しました。 | • ユーザーが拒否したため、ポリシーに準拠していない（外部デバイスのみ）。<br>• エラーにより、ポリシーに準拠していない。<br>• ポリシーを適用したら再起動する必要がある。<br>• 暗号化ポリシーが指定されていない。<br>• サポートされていない。<br>• ポリシーを適用するとき。 |
| モバイルデバイスの設定がポリシーに適合していません | コンプライアンスルールをチェックしたところ、モバイルデバイスの設定が Kaspersky Endpoint Security for Android ポリシーで指定された設定と異なります。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| 未処理のセキュリティ問題が検出されました | 未処理のセキュリティ問題がデバイス上でいくつか見つかりました。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| 製品が定義したデバイスのステータス | デバイスのステータスが管理対象アプリケーションによって定義されています。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| デバイスに空き容量がありません | デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［緊急］または［警告］から［*OK*］に変更されます。 | 0 MB より大きい値。 |
| デバイスが管理対象外になりました | デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |
| プロテクションが無効です | デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。<br>この場合、セキュリティ製品の状態は*停止中*またはエラーとなり、*開始中*、*実行中*、*中断中*とは異なります。 | 0 分より大きい値 |
| セキュリティ製品が実行されていません | デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。 | • 切り替えスイッチをオフ<br>• 切り替えスイッチをオン |

Kaspersky Security Center Linux では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、**定義データベースがアップデートされていません**条件の値が**3 日より大きい値**の場合はクライアントデバイスに*警告*ステータスが割り当てられ、条件値が**7 日より大きい値**の場合は*緊急*ステータスが割り当てられます。

Kaspersky Security Center Linux を旧バージョンからアップグレードしても、ステータスを*緊急*または*警告*に割り当てるための**定義データベースがアップデートされていません**条件の値は変更されません。

Kaspersky Security Center Linux によってデバイスにステータスが割り当てられると、一部の条件（上表の条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは定義データベースがアップデートされていません条件を満たしていたために、緊急ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスには*OK*ステータスが割り当てられます。

# デバイスのステータスの切り替えの設定

デバイスに「緊急」または「警告」ステータスを割り当てる条件を変更できます。

*デバイスのステータスの「緊急」への切り替えを有効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。
5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［緊急］ステータスを割り当てる条件をオンにします。




親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。

7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

*デバイスのステータスの「警告」への切り替えを有効にするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［*警告*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

# 通知の設定

Kaspersky Security Center Linux で発生するイベントに関する通知を設定できます。次の種別の通知を、通知方法の選択に応じて使用できます：

- メール：イベントが発生すると、指定されたメールアドレスに通知を送信します。
- SMS：イベントが発生すると、指定された電話番号に通知を送信します。
- 実行ファイル：イベントが発生すると、管理サーバーで実行ファイルが実行されます。

*Kaspersky Security Center Linux で発生したイベントの通知の配信を設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**通知**］セクションをクリックし、右側のペインで、設定する通知方法のタブを選択します：
   - **メール**

［**メール**］タブでは、メールによるイベントの通知を設定できます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**DNS MX ルックアップを使用**］を有効にすると、IP アドレスの複数の MX レコードを、SMTP サーバーの同一の DNS 名に使用できます。同一 DNS 名に複数の MX レコードが存在し、各レコードのメール受信の優先度の値が異なる場合があります。管理サーバーは SMTP サーバーへのメール通知の 送信を、MX レコードの優先度の昇順に試行します。

［**DNS MX ルックアップを使用**］を有効にし、TLS 設定の使用は有効にしない場合、メール通知を保護する追加の方法として、サーバーデバイスで DNSSEC 設定を使用することを推奨します。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定** ］をクリックして TLS 接続用の証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center Linux は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center Linux は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。

［**件名**］で、メールの件名を指定できます。このフィールドを空白にすることもできます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に自動的に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス：指定されていない場合は、受信者のアドレスを使用します。 注意：実在しないアドレスは使用しないことを推奨します**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**通知メッセージ**］には、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントのより詳細な情報についての代替パラメータを追加して、メッセージを編集することができます。

> 通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

- SMS

［**SMS**］タブでは、携帯電話へ送信する様々なイベントの SMS 通知を設定できます。SMS メッセージはメールゲートウェイを通して送信されます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定**］をクリックして SMTP サーバーのクライアント認証用の証明書を指定できます。信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center Linux は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center Linux は SMTP サーバーに接続できません。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。通知は、指定したメールアドレスに関連付けられている電話番号に送信されます。

［**件名**］で、メールの件名を指定できます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス：指定されていない場合は、受信者のアドレスを使用します。 注意：実在しないアドレスは使用しないことを推奨します**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**SMS メッセージの受信者の電話番号**］フィールドで、SMS 通知の受信者の携帯電話番号を指定します。

［**通知メッセージ**］では、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージを指定できます。このメッセージには、イベント名、デバイス名、ドメイン名などの代替パラメータを含めることができます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**テストメッセージの送信**］をクリックして、通知が正しく設定されているか確認します。指定した宛先にテスト通知が送信されます。

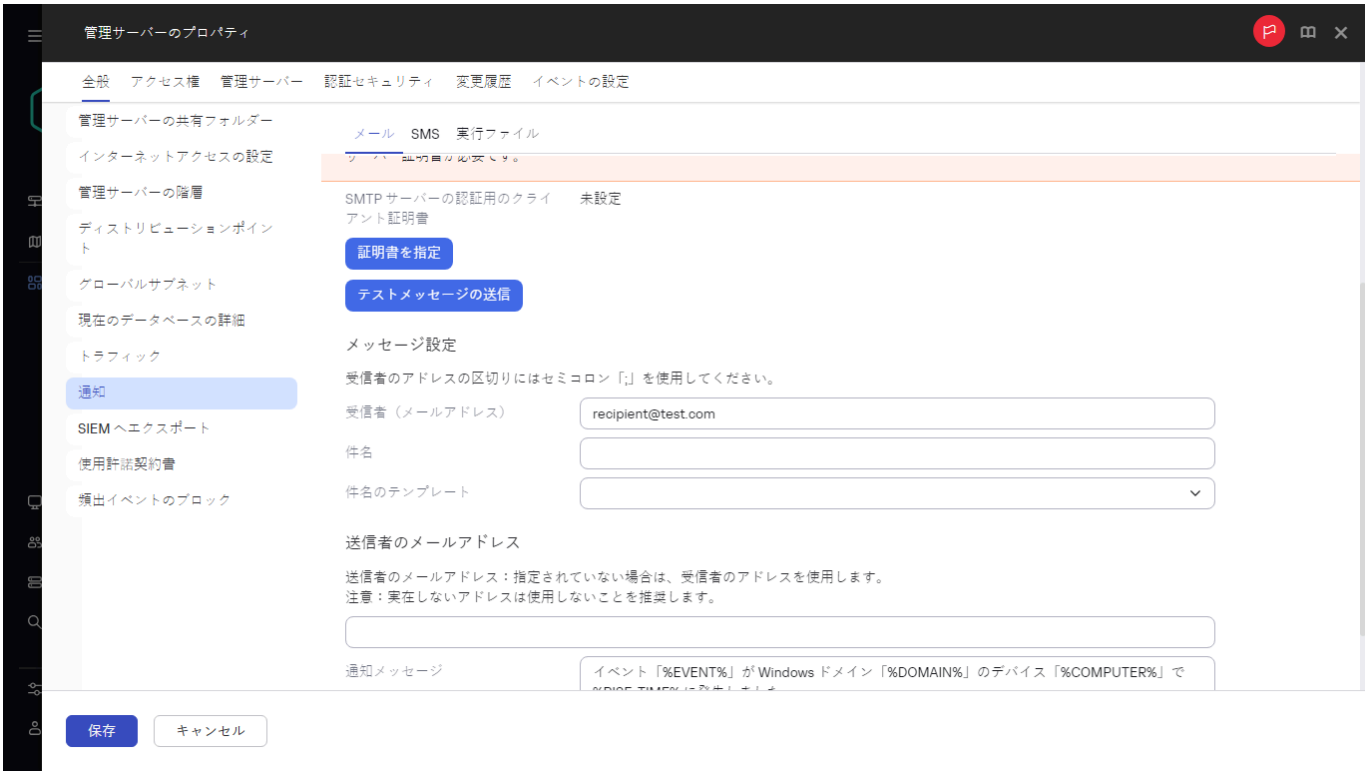
［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

- **実行ファイル**

この通知方法を選択すると、イベントの発生時に起動するアプリケーションを入力フィールドで選択できます。

［**イベント発生時に管理サーバーで実行される実行ファイル**］で、実行するファイルのあるフォルダーとファイル名を指定します。ファイルを指定する前に、通知メッセージで送信されるイベントの詳細を定義するファイルを準備してプレースホルダを指定してください。指定するフォルダーとファイルは、管理サーバー上に配置する必要があります。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。




通知方法の選択

3. タブで通知の設定を指定します。

4. ［OK］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

保存した通知の配信設定は、Kaspersky Security Center Linux で発生するすべてのイベントに適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

# テストの通知

イベント通知が送信されているかどうかを確認するには、クライアントデバイスで EICAR テストウイルスを検知したことの通知を使用します。

*イベント通知の送信を検証するには：*

1. クライアントデバイスでファイルシステムのリアルタイム保護タスクを停止し、EICAR テストウイルスをクライアントデバイスにコピーします。ファイルシステムのリアルタイム保護タスクを再び有効にします。
2. EICAR テストウイルスがあるクライアントデバイスを含む管理グループまたはそのデバイスに対してスキャンタスクを実行します。

   スキャンタスクが正しく設定されていれば、テストウイルスが検知されます。通知が正しく設定されていれば、ウイルスが検知されたと通知されます。

*テストウイルスの検知記録を開くには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 抽出名［**最近のイベント**］をクリックします。

   表示されるウィンドウに、テストウイルスに関する通知が表示されます。

EICAR テストウイルスには、デバイスに損害を与えるコードは含まれていません。ただし、ほとんどの製造元のセキュリティ製品で、このファイルはウイルスと判断されます。このテストウイルスは、EICAR の公式 Web サイトからダウンロードできます。

# 実行ファイルの起動により表示されるイベント通知

Kaspersky Security Center Linux は、実行ファイルを起動することにより、クライアントデバイスでのイベントについて管理者に通知できます。この実行ファイルには、管理者にリレーするイベントの環境変数を持つ別の実行ファイルを含める必要があります（下表参照）。

イベントを説明するための環境変数

| 環境変数 | 環境変数の説明 |
| --- | --- |
| $SEVERITY | イベントの重要度。指定可能な値：<br>• **情報**<br>• **警告**<br>• **エラー**<br>• **緊急** |
| $COMPUTER | イベントが発生したデバイスの名前。<br>デバイス名の最大長は 256 文字です。 |
| $DOMAIN | イベントが発生したデバイスのドメイン名。 |
| $EVENT | イベントタイプの名前。<br>イベントタイプ名の最大長は 50 文字です。 |

| 環境変数 | 環境変数の説明 |
| --- | --- |
| $DESCR | イベントの説明。<br>説明の最大長は 1000 文字です。 |
| $RISE_TIME | イベント作成時間。 |
| $KLCSAK_EVENT_TASK_DISPLAY_NAME | タスク名。<br>タスク名の最大長は 100 文字です。 |
| $KL_PRODUCT | アプリケーション名。 |
| $KL_VERSION | 製品のバージョン番号。 |
| $KLCSAK_EVENT_SEVERITY_NUM | イベントの重要度番号。指定可能な値：<br>• 1 – **情報**<br>• 2 – **警告**<br>• 3 – **エラー**<br>• 4 – **緊急** |
| $HOST_IP | イベントが発生したデバイスの IP アドレス。 |
| $HOST_CONN_IP | イベントが発生したデバイスの接続 IP アドレス。 |

例：
イベント通知は、実行ファイル（script1.bat など）の内部で、$COMPUTER 環境変数が設定された別の実行ファイル（script2.bat など）が起動されることによって送信されます。イベントが発生すると、管理者のデバイスで script1.bat ファイルが実行され、次に script2.bat ファイルが $COMPUTER 環境変数で実行されます。次に管理者は、イベントが発生したデバイスの名前を受信します。

# カスペルスキーからの通知

このセクションでは、カスペルスキーからの通知の使用、設定、無効にする方法について説明します。

## カスペルスキーからの通知について

カスペルスキーからの通知（[**監視とレポート**] → [**カスペルスキーからの通知**]）には、Kaspersky Security Center Linux のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。このセクションの情報は、古い通知を削除し、新しい情報を追加することで定期的に更新されます。

Kaspersky Security Center Linux は、現在接続されている管理サーバーおよび管理サーバーの管理対象デバイスにインストールされているカスペルスキー製品に関連するカスペルスキーからの通知のみ表示します。プライマリ、セカンダリ、または仮想サーバーなど管理サーバーの種別に関係なく個別に通知が表示されます。

カスペルスキーからの通知を受け取るために、管理サーバーにはインターネット接続が必要です。

通知には次の種別の情報が含まれます：

- セキュリティ関連告知

  お客様のネットワーク内にインストールされたカスペルスキー製品を最新かつ機能の制限がない状態に保つためのセキュリティ関連告知通知には、カスペルスキー製品の重要なアップデート、既知の脆弱性に対する修正、カスペルスキー製品の問題を修正する方法に関する情報が含まれることがあります。既定では、セキュリティ関連の通知は有効になっています。通知が必要ない場合は、この機能を無効にできます。

  お客様のネットワーク保護の設定に対応した情報を表示するために、Kaspersky Security Center Linux はデータをカスペルスキーのクラウドサーバーに送信し、ネットワーク内にインストールされたカスペルスキー製品に関連する通知のみを受け取ります。サーバーに送信される可能性のあるデータセットに関しては、Kaspersky Security Center の管理サーバーをインストールする際に同意いただいた使用許諾契約書で説明されています。

- マーケティング関連告知

  マーケティング関連告知には、カスペルスキー製品に関するお得な情報やキャンペーン、カスペルスキーからのニュースなどが含まれます。マーケティング関連の告知は既定で無効になっています。この種類の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでマーケティング関連告知を無効にできます。

  お客様のネットワークのデバイスの保護や日々の作業に役立つ可能性のある情報のみを表示するため、Kaspersky Security Center Linux はカスペルスキーのクラウドサーバーにデータを送信し、適切な通知を受け取ります。サーバーに送信される可能性のあるデータセットは、KSN に関する声明の処理されるデータに関する項で説明されています。

新しい情報は、重要度に基づいて次のカテゴリに分類されます：

1. 緊急の情報
2. 重要なニュース
3. 警告
4. 情報

カスペルスキーからの通知セクションに新しい情報が表示された際に、Kaspersky Security Center Web コンソールには通知の重要度のレベルに応じた通知ラベルが表示されます。ラベルをクリックして、［カスペルスキーからの通知］セクションで通知を表示できます。

カスペルスキーからの通知の設定で、表示する通知のカテゴリや通知を表示する位置を含む設定ができます。通知が必要ない場合は、この機能を無効にできます。

# カスペルスキーからの通知を設定する

［カスペルスキーからの通知］セクションで、表示する通知のカテゴリおよび通知を表示する位置を含むカスペルスキーからの通知の設定を変更できます。

*カスペルスキーからの通知を設定するには：*

1. メインメニューで、［**監視とレポート**］→［**カスペルスキーからの通知**］の順に選択します。
2. ［**設定**］をクリックします。

   カスペルスキーからの通知の設定ウィンドウが開きます。

3. 次の設定を指定します：

   - 表示する通知の重要度を選択します。その他のカテゴリの通知は表示されません。
   - 通知ラベルを表示する場所を選択します。ラベルはすべてのコンソールセクション、または［**監視とレポート**］セクションおよびそのサブセクションに表示することができます。

4. ［**OK**］をクリックします。

   カスペルスキーからの通知が設定されました。

# カスペルスキーからの通知を無効にする

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center Linux のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知には、セキュリティに関するものとマーケティングに関するものの 2 種類の情報があります。これらのお知らせは、種類ごとに無効にできます。

*セキュリティ関連告知を無効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**カスペルスキーからの通知**］を選択します。
3. ［**セキュリティ関連告知が［無効］です**］にします。
4. ［**保存**］をクリックします。

   カスペルスキーからの通知が無効になります。

マーケティング関連の告知は既定で無効になっています。マーケティング関連の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでこの種類のお知らせは無効にできます。

*マーケティング関連の告知を無効にするには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。
3. ［**Kaspersky Security Network の使用が［有効］です**］をオフにします。
4. ［**保存**］をクリックします。

   マーケティング関連の告知が無効になります。

# 脅威の検知に関する情報の表示

警告に関する情報の表示を有効または無効にできます。

*メインメニューの［**アラート**］セクションでの表示をオンまたはオフにするには：*

1. メインメニューで、［**設定**］→［**インターフェイスのオプション**］の順にクリックします。
2. ［**EDR アラートを表示**］をオンまたはオフにします。
3. ［**保存**］をクリックします。

オプションをオンにすると、コンソールのメインメニューの［**監視とレポート**］セクションに［**アラート**］サブセクションが表示されます。［**アラート**］サブセクションには、エンドポイントデバイスで検出された脅威に関する情報が表示されます。また、警告に関する情報を表示するウィジェットを追加することもできます。

検知された脅威の詳細情報を正しくアラートカードに表示するには、Kaspersky Endpoint Agent プラグインおよび互換性のあるバージョンの Kaspersky Endpoint Security プラグイン（Kaspersky Endpoint Security for Linux 12.1 以降、Kaspersky Endpoint Security for Mac 12.1 以降、または Kaspersky Endpoint Security for Windows 12.6 以降）をインストールする必要があります。

［**フィルター**］メニューを使用して、日付とフィールド値でアラートをフィルターします。

［**オブジェクト種別**］フィールドには次の値が含まれます：

- 不明
- フィッシングリンク
- ウイルス
- トロイの木馬
- 悪意のあるツール
- バックドア
- ワーム
- その他の製品
- アドウェア
- アダルト
- 危険な圧縮プログラム
- 危険な動作

［**自動応答**］フィールドには次の値が含まれます：

- 悪意のあるオブジェクトが検知されました
- オブジェクトが削除されました
- オブジェクトが駆除されました
- オブジェクトが駆除されませんでした
- オブジェクトが隔離に移動されました
- パスワードで保護された圧縮ファイルが検知されました
- ウイルスが検知されました

# Cloud Discovery

Kaspersky Security Center Cloud Linux は、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と判断されるクラウドサービスへのアクセスをブロックできます。Cloud Discovery は、ブラウザーやデスクトップアプリケーションからこれらのサービスにアクセスしようとするユーザーの試行を追跡します。また、暗号化されていない接続（HTTP プロトコルなどを使用）経由でクラウドサービスにアクセスしようとするユーザーの試行も追跡します。この機能は、シャドー IT によるクラウドサービスの使用を検知して停止するのに役立ちます。

ブロック機能は、Kaspersky Next EDR Optimum または Kaspersky Next XDR Expert ライセンスでKaspersky Security Center Linux をアクティベートした場合のみ使用できます。

ブロック機能は、Kaspersky Endpoint Security 11.2 for Windows 以降を使用している場合にのみ使用できます。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。

Cloud Discovery 機能を有効化し、機能を有効にするセキュリティポリシーまたはプロファイルを選択できます。各セキュリティポリシーまたはプロファイルで個別に機能を有効化または無効化することもできます。ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。

クラウドサービスへのアクセスをブロックできるようにするには、次の条件を満たしている必要があります。

- Kaspersky Endpoint Security 11.2 for Windows 以降を使用している。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。
- 不要なクラウドサービスへのアクセスをブロックする機能を含む Kaspersky Next のライセンスレベルを購入しました。詳細については、Kaspersky Next ヘルプを参照してください。

Cloud Discovery ウィジェットと Cloud Discovery レポートには、クラウドサービスへのアクセスの成功およびブロックされた試行に関する情報が表示されます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center Linux は、機能が有効になっているセキュリティポリシーまたはプロファイルによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

# ウィジェットを使用して Cloud Discovery を有効にする

Cloud Discovery 機能を使用すると、この機能が有効になっているセキュリティポリシーによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得できます。Cloud Discovery は、Kaspersky Endpoint Security for Windows ポリシーに対してのみ有効化または無効化できます。

Cloud Discovery 機能を有効にする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。
- Kaspersky Endpoint Security for Windows のプロパティを使用する。

  Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの［Cloud Discovery］セクションを参照してください。

Cloud Discovery 機能は、Kaspersky Endpoint Security for Windows のポリシーのパラメータでのみ無効にできることにご注意ください。

Cloud Discovery を有効にするには、［**一般機能：基本機能**］機能領域で［**書き込み**］権限が必要です。

*Cloud Discovery ウィジェットを使用して Cloud Discovery 機能を有効にするには：*

1. Kaspersky Security Center Linux に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. **Cloud Discovery** ウィジェットで、［**有効にする**］をクリックします。

   Kaspersky Endpoint Security for Windows バージョン 12.4 がインストールされている場合は、Kaspersky Endpoint Security for Windows ポリシープロパティで Cloud Discovery 機能を有効にします。詳細については、Kaspersky Endpoint Security for Windows ヘルプの Cloud Discovery セクションを参照してください。

   Kaspersky Endpoint Security for Windows のバージョン 12.4 より前のバージョンをお持ちの場合は、Kaspersky Endpoint Security for Windows プラグインをバージョン 12.5 にアップデートしてください。
4. 開いた［**Cloud Discovery を有効にする**］ウィンドウで、機能を有効にするセキュリティポリシーを選択し、［**有効にする**］をクリックします。

   次のポリシー設定が自動的に有効になります：**Web ページと連携するため Web トラフィック内にスクリプトを埋め込む**、**Web セッションの監視**、**暗号化された接続のスキャン**。

Cloud Discovery 機能が有効になり、ウィジェットがダッシュボードに追加されます。

# Cloud Discovery ウィジェットをダッシュボードに追加する

**Cloud Discovery** ウィジェットをダッシュボードに追加して、管理対象デバイス上のクラウドサービスの使用を監視できます。

Cloud Discovery ウィジェットをダッシュボードに追加するには、［**一般機能：基本機能**］機能領域で**書き込み**権限を持っている必要があります。

*Cloud Discovery ウィジェットをダッシュボードに追加するには：*

1. Kaspersky Security Center Linux に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. ダッシュボードで、［**Web ウィジェットを追加または復元**］をクリックします。
4. 使用可能なウィジェットのリストで、山形アイコン（›）［**その他**］カテゴリの横にあります。
5. ［**Cloud Discovery**］ウィジェットを選択し、［**追加**］をクリックします。
   Cloud Discovery 機能が無効になっている場合は、［ウィジェットを使用して Cloud Discovery を有効にする］セクションの手順に従ってください。

選択したウィジェットはダッシュボードの一番下に追加されます。

# クラウドサービスの使用情報を確認する

クラウドサービスへのアクセスの試行に関する情報を示す**クラウド検出**ウィジェットを表示できます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center Linux は、この機能が有効になっているセキュリティプロファイルによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

表示する前に、次のことを確認してください：

- Cloud Discovery ウィジェットがダッシュボードに追加されている。
- Cloud Discovery 機能が有効になっています。
- ［**読み取り**］権限が、［**一般的な機能：基本機能**］の機能領域で許可されている。

*Cloud Discovery ウィジェットを表示するには：*

1. Kaspersky Security Center Linux に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
   ［**Cloud Discovery**］ウィジェットがダッシュボードに表示されます。

3. ［**Cloud Discovery**］ウィジェットの左側で、クラウドサービスのカテゴリを選択します。

   ウィジェットの右側のテーブルには、選択したカテゴリから、ユーザーが最も頻繁にアクセスを試行するサービスが最大 5 つ表示されます。成功した試行とブロックされた試行の両方がカウントされます。

4. ウィジェットの右側で、特定のサービスを選択します。

   以下の表には、サービスへのアクセスを最も頻繁に試行するデバイスが最大 10 個表示されます。このテーブルでは、成功したアクセス試行に関するレポートとブロックされたアクセス試行に関するレポートの 2 種類のレポートを作成できます。

   さらにこのテーブルでは、特定のデバイスのクラウドサービスへのアクセスをブロックすることも可能です。

ウィジェットには、要求された情報が表示されます。

表示されたウィジェットでは、次の操作を実行できます：

- ［**監視とレポート**］→［**レポート**］セクションに進み、Cloud Discovery レポートを表示します。
- 選択したクラウドサービスへのアクセスをブロックまたは許可します。

ブロック機能は、Kaspersky Next EDR Optimum または Kaspersky Next XDR Expert ライセンスで Kaspersky Security Center Linux をアクティベートした場合のみ使用できます。

ブロック機能は、Kaspersky Endpoint Security 11.2 for Windows 以降を使用している場合にのみ使用できます。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。

# クラウドサービスのリスクレベル

Cloud Discovery は、クラウドサービスごとにリスクレベルを提供します。リスクレベルは、組織のセキュリティ要件に適合しないサービスを判断するのに役立ちます。たとえば、特定のサービスへのアクセスをブロックするかどうかを決定する時に、リスクレベルを考慮することができます。

リスクレベルは推定指標であり、クラウドサービスの品質やサービス提供元に関しては言及していません。リスクレベルは、カスペルスキーのエキスパートによる推奨事項でしかありません。

クラウドサービスのリスクレベルは、Cloud Discovery ウィジェット、および監視対象のすべてのクラウドサービスのリストに表示されます。

# 不要なクラウドサービスへのアクセスをブロックする

ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。以前にブロックされたクラウドサービスへのアクセスを許可することもできます。

他の考慮事項の中でも、特定のサービスへのアクセスをブロックするかどうかを決定する際に、リスクレベルを考慮に入れることを推奨します。

セキュリティポリシーまたはプロファイルのクラウドサービスへのアクセスをブロックまたは許可できます。

不要なクラウドサービスへのアクセスをブロックする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。

  この場合、サービスへのアクセスを 1 つずつブロックできます。

- Kaspersky Endpoint Security for Windows のプロパティを使用する。

  この場合、サービスへのアクセスを 1 つずつブロックすることも、1 つのカテゴリ全体をまとめてブロックすることもできます。

  Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの［Cloud Discovery］セクションを参照してください。

*ウィジェットを使用してクラウドサービスへのアクセスをブロックまたは許可するには：*

1. Cloud Discovery ウィジェットを開き、必要なクラウドサービスを選択します。
2. ［**サービスを使用するデバイス上位 10 台**］ペインで、サービスをブロックまたは許可するセキュリティポリシーまたはプロファイルを見つけます。
3. 必要な行の［**ポリシーまたはプロファイルのアクセスステータス**］列で、次のいずれかを実行します。
   - サービスをブロックするには、ドロップダウンリストで［**ブロック**］を選択します。
   - サービスを許可するには、ドロップダウンリストで［**許可**］を選択します。
4. ［**保存**］をクリックします。

選択したサービスへのアクセスは、セキュリティポリシーまたはプロファイルに対してブロックまたは許可されています。

# SIEM システムへのイベントのエクスポート

このセクションでは、SIEM システムへのイベントのエクスポートの設定について説明します。

## SIEM システムへのイベントのエクスポートの設定

Kaspersky Security Center Linux では、Syslog 形式を使用する SIEM システムへエクスポートする方法、または Kaspersky Security Center のデータベースから直接 SIEM システムにイベントをエクスポートする方法のどちらかで SIEM システムへのイベントのエクスポートを許可します。このシナリオを完了すると、管理サーバーはイベントを SIEM システムに自動的に送信します。

### 必須条件

Kaspersky Security Center Linux でイベントのエクスポートの設定を開始する前に：

- イベントのエクスポート方法の詳細を参照してください。
- システムの設定値を確認してください。

このシナリオのステップは、任意の順序で実行できます。

イベントを SIEM システムにエクスポートするプロセスは、次の手順で構成されます：

- **Kaspersky Security Center Linux からイベントを受信するように SIEM システムを設定する**

  手順：SIEM システムへのイベントのエクスポートの設定

- **SIEM システムにエクスポートするイベントの選択**

  SIEM システムにエクスポートするイベントをマークします。最初に、すべての管理対象のカスペルスキー製品内で発生する一般的なイベントをマークします。それから、特定の管理対象のカスペルスキー製品のイベントをマークします。

- **SIEM システムへのイベントのエクスポートの設定**

  次のいずれかの方法でイベントをエクスポートします：

  - TCP / IP、UDP、または TLS over TCP プロトコルを使用
  - Kaspersky Security Center データベースからのイベントの直接エクスポートを使用（データベースでは定義済みのパブリックビューのセットを使用できます。これらのパブリックビューの詳細については、「klakdb.chm のドキュメント」を参照してください）

### 結果

エクスポートするイベントを選択した場合、SIEM システムへのイベントのエクスポートの設定後にエクスポート結果を表示できます。

# 事前準備

Kaspersky Security Center Linux 管理コンソールでイベントの自動エクスポートを設定する場合は、SIEM システム設定の一部を指定する必要があります。Kaspersky Security Center Linux の設定を準備できるように、SIEM システムの設定を事前に確認しておいてください。

SIEM システムへのイベントの自動送信を正しく設定するには、次の設定の値を把握する必要があります：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムサーバーのポート**

  Kaspersky Security Center Linux と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

  Kaspersky Security Center Linux から SIEM システムへのメッセージの送信に使われるプロトコル。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

# イベントのエクスポートについて

Kaspersky Security Center Linux では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。

イベントのエクスポートは、組織および技術レベルでセキュリティ問題に対処し、セキュリティ監視サービスを提供し、各種ソリューションからの情報を統合できる、一元化されたシステム内で使用できます。これらは SIEM システムで、ネットワークのハードウェアとアプリケーション、またはセキュリティオペレーションセンター（SOC）によって生成されたセキュリティアラートとイベントをリアルタイムで分析します。

これらのシステムは、ネットワーク、セキュリティ、サーバー、データベース、アプリケーションなど多くのソースからのデータを受信します。SIEM システムは、重要なイベントを見逃すことがないように、監視対象データを統合する機能も提供します。さらに、緊急のセキュリティ問題を管理者に通知するために、相互に関連するイベントとアラートの分析を自動的に実行します。アラートはダッシュボードから発することも、メールなどのサードパーティのチャネルから送信することもできます。

Kaspersky Security Center Linux から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Linux とイベントのレシーバである SIEM システムの 2 つが関係します。イベントを正常にエクスポートするには、SIEM システムと Kaspersky Security Center Linux の両方で設定する必要があります。どちらを先に設定してもかまいません。Kaspersky Security Center Linux からのイベントの送信を設定してから、SIEM システムによるイベントの受信を設定することも、逆の順序で設定することもできます。

## イベントのエクスポートの Syslog 形式

Syslog 形式のイベントを任意の SIEM システムに送信できます。Syslog 形式を使用すると、管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントをすべてリレーできます。Syslog 形式でイベントをエクスポートする場合は、SIEM システムにリレーするイベントの種別を正確に選択できます。

## SIEM システムによるイベントの受信

SIEM システムは、Kaspersky Security Center Linux からイベントを受信して適切に解析する必要があります。これらの目的に対応できるように、SIEM システムを適切に設定する必要があります。設定は、利用する具体的な SIEM システムによります。ただし、レシーバとパーサーの設定など、すべての SIEM システムの設定で一般的なステップがいくつかあります。

# SIEM システムでのイベントのエクスポートの設定について

Kaspersky Security Center Linux から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Linux とイベントのレシーバである SIEM システムの 2 つが関係します。イベントのエクスポートは、SIEM システムと Kaspersky Security Center Linux の両方で設定する必要があります。

SIEM システムで指定する設定は、使用している個々のシステムにより異なります。一般に、すべての SIEM システムでレシーバを設定する必要があり、受信イベントを解析するためのメッセージパーサーを任意で設定します。

## レシーバの設定

Kaspersky Security Center Linux から送信されたイベントを受信するには、SIEM システムでレシーバを設定する必要があります。一般に、SIEM システムで次の設定を指定する必要があります：

- **エクスポートプロトコル**

  メッセージ送信プロトコル（UDP、TCP、TLS over TCP）。このプロトコルは、Kaspersky Security Center Linux で指定したプロトコルと同じにする必要があります。

- **ポート**

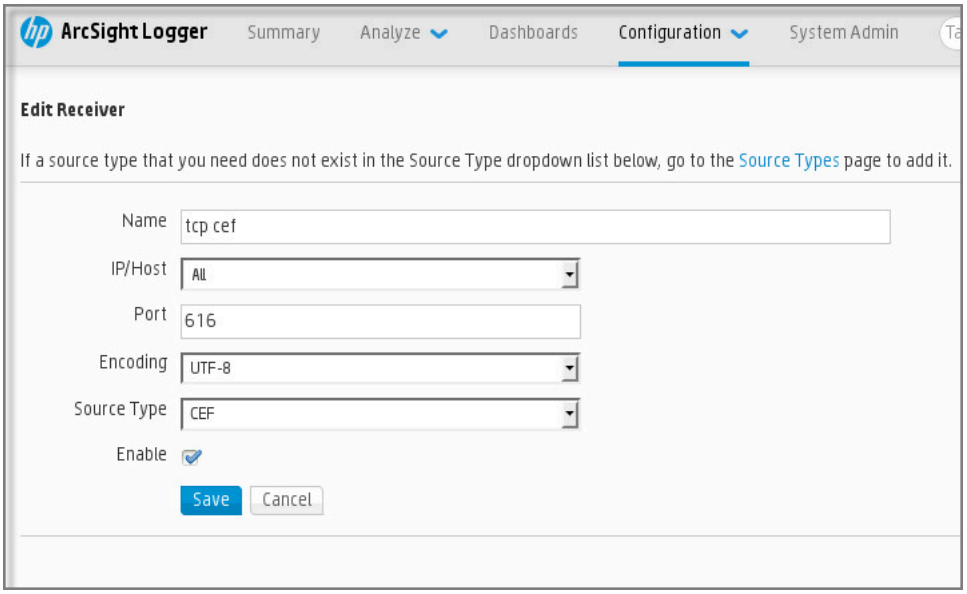
  Kaspersky Security Center Linux に接続するポート番号を指定します。このポートは SIEM システムの設定中に Kaspersky Security Center Linux で指定したポートと同じポートである必要があります。

- **データ形式**

  Syslog 形式を指定します。

使用する SIEM システムによっては、受信者の設定を一部追加で指定する必要があります。

次の図は、ArcSight の受信者のセットアップ画面を示します。




ArcSight でのレシーバのセットアップ

### メッセージパーサー

エクスポートされたイベントはメッセージとして SIEM システムに渡されます。SIEM システムでイベントに関する情報が利用できるように、これらのメッセージを適切に解析する必要があります。メッセージパーサーは SIEM システムの一部です。イベントの ID、深刻度、説明、パラメータなど関連フィールドにメッセージの内容を分けるために使用します。メッセージの内容を分けることで、SIEM システムは Kaspersky Security Center Linux から受信したイベントを処理して、SIEM システムデータベースに保管することができます。

## Syslog 形式で SIEM システムにエクスポートするイベントのマーキング

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントを選択する必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択されている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

# Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング

管理対象デバイスにインストールされた特定の管理対象アプリケーションで発生したイベントをエクスポートする場合は、エクスポートするイベントをそのアプリケーションのポリシーでマークします。この場合、マークされたイベントが、ポリシーの範囲に含まれるすべてのデバイスからエクスポートされます。

*特定の管理対象アプリケーションからエクスポートするイベントをマークするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. イベントをマークするアプリケーションのポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。
3. ［**イベントの設定**］セクションに移動します。
4. SIEM にエクスポートするイベントに隣接するチェックボックスをオンにします。
5. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

6. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。
7. ［**保存**］をクリックします。

管理対象アプリケーションからマークされたイベントを、SIEM システムへエクスポーされる準備ができています。

特定の管理デバイスのために、SIEM システムへエクスポートするイベントをマークできます。以前エクスポートしたイベントがアプリケーションのポリシーでマークされた場合、管理対象デバイスのためにマークされたイベントを再定義することはできません。

*管理対象デバイスにエクスポートするイベントをマークするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、必要なデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. ［**アプリケーション**］セクションに移動します。
4. アプリケーションのリストで、必要なアプリケーションの名前のリンクをクリックします。
5. ［**イベントの設定**］セクションに移動します。
6. SIEM にエクスポートするレイベントに隣接するチェックボックスをオンにします。

7. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマークすることもできます。

8. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

## Syslog 形式でエクスポートする一般的なイベントのマーキング

Syslog 形式を使用して、管理サーバーが SIEM システムにエクスポートする一般的なイベントをマーキングすることができます。

*SIEM システムにエクスポートする一般的なイベントをマークするには：*

1. 次のいずれかの手順を実行します：

   - メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（⚙）をクリックします。
   - メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動し、ポリシーのリンクをクリックします。

2. 表示されたウィンドウで、［**イベントの設定**］タブを選択します。

3. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

4. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

# Syslog 形式を使用したイベントのエクスポートについて

Syslog 形式を使用すると、管理サーバー、管理対象デバイスにインストールされた他のカスペルスキー製品で発生したイベントを SIEM システムにエクスポートできます。

Syslog は標準メッセージロギングプロトコルです。メッセージを生成するソフトウェア、メッセージを保管するシステム、メッセージを報告、分析するソフトウェアを分けることができます。各メッセージには、メッセージを生成したソフトウェアの種別を示す機能コードのラベルが付けられ、重要度が割り当てられます。

Syslog 形式は、インターネット技術タスクフォース（インターネット標準）によって公開されている RFC（Request for Comments）の文書で定義されています。Kaspersky Security Center Linux から外部システムへのイベントのエクスポートには、RFC 5424 標準が使用されます。

Kaspersky Security Center Linux で、Syslog 形式を使用して外部システムにイベントがエクスポートされるように設定できます。

エクスポートのプロセスは次の 2 つのステップで構成されます：

1. イベントの自動エクスポートの有効化。このステップでは、イベントを SIEM システムに送信するように Kaspersky Security Center Linux を設定します。自動エクスポートを有効にすると、Kaspersky Security Center Linux は即座にイベントの送信を開始します。

2. 外部システムにエクスポートするイベントの選択。このステップでは、SIEM システムにエクスポートするイベントを選択します。

# イベントを SIEM システムにエクスポートするための Kaspersky Security Center Linux の設定

イベントを SIEM システムにエクスポートするには、Kaspersky Security Center Linux でエクスポートプロセスを設定する必要があります。

*Kaspersky Security Center Web コンソールで SIEM システムへのエクスポートを設定するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**SIEM**］セクションを選択します。

3. ［**設定**］をクリックします。
   ［**エクスポート設定**］セクションが開きます。

4. ［**エクスポート設定**］セクションで設定を指定します：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムのポート**

  Kaspersky Security Center Linux と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Linux の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

メッセージを SIEM システムに送信するために使用するプロトコルを選択します。TCP、UDP、TLS over TCP プロトコルのいずれかを選択できます。

TLS over TCP プロトコルを選択した場合は、次の TLS 設定を指定します：

- **サーバー認証**

  ［**サーバー認証**］フィールドでは、**信頼する証明書**または **SHA フィンガープリント**を選択できます：

  - **信頼できる証明書**：信頼できる認証局（CA）からルート証明書を含む完全な証明書チェーンを受け取り、そのファイルを Kaspersky Security Center Linux にアップロードすることができます。Kaspersky Security Center Linux は、SIEM システムサーバーの証明書チェーンも信頼できる CA によって署名されているかどうかを確認します。

    信頼できる証明書を追加するには、［**CA 証明書を参照**］をクリックして、証明書をアップロードします。

  - **SHA フィンガープリント**：Kaspersky Security Center Linux では、SIEM システムの完全な証明書チェーン（ルート証明書を含む）の SHA1 サムプリントを指定できます。SHA1 サムプリントを追加するには、［**サムプリント**］フィールドでサムプリントを入力し、［**追加**］をクリックします。

  ［**クライアント認証を追加する**］を使用して、Kaspersky Security Center Linux を認証する証明書を生成することができます。このようにして、Kaspersky Security Center Linux が発行した自己署名証明書を使用します。この場合、SIEM システムサーバーの認証に、信頼できる証明書と SHA フィンガープリントの両方を使用することができます。

- **サブジェクト名 / サブジェクト代替名を追加する**

  サブジェクト名は、証明書を受け取るドメインの名前です。SIEM システムサーバーのドメイン名が SIEM システムサーバー証明書のサブジェクト名と一致しない場合、Kaspersky Security Center Linux は SIEM システムサーバーに接続できません。しかし、SIEM システムサーバーは証明書内で名前が変更された場合にドメイン名を変更することがあります。この場合、サブジェクト名を［**サブジェクト名 / サブジェクト代替名を追加する**］で指定することができます。指定されたサブジェクト名のいずれかが SIEM システム証明書のサブジェクト名と一致する場合、Kaspersky Security Center Linux は SIEM システムサーバー証明書を検証します。

- **クライアント認証を追加する**

  クライアント認証用に、自身の証明書を挿入するか、Kaspersky Security Center Linux で生成することができます。

  - **証明書を挿入する**:CA など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

    - **X.509 証明書 PEM**：［**証明書のファイル**］フィールドに証明書のファイルをアップロードし、［**鍵のファイル**］フィールドに秘密鍵のファイルをアップロードします。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルがアップロードされたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - **X.509 証明書 PKCS12**：証明書と秘密鍵を含む単一のファイルを［**証明書のファイル**］フィールドにアップロードします。ファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- **鍵を生成する**：Kaspersky Security Center Linux で自己署名証明書を生成できます。Kaspersky Security Center Linux は生成された自己署名証明書を保存し、証明書の公開部分または SHA-1 フィンガープリントを SIEM システムに渡すことができます。

5. 必要に応じて、管理サーバーデータベースからアーカイブイベントをエクスポートし、アーカイブイベントのエクスポートを開始する日付を設定できます：

   a. ［**エクスポートの開始日を設定**］をクリックします。

   b. 表示されたセクションの［**エクスポートの開始日**］に、開始日を指定します。

   c. ［**OK**］をクリックします。

6. オプションを［**SIEM システムデータースへのイベントの自動エクスポートが［有効］です**］に切り替えます。

7. SIEM システム接続が正常に設定されていることを確認するには、［**接続の確認**］をクリックします。

   SIEM システムサーバーとの接続が確立され、テストイベントが送信されます。接続のステータスが表示されます。

   チェックは TCP/IP および TLS over TCP プロトコルに対してのみ実行されます。

8. ［**保存**］をクリックします。

SIEM システムへのエクスポートが設定されました。これで、イベントの受信を SIEM システムで設定した場合は、マーキングされたイベントが管理サーバーから SIEM システムにエクスポートされます。エクスポートの開始日を設定した場合、管理サーバーは指定された日付からも管理サーバーデータベース内のマーキングされたイベントをエクスポートします。

# データベースからのイベントの直接エクスポート

Kaspersky Security Center Linux インターフェイスを使わなくても、Kaspersky Security Center Linux のデータベースから直接イベントを取得できます。パブリックビューに対して直接クエリを実行してイベントデータを取得することも、既存のパブリックビューを基に独自のビューを作成して、必要なデータを取得するようにアドレス指定することもできます。

## パブリックビュー

Kaspersky Security Center Linux のデータベースには、パブリックビューの便利なセットをご用意しています。これらのパブリックビューの詳細は、klakdb.chm のドキュメントを参照してください。

v_akpub_ev_event パブリックビューには、データベース内のイベントパラメータを表す一連のフィールドが含まれています。klakdb.chm ドキュメントには、デバイス、アプリケーション、ユーザーなど、他の Kaspersky Security Center Linux のエンティティに対応するパブリックビューに関する情報も含まれています。この情報はクエリに使用できます。

このセクションでは、klsql2 ユーティリティを使って SQL クエリを実行する手順について説明し、クエリの例を示します。

SQL クエリまたはデータベースビューを作成する時には、データベースと連携する他のプログラムも使用できます。Kaspersky Security Center Linux のデータベースへの接続に必要なインスタンス名やデータベース名などのパラメータの表示方法についても、該当セクションを参照してください。

## klsql2 ユーティリティを使用した SQL クエリの実行

この記事では、klsql2 ユーティリティの使用方法と、このユーティリティを使用して SQL クエリを実行する方法について説明します。インストールされている Kaspersky Security Center Linux バージョンに含まれている klsql2 ユーティリティバージョンを使用します。

*klsql2 ユーティリティを使用するには：*

1. 管理サーバーがインストールされているディレクトリに移動します。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。
2. このディレクトリに、.sql 拡張子を持つ空のファイルを作成します。
3. テキストエディターで、作成した .sql ファイルを開きます。
4. 必要な SQL クエリを .sql ファイルに入力して、ファイルを保存します。
5. 管理サーバーがインストールされたデバイスで、次のコマンドをコマンドラインに入力して、.sql ファイルから SQL クエリを実行し、結果を result.xml ファイルに保存します：
   `sudo ./klsql2 -i src.sql -u <ユーザー名> -p <パスワード> -o result.xml`
   **<ユーザー名>**と**<パスワード>**は、定義データベースにアクセスできるユーザーアカウントの資格情報です。
6. 必要に応じて、データベースにアクセスできるユーザーアカウントのログインとパスワードを入力してください。
7. 新しく作成されたファイル result.xml を開いて、SQL クエリ結果を確認します。

.sql ファイルを編集して、パブリックビューに対する任意の SQL クエリを作成することができます。次に、コマンドラインからクエリを実行して、結果をファイルに保存します。

## klsql2 ユーティリティでの SQL クエリの例

このセクションでは、klsql2 ユーティリティによって実行された SQL クエリの例を示します。

次の例では、過去 7 日間にデバイスで発生したイベントを取得し、発生した順にイベントを表示します。イベントは新しい順に表示されます。

PostgreSQL の例：

```
SELECT
  /* イベントの識別子 */
  "e"."nId",

  /* イベントが発生した時刻 */
  "e"."tmRiseTime",

  /*  イベント種別の内部名 */
  "e"."strEventType",

  /* イベント種別の表示名 */
  "e"."wstrEventTypeDisplayName",

  /* イベントについて表示される説明 */
  "e"."wstrDescription",

  /* イベントについて表示される説明 */
  "e"."wstrGroupName",

  /* イベントが発生したデバイスの表示名 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* イベントが発生したデバイスの IP アドレス */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL または MariaDB の例：

```
SELECT

  /* イベントの識別子 */
  `e`.`nId`,

  /* イベントが発生した時刻 */
  `e`.`tmRiseTime`,

  /* イベント種別の内部名 */
  `e`.`strEventType`,

  /* イベント種別の表示名 */
  `e`.`wstrEventTypeDisplayName`,

  /* イベントについて表示される説明 */
  `e`.`wstrDescription`,

  /* デバイスグループ名 */
  `e`.`wstrGroupName`,

  /* イベントが発生したデバイスの表示名 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* イベントが発生したデバイスの IP アドレス */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

# Kaspersky Security Center Linux データベース名の表示

MySQL、MariaDB のいずれかのデータベース管理ツールで Kaspersky Security Center Linux のデータベースにアクセスする場合は、SQL スクリプトエディターから接続できるようにその定義データベースの名前を調べる必要があります。

*Kaspersky Security Center Linux のデータベースの名前を表示するには：*

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**現在のデータベースの詳細**］セクションを選択します。

   データベース名は［**データベース名**］フィールドに指定されます。このデータベース名を使用して、SQL クエリ内のデータベースのアドレスを指定します。

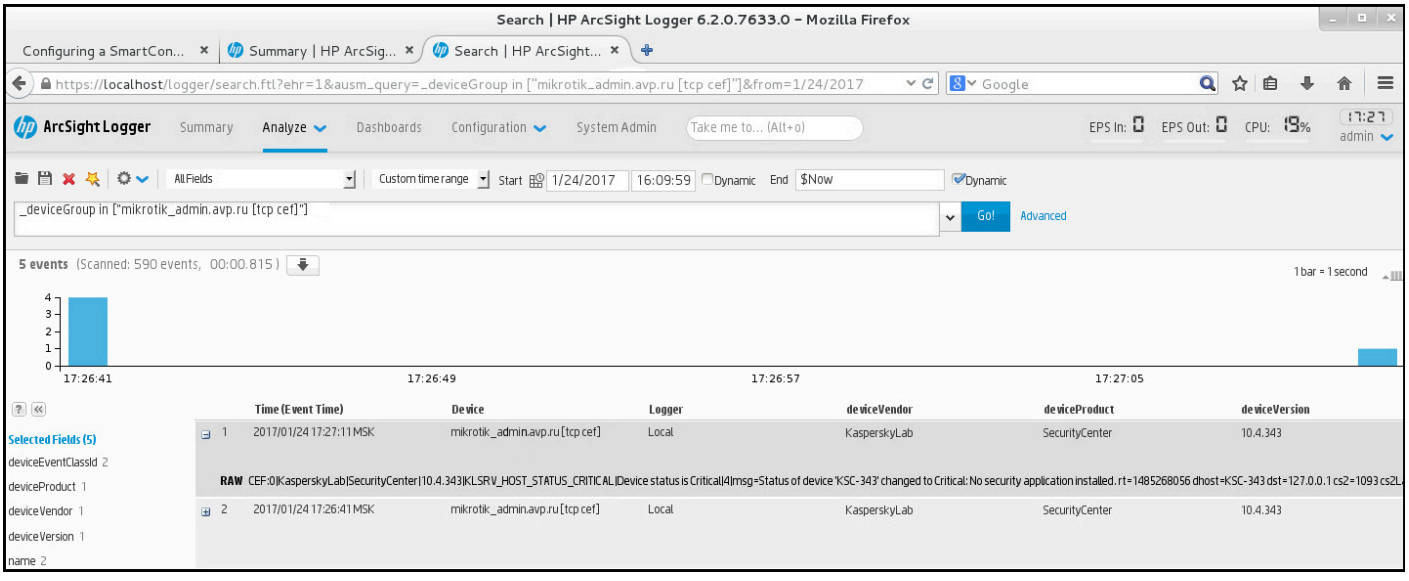
# エクスポート結果の表示

イベントのエクスポート手順が正常に完了するようにコントロールすることができます。それには、イベントのエクスポートとともにメッセージが SIEM システムで受信されているかどうかを確認します。

Kaspersky Security Center Linux から送信されたイベントが SIEM システムで受信され、適切に解析されている場合、設定は両者で適切に行われています。イベントが受信されない場合は、Kaspersky Security Center Linux で指定した設定を SIEM システムの設定と比べて確認してください。

次の図は、ArcSight にエクスポートされたイベントを示します。たとえば、最初のイベントは重大な管理サーバーイベントです：「*デバイスのステータスが「緊急」です。*」

エクスポートされたイベントの SIEM システムでの表示は、使用している SIEM システムによって異なります。




イベントの例

# オブジェクトリビジョンの管理

このセクションでは、オブジェクトのリビジョン管理について説明します。Kaspersky Security Center Linux では、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、*リビジョン*が作成されます。各リビジョンには番号が付いています。

リビジョン管理に対応するオブジェクトは次の通りです：

- 管理サーバーのプロパティ
- ポリシー
- タスク
- 管理グループ
- ユーザーアカウント
- インストールパッケージ

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを表示する（ポリシーに対してのみ使用可能）
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンを JSON ファイルとして保存する（ポリシーに対してのみ使用可能）

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- **リビジョン**ーオブジェクトのリビジョン番号
- **時間**ーオブジェクトが変更された日時
- **ユーザー**ーオブジェクトを変更したユーザーの名前
- **ユーザーデバイスの IP アドレス**ーオブジェクトが変更されたデバイスの IP アドレス。
- **Web コンソールの IP アドレス**ーオブジェクトが変更された Kaspersky Security Center Web コンソールの IP アドレス。
- **処理**ーオブジェクトに対する操作
- **説明**ーオブジェクト設定に対して行われた変更に関連するリビジョンの説明

  既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明の編集**］をクリックします。表示されたウィンドウで、リビジョンの説明を入力します。

# ポリシーレビジョンの表示と保存

Kaspersky Security Center Linux では、一定期間にポリシーにどのような変更が加えられたかを確認したり、これらの変更に関する情報をファイルに保存したりできます。

対応する管理 Web プラグインがこの機能をサポートしている場合、ポリシーリビジョンの表示と保存が可能です。

*ポリシーリビジョンを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 表示したいリビジョンのポリシーをクリックし、［**変更履歴**］セクションに移動します。
3. ポリシーリビジョンのリストで、表示したいリビジョンの番号をクリックします。

   リビジョンのサイズが 10 MB を超える場合、Kaspersky Security Center Web コンソールを使用して表示することはできません。選択したリビジョンを JSON ファイルに保存するように要求されます。

   リビジョンサイズが 10 MB を超えない場合、選択したポリシーリビジョンの設定を含む HTML 形式のレポートが表示されます。レポートはポップアップウィンドウに表示されるため、ブラウザーでポップアップが許可されていることを確認してください。

*ポリシーリビジョンを JSON ファイルに保存するには、*

ポリシーリビジョンのリストで、保存するリビジョンを選択し、［**ファイルに保存**］をクリックします。

リビジョンが JSON ファイルに保存されます。

# 以前のリビジョンへのオブジェクトのロールバック

必要に応じて、オブジェクトの変更をロールバックできます。たとえば、ポリシーの設定を特定の日付の状態まで戻さなければならない場合があります。

*オブジェクトの変更をロールバックするには：*

1. オブジェクトのプロパティウィンドウで［**変更履歴**］タブを表示します。
2. オブジェクトのリビジョンのリストで、変更のロールバック先となるリビジョンを選択します。
3. ［**ロールバック**］をクリックします。
4. ［**OK**］をクリックして処理内容を確定します。

オブジェクトが、選択したリビジョンにロールバックされます。オブジェクトのリビジョンのリストには、実行された処理の記録が表示されます。リビジョンの説明には、オブジェクトを元に戻したリビジョン番号に関する情報が表示されます。

ロールバック操作は、ポリシーオブジェクトとタスクオブジェクトでのみ使用できます。

# オブジェクトの削除

このセクションでは、オブジェクトの削除について説明します。

次のオブジェクトを削除できます：

- ポリシー
- タスク
- インストールパッケージ
- 仮想管理サーバー
- ユーザー
- セキュリティグループ
- 管理グループ

*オブジェクトを削除するには：*

1. Kaspersky Security Center Web コンソールの必要なセクションを開き、オブジェクトを選択します。
2. ツールバーで、［**削除**］をクリックします。
3. 表示されたウィンドウで、［**OK**］をクリックして処理を確定します。

   選択したルールが削除されます。

オブジェクトを削除しても、オブジェクトの情報はデータベースに保存されます。削除されたオブジェクトの情報の保存期間は、オブジェクトの履歴の保存期間（推奨期間は 90 日）と同じです。［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、保存期間を変更できます。

## クライアントデバイスの削除について

管理グループから管理対象デバイスを削除すると、アプリケーションはそのデバイスを未割り当てデバイスグループに移動します。デバイスの削除後、インストールされているカスペルスキー製品（ネットワークエージェント、Kaspersky Endpoint Security などのセキュリティ製品）はデバイス上に残ります。

Kaspersky Security Center Linux は、次のルールに従って、未割り当てデバイスグループ内のデバイスを処理します：

- デバイス移動ルールを設定しており、デバイスが移動ルールの基準を満たしている場合、デバイスはルールに従って管理グループに自動的に移動されます。
- デバイスは未割り当てデバイスグループに保存され、デバイス保持ルールに従ってグループから自動的に削除されます。

  デバイスの保持ルールは、ディスク全体の暗号化で暗号化された1つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除します。

  > 暗号化されたドライブを含むデバイスを削除すると、ドライブの復号化に必要なデータも削除されます。このようなデバイス（[Unassigned devices**未割り当てデバイス**Managed Devices**管理対象デバイス**] **リスクを理解した上で、選択したデバイスを削除します**］をオンにした場合は、その後のデータ削除を認識していることを意味します。

  ドライブを復号化するには、次の条件を満たす必要があります：

  - デバイスは管理サーバーに再接続され、ドライブの復号化に必要なデータが復元されます。
  - デバイスのユーザーは復号化パスワードを覚えています。
  - ドライブの暗号化に使用されたセキュリティ製品（Kaspersky Endpoint Security for Windows など）は、デバイスにまだインストールされています。

  ドライブが Kaspersky Disk Encryption 技術によって暗号化されている場合は、FDERT 復元ユーティリティを使用してデータの回復を試行することもできます。

未割り当てデバイスグループからデバイスを手動で削除すると、アプリケーションはそのデバイスをリストから削除します。デバイスを削除した後、インストールされているカスペルスキー製品はデバイス上に残ります。その後、デバイスがまだ管理サーバーに表示されており、定期的なネットワークポーリングを設定している場合、Kaspersky Security Center Linux はネットワークポーリング中にデバイスを検出し、未割り当てデバイスグループに追加します。したがって、デバイスが管理サーバーに表示されない場合にのみ、デバイスを手動で削除することが合理的です。

# 隔離とバックアップからのファイルのダウンロードと削除

このセクションでは、Kaspersky Security Center Web コンソールでファイルをダウンロードする方法、および隔離とバックアップからファイルを削除する方法について説明します。

## 隔離とバックアップからのファイルのダウンロード

次の 2 つの条件のいずれかが満たされた場合にのみ、隔離とバックアップからファイルをダウンロードできます：[**管理サーバーから切断しない**］がオンになっているか、接続ゲートウェイが使用されている。いずれの条件も満たさない場合は、ダウンロードできません。

*隔離またはバックアップにあるファイルのコピーをハードディスクに保存するには：*

1. 次のいずれかの手順を実行します：

   - Quarantineからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**隔離**］の順に移動します。

   - バックアップからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**バックアップ**］の順に移動します。

2. 表示されるウィンドウで、ダウンロードするファイルを選択し、［**ダウンロード**］をクリックします。

   ダウンロードが開始されます。クライアントデバイスで隔離に配置されたファイルのコピーが、指定したフォルダーに保存されます。

# 隔離、バックアップ、またはアクティブな脅威リポジトリからのオブジェクトの削除について

クライアントデバイスにインストールされているカスペルスキーのセキュリティ製品がオブジェクトを隔離、バックアップ、またはアクティブな脅威リポジトリに配置すると、追加されたオブジェクトに関する情報が［**隔離**］、［**バックアップ**］、または Kaspersky Security Center Linux の［**アクティブな脅威**］セクションに送信されます。これらのセクションのいずれかを開いた際に、リストからオブジェクトを選択して［**削除**］をクリックすると、Kaspersky Security Center Linux は次のいずれかのアクションまたは両方の処理を実行します：

- 選択したオブジェクトをリストから削除する

- 選択したオブジェクトをリポジトリから削除する

実行する処理は、選択したオブジェクトをリポジトリに配置したカスペルスキー製品によって定義されます。カスペルスキー製品は、［**エントリを追加したアプリケーション**］フィールドで指定されています。実行する処理の詳細については、カスペルスキー製品のマニュアルを参照してください。

# Kaspersky Security Center Web コンソールとその他のカスペルスキー製品の連携

このセクションでは、Kaspersky Security Center Web コンソールから Kaspersky Managed Detection and Response など、別のカスペルスキー製品へのアクセスを設定する方法について説明します。また、このセクションでは、SIEM システムへのエクスポートを設定する方法についても説明します。

## バックグラウンド接続の確立

Kaspersky Security Center Linux と Kaspersky Managed Detection and Response（MDR とも表記）など、その他のカスペルスキー製品またはソリューションとの間の連携を設定するには、Kaspersky Security Center Web コンソールと管理サーバー間でバックグラウンド接続を確立する必要があります。使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合のみ、この接続を確立することができます。

連携は、Kaspersky Managed Detection and Response と Windows ベースの Kaspersky Security Center 間でのみ設定できます。

*バックグラウンド接続を確立するには：*

1. メインメニューで、［**設定**］→［**連携**］の順にクリックします。
2. ［**連携**］セクションで、バックグラウンド接続を確立するためのスイッチ［**連携用のバックグラウンド接続が［有効］です**］の位置に切り替えます。
3. 表示された［**バックグラウンド接続を有効にする**］セクションで、［**OK**］をクリックします。

Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されました。管理サーバーはバックグラウンド接続用のアカウントを作成し、このアカウントは Kaspersky Security Center Linux と別のカスペルスキー製品またはソリューション間での連携を管理するサービスアカウントとして使用されます。このサービスアカウントの名前には NWCSvcUser プレフィックスが含まれます。セキュリティの理由から、管理サーバーはサービスアカウントのパスワードを 30 日ごとに自動で変更します。サービスアカウントは手動で削除できません。管理サーバーは、サービス連携接続を無効にした際にこのアカウントを自動で削除します。管理サーバーは、それぞれの Kaspersky Security Center Web コンソールと管理コンソールに対して単一のサービスアカウントを作成し、すべてのサービスアカウントを「ServiceNwcGroup」という名前のセキュリティグループに割り当てます。管理サーバーはこのセキュリティグループを Kaspersky Security Center Linux のインストールプロセス中に自動で作成します。このセキュリティグループは手動で削除できません。

# クライアントデバイスのリモート診断

Windows ベースと Linux ベースのクライアントデバイス上での次の操作のリモート実行についてリモート診断を使用できます：

- トレースの有効化と無効化、トレースレベルの変更、トレースファイルのダウンロード
- システム情報とアプリケーション設定のダウンロード
- イベントログのダウンロード
- アプリケーションのダンプファイルの生成
- 診断の開始および診断レポートのダウンロード
- アプリケーションの起動、停止、再起動

クライアントデバイスからダウンロードしたイベントログと診断レポートを、管理者自身による問題のトラブルシューティングに活用できます。また、テクニカルサポートにお問い合わせいただいた場合、テクニカルサポートの担当者がより詳細な分析を行うために、トレースファイル、ダンプファイル、イベントログ、診断レポートをクライアントデバイスからダウンロードするように求められる場合もあります。

## リモート診断ウィンドウを開く

Windows ベースと Linux ベースのクライアントデバイスのリモート診断を実行するには、リモート診断ウィンドウを開く必要があります。

*リモート診断ウィンドウを開くには：*

1. リモート診断ウィンドウを開くデバイスを選択するには、次のいずれかを実行します：
   - デバイスが管理グループに属している場合は、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
   - デバイスが未割り当てデバイスグループに属している場合は、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**詳細**］タブをクリックします。
4. ［**詳細**］タブで、［**リモート診断**］をクリックします。
   クライアントデバイスの［**リモート診断**］ウィンドウが開きます。管理サーバーとクライアントデバイス間の接続が確立されていない場合、エラーメッセージが表示されます。

あるいは、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得する必要がある場合は、このデバイスで collect.sh スクリプトを実行できます。

# アプリケーションのトレースの有効化と無効化

Xperf トレースを含む、アプリケーションのトレースを有効または無効にできます。

## トレースの有効化および無効化

*リモートデバイスでのトレースを有効または無効にするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションリストで、トレースを有効または無効にするアプリケーションを選択します。
   リモート診断オプションのリストが表示されます。

4. トレースを有効にする場合：

   a. ［**トレース**］セクションで［**トレースを有効化**］をクリックします。

   b. ［**トレースレベルを変更**］ウィンドウで表示される設定の既定値は変更しないことを推奨します。設定値の編集が必要な場合は、テクニカルサポート担当者が必要な変更をご案内します。次の設定を使用できます：

   - **トレースレベル**

     トレースレベルでは、トレースファイルに含める情報の詳細度を指定できます。

   - **ローテーションありトレース**

     トレース情報を上書きし、トレースファイルのサイズが過剰に大きくなるの防止します。トレース情報を保存するために使用できるファイルの最大数と、各ファイルの最大サイズを指定します。トレースファイルの数が指定した最大数と同じになり、書き込み中のファイルのサイズが指定した最大サイズに達すると、新しいトレースファイルを作成できるように最も古いトレースファイルが削除されます。

     ローテーションありトレースは、Kaspersky Endpoint Security でのみ使用可能です。

   c. ［**保存**］をクリックします。

   選択したアプリケーションのトレースが有効になります。場合によっては、トレースを有効にするには、セキュリティ製品とタスクを再起動しなければならないことがあります。

   Linux ベースのクライアントデバイスでは、ネットワークエージェントコンポーネントのアップデーターのトレースは、ネットワークエージェント設定によって規制されます。したがって、Linux を実行しているクライアントデバイスでは、このコンポーネントに対して［**トレースを有効化**］および［**トレースレベルを変更**］がオフになっています。

5. 選択したアプリケーションのトレースを無効にする場合は、［**トレースを無効化**］をクリックします。

   選択したアプリケーションのトレースが無効になります。

## Xperf トレースの有効化

Kaspersky Endpoint Security では、テクニカルサポート担当者がシステムのパフォーマンス情報の Xperf トレースを有効にするようにお願いする場合があります。

*Xperf トレースを有効にして設定するか、無効にするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストから Kaspersky Endpoint Security for Windows を選択します。

   Kaspersky Endpoint Security for Windows のリモート診断オプションのリストが表示されます。

4. ［**Xperf トレース**］セクションで［**Xperf トレースを有効化**］をクリックします。

   Xperf トレースが既に有効になっている場合、［**Xperf トレースを無効化**］が代わりに表示されます。Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、このボタンをクリックしてください。

5. ［**Xperf トレースのレベルを変更**］ウィンドウが開くので、テクニカルサポート担当者からの依頼内容に応じて、次の操作を実行してください：

   a. 次のいずれかのトレースレベルを選択します：

   - **低レベル**

     この種別のトレースファイルには、システムに関する最小限の量の情報が含まれています。

     既定では、このオプションがオンです。

   - **高レベル**

     この種別のトレースファイルには*低レベル*のトレースファイルより詳細な情報が含まれています。*低レベル*のトレースファイルではパフォーマンスを十分に評価できない場合などに、テクニカルサポートの担当者から提出を求められることがあります。*高レベル*のトレースファイルには、ハードウェア、オペレーティングシステム、プロセスとアプリケーションの開始と終了のリスト、パフォーマンスの評価に使用されたイベント、Windows システム評価ツールからのイベントなどに関する情報を含む技術情報が含まれます。

   b. 次のいずれかの Xperf トレース種別を選択します：

   - **基本**

     Kaspersky Endpoint Security の動作中にトレース情報が取得されます。

     既定では、このオプションがオンです。

   - **再起動時**

     管理対象デバイスでのオペレーティングシステムの起動時にトレース情報を受信します。このトレース種別は、デバイスが起動してから Kaspersky Endpoint Security が起動するまでの間にシステムパフォーマンスに影響を与える問題が発生している場合に使用すると効果的です。

   ［**ローテーションファイルのサイズ（MB）**］を有効にし、トレースファイルのサイズが過剰に大きくなるのを防止するように依頼される場合もあります。続いて、トレースファイルの最大サイズを設定します。ファイルが指定した最大サイズに達すると、最も古いトレース情報が削除され、新しい情報が上書きされます。

   c. ローテーションするファイルサイズを定義します。

   d. ［**保存**］をクリックします。

   Xperf トレースが有効になり設定されます。

6. Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、［**Xperf トレース**］セクションの［**Xperf トレースを無効化**］をクリックしてください。

   Xperf トレースが無効になります。

# アプリケーションのトレースファイルのダウンロード

*アプリケーションのトレースファイルをダウンロードするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、トレースファイルをダウンロードするアプリケーションを選択します。
4. ［**トレース**］セクションで、［**トレースファイル**］をクリックします。
   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。
5. ダウンロードするファイルをトレースファイルのリストから選択します。
6. 次のいずれかの手順を実行します：

   - ［**ダウンロード**］をクリックして、選択したファイルをダウンロードします。ダウンロードするファイルを1つまたは複数選択できます。
   - 選択したファイルの一部をダウンロード：

     a. ［**一部をダウンロード**］をクリックします。
     複数のファイルの一部を同時にダウンロードすることはできません。複数のトレースファイルを選択すると、［**一部をダウンロード**］がオフになります。

     b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするファイルの部分を指定します。
     Linux ベースのデバイスの場合、ファイル部分名の編集は使用できません。

     c. ［**ダウンロード**］をクリックします。

選択したファイル、またはその一部が指定の場所にダウンロードされます。

# トレースファイルの削除

不要になったトレースファイルを削除することができます。

*トレースファイルを削除するには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. 表示された［モート診断］ウィンドウで、［**イベントログ**］タブを選択します。

3. ［**トレースファイル**］セクションで、削除するトレースファイルに応じて［**Windows Update ログ**］または［**リモートインストールログ**］をクリックします。

   ［**Windows Update ログ**］は、Windows ベースのクライアントデバイスでのみ使用できます。

   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。

4. 削除するファイルをトレースファイルのリストから1つまたは複数選択します。

5. ［**削除**］をクリックします。

   選択したトレースファイルが削除されます。

# アプリケーション設定のダウンロード

*クライアントデバイスからアプリケーション設定をダウンロードするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

3. ［**アプリケーション設定**］セクションで［**ダウンロード**］をクリックして、クライアントデバイスにインストールされたアプリケーションの設定に関する情報をダウンロードします。

情報を含む ZIP アーカイブが指定された場所にダウンロードされます。

# クライアントデバイスからシステム情報のダウンロード

*クライアントデバイスからアプリケーション設定をダウンロードするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. ［リモート診断］ウィンドウで［**システム情報**］タブを選択します。

3. ［**ダウンロード**］をクリックして、クライアントデバイスに関するシステム情報をダウンロードします。

   Linux ベースのデバイスに関するシステム情報を取得すると、緊急終了したアプリケーションのダンプファイルが結果のファイルに追加されます。

情報を含むファイルが指定された場所にダウンロードされます。

# イベントログのダウンロード

*リモートデバイスからイベントログをダウンロードするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウの［**イベントログ**］タブで、［**全デバイスのログ**］をクリックします。
3. ［**全デバイスのログ**］ウィンドウで、関連するログを1つまたは複数選択します。
4. 次のいずれかの手順を実行します：
   - ［**ファイル全体をダウンロード**］をクリックして、選択したログをダウンロードします。
   - 選択したログの一部をダウンロード：
     a. ［**一部をダウンロード**］をクリックします。
     複数のログの一部を同時にダウンロードすることはできません。複数のイベントログを選択すると、［**一部をダウンロード**］がオフになります。
     b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするログの部分を指定します。
     Linux ベースのデバイスの場合、ログ部分名の編集は使用できません。
     c. ［**ダウンロード**］をクリックします。

選択したイベントログ、またはその一部が指定の場所にダウンロードされます。

# アプリケーションの起動、停止、再起動

クライアントデバイス上でアプリケーションを起動、停止、再起動することができます。

*アプリケーションを起動、停止、再起動するには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、起動、停止、または再起動するアプリケーションを選択します。

4. 次のいずれかのボタンをクリックして処理を選択します：

   - **アプリケーションの停止**
     アプリケーションが現在実行されていないと、このボタンは使用できません。
   - **アプリケーションの再開**
     アプリケーションが現在実行されていないと、このボタンは使用できません。
   - **アプリケーションの開始**
     アプリケーションの実行が現在停止されていないと、このボタンは使用できません。

選択した処理に応じて、必要なアプリケーションがクライアントデバイス上で起動、停止、再起動します。

ネットワークエージェントを再起動すると、デバイスと管理サーバーとの現在の接続が失われることを伝えるメッセージが表示されます。

# Kaspersky Security Center Linux ネットワークエージェントのリモート診断を実行し、結果をダウンロードする

*リモートデバイスで Kaspersky Security Center Linux ネットワークエージェントの診断を開始し、結果をダウンロードするには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、［**Kaspersky Security Center Linux ネットワークエージェント**］を選択します。
   リモート診断オプションのリストが表示されます。

4. ［**診断レポート**］セクションで［**診断を実行**］をクリックします。
   リモート診断が開始され、診断レポートが生成されます。診断が完了すると、［**診断レポートをダウンロード**］が使用可能になります。

5. ［**診断レポートをダウンロード**］をクリックしてレポートをダウンロードします。

レポートが指定した場所にダウンロードされます。

# クライアントデバイスでのアプリケーションの実行

場合によっては、カスペルスキーサポートの担当者の指示に従って、クライアントデバイス上でアプリケーションを実行する必要があります。そのデバイスにアプリケーションをインストールする必要はありません。

クライアントデバイスでカスタムスクリプトを実行する場合は、KLACDT_SAVE_SETTING 環境変数を使用して、実行結果を保存するパスを決定できます。例：

- Windows ベースのデバイスの場合：

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Linux ベースのデバイスの場合：

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

*クライアントデバイス上でアプリケーションを実行するには：*

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブを選択します。
3. ［**オブジェクト種別**］フィールドで、アップロードするオブジェクトのタイプを選択します：
   - 実行ファイルをアップロードするには、［**ファイル**］を選択します。
   - **フォルダー**を選択して、クライアントデバイスで実行するアプリケーションを含むフォルダーをアップロードします。

     このオブジェクトタイプを選択すると、［**実行する実行ファイルの名前**］フィールドが表示されます。このフィールドに、フォルダー内の実行ファイルの名前を指定します。ファイルへの相対パスを指定することもできます。
   - ［**アーカイブ**］を選択し、クライアントデバイスで実行するアプリケーションを含む ZIP アーカイブをアップロードします。

     このオブジェクトタイプを選択すると、［**実行する実行ファイルの名前**］フィールドが表示されます。このフィールドに、フォルダー内の実行ファイルの名前を指定します。ファイルへの相対パスを指定することもできます。

     > ZIP アーカイブにはユーティリテフォルダーが含まれている必要があります。このフォルダーには、リモートデバイスで実行する実行ファイルが含まれています。
4. システムウィンドウでオブジェクトを選択するか、アップロードフィールドにドラッグして、オブジェクトをアップロードします。
5. 必要に応じて、［**コマンドラインの引数**］フィールドで、実行ファイルの実行時に渡されるコマンドライン引数を指定します。
6. ［**アップロードして実行**］をクリックして、クライアントデバイス上で選択したアプリケーションを実行します。
7. アプリケーションの実行が正常に完了したら、［**アプリケーションの実行結果をダウンロード**］をクリックして実行結果をダウンロードします。

   > アプリケーションの実行結果は、新しい診断を実行するか、ウィンドウを閉じるまで保存されます。

アプリケーションを使用したクライアントデバイスのリモート診断が完了します。

# Linux ベースのクライアントデバイスでのリモート診断の実行

Kaspersky Security Center Linux を使用すると、クライアントデバイスから基本的な診断情報をダウンロードできます。あるいは、カスペルスキーの collect.sh スクリプトを使用して、Linux ベースのデバイスに関する診断情報を取得することもできます。このスクリプトは、診断が必要な Linux ベースのクライアントデバイス上で実行され、診断情報、このデバイスのシステム情報、アプリケーションのトレースファイル、デバイスログ、および緊急終了したアプリケーションのダンプファイルを含むファイルを生成します。

collect.sh スクリプトを使用して、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得することを推奨します。Kaspersky Security Center Linux を通じて診断情報をリモートでダウンロードする場合は、リモート診断インターフェイスのすべてのセクションを実行する必要があります。また、Linux ベースのデバイスの診断情報は完全には取得されない可能性があります。

生成された診断情報を含むファイルをカスペルスキーテクニカルサポートに送信する必要がある場合は、ファイルを送信する前にすべての機密情報を削除してください。

*collect.sh スクリプトを使用して Linux ベースのクライアントデバイスから診断情報をダウンロードするには、次の手順を実行します：*

1. collect.sh スクリプトをダウンロードするアーカイブ collect.tar.gz に含まれています。
2. ダウンロードしたアーカイブを、診断する必要がある Linux ベースのクライアントデバイスにコピーします。
3. 次のコマンドを実行して、アーカイブ collect.tar.gz を解凍します：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 次のコマンドを実行して、スクリプトの実行権限を指定します：

   ```
   # chmod +x collect.sh
   ```

5. 管理者権限を持つアカウントを使用して、collect.sh スクリプトを実行します：

   ```
   # ./collect.sh
   ```

診断情報を含むファイルが生成され、フォルダー /tmp/$HOST_NAME-collect.tar.gz に保存されます。

# クライアントデバイス上のサードパーティ製品と実行ファイルの管理

このセクションでは、Kaspersky Security Center Linux の機能のうち、クライアントデバイス上で実行されるサードパーティ製品と実行ファイルの管理について説明します。

# アプリケーションコントロールを使用して実行ファイルを管理する

アプリケーションコントロールコンポーネントを使用すると、ユーザーデバイス上の実行ファイルの起動を許可またはブロックできます。アプリケーションコントロールコンポーネントは、Windows ベースおよび Linux ベースのオペレーティングシステムをサポートします。

Linux ベースのオペレーティングシステムの場合、Application Control コンポーネントは Kaspersky Endpoint Security 11.2 for Linux 以降から使用できます。

## 必須条件

- 組織内に Kaspersky Security Center Linux が導入されている。
- Kaspersky Endpoint Security for Linux または Kaspersky Endpoint Security for Windows のポリシーが作成され、有効になっている。ポリシーでアプリケーションコントロールコンポーネントが有効になっています。

## 実行するステップ

アプリケーションコントロールのユーザーシナリオは次のステップに分かれています：

1. **クライアントデバイス上の実行ファイルのリストの作成と表示**

   このステップでは、管理対象デバイスでどのような実行ファイルが検知されたかを把握できます。実行ファイルのリストを表示して、許可対象の実行ファイルと禁止対象の実行ファイルのリストと照合してください。組織の情報セキュリティポリシーに関連した制限が実行ファイルに対して必要になる場合もあります。

   実行手順の説明：クライアントデバイス上の実行ファイルのリストの取得と表示

2. **組織内で使用される実行ファイルのカテゴリを作成する**

   管理対象デバイスに保管されている実行ファイルのリストを分析します。分析に基づいて、実行ファイルのカテゴリを作成します。組織で使用される標準的な実行ファイル群をカバーする「作業用アプリケーション」カテゴリを作成することを推奨します。異なるセキュリティグループがそれぞれの業務で実行ファイルセットを使用する場合、セキュリティグループごとに別のカテゴリを作成することができます。

   アプリケーションコントロールルールのいずれにも一致しない設定の実行ファイルの起動は、コンポーネントの選択された動作モードによって規制されます：

   - *拒否リスト*：このモードは、ブロックルールで指定された実行ファイル以外のすべての実行ファイルの起動を許可する場合に使用します。既定ではこのモードが選択されます。

- *許可リスト*：このモードは、許可ルールで指定された実行ファイル以外のすべての実行ファイルの起動をブロックしたい場合に使用します。

アプリケーションコントロールルールは、実行ファイルのカテゴリを通じて実装されます。Kaspersky Security Center Linux では、実行ファイルには 3 種類のカテゴリがあります：

- 手動でコンテンツを追加するカテゴリ：ファイルのメタデータ、ハッシュコード、証明書、パスなど、実行ファイルをカテゴリに含めるための条件を指定します。
- 選択したデバイスの実行ファイルを含むカテゴリ：デバイスを指定して、デバイス上に存在する実行ファイルを自動的にカテゴリに含めます。
- 選択したフォルダーの実行ファイルを含むカテゴリ：フォルダーを指定して、フォルダー上に存在する実行ファイルを自動的にカテゴリに含めます。

**3 Kaspersky Endpoint Security ポリシーでのアプリケーションコントロール機能の設定**

上述したステージで作成したカテゴリを使用して、Kaspersky Endpoint Security for Linux ポリシー内でアプリケーションコントロール機能を設定します。

実行手順の説明：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定

**4 アプリケーションコントロール機能のテストモードでの有効化**

アプリケーションコントロールルールが業務で必要な実行ファイルをブロックしないことを確認するため、新規ルールの作成後にテストを有効にして動作を検証することを推奨します。テストモードで実行している場合、Kaspersky Endpoint Security for Windows は、アプリケーションコントロールルールで起動が禁止されている実行ファイルをブロックせず、その起動について管理サーバーに通知します。

アプリケーションコントロールルールのテストでは、次の手順の実施を推奨します：

- 必要に応じたテスト期間を指定する。必要なテスト期間は数日から 2 カ月ほどまで、ルールに応じて異なります。
- アプリケーションコントロールの動作テストによって記録されたイベントを分析する。

Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を有効にします。

**5 アプリケーションコントロールコンポーネントの設定の変更**

必要に応じて、アプリケーションコントロール設定に変更を行います。テスト結果に応じて、アプリケーションコントロールコンポーネントのイベントに関連していた実行ファイルを「手動でコンテンツを追加するカテゴリ」に追加できます。

手順：Kaspersky Security Center Web コンソール：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

**6 アプリケーションコントロールルールの実運用での適用**

アプリケーションコントロールルールのテストとカテゴリの設定が完了したら、運用モードで実際にアプリケーションコントロールルールを適用できます。

Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を無効にします。

**7 アプリケーションコントロールの設定の検証**

次の手順がすべて完了していることを確認してください：

- 実行ファイルのカテゴリを作成しました。
- カテゴリを使用してアプリケーションコントロールルールの設定します。
- アプリケーションコントロールルールの実運用での適用。

### 結果

シナリオが完了すると、管理対象デバイス上の実行ファイルの起動がコントロールされます。ユーザーは、組織で許可されている実行ファイルのみを実行することができ、組織で禁止されている実行ファイルを実行することはできません。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

## クライアントデバイス上の実行ファイルのリストの取得と表示

クライアントデバイスに保存されている実行ファイルのリストは、次のいずれかの方法で取得できます：

- Kaspersky Endpoint Security ポリシーでアプリケーションの起動に関する通知をオンにします。
- インベントリタスクを作成します。

### Kaspersky Endpoint Security ポリシーでアプリケーションの起動に関する通知をオンにする

*アプリケーションの開始に関する通知を有効にするには：*

1. Kaspersky Endpoint Security のポリシー設定を開き、［**全般設定**］→［**レポートとストレージ**］に移動します。
2. ［**管理サーバーへのデータ転送**］設定グループで、［**起動したアプリケーションについて**］をオンにして、変更を保存します。

ユーザーが実行ファイルを起動しようとすると、これらのファイルに関する情報がクライアントデバイス上の実行ファイルのリストに追加されます。Kaspersky Endpoint Security はこの情報をネットワークエージェントに送信し、ネットワークエージェントはそれを管理サーバーに送信します。

### インベントリタスクの作成

Kaspersky Endpoint Security for Linux のバージョン 11.2 以降では、実行ファイルのインベントリ機能を使用できます。

インストールされているアプリケーションに関する情報を取得しながらデータベースの負荷を軽減できます。定義データベース容量を節約するには、ソフトウェアの標準セットがインストールされている参照デバイスでインベントリタスクを実行してください。推奨されるデバイス数は、1～3 台です。

*クライアントデバイス上の実行ファイルのインベントリタスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ［**新規タスク設定**］ページの［**アプリケーション**］ドロップダウンリストで、クライアントデバイスのオペレーティングシステムの種別に応じて Kaspersky Endpoint Security for Linux または Kaspersky Endpoint Security for Windows を選択します。
4. ［**タスク種別**］ドロップダウンリストから、［**インベントリ**］を選択します。
5. ［**タスク作成の終了**］ページで、［**終了**］をクリックします。

新規タスクウィザードの終了後、指定した設定で**インベントリ**タスクが作成されます。必要に応じて、作成したタスクの設定を編集できます。作成したタスクはタスクリストに表示されます。

インベントリタスクの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

**インベントリ**タスクの実行が完了すると、管理対象デバイス上に保管された実行ファイルのリストが作成され、このリストを表示できるようになります。

インベントリ中に、次の形式の実行ファイルを検出できます（インベントリタスクのプロパティで選択したオプションによって変わります）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR、HTML。

## 管理対象デバイスに保管されている実行ファイルのリストを表示する

*クライアントデバイス上に保管された実行ファイルのリストを表示するには：*

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に選択します。

クライアントデバイス上に保管された実行ファイルのリストが表示されます。

必要に応じて、管理対象デバイスの実行ファイルを、Kaspersky Security Center Web コンソールが開いているデバイスに送信できます。

*実行ファイルを送信するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に選択します。
2. 送信する実行ファイルのリンクをクリックします。

3. 表示されたウィンドウで、［**デバイス**］セクションに移動し、実行ファイルの送信元の管理対象デバイスのチェックボックスをオンにします。

実行ファイルを送信する前に、［**管理サーバーから切断しない**］にして管理対象デバイスが管理サーバーに直接接続されていることを確認してください。

4. ［**送信**］をクリックします。

選択した実行ファイルがダウンロードされ、Kaspersky Security Center Web コンソールが開いているデバイスに送信されます。

# コンテンツが手動で追加されるアプリケーションカテゴリの作成

組織内で起動を許可またはブロックする実行ファイルのテンプレートとしての条件を、単独でまたは組み合わせて指定できます。一定の条件に一致する実行ファイルをまとめて管理するために、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

*コンテンツが手動で追加されるアプリケーションカテゴリを作成するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**S］→［**アプリケーションカテゴリ**］の順に選択します。

アプリケーションカテゴリのリストが表示されます。

2. ［**追加**］をクリックします。

新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリの作成方法の選択**］ステップで、アプリケーションカテゴリ名を指定して、［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択します。

4. ［**条件**］ステップで［**追加**］をクリックして、作成中のカテゴリに含めるファイルの条件を追加します。

5. ［**条件の基準**］ステップで、カテゴリを作成するルールの種別をリストから選択します：

- **KL カテゴリから選択**

  このオプションをオンにすると、カスペルスキー製品のカテゴリを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。指定したカスペルスキー製品カテゴリのアプリケーションが、アプリケーションカテゴリに追加されます。

- **リポジトリから証明書を選択**

  このオプションをオンにすると、保管領域の証明書を指定できます。カテゴリ条件は、指定された証明書によって署名された実行ファイルのみに一致します。

- **アプリケーションのパスを指定（マスクをサポート）**

  このオプションをオンにすると、クライアントデバイス上のフォルダーのパスを指定できます。そのフォルダーに含まれる実行ファイルが、アプリケーションカテゴリに追加されます。

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを実行するメディアの種別（任意のドライブまたはリムーバブルドライブ）を指定できます。指定した種別のドライブ上で実行されたアプリケーションが、アプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルリストから選択**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストを使用して、アプリケーションを選択してカテゴリに追加できます。

  - **アプリケーションレジストリから選択**

このオプションをオンにすると、アプリケーションレジストリが表示されます。レジストリからアプリケーションを選択すると、選択したアプリケーションのメタデータが入力されたパラメータを含むウィンドウが開きます：

- ファイル名。
- ファイルバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
- アプリケーション名。
- アプリケーションのバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
- 製造元。

指定したパラメータを満たす実行ファイルの起動のみがブロックされ、選択したアプリケーションの起動はブロックされないことに注意してください。選択したアプリケーションメタデータが、アプリケーションの起動時に起動される実行ファイルのメタデータと一致する場合は、次の手順に進むことができます。それ以外の場合は、実行ファイルのメタデータと一致するように値を手動で変更する必要があります。

- **手動で指定**

このオプションをオンにした場合、ファイルのハッシュ、メタデータ、証明書のいずれかを、アプリケーションカテゴリにアプリケーションを追加する条件として指定する必要があります。

**ファイルのハッシュ**

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバー定義データベースに保存されます。

暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。Kaspersky Endpoint Security for Linux は、SHA256 コンピューティングをサポートしています。

カテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security for Linux である場合は、［**SHA256**］をオンにします。
- Kaspersky Endpoint Security for Windows を使用する場合にのみ、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

**メタデータ**

このオプションをオンにすると、ファイル名、バージョン、製造元などのファイルのメタデータを指定できます。カテゴリ条件は、同じメタデータを持つ実行ファイルのみに一致します。

**証明書**

このオプションをオンにすると、保管領域の証明書を指定できます。カテゴリ条件は、指定された証明書によって署名された実行ファイルのみに一致します。

- **アーカイブフォルダーから選択**

このオプションをオンにすると、アーカイブフォルダーのファイルを指定でき、ユーザーカテゴリにアプリケーションを追加するために使用する条件を選択できます。アーカイブフォルダーが解凍され、選択した条件がフォルダー内にあるファイルに適用されます。条件として、以下の基準のいずれかを選択することができます：

- **ファイルのハッシュ**

  MD5 または SHA256 のどちらを使用してハッシュ値を計算するかを選択します。アーカイブフォルダーにあるファイルとハッシュ値が同じであるアプリケーションが、アプリケーションカテゴリに追加されます。

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、MD5 ハッシュ関数を選択します。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

- **メタデータ**

  基準として使用するメタデータを選択します。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

- **証明書**

  基準として使用する証明書のプロパティ（証明書の発行先、フィンガープリント、発行元）を選択します。同じプロパティを持つ証明書で署名された実行ファイルはユーザーカテゴリに追加されます。

このオプションをオンにすると、アーカイブフォルダーのファイルを指定でき、ユーザーカテゴリにアプリケーションを追加するために使用する条件を選択できます。アーカイブフォルダーが解凍され、選択した条件がフォルダー内にあるファイルに適用されます。条件として、以下の基準のいずれかを選択することができます：

- **ファイルのハッシュ**

  MD5 または SHA256 のどちらを使用してハッシュ値を計算するかを選択します。アーカイブフォルダーにあるファイルとハッシュ値が同じであるアプリケーションが、アプリケーションカテゴリに追加されます。

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、MD5 ハッシュ関数を選択します。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

- **メタデータ**

  基準として使用するメタデータを選択します。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

- **証明書**

  基準として使用する証明書のプロパティ（証明書の発行先、フィンガープリント、発行元）を選択します。同じプロパティを持つ証明書で署名された実行ファイルはユーザーカテゴリに追加されます。

選択した基準が、条件のリストに追加されます。

アプリケーションカテゴリの作成基準は、個数の制限なく必要な数だけ追加できます。

6. ［**除外**］ステップで［**追加**］をクリックして、作成中のカテゴリから除外するファイルの条件を追加します。

7. ［**条件の基準**］ステップで、カテゴリ作成用のルールの種別を選択したときと同様に、リストからルールの種別を選択します。

ウィザードを最後まで完了すると、アプリケーションカテゴリが作成されます。新しいルールがアプリケーションカテゴリのリストに表示されます。アプリケーションコントロールを設定時に作成したアプリケーションカテゴリを使用できます。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# 選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成

選択したデバイス上に存在する実行ファイルを、許可またはブロックする実行ファイルのテンプレートとして使用できます。選択したデバイス上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

次の前提条件が満たされていることを確認してください：

- Kaspersky Endpoint Security ポリシーでアプリケーションコントロールコンポーネントが有効になっています。
- 管理対象デバイスに保存されている実行ファイルのリストが取得されました。

*選択したデバイスの実行ファイルを含むアプリケーションカテゴリを作成するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

   実行ファイルのカテゴリのリストを含むページが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. **カテゴリの作成方法の選択**ステップで、カテゴリ名を指定し、**選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**オプションに追加されます。

4. ［**追加**］をクリックします。

5. 表示されるウィンドウで、アプリケーションカテゴリの作成に実行ファイルを使用するデバイスを選択します。

6. 次の設定を指定します：

- **ハッシュ値計算アルゴリズム**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバー定義データベースに保存されます。

  暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。Kaspersky Endpoint Security for Linux は、SHA256 コンピューティングをサポートしています。

  カテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のオプションを選択します：

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security for Linux である場合は、［**SHA256**］をオンにします。

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

  既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

  ［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **データを管理サーバーのリポジトリと同期**

  指定したフォルダーでの変更内容を管理サーバーに定期的にチェックさせる場合は、このオプションを使用します。

  既定では、このオプションはオフです。

  このオプションをオンにする場合、指定したフォルダーでの変更内容をチェックする間隔（時間単位）を指定します。既定の間隔は 24 時間です。

- **ファイル種別**

  このセクションでは、アプリケーションカテゴリを作成するのに使用するファイルの種別を指定できます。

  **すべてのファイル**：カテゴリの作成時にすべてのファイルが使用されます。既定では、このオプションがオンです。

  **アプリケーションカテゴリ以外のファイルのみ**：カテゴリの作成時に、アプリケーションカテゴリ以外のファイルのみが使用されます。

- **フォルダー**

このセクションでは、選択したデバイス上で、アプリケーションカテゴリを作成するのに使用するファイルが含まれているフォルダーを指定できます。

**すべてのフォルダー**：カテゴリの作成時にすべてのフォルダーのファイルが使用されます。既定では、このオプションがオンです。

**指定フォルダー**：カテゴリの作成時に指定したフォルダーのファイルのみが使用されます。このオプションをオンにする場合、フォルダーのパスを指定する必要があります。

ウィザードが終了すると、実行ファイルのカテゴリが作成されます。カテゴリーのリストに表示されます。作成したカテゴリは、アプリケーションコントロールの設定時に使用できます。

# 選択したフォルダーの実行ファイルを含むアプリケーションカテゴリの作成

選択したフォルダー上に存在する実行ファイルを、組織内で許可またはブロックする実行ファイルの条件として使用できます。選択したフォルダー上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

*選択したフォルダーの実行ファイルを含むカテゴリを作成するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に移動します。

   カテゴリー覧のページが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリの作成方法の選択**］ステップで、カテゴリ名を指定して［**特定のフォルダーの実行ファイルを含むカテゴリ：指定されたフォルダーにコピーされたアプリケーションの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］を選択します。

4. カテゴリの作成に使用される実行ファイルのフォルダーを指定します。

5. 次の設定を定義します：

- **ダイナミックリンクライブラリ（DLL）をこのカテゴリに含める**

  アプリケーションカテゴリにはダイナミックリンクライブラリ（DLL 形式のファイル）が含まれ、アプリケーションコントロールコンポーネントでは、システムで実行されているそのようなライブラリの処理を記録します。このカテゴリに DLL ファイルを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

  既定では、このチェックボックスはオフです。

- **このカテゴリ内のスクリプトデータを含める**

  アプリケーションカテゴリにはスクリプトのデータが含まれ、ウェブ脅威対策によってスクリプトはブロックされません。このカテゴリにスクリプトデータを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

  既定では、このチェックボックスはオフです。

- **ハッシュ値計算アルゴリズム**：**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）/ このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバー定義データベースに保存されます。

  暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。Kaspersky Endpoint Security for Linux は、SHA256 コンピューティングをサポートしています。

  カテゴリ内のファイルに、Kaspersky Security Center Linux によるハッシュ値計算のオプションを選択します：

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security for Linux である場合は、［**SHA256**］をオンにします。

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

  既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

  ［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **変更のあったフォルダーを強制スキャンする**

このオプションを有効にすると、カテゴリコンテンツ追加のフォルダーでの変更が定期的にチェックされます。チェックボックスに隣接する入力フィールドで、チェックの頻度を時間単位で指定できます。既定では、24 時間ごとに強制的にチェックされます。

このオプションを無効にすると、フォルダーが強制的にチェックされることはありません。ファイルの修正、追加または削除があった場合、サーバーはそのファイルにアクセスを試みます。

既定では、このオプションはオフです。

ウィザードが終了すると、実行ファイルのカテゴリが作成されます。カテゴリーのリストに表示されます。カテゴリはアプリケーションコントロールの設定で使用できます。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# アプリケーションカテゴリのリストの表示

設定された実行ファイルのカテゴリと各カテゴリの設定の一覧を表示できます。

*アプリケーションカテゴリのリストを表示するには：*

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

カテゴリー覧のページが表示されます。

*アプリケーションカテゴリのプロパティを表示するには、*

カテゴリの名前をクリックします。

カテゴリのプロパティウィンドウが表示されます。プロパティはいくつかのタブにグループ化されています。

# イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

Kaspersky Endpoint Security のポリシーでアプリケーションコントロールの設定が完了すると、イベントのリストに次のイベントが表示されます：

- **アプリケーションの起動が禁止されました**（*緊急*イベント）：このイベントは、アプリケーションコントロールの設定で、実際にルールを適用するように指定した場合に表示されます。
- **アプリケーションの起動がテストモードでブロックされています**（*情報*イベント）：このイベントは、アプリケーションコントロールの設定で、ルールをテストするように指定した場合に表示されます。
- **アプリケーションの起動禁止に関する管理者へのメッセージ**（*警告*イベント）。このイベントは、アプリケーションコントロールの設定で実際にルールを適用するように指定しており、起動時にブロックされたアプリケーションへのアクセスをユーザーが要求した場合に表示されます。

アプリケーションコントロールの動作に関するイベントを表示するために、イベントの抽出を作成しておくことを推奨します。

アプリケーションコントロールイベントの対象となった実行ファイルを、既存のアプリケーションカテゴリや新規に作成するアプリケーションカテゴリに追加できます。実行ファイルは、手動でコンテンツを追加するタイプのアプリケーションカテゴリにのみ追加できます。

*アプリケーションコントロールイベントの対象となった実行ファイルをアプリケーションカテゴリに追加するには：*

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

   イベントの抽出のリストが表示されます。

2. アプリケーションコントロールに関するイベントを表示するためのイベントの抽出を選択し、イベントの抽出を実行します。

   アプリケーションコントロールに関するイベントを表示するためのイベントの抽出をまだ作成していない場合は、代わりに「**最近のイベント**」などの事前定義済みのイベントの抽出を選択して実行することもできます。

   イベントのリストが表示されます。

3. 対象となった実行ファイルをアプリケーションカテゴリに追加するイベントを選択し、［**カテゴリへ割り当て**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードのウィンドウで、関連する設定を指定します：

- ［**イベントに関係する実行ファイルへの処理**］セクションで、次のいずれかのオプションをオンにします：

  - **新規アプリケーションカテゴリへ追加**

    イベントに関連する実行ファイルを元に新しいアプリケーションカテゴリを作成する場合は、このオプションをオンにします。

    既定では、このオプションがオンです。

    このオプションを選択する場合は、新しいカテゴリ名を指定してください。

  - **アプリケーションカテゴリへ追加**

    イベントに関連する実行ファイルを既存のアプリケーションカテゴリに追加する場合は、このオプションをオンにします。

    既定では、このオプションはオフです。

    このオプションを選択する場合は、実行ファイルの追加先として、手動でコンテンツを追加するタイプのアプリケーションカテゴリを選択してください。

- ［**ルールの種別**］セクションで、次のいずれかを選択します：

  - **除外しない場合のルール**
  - **除外に追加する場合のルール**

- ［**条件として使用する情報**］セクションで、次のいずれかのオプションをオンにします：

  - **証明書の詳細情報（証明書がないファイルの場合 SHA256 ハッシュ）**

    ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

    それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

    実行ファイルの証明書の詳細（または証明書がないファイルの SHA256 ハッシュ機能）をカテゴリルールに追加する場合は、このオプションを選択します。

    既定では、このオプションがオンです。

  - **証明書の詳細情報（証明書のないファイルはスキップ）**

ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

実行ファイルの証明書の詳細をカテゴリルールに追加する場合は、このオプションを選択します。実行ファイルに証明書がない場合、そのファイルはスキップされます。このファイルに関する情報は、カテゴリに追加されません。

- **SHA256 のみ（ハッシュのないファイルはスキップ）**

  それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの SHA256 ハッシュ機能の詳細だけを追加する場合、このオプションをオンにします。

- **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

  Kaspersky Endpoint Security for Windows を使用する場合にのみ、このオプションを選択します。Kaspersky Endpoint Security for Linux は、MD5 ハッシュ関数をサポートしません。

  それぞれのファイルには固有の MD5 ハッシュ関数があります。MD5 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

5. ［**OK**］をクリックします。

ウィザードが完了すると、アプリケーションコントロールのイベントに関連付けられていた実行ファイルが、既存のアプリケーションカテゴリまたは新規に作成したアプリケーションカテゴリに追加されます。変更または新規に作成したアプリケーションカテゴリの設定を表示できます。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定

アプリケーションカテゴリの作成が完了すると、Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロールの設定時にこれらのカテゴリを使用できます。

*Kaspersky Endpoint Security for Windows ポリシーでアプリケーションコントロール機能を設定するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
   ポリシーのリストが表示されます。

2. **Kaspersky Endpoint Security for Windows** のポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。

3. ［**アプリケーション設定**］→［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に移動します。
   ［**アプリケーションコントロール**］ウィンドウでアプリケーションコントロール設定が表示されます。

4. ［**アプリケーションコントロール**］は既定でオンになっています。［**アプリケーションコントロールは無効です**］スイッチを切り替えて、オプションをオフにします。

5. ［**Application Control Settings**］設定で、動作モードを有効にしてアプリケーションコントロールルールを適用し、Kaspersky Endpoint Security for Windows がアプリケーションの起動をブロックできるようにします。
   アプリケーションコントロールルールをテストする場合は、［**アプリケーションコントロール設定**］セクションでテストモードを有効にします。テストモードでは、Kaspersky Endpoint Security for Windows はアプリケーションの起動をブロックしませんが、適用されたルールに関する情報をレポートに記録します。［**レポートの表示**］をクリックすると、この情報を表示できます。

6. Kaspersky Endpoint Security for Windows で、ユーザーがアプリケーションを起動したときの DLL モジュールの読み込みを監視する場合は、［**DLL モジュールの読み込みを管理**］をオンにします。
   モジュールに関する情報とモジュールを読み込んだアプリケーションに関する情報がレポートに保存されます。
   Kaspersky Endpoint Security for Windows は、［**DLL モジュールの読み込みを管理**］がオンになった後に読み込まれた DLL モジュールとドライバーのみを監視します。Kaspersky Endpoint Security for Windows の起動前に読み込まれていた DLL モジュールとドライバーも含めてすべての DLL モジュールとドライバーを監視する場合、［**DLL モジュールの読み込みを管理**］をオンにした後にデバイスを再起動してください。

7. （省略可能な手順）［**メッセージのテンプレート**］セクションで、アプリケーションの起動がブロックされたときに表示されるメッセージのテンプレートとお手元に送信されるメッセージのテンプレートを編集できます。

8. ［**アプリケーションコントロールモード**］設定で、［**拒否リスト**］モードまたは［**許可リスト**］モードを選択します。
   既定では、［**拒否リスト**］モードが選択されています。

9. ［**ルールリストの設定**］をクリックします。
   ［**拒否リストと許可リスト**］ウィンドウで、アプリケーションカテゴリを追加できます。既定では、［**拒否リスト**］モードをオンにするとは［**拒否リスト**］タブが選択され、［**許可リスト**］モードをオンにするとは［**許可リスト**］タブが選択されます。

10. ［**拒否リストと許可リスト**］ウィンドウで［**追加**］をクリックします。
    ［**アプリケーションコントロールルール**］ウィンドウが表示されます。

11. ［**カテゴリを選択してください**］をクリックします。
    ［**アプリケーションカテゴリ**］ウィンドウが開きます。

12. 作成済みのアプリケーションカテゴリを追加します。

［**編集**］をクリックすると、作成済みのカテゴリの設定を編集できます。

新しいカテゴリを作成するには、［**追加**］をクリックします。

リストからカテゴリを削除するには、［**削除**］をクリックします。

13. アプリケーションカテゴリのリストの編集が完了したら、［**OK**］をクリックします。

［**アプリケーションカテゴリ**］ウィンドウが閉じます。

14. ［**アプリケーションコントロール**ルール］ウィンドウの［**オブジェクトとその権限**］セクションで、アプリケーションコントロールルールを適用するユーザーとユーザーのグループのリストを作成します。

15. ［**OK**］をクリックして、設定を保存し［**アプリケーションコントロールルール**］ウィンドウを閉じます。

16. ［**OK**］をクリックして、設定を保存し［**拒否リストと許可リスト**］ウィンドウを閉じます。

17. ［**OK**］をクリックし、設定を保存して［**アプリケーションコントロール**］ウィンドウを閉じます。

18. Kaspersky Endpoint Security for Windows ポリシー設定のウィンドウを閉じます。

アプリケーションコントロールの設定が適用されます。ポリシーのクライアントデバイスへの適用が完了すると、実行ファイルの起動が管理されるようになります。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# クライアントデバイスにインストールされているアプリケーションのリストの取得と表示

Kaspersky Security Center Linux は、Linux または Windows を実行している管理対象クライアントデバイスにインストールされているすべてのソフトウェアのインベントリを作成します。

ネットワークエージェントが、デバイスにインストールされているアプリケーションのリストを作成し、管理サーバーに送信します。ネットワークエージェントがアプリケーションリストを更新するには約 10 ～ 15 分かかります。

Windows ベースのクライアントデバイスの場合、ネットワークエージェントは、インストールされているアプリケーションに関する大部分の情報を Windows レジストリから受け取ります。Linux ベースのクライアントデバイスの場合、パッケージマネージャーはインストールされているアプリケーションに関する情報をネットワークエージェントに提供します。

*管理対象デバイスにインストールされているアプリケーションのリストを表示するには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。

   このページでは、管理対象デバイスにインストールされているアプリケーションが表形式で表示されます。アプリケーションを選択して、そのプロパティ（ベンダー名、バージョン番号、実行ファイルのリスト、アプリケーションがインストールされたデバイスのリストなど）を表示します。

2. インストールされたアプリケーションの表のデータは、次のようにしてグループ化およびフィルタリングできます：

   - 表の右上隅にある設定アイコン（ ）をクリックします。

     呼び出された［**列の設定**］メニューで、表に表示する列を選択します。アプリケーションがインストールされたクライアントデバイスのオペレーティングシステムの種別を表示するには、［**OS の種別**］列を選択します。

   - 表の右上隅にあるフィルターアイコン（ ）をクリックして、呼び出されたメニューでフィルター条件を指定して適用します。

     インストールされているアプリケーションをフィルタリングした表が表示されます。

*特定の管理対象デバイスにインストールされているアプリケーションのリストを表示するには：*

メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**<デバイス名>**］→［**詳細**］→［**アプリケーションレジストリ**］の順に移動します。このメニューで、アプリケーションのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。

アプリケーションコントロールの詳細は、Kaspersky Endpoint Security for Linux のヘルプおよび Kaspersky Endpoint Security for Windows のヘルプを参照してください。

# サードパーティ製品について

Kaspersky Security Center Linux を使用してクライアントデバイスにインストールされたサードパーティ製のソフトウェアをアップデートしたり脆弱性を修正したりできます。Kaspersky Security Center Linux はサードパーティ製ソフトウェアを最新バージョンにのみアップデートします。

> サードパーティ製ソフトウェアのリストは変更可能であり、動的にアップデートされます。ユーザーのデバイスにインストールされたサードパーティ製ソフトウェアを Kaspersky Security Center Linux で適用可能なアップデートがあるかどうかは Kaspersky Security Center Web コンソールで使用可能なアップデートのリストで確認できます。

以下に概説する手順は、Kaspersky Security Center Linux でアップデートできるサードパーティ製ソフトウェアのリストを表示することのみを目的としています。タスクを開始せずに関連情報にアクセスするには、次の手順を実行します。

*Kaspersky Security Center Linux でアップデートできるサードパーティ製ソフトウェアのリストを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［ **タスク**］の順に移動します。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの［**新規タスク設定**］ステップで、次の設定を指定します：

   a. **アプリケーション**ドロップダウンリストで、［**Kaspersky Security Center Linux**］を選択します。

   b. **タスク種別**フィールドで、**アップデートのインストールと脆弱性の修正**を選択します。

4. ウィザードの［**タスク範囲**］ステップで、［**管理対象デバイス**］をオンにします。

5. ウィザードの**アップデートのインストールのルールを指定します**手順で、**追加**ボタンをクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

6. ウィザードの**ルールの種別の選択**手順で、**サードパーティ製品のアップデートのルール**オプションを選択します。

7. ウィザードの「**一般基準**」手順で、**（拒否されたもの以外の）すべてのアップデートをインストール**オプションを選択し、**次へ**をクリックします。

サードパーティ製ソフトウェアのリストが表示されます。

# サードパーティ製ソフトウェアのアップデートのインストール

Kaspersky Security Center Linux では、管理対象デバイスにインストールされているサードパーティ製ソフトウェアのアップデートを管理し、必要なアップデートをインストールしてソフトウェアの脆弱性を修正できます。

Kaspersky Security Center Cloud Linux は、*脆弱性とアプリケーションのアップデートの検索*タスクでアップデートを検索します。タスクが完了すると、管理サーバーはタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。適用可能なアップデートの情報を確認した後、アップデートをデバイスにインストールできます。

Kaspersky Security Center Linux はいくつかのアプリケーションについて、古いバージョンを削除して新しいバージョンをインストールしてアップデートします。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

サードパーティ製ソフトウェアのアップデートのメタデータがリポジトリにダウンロードされると、*アップデートのインストールと脆弱性の修正*タスクを使用してクライアントデバイスにアップデートをインストールできます。

> *アップデートのインストールと脆弱性の修正*タスクは、脆弱性とパッチ管理機能のライセンスをお持ちの場合にのみ作成できます。

このタスクが完了すると、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートのメタデータが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center Linux はそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にダウンロードされてインストールされます。

# シナリオ：サードパーティ製ソフトウェアのアップデート

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアをアップデートするシナリオについて説明します。「サードパーティ製ソフトウェア」とは、他のソフトウェアベンダーが提供しているアプリケーションを指します。

## 必須条件

サードパーティ製ソフトウェアのアップデートをインストールするには、管理サーバーをインターネットに接続する必要があります。

## 実行するステップ

サードパーティ製ソフトウェアのアップデートは段階的に進行します：

1. **必要なアップデートの検索**

   管理対象デバイスに必要なサードパーティ製ソフトウェアのアップデートを検索するには、[*脆弱性とアプリケーションのアップデートの検索*] タスクを実行します。タスクが完了すると、Kaspersky Security Center Linux はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   *脆弱性とアプリケーションのアップデートの検索*タスクは、管理サーバークイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前に*脆弱性とアプリケーションのアップデートの検索タスクを作成*するか、クイックスタートウィザードを実行してください。

   > *脆弱性とアプリケーションのアップデートの検索*タスクは、Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこのタスクを作成することはできません。

2. **検出されたアップデートのリストの表示**

   使用可能なサードパーティ製ソフトウェアのアップデートに関する情報を表示し、インストールするアップデートを決定します。それぞれのアップデートの詳細情報を確認するには、リスト内のアップデートの名前をクリックします。リスト内のそれぞれのアップデートについて、クライアントデバイスへのアップデートのインストールに関する統計情報を表示することもできます。

3. **アップデートのインストールの設定**

Kaspersky Security Center Linux でサードパーティ製ソフトウェアのアップデートのリストの取得が完了すると、*アップデートのインストールと脆弱性の修正*タスクを作成して、クライアントデバイスにアップデートをインストールできます。

> *アップデートのインストールと脆弱性の修正*タスクは、Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこのタスクを作成することはできません。

*アップデートのインストールと脆弱性の修正*タスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。*アップデートのインストールと脆弱性の修正*タスクは、脆弱性とパッチ管理機能のライセンスをお持ちの場合にのみ作成できることに注意してください。

一部のソフトウェアのアップデートのインストールでは、インストールするために使用許諾契約書（EULA）に同意する必要があります。使用許諾契約書に同意しない場合、アップデートはインストールされません。

アップデートのインストールタスクをスケジュールを指定して開始できます。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

### 4 タスクのスケジュール設定

アップデートのリストを最新の状態に維持するため、*脆弱性とアプリケーションのアップデートの検索*タスクが定期的に自動で実行されるようにスケジュールを指定してください。既定では、*脆弱性とアプリケーションのアップデートの検索*タスクは手動で開始するように設定されています。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。

タスクのスケジュールを指定する場合は、*脆弱性とアプリケーションのアップデートの検索*タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

### 5 サードパーティ製ソフトウェアのアップデートの承認と拒否（任意）

*アップデートのインストールと脆弱性の修正*タスクを作成している場合は、タスクのプロパティウィンドウでアップデートのインストールルールを指定できます。

それぞれのルールで、アップデートの次のようなステータスに応じて、インストールするアップデートを指定できます。*未定義*、*承認*、*承認却下*。たとえば、サーバー向けのタスクとして特定のタスクを作成し、*承認*ステータスのアップデートのインストールのみを許可するようにルールを設定したタスクを設定するなどの使用方法が考えられます。この場合、インストールするアップデートに手動で*承認*ステータスを設定します。このように設定すると、ステータスが*未定義*または*承認却下*のアップデートは、タスクでインストール先に指定したサーバーにインストールされません。

アップデートのインストールを管理するための*承認*ステータスの使用は、アップデートの数が少ない場合に効率的です。複数のアップデートをインストールするには、*アップデートのインストールと脆弱性の修正*タスクで設定できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、*承認*ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、管理サーバーが過負荷になる可能性があります。

既定では、ダウンロードされたソフトウェアアップデートのステータスは*未定義*です。［**ソフトウェアのアップデート**］リストで、アップデートのステータスを*承認*または*承認却下*に変更できます（［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動して操作）。

詳細については、サードパーティのソフトウェアアップデートの承認と拒否に関する手順を参照してください。

### 6 アップデートのインストールタスクの実行

*アップデートのインストールと脆弱性の修正*タスクを開始します。このタスクを開始すると、管理対象デバイスにアップデートがダウンロードされインストールされます。タスクが完了したら、タスクリストでのタスクのステータスが*正常終了*になっていることを確認します。

**7 アップデートのインストール結果に関するレポートの作成（任意）**

アップデートのインストールに関する詳細な統計情報を確認するには、サードパーティ製ソフトウェアのアップデートのインストール結果に関するレポートを作成します。

### 結果

*アップデートのインストールと脆弱性の修正*タスクを作成、設定した場合は、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center Linux はそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にインストールされます。

## サードパーティのソフトウェアアップデートのインストールオプション

*アップデートのインストールと脆弱性の修正*タスクを作成して実行することで、管理対象デバイスにサードパーティのソフトウェアアップデートプログラムと Windows Update からのアップデートプログラムをインストールできます。［*アップデートのインストールと脆弱性の修正*］タスクは、脆弱性とパッチ管理機能のライセンスをお持ちの場合にのみ作成できます。このタスクを使用して、他のベンダーの製品のアップデートプログラムをインストールできます。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

オプションとして、次の方法で必要なアップデートをインストールするタスクを作成できます：

- アップデートリストを開き、インストールするアップデートを指定する。

  その結果、選択したアップデートをインストールする新しいタスクが作成されます。オプションとして、選択したアップデートを既存のタスクに追加できます。

- アップデートのインストールウィザードを実行する。

  アップデートのインストールウィザードの機能は、脆弱性とパッチ管理ライセンスがある場合にのみ使用できます。

  このウィザードを使用すると、アップデートのインストールタスクの作成と設定手順が簡略化され、インストールするもののと同じアップデートで構成される冗長なタスクを作成せずに済みます。

# アップデートリストを使用してサードパーティ製ソフトウェアのアップデートをインストールする

*アップデートのリストを使用して、サードパーティ製ソフトウェアのアップデートをインストールするには：*

1. 次のいずれかのパスを使用して、アップデートプログラムのリストを開きます。

   - ［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］。
   - ［**アセット（デバイス）**］→［**管理対象デバイス**］→［<デバイス名>］→［**詳細**］→［**適用可能なアップデート**］。
   - ［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［<アプリケーション名>］→［**適用可能なアップデート**］。

   適用可能なアップデートのリストが表示されます。

2. インストールするアップデートに隣接するチェックボックスをオンにします。

3. ［**アップデートのインストール**］をクリックします。このボタンが表示されない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから［**アップデートのインストール**］を選択します。

   インストールするソフトウェアのアップデートによっては、使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、ソフトウェアのアップデートはインストールされません。

4. 次のいずれかのオプションをオンにします：

   - **新規タスク**

     新規タスクウィザードが起動します。脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクが事前選択されています。ウィザードの手順に従って、タスクの作成を完了します。

   - **アップデートのインストール（指定したタスクにルールを追加）**

     選択したアップデートを追加するタスクを選択します。脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクを選択します。選択したアップデートをインストールするための新しいルールが、選択したタスクに自動的に追加されます。選択したアップデートがタスクのプロパティに追加されます。

     タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

   新規タスクの作成を選択した場合は、新規タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。既存のタスクにアップデートを追加することを選択した場合、アップデートはタスクのプロパティに保存されます。

サードパーティ製ソフトウェアのアップデートプログラムをインストールするには、*アップデートのインストールと脆弱性の修正*タスクを開始する必要があります。このタスクを開始するには、タスクリストの［**開始**］をクリックするか、開始するタスクのプロパティでスケジュール設定を指定します。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

# アップデートのインストールウィザードを使用してサードパーティ製ソフトウェアのアップデートをインストールする

アップデートのインストールウィザードの機能は、脆弱性とパッチ管理ライセンスがある場合にのみ使用できます。

*アップデートのインストールウィザードを使用して、サードパーティ製ソフトウェアのアップデートをインストールするタスクを作成するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. インストールするアップデートに隣接するチェックボックスをオンにします。
3. ［**アップデートのインストールウィザードを実行**］をクリックします。
   アップデートのインストールウィザードが起動します。［**アップデートのインストールタスクを選択する**］ページには、次の種別の既存の全タスクのリストが表示されます。
   - *アップデートのインストールと脆弱性の修正*
   - *脆弱性の修正*

4. 選択したアップデートをインストールするタスクのみをウィザードに表示するには、［**このアップデートをインストールするタスクのリストを表示**］をオンにします。

5. 目的の対象を追加します：

- 既存のタスクを開始するには、*アップデートのインストールと脆弱性の修正*タスクの横にあるチェックボックスをオンにし、［**開始**］をクリックします。

  タスクはバックグラウンドモードで完了します。追加の操作は必要ありません。

- 既存のタスクに新しいルールを追加するには：

  a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。

  > 複数のタスクを選択した場合、［**ルールの追加**］は無効になります。

  *脆弱性の修正*タスクのルールを追加することはできません。*脆弱性の修正*タスクを選択した場合、次の通知が表示されます。「*アップデートをインストールするには、「アップデートのインストールと脆弱性の修正」タスクを使用します。*」

  b. ウィザードの「**アップデートのインストールルールを作成する**」手順で、新しいルールを設定します。

  - **この重要度レベルのアップデートのインストールルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

    選択したアップデートの重要度が*不明*の場合、このルールは表示されません。

  - **MSRC に基づく重要度レベルのアップデートのインストールルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

このルールは、Microsoft ソフトウェアのアップデートに対してのみ表示されます。選択したアップデートの重要度が*不明*の場合は表示されません。

- **この製造元によるアップデートのインストールルール**

  このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Center Linux は、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

  既定では、このオプションはオフです。

  このルールは、サードパーティのソフトウェアアップデートに対してのみ表示されます。

- **種別「」のアップデートのインストールルール**
- **選択したアプリケーションのアップデートのインストールルール**

  このルールは、サードパーティのソフトウェアアップデートに対してのみ表示されます。

- **選択したアップデートのインストールルール**
- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

  選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

  このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

  たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

  既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

- タスクを作成するには：

a. ［**新規タスク**］をクリックします。

b. ウィザードの「**アップデートのインストールルールを作成する**」手順で、新しいルールを設定します。

- **この重要度レベルのアップデートのインストールルール**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

  選択したアップデートの重要度が*不明*の場合、このルールは表示されません。

- **MSRC に基づく重要度レベルのアップデートのインストールルール**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

  このルールは、Microsoft ソフトウェアのアップデートに対してのみ表示されます。選択したアップデートの重要度が*不明*の場合は表示されません。

- **この製造元によるアップデートのインストールルール**

  このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Center Linux は、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

  既定では、このオプションはオフです。

  このルールは、サードパーティのソフトウェアアップデートに対してのみ表示されます。

- **種別「」のアップデートのインストールルール**

- **選択したアプリケーションのアップデートのインストールルール**

  このルールは、サードパーティのソフトウェアアップデートに対してのみ表示されます。

- **選択したアップデートのインストールルール**

- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

  選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

  このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

  たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

  既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

新規タスクウィザードでタスクの作成を続行します。アップデートのインストールウィザードで追加した新しいルールが、新規タスクウィザードに表示されます。タスク追加ウィザードを完了すると、［*アップデートのインストールと脆弱性の修正*］タスクがタスクリストに追加されます。

# 脆弱性とアプリケーションのアップデートの検索タスクの設定

［*脆弱性とアプリケーションのアップデートの検索*］タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

全般的なタスクの設定以外に、[*脆弱性とアプリケーションのアップデートの検索*] タスクでは、タスクの作成時または作成後に、作成したタスクのプロパティを編集する時に次の設定を指定できます：

- **Microsoft による脆弱性とアップデートのリストを検索する**

  脆弱性とアップデートの検索時に、Kaspersky Security Center Linux は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

  Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

  オプションの Microsoft Windows アップデートに関する情報が管理サーバーに送信されていません。

- **アップデートサーバーに接続してアップデートを取得する**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性*スキャンタスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］がオンかオフかに関係なく、［**Windows Update 検索モード**］セクションで［**無効**］が選択されている場合、Kaspersky Security Center Linux はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

  このオプションをオンにすると、Kaspersky Security Center Linux は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティアプリケーション（Kaspersky と Microsoft 以外のベンダーが作成したアプリケーション）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

  このオプションをオフにすると、Kaspersky Security Center Linux はサードパーティアプリケーションの脆弱性とアップデートを検索しません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定する**

  Kaspersky Security Center Linux が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

- **詳細な診断を有効にする**

  この機能をオンにすると、Kaspersky Security Center Linux リモート診断ユーティリティでネットワークエージェントによるトレースファイルの書き込みがオフになっていても、ネットワークエージェントがトレースファイルを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Linux リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

## タスクのスケジュールに関する推奨事項

［*脆弱性とアプリケーションのアップデートの検索*］タスクのスケジュールを設定する場合は、［**未実行のタスクを実行する**］と［**タスクの開始を自動的かつランダムに遅延させる**］の 2 つのオプションがオンになっていることを確認してください。

既定では、［*脆弱性とアプリケーションのアップデートの検索*］タスクは手動で開始するように設定されています。組織で採用されている規則などによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり翌日の朝に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

# ［脆弱性とアプリケーションのアップデートの検索］タスクの作成

*脆弱性とアプリケーションのアップデートの検索*タスクを使用して、Kaspersky Security Center Linux は管理対象デバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

*脆弱性とアプリケーションのアップデートの検索*タスクは、Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこのタスクを作成することはできません。

*脆弱性とアプリケーションのアップデートの検索*タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

*［脆弱性とアプリケーションのアップデートの検索］タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**脆弱性とアプリケーションのアップデートの検索**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。

6. 脆弱性とアップデートが必要なアプリケーションをスキャンする方法を指定します。

- **Microsoft による脆弱性とアップデートのリストを検索する**

  脆弱性とアップデートの検索時に、Kaspersky Security Center Linux は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

  Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

  オプションの Microsoft Windows アップデートに関する情報が管理サーバーに送信されていません。

- **アップデートサーバーに接続してアップデートを取得する**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性*スキャンタスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］がオンかオフかに関係なく、［**Windows Update 検索モード**］セクションで［**無効**］が選択されている場合、Kaspersky Security Center Linux はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center Linux は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティアプリケーション（Kaspersky と Microsoft 以外のベンダーが作成したアプリケーション）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、Kaspersky Security Center Linux はサードパーティアプリケーションの脆弱性とアップデートを検索しません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

タスクの作成後、タスクプロパティウィンドウの［**アプリケーション設定**］タブでこれらのオプションをオフにすることができます。

7. **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定する**

Kaspersky Security Center Linux が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

タスク作成後に、タスクプロパティウィンドウの［**アプリケーション設定**］タブで指定したパスを変更できます。

8. 必要に応じて、**詳細な診断を有効にする**

この機能をオンにすると、Kaspersky Security Center Linux リモート診断ユーティリティでネットワークエージェントによるトレースファイルの書き込みがオフになっていても、ネットワークエージェントがトレースファイルを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Linux リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

タスクの作成後、タスクプロパティウィンドウの［**アプリケーション設定**］タブでこのオプションをオフにすることができます。

9. **詳細な診断ファイルの最大サイズ（MB）**を指定します

   既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

   前の手順で詳細な診断をオンにした場合は、この値を指定する必要があります。タスクの作成後、タスクプロパティウィンドウの［**アプリケーション設定**］タブでこの値を変更できます。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

    タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

タスクが指定した設定で作成されます。タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

### タスクのスケジュールに関する推奨事項

［*脆弱性とアプリケーションのアップデートの検索*］タスクのスケジュールを設定する場合は、［**未実行のタスクを実行する**］と［**タスクの開始を自動的かつランダムに遅延させる**］の 2 つのオプションがオンになっていることを確認してください。

既定では、［*脆弱性とアプリケーションのアップデートの検索*］タスクは手動で開始するように設定されています。

*脆弱性とアプリケーションのアップデートの検索*タスクを特定時刻に開始するようにスケジュールすることもできます。たとえば、タスクプロパティウィンドウの［**スケジュール**］タブにある［**タスク開始**］ドロップダウンリストから、［**N 時間ごと**］を選択できます。この場合、組織で採用されている職場のルールによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻に*脆弱性とアプリケーションのアップデートの検索*タスクが実行されることに注意してください。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

## サードパーティ製品の使用可能なアップデートに関する情報の表示

クライアントデバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

*クライアントデバイスにインストールされたサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには、*

メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動します。

適用可能なアップデートのリストが表示されます。

ソフトウェアアップデートのリストの表示では、フィルターを指定できます。ソフトウェアアップデートのリストの右上にある［**フィルター**］アイコン（  ）をクリックして、フィルターを指定してください。ソフトウェアの脆弱性リストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

*アップデートのプロパティを表示するには：*

1. 目的のソフトウェアのアップデートの名前をクリックします。
2. アップデートのプロパティウィンドウが開き、次のタブごとにまとめられた情報が表示されます：

- **全般**

  このタブには、選択したアップデートの一般的な詳細が表示されます。

  - 承認ステータスのアップデート（ドロップダウンリストの新しいステータスをオンにすると、手動で変更できます）
  - アップデートが登録された日時
  - アップデートが作成された日時
  - アップデートの重要度
  - アップデートによって適用されるインストール要件
  - アップデートが属するアプリケーションファミリー
  - アップデートが適用されるアプリケーション
  - アップデートのリビジョン番号

- **属性**

  このタブには、選択したアップデートに関する詳細情報の取得に使用できる一連の属性が表示されます。表示される属性は、アップデートの公開元が Microsoft かサードパーティかによって異なります。

  このタブには、Microsoft のアップデートに関する次の情報が表示されます：

  - Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度
  - アップデートについて説明しているマイクロソフトサポート技術情報の記事へのリンク
  - アップデートについて説明しているマイクロソフトセキュリティ情報の記事へのリンク
  - アップデートの識別子（ID）

  このタブには、サードパーティの更新プログラムに関する次の情報が表示されます：

  - アップデートがパッチか、または配布パッケージか
  - アップデートのローカリゼーション言語
  - アップデートが自動インストールか手動インストールか
  - 適用後にアップデートが取り消されたかどうか
  - アップデートをダウンロードするためのリンク

- **デバイス**

  このタブには、選択したアップデートがインストールされているデバイスのリストが表示されます。

- **修正済みの脆弱性**

  このタブには、選択したアップデートで修正できる脆弱性のリストが表示されます。

- **アップデートの重複**

  このタブには、同じアプリケーションに対して公開された複数のアップデート間で起こり得るクロスオーバーが表示されます。つまり、選択したアップデートが他のアップデートより優先されるか、逆に他のアップデートが優先されるかを表示します（Microsoft のアップデートでのみ使用可能）。

- **このアップデートをインストールするタスク**

  このタブには、選択したアップデートのインストールをスコープに含むタスクのリストが表示されます。このタブでは、アップデート用の新しいリモートインストールタスクを作成することもできます。

*アップデートのインストールの統計情報を表示するには：*

1. 目的のソフトウェアのアップデートに隣接するチェックボックスをオンにします。
2. ［**アップデートのインストールステータスの統計**］をクリックします。

   アップデートのインストールステータスを示した図表が表示されます。ステータスをクリックすると、選択したステータスのデバイスのリストが開きます。

Windows を使用している選択した管理対象デバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

*選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、サードパーティ製ソフトウェアのアップデートを表示するデバイスの名前のリンクをクリックします。

   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**適用可能なアップデート**］セクションを選択します。インストール済みのアップデートのみを表示する場合は、［**インストールされたアップデートの表示**］をオンにします。

   選択したデバイス上で適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

# 使用可能なソフトウェアアップデートのリストのファイルへのエクスポート

Microsoft 製品などのサードパーティ製ソフトウェアに対するアップデートのリストを、CSV ファイルまたは TXT ファイルにエクスポートできます。エクスポートしたファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

*管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なすべてのアップデートのリストをファイルにエクスポートするには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動します。

   適用可能なアップデートのリストが表示されます。

   ただし、ソフトウェアアップデートのリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されているアップデート項目のみです。

   特定の更新プログラムのみをエクスポートする場合は、リストで必要なアップデートの横にあるチェックボックスをオンにします。

2. ファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。これらのボタンのいずれかが表示されていない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから必要なオプションを選択します。

Microsoft ソフトウェアを含むサードパーティ製ソフトウェアの適用可能なアップデートのリストを含むファイルが、現在のデバイスにダウンロードされます。

*選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをファイルにエクスポートするには：*

1. 選択した管理対象デバイスに対して適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

   適用可能なアップデートのリストが表示されます。

   ただし、ソフトウェアアップデートのリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されているアップデート項目のみです。

   特定の更新プログラムのみをエクスポートする場合は、リストで必要なアップデートの横にあるチェックボックスをオンにします。

   インストール済みのアップデートのみをエクスポートする場合、［**インストールされたアップデートの表示**］をオンにします。

2. ファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。これらのボタンのいずれかが表示されていない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから必要なオプションを選択します。

現在のデバイスに、選択した管理対象デバイスにインストールされている Microsoft 製品などのサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをエクスポートしたファイルがダウンロードされます。

# サードパーティ製ソフトウェアのアップデートの拒否と承認

*アップデートのインストールと脆弱性の修正*タスクを設定する際には、アップデートに特定のステータスが割り当てられていることをインストールの要件とするルールを作成できます。たとえば、次のようなステータスのアップデートのインストールのみを許可するようにルールを設定できます：

- 承認済みのアップデートのみ
- 承認済みのアップデートとステータスが未定義のアップデートのみ
- すべてのアップデート（ステータスを考慮しない）

インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

アップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデートの数が少ない場合に効率的です。複数のアップデートをインストールするには、*アップデートのインストールと脆弱性の修正*タスクのプロパティで設定できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、管理サーバーが過負荷になる可能性があります。

*1つ以上のアップデートを承認または拒否するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートを選択します。
3. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。これらのボタンのいずれかが表示されていない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから必要なオプションを選択します。
   アップデートの既定のステータスは*未定義*です。

選択したアップデートのステータスが、指定したステータスに変更されます。

オプションとして、特定のアップデートのプロパティで承認ステータスを変更できます。

*プロパティでアップデートを承認または拒否するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートの名前をクリックします。
   アップデートのプロパティウィンドウが開きます。
3. ［**全般**］セクションで、［**アップデート承認の状況**］ドロップダウンメニューのステータスを選択します。［*承認*］、［*承認却下*］、または［*未定義*］のいずれかのステータスを選択できます。
4. ［**保存**］をクリックして変更を保存します。

選択したアップデートのステータスが、指定したステータスに変更されます。

サードパーティ製のソフトウェアアップデートに［*承認却下*］を設定すると、これらのアップデートは、アップデートのインストールを予定しているがまだインストールしていないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。必要に応じて、ローカルで手動で削除できます。

# ［アップデートのインストールと脆弱性の修正］タスクの作成

［*アップデートのインストールと脆弱性の修正*］タスクは、脆弱性とパッチ管理が使用可能なライセンスがある場合にのみ使用できます。

*アップデートのインストールと脆弱性の修正*タスクは、管理対象デバイス上にインストールされたサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクでは、タスク設定で指定したルールに従って、複数のアップデートプログラムをインストールし、複数の脆弱性を修正できます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してアップデートのインストールまたは脆弱性の修正を実行するには、次のうち1つの操作を実行します：

- アップデートのインストールウィザードまたは脆弱性修正ウィザードを実行します。
- ［*アップデートのインストールと脆弱性の修正*］タスクを作成します。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクにアップデートのインストールに関するルールを追加します。

*［アップデートのインストールと脆弱性の修正］タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、［Kaspersky Security Center］を選択します。
4. ［**タスク種別**］リストで、［**アップデートのインストールと脆弱性の修正**］タスクタイプを選択します。
   タスクが表示されない場合は、［**システム管理**：**脆弱性とパッチ管理**］機能領域の**読み取り**、**書き込み**、および**実行**権限がアカウントに付与されていることを確認してください。これらのアクセス権がない場合、*アップデートのインストールと脆弱性の修正*タスクを作成および設定することはできません。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
   タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
6. ［タスクを割り当てるデバイス］を選択します。

7. ウィザードの**アップデートのインストールのルールを指定します**手順で、アップデートインストールのルールを追加します。

これらのルールはクライアントデバイスでのアップデートのインストールに適用されます。ルールが指定されていない場合、タスクはなにも実行しません。ルールの使用法については、「アップデートインストールのルール」を参照してください。

これらのルールはクライアントデバイスへのアップデートのインストールに適用されます。ルールを指定しない場合、タスクは何も実行しません。

8. 次の設定を指定します：

- **デバイスの再起動時またはシャットダウン時にインストールを開始する**

  このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

  アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

  既定では、このオプションはオフです。

- **必要なシステムコンポーネントをインストールする**

  このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象としては、オペレーティングシステムのアップデートなどが考えられます。

  このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

  既定では、このオプションはオフです。

- **アップデート中に新しい製品のバージョンのインストールを許可する**

  このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

  このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

  既定では、このオプションはオンです。

  > 製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

  このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

  Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

  このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

  既定では、このオプションはオフです。

  - **アップデートのダウンロード先**

    このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

  この機能をオンにすると、Kaspersky Security Center Linux リモート診断ユーティリティでネットワークエージェントによるトレースファイルの書き込みがオフになっていても、ネットワークエージェントがトレースファイルを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Linux リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

  - **詳細な診断ファイルの最大サイズ（MB）**

    既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

ウィザードの次のステップに進みます。

9. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1分から1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

  ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。

  このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。

  このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。

  既定では、このオプションはオフです。

10. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。

    このオプションをオンにしない場合、タスクは既定の設定で作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    新規タスクウィザードがタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

    > タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

    タスクが作成、設定され、タスクリストに表示されます。

12. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。

    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、アップデートがインストールされ、脆弱性が修正されます。

# アップデートインストールのルールの追加

> この機能は、脆弱性とパッチ管理 ライセンスでのみ使用できます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してソフトウェアのアップデートをインストールする、またはソフトウェアの脆弱性を修正する場合は、アップデートインストールのルールを指定する必要があります。これらのルールにより、インストールするアップデートと修正する脆弱性が決定されます。

厳密な設定内容は、追加するルールがすべてのアップデート、Windows Update 更新プログラム、サードパーティアプリケーション（カスペルスキーと Microsoft 以外のベンダーが作成した製品）のアップデートのいずれを対象とするのかによって異なります。Windows Update 更新プログラムまたはサードパーティアプリケーションのアップデートのいずれかを対象にルールを追加する場合は、アップデートをインストールする特定のアプリケーションとバージョンを選択できます。すべてのアップデートのルールを追加する場合は、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

次の方法で、アップデートのインストールのルールを追加できます：

- *新規*のアップデートのインストールと脆弱性の修正タスクの作成中にルールを追加する。
- 既存の *アップデートのインストールと脆弱性の修正*タスクの［**アプリケーション設定**］タブでルールを追加する。
- アップデートのインストールウィザードまたは脆弱性修正ウィザード。

## すべてのアップデートにルールを追加する

*すべてのアップデートを対象とするルールを追加するには：*

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ウィザードの**ルールの種別の選択**手順で、［**すべてのアップデートのルール**］を選択します。
3. ウィザードの「**全般基準**」ステップで、次の設定を指定します。

- **インストールするアップデートの設定**

  クライアントデバイスにインストールする必要がある更新を選択します。
  - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
  - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
  - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

ウィザードの次のステップに進みます。

4. インストールするアップデートの選択：

- **すべての適用可能なアップデートをインストールする**

  ウィザードの「**全般基準**」ステップで指定した基準に合致するソフトウェアのアップデートをすべてインストールします。既定では、この項目が選択されます。

- **リストのアップデートのみをインストールする**

  手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

  特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

  - **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

    選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

    このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

    たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

    既定では、このオプションはオンです。

ウィザードの次のステップに進みます。

5. 選択したアップデートのインストールで修正する脆弱性を選択します：

- **他の基準に一致するすべての脆弱性を修正する**

  ウィザードの「**全般基準**」ステップで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

- **リストの脆弱性のみを修正する**

  手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

  特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

ウィザードの次のステップに進みます。

6. 追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**アプリケーション設定**］タブで変更できます。

新しいルールが作成、設定され、新規タスクウィザードのルールテーブルに表示されます。

## Windows Update からのアップデートに対するルールの追加

*Windows Update からのアップデートに対して新しいルールを追加するには：*

1. ［**追加**］をクリックします。

   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. **Windows Update のルール**を選択します。

   ウィザードの次のステップに進みます。

3. ウィザードの「**全般基準**」ステップで、次の設定を指定します。

- **インストールするアップデートの設定**

  クライアントデバイスにインストールする必要がある更新を選択します。

  - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
  - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
  - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

- **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ウィンドウで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

## サードパーティ製アプリケーションのアップデートに対するルールの追加

*サードパーティ製品のアップデートを対象とする新しいルールを追加するには：*

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ウィザードの「**ルールの種別の選択**」手順で、［**サードパーティ製品のアップデートのルール**］を選択します。
3. ウィザードの「**全般基準**」ステップで、次の設定を指定します。
   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。
   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。

   ウィザードの次のステップに進みます。
4. アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。
   既定では、すべてのアプリケーションがオンです。
   ウィザードの次のステップに進みます。
5. 追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**アプリケーション設定**］タブで変更できます。

新しいルールが作成、設定され、新規タスクウィザードのルールテーブルに表示されます。

# タスク作成後に指定された、アップデートのインストールと脆弱性の修正タスクの設定

*アップデートのインストールと脆弱性の修正*タスクを作成した後、タスクプロパティウィンドウの［**アプリケーション設定**］タブで次の設定を指定できます：

- **テストインストール** セクションで：
  - **スキャンしない**：アップデートのテストインストールを実行しない場合は、このオプションを選択します。
  - **選択されたデバイスでスキャンを実行**：選択したデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**追加**］をクリックし、アップデートのテストインストールを実行する必要があるデバイスを選択します。
  - **指定されたグループのデバイスでスキャンを実行**：特定のグループ内のデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**テストグループの指定**］に、テストインストールを実行するデバイスのグループを指定します。
  - **指定された割合のデバイスにスキャンを実行**：特定の割合のデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**対象の全デバイス内でテストデバイスが占める割合**］に、アップデートのテストインストールを実行するデバイスの割合をパーセントで指定します。

  ［**スキャンしない**］以外のいずれかのオプションを選択する時は、［**インストールを続行するかどうかを判定する時間（時間）**］で、アップデートのテストインストールを行ってからすべてのデバイスに対してアップデートのインストールを開始するまでの待機時間を指定します。
- ［**インストールするアップデート**］セクションで、タスクでインストールされるアップデートのリストを確認できます。適用するタスク設定の条件に一致するアップデートのみが表示されます。

スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

# サードパーティ製品の自動アップデート

一部のサードパーティ製品は自動的にアップデートできます。アプリケーションのベンダーは、アプリケーションが自動アップデート機能をサポートするかどうかを定義します。管理対象デバイスにインストールされているサードパーティ製品が自動アップデートをサポートしている場合は、アプリケーションのプロパティで自動アップデートの設定を指定できます。自動アップデート設定の変更後、ネットワークエージェントは、アプリケーションがインストールされている各管理対象デバイスにその新しい設定を適用します。

自動アップデートの設定は、脆弱性とパッチ管理機能の他のオブジェクトと設定から独立しています。たとえば、この設定はアップデート承認の状況や、*アップデートのインストールと脆弱性の修正*、*脆弱性の修正*などのアップデートのインストールタスクには依存しません。

*サードパーティ製品の自動アップデート設定を行うには：*

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。

2. 自動アップデート設定を変更するアプリケーションの名前をクリックします。

   検索を簡略化するには、［**自動アップデートのステータス**］および［**自動アップデートの管理**］列でリストをフィルタリングできます。

   アプリケーションプロパティのウィンドウが開きます。

3. ［**全般**］セクションで、次の設定の値を選択します。

   **自動アップデートのステータス**。

   次のいずれかのオプションをオンにします：

   - **未定義**

     自動アップデート機能は無効になっています。Kaspersky Security Linux Center は、*アップデートのインストールと脆弱性の修正*、*脆弱性の修正*の各タスクを使用して、サードパーティアプリケーションのアップデートをインストールします。

   - **許可**

     製造元がアプリケーションのアップデートをリリースすると、このアップデートは管理対象デバイスに自動的にインストールされます。追加の操作は必要ありません。

   - **ブロック**

     アプリケーションのアップデートは自動的にインストールされません。Kaspersky Security Linux Center は、*アップデートのインストールと脆弱性の修正*、*脆弱性の修正*の各タスクを使用して、サードパーティアプリケーションのアップデートをインストールします。

4. ［**保存**］をクリックして変更を保存します。

選択したアプリケーションに自動アップデートの設定が適用されます。

# サードパーティ製ソフトウェアの脆弱性の修正

このセクションでは、管理対象デバイスにインストールされているソフトウェアの脆弱性の修正に関連する Kaspersky Security Center Linux の機能について説明します。

# ソフトウェアの脆弱性の検知と修正

Kaspersky Security Center Linux では、Microsoft Windows オペレーティングシステムを実行している管理対象デバイスのソフトウェアの脆弱性を検知して修正することができます。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性が検知されます。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

## ソフトウェア脆弱性の検知

ソフトウェアの脆弱性の検知では、Kaspersky Security Center Linux は既知の脆弱性のデータベースに記録されている情報を使用します。この定義データベースは、カスペルスキーの専門家によって作成され、最新の状態に保たれています。データベースには、脆弱性の説明、脆弱性の検知日、脆弱性の深刻度などの情報が含まれています。ソフトウェアの脆弱性に関する詳細情報は、カスペルスキーの Web サイトにあります。

Kaspersky Security Center Linux は、*脆弱性とアプリケーションのアップデートの検索*タスクを使用してソフトウェアの脆弱性を検知します。

## ソフトウェア脆弱性の修正

ソフトウェアの脆弱性の修正では、Kaspersky Security Center Linux はソフトウェアベンダーから提供されているソフトウェアのアップデートを使用します。ソフトウェアのアップデートのメタデータは、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクの実行の結果として、管理サーバーのリポジトリにダウンロードされます。このタスクは、カスペルスキー製品とサードパーティ製ソフトウェアのアップデートのメタデータをダウンロードするためのタスクです。このタスクは、Kaspersky Security Center Linux のクイックスタートウィザードによって自動的に作成されます。*管理サーバーのリポジトリへのアップデートのダウンロードタスク*を手動で作成することもできます。

脆弱性を修正するためのソフトウェアのアップデートは、配布パッケージまたはパッチの形式で提供されます。ソフトウェアの脆弱性を修正するソフトウェアのアップデートは、「*修正*」という名称で呼ばれます。*推奨される修正*は、カスペルスキーのスペシャリストがインストールを推奨する修正です。*ユーザー修正*は、インストールするようにユーザーが手動で指定する修正です。ユーザー修正をインストールするには、修正を含むインストールパッケージを事前に作成する必要があります。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center Linux ライセンスを使用している場合、*アップデートのインストールと脆弱性の修正*タスクを使用できます。このタスクでは、推奨される修正をインストールして、検知された複数の脆弱性を自動的に修正します。このタスクを使用する場合、脆弱性を修正するためのルールを手動で指定できます。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center Linux ライセンスを使用していない場合、*脆弱性の修正*タスクを使用できます。このタスクを使用すると、Microsoft 製品に対して推奨される修正とその他のサードパーティ製ソフトウェアに対するユーザー修正をインストールして脆弱性を修正できます。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書（EULA）への同意を要求された場合、EULA に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

# シナリオ：サードパーティ製ソフトウェアの脆弱性の検知と修正

このセクションでは、Windows オペレーティングシステムを使用している管理対象デバイスで、脆弱性を検知して修正する方法について説明しています。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性の検知と修正を実行できます。

## 必須条件

- 組織内に Kaspersky Security Center Linux が導入されている。
- 組織内に Windows を使用している管理対象デバイスが存在する。
- 管理サーバーで次のタスクを実行する場合は、インターネット接続が必要になります：
  - Microsoft ソフトウェアの脆弱性に対して推奨される修正のリストを作成する。このリストは、カスペルスキーのスペシャリストにより作成され、定期的に更新されます。
  - Microsoft 製ソフトウェア以外のサードパーティ製ソフトウェアで脆弱性を修正する場合。

## 実行するステップ

ソフトウェアの脆弱性の検知と修正は、次の手順で進みます：

1. **管理対象デバイスにインストールされているソフトウェアの脆弱性のスキャン**

   管理対象デバイスにインストールされているソフトウェアの脆弱性を検知するには、*脆弱性とアプリケーションのアップデートの検索*タスクを実行します。タスクが完了すると、Kaspersky Security Center Linux はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   *脆弱性とアプリケーションのアップデートの検索*タスクは、Kaspersky Security Center Linux のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にウィザードを実行するか手動でタスクを作成してください。

*脆弱性とアプリケーションのアップデートの検索*タスクは、Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこのタスクを作成することはできません。

### 2 検知されたソフトウェアの脆弱性の表示

**ソフトウェアの脆弱性**リストを確認して、どの脆弱性を修正する必要があるかを決定します。それぞれの脆弱性の詳細情報を確認するには、リスト内の脆弱性の名前をクリックします。リスト内のそれぞれの脆弱性について、管理対象デバイス上の脆弱性に関する統計情報を表示することもできます。

### 3 脆弱性の修正の設定

管理対象デバイス上でソフトウェアの脆弱性が検知された場合、*アップデートのインストールと脆弱性の修正*タスクまたは*脆弱性の修正*タスクを使用して修正できます。

*アップデートのインストールと脆弱性の修正*タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。このタスクは、脆弱性とパッチ管理機能を利用できるライセンスを使用している場合にのみ作成できます。ソフトウェア脆弱性を修正するために、［*アップデートのインストールと脆弱性の修正*］タスクは推奨されるソフトウェアアップデートを使用します。

*脆弱性の修正*タスクは、脆弱性とパッチ管理機能を使用できるライセンスがなくても使用できます。このタスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するために使用するユーザー修正を手動で指定する必要があります。*脆弱性の修正*タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。

*アップデートのインストールと脆弱性の修正*タスクと*脆弱性の修正*タスクは、Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこれらのタスクを作成することはできません。

脆弱性修正ウィザードを起動すると、これらのタスクのいずれかを自動的に作成できます。または、手動でタスクを作成することもできます。

*アップデートのインストールと脆弱性の修正*タスクを作成した場合、管理対象デバイス上の脆弱性が自動的に修正されます。作成したタスクの起動時に、適用可能なソフトウェアアップデートのリストとタスクの設定で指定されたルールとが照合されます。特定のルールの条件に一致するすべてのソフトウェアアップデートが管理サーバーのリポジトリにダウンロードされ、ソフトウェアの脆弱性を修正するためにインストールされます。

*脆弱性の修正*タスクを作成した場合、Microsoft 製品のソフトウェア脆弱性のみが修正されます。

### 4 タスクのスケジュール設定

脆弱性のリストを最新の状態に保つために、*脆弱性とアプリケーションのアップデートの検索*タスクを定期的に自動的に実行するようにスケジュールします。推奨されるタスクの実行頻度は週に 1 回です。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。*脆弱性の修正*タスクのスケジュールを設定する場合は、タスクを開始する前に、毎回 Microsoft 製品の修正を選択するか、サードパーティ製ソフトウェアのユーザー修正を指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、*脆弱性とアプリケーションのアップデートの検索*タスクの作成が完了してからこれらのタスクが開始されるようにしてください。

### 5 検知されたソフトウェアの脆弱性への非対応の判断（必要に応じて実施）

すべての管理対象デバイス上または選択した特定のデバイス上で、特定のソフトウェアの脆弱性を無視できます。

6 **脆弱性の修正タスクの実行**

［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを開始します。タスクが完了したら、タスクリストでのタスクのステータスが*正常終了*になっていることを確認します。

7 **ソフトウェアの脆弱性の修正結果のレポートの作成（任意）**

脆弱性の修正に関する詳細な統計情報を確認するには、脆弱性レポートを生成します。このレポートには、修正されなかったソフトウェアの脆弱性に関する情報が表示されます。これにより、組織で使用されている Microsoft 製ソフトウェアを含むサードパーティ製ソフトウェアの脆弱性を特定し、対処できるようになります。

8 **サードパーティ製ソフトウェアの脆弱性の検知と修正に関する設定の確認**

次の手順がすべて完了していることを確認してください：

- 管理対象デバイス上のソフトウェアの脆弱性のリストを作成して内容を確認した。
- 必要に応じて、特定のソフトウェアの脆弱性を無視した。
- 脆弱性を修正するタスクを設定した。
- タスクの実行順序として、ソフトウェアの脆弱性を検知するタスクが実行された後に脆弱性を修正するタスクが実行されるようにスケジュールを指定した。
- ソフトウェアの脆弱性を修正するタスクが起動したことを確認した。

# サードパーティ製ソフトウェアの脆弱性の修正

サードパーティ製ソフトウェアの脆弱性を見つけるには、*脆弱性とアプリケーションのアップデートの検索タスクを作成して実行し*、ソフトウェアの脆弱性のリストを取得します。ソフトウェアの脆弱性のリストの取得が完了すると、Windows を実行している管理対象デバイスで脆弱性を修正できます。

Microsoft 製品を含めて、オペレーティングシステムとサードパーティ製ソフトウェアの脆弱性を修正するには、脆弱性の修正タスクまたはアップデートのインストールと脆弱性の修正タスクを作成して実行します。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

オプションとして、次の方法でソフトウェアの脆弱性を修正するタスクを作成できます：

- 脆弱性リストを開き、修正する脆弱性を指定する。

  その結果、ソフトウェアの脆弱性を修正する新しいタスクが作成されます。オプションとして、選択した脆弱性を既存のタスクに追加できます。

- 脆弱性修正ウィザードを実行する。

  脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合にのみ使用できます。

  このウィザードにより、脆弱性の修正タスクの作成と設定手順が簡略化され、冗長なタスクを作成せずに済みます。

## 脆弱性リストを使用してソフトウェアの脆弱性を修正する

*脆弱性リストを使用してソフトウェアの脆弱性を修正するには：*

1. 次のいずれかの方法で脆弱性のリストを開きます：

   - メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   - メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［<デバイス名>］→［**詳細**］→［**ソフトウェアの脆弱性**］の順に移動します。
   - メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［<アプリケーション名>］→［**脆弱性**］の順に選択します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアの脆弱性のリストを掲載したリストが表示されます。

2. 脆弱性のリストで、修正する脆弱性の横にあるチェックボックスをオンにして、［**脆弱性の修正**］ボタンをクリックします。

   選択した脆弱性の一部について推奨されるソフトウェアアップデートが存在しない場合、通知メッセージが表示されます。

   一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書への同意を要求された場合、使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

3. 次のいずれかのオプションをオンにします：

   - **新規タスク**

     新規タスクウィザードが起動します。脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合は、アップデートのインストールと脆弱性の修正タスクが事前選択されています。ライセンスをお持ちでない場合は、脆弱性の修正タスクが事前選択されています。ウィザードの手順に従って、タスクの作成を完了します。

   - **脆弱性の修正（指定したタスクにルールを追加）**

     選択した脆弱性を追加するタスクを選択します。脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合は、アップデートのインストールと脆弱性の修正タスクを選択します。選択した脆弱性を修正するための新しいルールが、選択したタスクに自動的に追加されます。ライセンスをお持ちでない場合は、脆弱性の修正タスクを選択します。選択した脆弱性がタスクのプロパティに追加されます。

     タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

   タスクの作成を選択した場合は、タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。脆弱性を既存のタスクに追加することを選択した場合、脆弱性はタスクのプロパティに保存されます。

サードパーティ製ソフトウェアの脆弱性を修正するには、アップデートのインストールと脆弱性の修正タスク、または脆弱性の修正タスクを開始します。作成したタスクが脆弱性の修正タスクである場合は、タスクの設定リストのソフトウェアアップデートを手動で指定する必要があります。

## 脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正する

脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合にのみ使用できます。

*脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアの脆弱性のリストを掲載した表が表示されます。

2. 修正する脆弱性に隣接するチェックボックスをオンにします。

3. ［**脆弱性修正ウィザードを実行**］をクリックします。

   > 複数の脆弱性を選択した場合、ボタンは無効になります。

   脆弱性修正ウィザードが起動します。既存のタスクのリストが表示されます。このリストには、次の種別のタスクが含まれます。

   - アップデートのインストールと脆弱性の修正
   - 脆弱性の修正

   新しいアップデートをインストールする脆弱性の修正タスクを変更することはできません。新しいアップデートをインストールする際に使用できるのは、アップデートのインストールと脆弱性の修正タスクのみです。

4. 選択した脆弱性を修正するタスクのみをウィザードに表示する場合は、［**この脆弱性を修正するタスクのみ表示**］をオンにします。

5. 次のいずれかの手順を実行します：

- タスクを開始するには、タスク名の横にあるチェックボックスをオンにして、［**開始**］をクリックします。

  追加の操作は必要ありません。ウィザードを閉じることができます。タスクはバックグラウンドモードで完了します。

- 既存のアップデートのインストールと脆弱性の修正タスクに新しいルールを追加するには：

  a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。

  > 複数のタスクを選択した場合、［**ルールの追加**］は無効になります。

  脆弱性の修正タスクのルールを追加することはできません。脆弱性の修正タスク選択した場合、次の通知が表示されます。「更新プログラムをインストールするには、「アップデートのインストールと脆弱性の修正」タスクを使用します。」

  b. 開いたページで、新しいルールを構成します：

  - **この深刻度の脆弱性すべてを修正するルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

  - **選択した脆弱性に対して推奨されるものとして定義されているアップデートと同じタイプのアップデートによって脆弱性を修正するためのルール**

    このルールは、Microsoft ソフトウェアの脆弱性に対してのみ表示されます。

  - **選択した製造元のアプリケーションの脆弱性を修正するルール**

    このルールは、サードパーティ製ソフトウェアの脆弱性に対してのみ表示されます。

  - **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**

    このルールは、サードパーティ製ソフトウェアの脆弱性に対してのみ表示されます。

  - **選択した脆弱性を修正するルール**

  - **この脆弱性を修正するアップデートを承認する**

選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

c. ［**追加**］をクリックします。

タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

- タスクを作成するには：

a. ［**新規タスク**］をクリックします。

b. 開いたページで、新しいルールを構成します：

- **この深刻度の脆弱性すべてを修正するルール**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **選択した脆弱性に対して推奨されるものとして定義されているアップデートと同じタイプのアップデートによって脆弱性を修正するためのルール**

このルールは、Microsoft ソフトウェアの脆弱性に対してのみ表示されます。

- **選択した製造元のアプリケーションの脆弱性を修正するルール**

このルールは、サードパーティ製ソフトウェアの脆弱性に対してのみ表示されます。

- **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**

このルールは、サードパーティ製ソフトウェアの脆弱性に対してのみ表示されます。

- **選択した脆弱性を修正するルール**

- **この脆弱性を修正するアップデートを承認する**

選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

c. ［**追加**］をクリックします。

d. 新規タスクウィザードで新規タスクウィザード。

脆弱性修正ウィザードで追加した新しいルールは、新規タスクウィザードの「**アップデートのインストールのルールを指定します**」手順に表示されます。ウィザードを完了すると、アップデートのインストールと脆弱性の修正タスクがタスクリストに追加されます。

# 脆弱性の修正タスクの作成

*脆弱性の修正*タスクを使用すると、管理対象デバイスのソフトウェアの脆弱性を修正できます。Microsoft 製品を含めて、サードパーティ製ソフトウェアの脆弱性を修正できます。

> *脆弱性の修正*タスクは Windows デバイスに対してのみ作成できます。他のオペレーティングシステムで実行されているデバイスに対してこのタスクを作成することはできません。

脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合にのみ、新しい*脆弱性の修正*タスクを作成できます。

新しい脆弱性を修正するには、それらの脆弱性を既存の［*脆弱性の修正*］タスクに追加します。*アップデートのインストールと脆弱性の修正*タスクを*脆弱性の修正*の代わりに使用することを推奨します。［*アップデートのインストールと脆弱性の修正*］タスクを使用すると、定義したルールに従って、複数の更新をインストールし、複数の脆弱性を自動的に修正できます。

> 管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

*脆弱性の修正タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

   > または、デバイスのプロパティウィンドウの［**タスク**］タブでこのタスクを作成することもできます。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**アプリケーション**］ドロップダウンリストで、［Kaspersky Security Center］を選択します。

4. ［**タスク種別**］リストで、［**脆弱性の修正**］タスクタイプを選択します。

5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。

   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

6. ［タスクを割り当てるデバイス］を選択します。

   ウィザードの次のステップに進みます。

7. ［**追加**］をクリックします。

   脆弱性のリストが表示されます。

8. 脆弱性のリストで、修正する脆弱性の横にあるチェックボックスをオンにして、［**OK**］ボタンをクリックします。

   Microsoft ソフトウェアの脆弱性には通常、推奨される修正が用意されています。その他の操作は必要ありません。

   他の製造元のソフトウェアの脆弱性については、まず修正する脆弱性ごとにユーザー修正を指定する必要があります。その後、それらの脆弱性を*脆弱性の修正*タスクに追加できるようになります。

   ウィザードの次のステップに進みます。

9. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1分から1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

ウィザードの次のステップに進みます。

10. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

  タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

11. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。

    このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

12. ［**終了**］をクリックします。

    ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

    > タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

    タスクが作成、設定され、［**アセット（デバイス）**］→［**タスク**］のタスクリストに表示されます。

13. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。

    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、選択した脆弱性が修正されます。

# サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択

［*脆弱性の修正*］タスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するソフトウェアアップデートを手動で指定する必要があります。*脆弱性の修正*タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正を使用します。

*ユーザー修正*は、脆弱性を修正するために管理者が手動でインストールを指定するソフトウェアアップデートです。

*サードパーティ製ソフトウェアの脆弱性へのユーザー修正を選択するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアの脆弱性のリストを掲載したリストが表示されます。

2. ソフトウェア脆弱性のリストで、ユーザー修正を適用するように指定する脆弱性の名前のリンクをクリックします。

   選択した脆弱性のプロパティウィンドウが表示されます。

3. 左側のペインで、［**ユーザーによる修正とその他の修正**］セクションを選択します。

   選択したソフトウェア脆弱性に対するユーザー修正のリストが表示されます。

4. ［**追加**］をクリックします。

   適用可能なインストールパッケージのリストが表示されます。ここで表示されるインストールパッケージのリストは、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］リストの順に移動して表示されるリストと同じものです。

   選択している脆弱性に対するユーザー修正を含んだインストールパッケージを作成していない場合、［**新規**］をクリックして新規パッケージウィザードに従うことにより、パッケージを作成できます。

5. 選択した脆弱性に対するユーザー修正を含んだインストールパッケージを1つ以上選択します。

6. ［**保存**］をクリックします。

ソフトウェア脆弱性に対するユーザー修正を含んだインストールパッケージが指定されます。*脆弱性の修正*タスクを開始すると、インストールパッケージがインストールされ、ソフトウェアの脆弱性が修正されます。

# 管理対象デバイスで検知されたすべてのソフトウェア脆弱性に関する情報の表示

管理対象デバイスでのソフトウェアの脆弱性スキャンが完了すると、検知されたソフトウェア脆弱性のリストを表示できます。管理サーバーの階層に対してタスクを実行すると、選択した管理サーバーに対してのみ、脆弱性が検知された管理対象デバイスのリストを表示できます。

また、脆弱性レポートの生成と表示も実行できます。

*管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストを表示するには：*

メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

クライアントデバイスで検知された脆弱性のリストが表示されます。

*ソフトウェアの脆弱性のリストを調整するには、*

ソフトウェアの脆弱性リストの右上にある［**フィルター**］アイコン（）をクリックして、必要なフィルターを選択します。ソフトウェアの脆弱性リストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

リスト内の任意の脆弱性に関する詳細情報を取得できます。

*ソフトウェアの脆弱性に関する情報を取得するには、*

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

ソフトウェアの脆弱性のプロパティウィンドウが開きます。

# 指定した管理対象デバイスで検知されたソフトウェア脆弱性に関する情報の表示

指定した管理対象の Windows デバイスで検知されたソフトウェア脆弱性に関する情報を表示できます。

*指定した管理対象デバイスで検知されたソフトウェア脆弱性のリストを表示するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、検知されたソフトウェア脆弱性を表示するデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。

   選択した管理対象デバイスで検知された脆弱性のリストが表示されます。

*選択したソフトウェア脆弱性のプロパティを表示するには：*

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

選択したソフトウェア脆弱性のプロパティウィンドウが表示されます。

# 管理対象デバイス上の脆弱性に関する統計情報の表示

管理対象デバイス上でのそれぞれのソフトウェア脆弱性に関する統計情報を表示できます。統計情報は図表として表示されます。図表には、次のステータスごとに該当するデバイス数が表示されます：

- *無視：<デバイス数>*：脆弱性のプロパティでその脆弱性を無視するように手動で設定した場合に、このステータスが割り当てられます。
- *修正済み：<デバイス数>*：脆弱性を修正するためのタスクが正常に完了した場合に、このステータスが割り当てられます。
- *修正をスケジュール済み：<デバイス数>*：脆弱性を修正するためのタスクを作成済みだが、タスクがまだ実行されていない場合に、このステータスが割り当てられます。
- *パッチが適用済み：<デバイス数>*：脆弱性の修正をするためのソフトウェアのアップデートを手動で選択したが、そのソフトウェアのアップデートでは脆弱性が修正されていない場合に、このステータスが割り当てられます。
- *修正が必要：<デバイス数>*：脆弱性が一部の管理対象デバイスでのみ修正されており、さらに多くの管理対象デバイスで脆弱性を修正する必要がある場合に、このステータスが割り当てられます。

*管理対象デバイス上の脆弱性に関する統計情報を表示するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたアプリケーションの脆弱性のリストが表示されます。
2. 脆弱性の横にあるチェックボックスをオンにします。
3. ［**デバイスの脆弱性の統計**］をクリックします。

> 複数の脆弱性を選択した場合、［**デバイスの脆弱性の統計**］は無効になります。

脆弱性のステータスを示した図表が表示されます。それぞれのステータスをクリックすると、選択したステータスの脆弱性が存在するデバイスのリストが表示されます。

# ソフトウェア脆弱性のリストのファイルへのエクスポート

表示されている脆弱性のリストを CSV ファイルまたは TXT ファイルとしてダウンロードできます。これらのファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

*管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストをファイルにエクスポートするには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたアプリケーションのソフトウェアの脆弱性のリストが表示されます。
   既定では、現在のページに表示されている脆弱性のみがエクスポートされます。
   特定の脆弱性のみをエクスポートする場合は、その脆弱性の横にあるチェックボックスをオンにします。
2. ファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。これらのボタンのいずれかが表示されていない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから必要なオプションを選択します。

ソフトウェアの脆弱性のリストを含むファイルがデバイスにダウンロードされます。

*指定した管理対象デバイスで検知されたソフトウェア脆弱性のリストをエクスポートするには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、検知されたソフトウェア脆弱性を表示するデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。

選択した管理対象デバイスで検知された脆弱性のリストが表示されます。

既定では、現在のページに表示されている脆弱性のみがエクスポートされます。

特定の脆弱性のみをエクスポートする場合は、その脆弱性の横にあるチェックボックスをオンにします。

1. ファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。これらのボタンのいずれかが表示されていない場合は、省略記号ボタンをクリックし、ドロップダウンメニューから必要なオプションを選択します。

ソフトウェアの脆弱性のリストを含むファイルがデバイスにダウンロードされます。

# 検知されたソフトウェアの脆弱性への非対応の判断

必要に応じて、検知されたソフトウェア脆弱性を無視することもできます。ソフトウェア脆弱性に対応しない理由として、次が考えられます：

- 管理者として、該当するソフトウェアの脆弱性が組織内で緊急なものではないと判断した場合。
- 脆弱性の修正を適用すると、該当するソフトウェアでデータの破損などが生じる可能性があることが判明した場合。
- 管理者として、管理対象デバイスを保護する別の対策を使用しているため、ソフトウェア脆弱性が組織ネットワークにとって危険ではないと判断した場合。

すべてのデバイス上または選択した特定のデバイス上で、ソフトウェア脆弱性を無視できます。

*すべての管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：*

1. メインメニューで、［**操作**］→［**パッチ管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたアプリケーションのソフトウェアの脆弱性のリストが表示されます。
2. ソフトウェア脆弱性のリストで、対応せずに無視する脆弱性の名前のリンクをクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが開きます。
3. ［**全般**］タブで、［**脆弱性を無視**］をオンにします。
4. ［**保存**］をクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが閉じます。

すべての管理対象デバイスで、対象のソフトウェア脆弱性が無視されます。

*選択した管理対象デバイスで、特定のソフトウェアの脆弱性に対応せずに無視するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、特定のソフトウェア脆弱性を無視するデバイスの名前のリンクをクリックします。
   デバイスのプロパティウィンドウが表示されます。
3. デバイスのプロパティウィンドウで［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。
   デバイスで検知された脆弱性のリストが表示されます。

5. ソフトウェア脆弱性のリストで、選択しているデバイス上で対応せずに無視する脆弱性を選択します。
   ソフトウェア脆弱性のプロパティウィンドウが開きます。
6. ソフトウェア脆弱性のプロパティウィンドウの［**全般**］タブで、［**脆弱性を無視**］をオンにします。
7. ［**保存**］をクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが閉じます。
8. デバイスのプロパティウィンドウを閉じます。

選択したデバイスで、対象のソフトウェア脆弱性が無視されます。

無視することを選択したソフトウェアの脆弱性は、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクが完了しても修正されません。脆弱性のリストで、無視することを選択した脆弱性をフィルターを使用して表示から除外することができます。

# 定義データベースからのサードパーティ製品のインストールパッケージの作成

Kaspersky Security Center Web コンソールでは、インストールパッケージを使用してサードパーティ製品のリモートインストールを実行できます。このようなサードパーティ製品は、専用の定義データベースに格納されています。この定義データベースは、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを初めて実行した時に自動的に作成されます。

脆弱性とパッチ管理が使用可能なライセンスをお持ちの場合のみ、カスペルスキーの定義データベースからサードパーティ製アプリケーションのインストールパッケージを作成できます。

*定義データベースからサードパーティ製品のインストールパッケージを作成するには：*

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. ［**追加**］をクリックします。
   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**カスペルスキーのデータベースからアプリケーションを選択してインストールパッケージを作成する**］を選択します。

   この機能は、脆弱性とパッチ管理が使用可能なライセンスでのみ使用できます。

   ウィザードの次のステップに進みます。
4. インストールパッケージを作成するアプリケーションを選択します。
   ウィザードの次のステップに進みます。

5. ドロップダウンリストから関連するローカリゼーション言語を選択し、［次へ］をクリックします。

このステップは、アプリケーションに複数の言語オプションが用意されている場合にのみ表示されます。

6. インストールの使用許諾契約書に同意するように要求された場合は、ウィザードの**使用許諾契約書とプライバシーポリシー**の手順で、次の操作を行います。

a. ［**表示**］をクリックすると、ベンダーの Web サイトで使用許諾契約書を読んだり、ライセンスの更新を表示したりできます。

b. ［**この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します**］を選択します。

c. リストに表示されるすべての使用許諾契約書とプライバシーポリシーに同意するには、［**すべて同意する**］をクリックします。

7. ウィザードの［**新規インストールパッケージの名前**］ステップで、［**パッケージ名**］にインストールパッケージの名前を入力し、［**次へ**］をクリックします。

新しく作成されたインストールパッケージが管理サーバーにアップロードされます。新規パッケージウィザードに、インストールパッケージが正常に作成されたことを通知するメッセージが表示されます。

8. ［**終了**］をクリックします。

新しく作成されたインストールパッケージがインストールパッケージのリストに表示されます。このパッケージは、*アプリケーションのリモートインストールタスク*を作成または再設定する際に選択できます。

*脆弱性とパッチ管理が使用可能なライセンス*アプリケーションのリモートインストールアプリケーションのリモートインストールタスクを作成および再設定できます。

# 定義データベースからのサードパーティ製品のインストールパッケージの設定に関する表示と変更

以前に定義データベースに一覧表示されているサードパーティ製品のインストールパッケージを作成している場合は、後でこれらのパッケージの設定を表示および変更できます。

定義データベースから作成されたサードパーティアプリケーションのインストールパッケージの設定を変更することは、脆弱性とパッチ管理が使用可能なライセンスの下でのみ行うことができます。

*定義データベースからサードパーティ製品のインストールパッケージの設定を表示および変更するには：*

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。

2. 表示されたインストールパッケージのリストで、関連するパッケージの名前をクリックします。

プロパティウィンドウが表示されます。

3. 必要に応じて設定を変更します。

4. ［**保存**］をクリックします。

変更した設定が保存されます。

# 定義データベースからのサードパーティ製品のインストールパッケージの設定

サードパーティアプリケーションのインストールパッケージの設定は、次のタブにグループ化されています：

以下にリストされているすべての設定が既定で表示されるわけではありません。必要な列を追加するには、［**フィルター**］をクリックし、リストから関連する列名を選択します。

- ［**全般**］タブ：
  - 手動で編集できるインストールパッケージの名前を含む入力フィールド
  - **アプリケーション**

    インストールパッケージが作成されるサードパーティ製品の名前。
  - **バージョン**

    インストールパッケージが作成されるサードパーティ製品のバージョン番号。
  - **サイズ**

    サードパーティのインストールパッケージのサイズ（キロバイト単位）。
  - **作成日時**

    サードパーティのインストールパッケージが作成された日時。
  - **パス**

    サードパーティのインストールパッケージが保存されているネットワークフォルダーのパス。
- ［**インストール手続き**］タブ：
  - **必要なシステムコンポーネントをインストールする**

    このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象としては、オペレーティングシステムのアップデートなどが考えられます。

    このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

    既定では、このオプションはオフです。
  - アップデートのプロパティを表示し、次の列を含む表：

- **名前**

  アップデートの名前。

- **説明**

  アップデートの説明。

- **ソース**

  アップデート元、つまり、Microsoft または別のサードパーティ開発元のいずれによってリリースされたものであるか。

- **種別**

  アップデートの種別、つまり、対象とするのがドライバーまたはアプリケーションのいずれであるか。

- **カテゴリ**

  Microsoft のアップデート（緊急更新プログラム、定義更新プログラム、ドライバー、機能パック、セキュリティ更新プログラム、サービスパック、ツール、更新プログラムロールアップ、更新プログラム、またはアップグレード）に対して表示される Windows Server Update Services（WSUS）カテゴリ。

- **MSRC による重要度**

  Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度。

- **重要度**

  カスペルスキーによって定義されたアップデートの重要度。

- **パッチ重要度レベル**

  カスペルスキー製品を対象とする場合のパッチの重要度。

- **記事**

  アップデートについて説明するナレッジベースの記事の識別子（ID）。

- **セキュリティ情報**

  アップデートについて説明するセキュリティ情報の ID。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「インストール用に未割り当て」であるかどうかを表示します。

- **インストール予定**

  アップデートのステータスが「インストール予定」であるかどうかを表示します。

- **インストール中**

  アップデートのステータスが「インストール中」であるかどうかを表示します。

- **インストール済み**

  アップデートのステータスが「インストール済み」であるかどうかを表示します。

- **失敗**

  アップデートのステータスが「失敗」であるかどうかを表示します。

- **再起動が必要です**

  アップデートのステータスが「再起動が必要」であるかどうかを表示します。

- **登録日**

  アップデートが登録された日時を表示します。

- **対話モードでのインストール**

  アップデートのインストール中にユーザーとの対話が必要であるかどうかを表示します。

- **アップデート承認の状況**

  アップデートのインストールが承認済みであるかどうかを表示します。

- **リビジョン**

  アップデートの現在のリビジョン番号を表示します。

- **アップデート ID**

  アップデートの ID を表示します。

- **アプリケーションのバージョン**

  アプリケーションのアップデート後のバージョン番号を表示します。

- **より古い**

  該当するアップデートを置換できる他のアップデートを表示します。

- **より新しい**

  このアップデートで置換できる他のアップデートを表示します。

- **使用許諾契約書の条項に同意する必要があります**

  アップデート時に使用許諾契約書（EULA）への同意が必要であるかどうかを表示します。

- **詳細 URL**

  アップデートの製造元の名前を表示します。

- **アプリケーションファミリー**

  アップデートが属するアプリケーションファミリーの名前を表示します。

- **アプリケーション**

  アップデートが属するアプリケーションの名前を表示します。

- **ローカリゼーション言語**

  アップデートの言語を表示します。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「新しいバージョンのインストール用に未割り当て」であるかどうかを表示します。

- **必須アップデートのインストールが必要**

  アップデートのステータスが「必須コンポーネントのインストールが必要」であるかどうかを表示します。

- **ダウンロード方法**

  アップデートのダウンロード方法を表示します。

- **パッチ**

  アップデートがパッチであるかどうかを表示します。

- **未インストール**

  アップデートのステータスが「未インストール」であるかどうかを表示します。

- **作成日時**

- ［**設定**］タブには、インストール中にコマンドラインパラメータとして使用される、インストールパッケージの設定とその名前、説明、および値が表示されます。パッケージにそのような設定が用意されていない場合は、対応するメッセージが表示されます。これらの設定の値を変更できます。

- ［**変更履歴**］タブにはインストールパッケージのリビジョンが表示され、次の列が含まれます：

  - **リビジョン**ーインストールパッケージのリビジョン番号を表示します。

  - **時間**ーインストールパッケージ設定が変更された日時。

  - **ユーザー**ーインストールパッケージの設定を変更したユーザーの名前。

  - **ユーザーデバイスの IP アドレス**ーオブジェクトが変更されたデバイスの IP アドレス。

  - **Web コンソールの IP アドレス**ーオブジェクトが変更された Kaspersky Security Center Web コンソールの IP アドレス。

  - **処理**ーリビジョン内のインストールパッケージで実行された処理を一覧表示します。

  - **説明**ーインストールパッケージの設定に加えられた変更に関連するリビジョンの説明。

    既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明の編集**］をクリックします。表示されたウィンドウで、リビジョンの説明を入力します。

# 隔離されたネットワークでの脆弱性の修正

このセクションでは、インターネット接続のない管理サーバーに接続されている管理対象デバイスのサードパーティ製ソフトウェアの脆弱性を修正するために実行できる手順について説明します。

# シナリオ：分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正

分離されたネットワーク内の管理対象デバイスにインストールされているサードパーティ製ソフトウェアのアップデートをインストールして脆弱性を修正できます。このネットワークには管理サーバーと、そこに接続されているインターネット接続のない管理対象デバイスが含まれます。このようなネットワークの脆弱性を修正するには、インターネットに接続された管理サーバーが必要です。インターネットにアクセスできる管理サーバーを使用することで、パッチ（アップデート）をダウンロードし、それを分離された管理サーバーに送信できるようになります。

Kaspersky Security Center を使用して、分離された管理サーバー上で製造元が発行したサードパーティ製品のアップデートはダウンロードすることができますが、Microsoft 製品のアップデートはダウンロードすることはできません。

分離されたネットワーク上での脆弱性の修正プロセスの詳細については、「このプロセスの説明とスキーム」を参照してください。

## 必須条件

開始する前に、次を実行します：

1. インターネットに接続してパッチをダウンロードするためのデバイスを1つ割り当てます。このデバイスは、インターネットにアクセス可能な管理サーバーと判断されます。
2. 次の端末にバージョン15.1以降のKaspersky Security Center Linuxをインストールします：
   - インターネットに接続されている管理サーバーとして動作する割り当て済みデバイス
   - インターネットから分離された管理サーバーとして動作する分離されたデバイス（以降「分離された管理サーバー」と表記）
3. すべての管理サーバーに、アップデートとパッチをダウンロードして保存できる十分なディスク容量があることを確認してください。

## 実行するステップ

分離された管理サーバーの管理対象デバイスへのアップデートのインストールとサードパーティ製ソフトウェアの脆弱性の修正には、次の段階があります。

**1 インターネットにアクセス可能な管理サーバーの設定**

必要なサードパーティ製ソフトウェアアップデートのリクエストを処理し、パッチをダウンロードするためにインターネットにアクセス可能な管理サーバーを準備します。

**2 分離された管理サーバーの設定**

分離された管理サーバーを準備します。分離された管理サーバーは定期的に必要な更新のリストを作成して、インターネットにアクセス可能な管理サーバーによってダウンロードされたパッチを処理できます。設定後、分離された管理サーバーはインターネットからパッチをダウンロードしようとすることはありません。その代わり、パッチ経由でアップデートを取得します。

**3 分離された管理サーバーへのパッチの送信とアップデートのインストール**

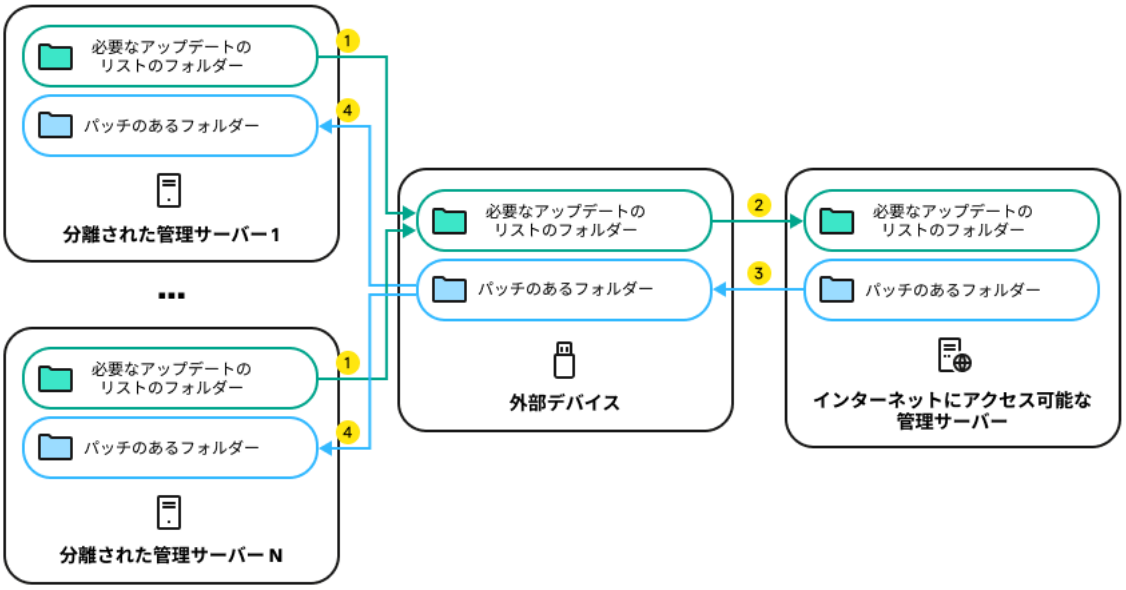
管理サーバーの設定が完了すると、インターネットにアクセス可能な管理サーバーから分離された管理サーバーに必要なアップデートリストとパッチを送信することができるようになります。次に、パッチからのアップデートと修正が、*アップデートのインストールと脆弱性の修正*タスクを使用して管理対象デバイスにインストールされます。

## 結果

サードパーティ製ソフトウェアのアップデートは、分離された管理サーバーに送信され、Kaspersky Security Center Linuxを使用して接続された管理対象デバイスにインストールされます。管理サーバーを1回設定するだけで、その後は必要に応じて、たとえば1日に1回または数回アップデートを取得できます。

# 分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正について

分離されたネットワークでのサードパーティ製品の脆弱性の修正プロセスについては下図に示す通りです。このプロセスは定期的に繰り返すことができます。




インターネットにアクセス可能な管理サーバーと分離された管理サーバー間でのパッチと必要なアップデートのリストを送信するプロセス

インターネットから分離されたすべての管理サーバーは（以降、「分離された管理サーバー」と表記）、この管理サーバーに接続された管理対象デバイス上にインストールしなければならないアップデートのリストを生成します。このアップデートのリストは、必要なアップデートを含むパッチの ID で名前が付けられた一連のバイナリファイルとして特定のフォルダーに保存されます。したがって、リスト内の各ファイルは特定のパッチに対応します。

必要なアップデートのリストは、分離された管理サーバーから、外部デバイスによるインターネットアクセスを使用して割り当てられた管理サーバーに転送されます。その後、指定された管理サーバーはインターネットからパッチをダウンロードし、指定されたフォルダーに保存します。

すべてのパッチがダウンロードされ、指定されたフォルダーに配置されると、必要なアップデートのリストが取得されたそれぞれの分離された管理サーバーに転送されます。パッチは、分離された各管理サーバー上に特別に作成されたフォルダーに保存されます。

結果、*アップデートのインストールと脆弱性の修正*タスクが分離された管理サーバーの管理対象デバイスにパッチを実行し、アップデートをインストールします。

# 分離されたネットワークで脆弱性を修正するためのインターネットにアクセス可能な管理サーバーの構成

分離されたネットワークで脆弱性の修正およびパッチの送信を準備するには、最初にインターネットにアクセス可能な管理サーバーを設定し、次に分離された管理サーバーを設定します。

*インターネットにアクセス可能な管理サーバーを設定するには：*

1. 管理サーバーがインストールされているディスクに 2 つのフォルダーを作成します。

   - 必要なアップデートのリストのフォルダー
   - パッチのフォルダー

   これらのフォルダーには必要に応じて名前を付けることができます。

2. オペレーティングシステムの標準の管理ツールを使用して、作成したフォルダーで KLAdmins グループに**変更**アクセス権限を付与します。

3. klscflag ユーティリティを使用して、管理サーバーのプロパティにフォルダーのパスを指定します。

   コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

4. コマンドラインで次のコマンドを実行します：

   - パッチのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<フォルダーのパス>"`
   - 必要なアップデートのリストのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<フォルダーのパス>"`

   例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/パッチ用フォルダ"`

5. 必要であれば、klscflag ユーティリティを使用して、管理サーバーが新しいパッチリクエストをチェックする頻度を指定します：
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <頻度の値（秒）>`

   既定値は 120 秒です。

   例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. 管理対象デバイスにインストールされているサードパーティ製ソフトウェアのパッチに関する情報を取得するには、*脆弱性とアプリケーションのアップデートの検索*タスクを作成し、タスクスケジュールを設定します。

7. *脆弱性の修正*タスクを作成し、脆弱性を修正するために使用されるサードパーティ製ソフトウェアのパッチを指定して、タスクスケジュールを設定します。

   スケジュールで指定されているよりも早く実行したい場合は、手動でタスクを実行します。タスクを開始する順序は重要です。*脆弱性の修正*タスクは、*脆弱性とアプリケーションのアップデートの検索*タスクを完了した後に実行する必要があります。

8. 管理サーバーサービスを再起動します。

インターネットにアクセス可能な管理サーバーで、アップデートをダウンロードして分離された管理サーバーに送信する準備が整いました。脆弱性の修正を開始する前に、分離された管理サーバーを設定してください。

# 分離されたネットワークの脆弱性を修正するための分離された管理サーバーの設定

インターネットにアクセス可能な管理サーバーを設定してから、ネットワーク内の分離されたすべての管理サーバーを準備してください。分離された管理サーバーに接続された管理対象デバイスの脆弱性を修正し、アップデートをインストールします。

*分離された管理サーバーを設定するには、各管理サーバーに対して以下の手順に従います：*

1. 脆弱性とパッチ管理（VAPM）機能のライセンスをアクティベートします。
2. 管理サーバーがインストールされているディスクに 2 つのフォルダーを作成します。
   - 必要なアップデートのリストのフォルダー
   - パッチのフォルダー

   これらのフォルダーには必要に応じて名前を付けることができます。
3. オペレーティングシステムの標準の管理ツールを使用して、作成したフォルダーで KLAdmins グループに**変更**権限を付与します。
4. klscflag ユーティリティを使用して、管理サーバーのプロパティにフォルダーのパスを指定します。

   コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。
5. コマンドラインで次のコマンドを実行します：
   - パッチのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<フォルダーのパス>"`
   - 必要なアップデートのリストのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<フォルダーのパス>"`

   例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`
6. 必要であれば、klscflag ユーティリティを使用して、分離された管理サーバーが新しいパッチをチェックする頻度を指定します：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <頻度の値（秒）>`

   既定値は 120 秒です。

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. 必要であれば、klscflag ユーティリティを使用して、パッチの SHA256 ハッシュを計算します：
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   このコマンドを実行すると、分離された管理サーバーに転送されてからパッチが変更されていないことと、必要なアップデートを含む正しいパッチを受け取ったことを確認できます。

   既定では、Kaspersky Security Center Linux はパッチの SHA256 ハッシュを計算しません。このオプションをオンにすると、分離された管理サーバーがパッチを受信した後、Kaspersky Security Center Linux はそれらのハッシュを計算し、取得した値を管理サーバーデータベースに保存されているハッシュと比較します。計算されたハッシュがデータベース内のハッシュと一致しない場合はエラーが発生し、間違ったパッチを置き換える必要があります。

8. 管理対象デバイスにインストールされているサードパーティ製ソフトウェアのパッチに関する情報を取得するには、「*脆弱性とアプリケーションのアップデートの検索*」タスクを作成し、タスクスケジュールを設定します。

9. *脆弱性の修正*タスクを作成し、脆弱性を修正するために使用されるサードパーティ製ソフトウェアのパッチを指定して、タスクスケジュールを設定します。

   スケジュールで指定されているよりも早く実行したい場合は、手動でタスクを実行します。タスクを開始する順序は重要です。*脆弱性の修正*タスクは、*脆弱性とアプリケーションのアップデートの検索*タスクを完了した後に実行する必要があります。

10. 管理サーバーサービスを再起動します。

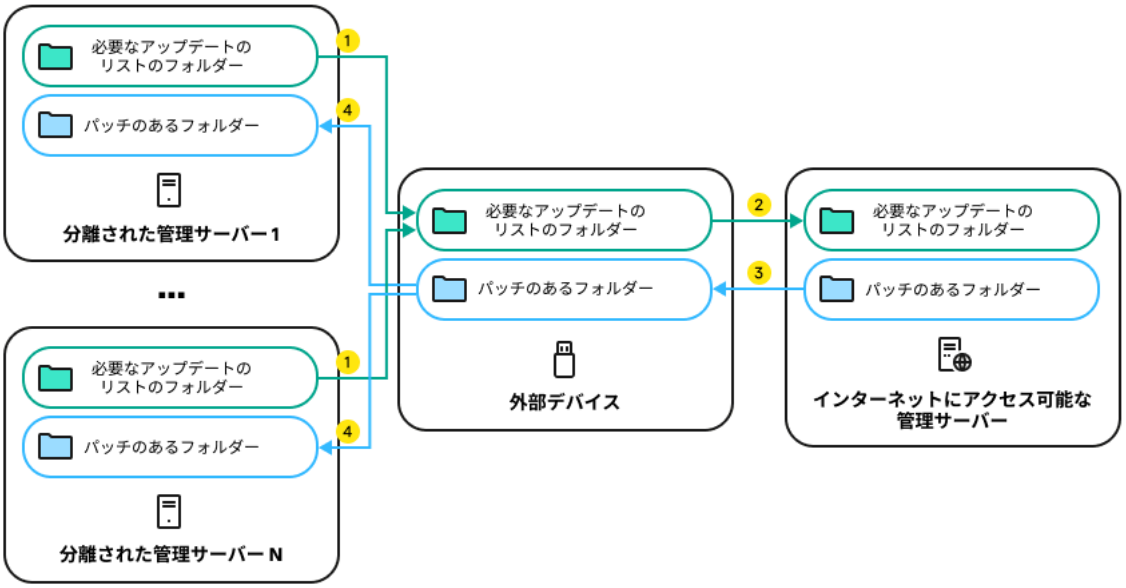
すべての管理サーバーを設定すると、パッチと必要なアップデートのリストを送信し、分離されたネットワーク内の管理対象デバイスのサードパーティ製ソフトウェアの脆弱性を修正できるようになります。

# 分離されたネットワークでのパッチの送信とアップデートのインストール

管理サーバーの設定を完了してから、インターネットにアクセス可能な管理サーバーから分離された管理サーバーにアップデートを含むパッチを転送できます。アップデートは、たとえば、1日に1回または数回など、必要に応じて何度でも送信およびインストールできます。

管理サーバー間でパッチと必要なアップデートのリストを転送するには、リムーバブルドライブなどの外付けドライブが必要です。したがって、外付けドライブにパッチをダウンロードして保存する十分なディスク容量があることを確認してください。

パッチを送信するプロセスと必要なアップデートのリストは下図の通りです：




インターネットにアクセス可能な管理サーバーと分離された管理サーバー間でのパッチと必要なアップデートのリストを送信するプロセス

*分離された管理サーバーに接続されている管理対象デバイスにアップデートをインストールして脆弱性を修正するには：*

1. 実行されていない場合は、*アップデートのインストールと脆弱性の修正*タスクを実行します。
2. 外付けドライブを分離された任意の管理サーバーに接続します。
3. 外付けドライブに 2 つのフォルダーを作成します。1つは必要なアップデートのリスト用で、もう1つはパッチ用です。これらのフォルダーには任意の名前を付けることができます。

   以前にフォルダーを作成していた場合は、それらを消去します。
4. すべての分離された管理サーバーから必要なアップデートのリストをコピーして、外付けドライブ上にある必要なアップデートのリスト用のフォルダーに貼り付けます。

   結果、すべての分離された管理サーバーから取得したすべてのリストを1津のフォルダーに集約したことになります。このフォルダーには、分離されたすべての管理サーバーに必要なパッチの ID が付いたバイナリファイルが含まれます。
5. 外付けドライブをインターネットにアクセス可能な管理サーバーに接続します。
6. 外付けドライブから必要なアップデートのリストをコピーして、インターネットにアクセス可能な管理サーバー上にある必要なアップデート用のフォルダーに貼り付けます。

   すべての必要なパッチは、管理サーバー上にあるパッチ用のフォルダーにインターネットから自動的にダウンロードされます。これには数時間かかる場合があります。
7. 必要なパッチがすべてダウンロードされていることを確認してください。この目的のために、次の操作のうち1つを実行できます：

   - インターネットにアクセス可能な管理サーバー上のパッチがないかフォルダーを確認してください。必要なアップデートのリストで指定されたすべてのパッチは、必要なフォルダーにダウンロードされます。これは、必要なパッチの数が少ない場合に便利です。
   - シェルスクリプトなどの特別なスクリプトを準備します。多数のパッチを入手した場合、すべてのパッチがダウンロードされたことを自分で確認するのは難しくなります。このような場合は、チェックを自動化することをお勧めします。

8. インターネットにアクセス可能な管理サーバーからパッチをコピーして、外付けドライブの対応するフォルダーに貼り付けます。

9. 分離されたすべての管理サーバーにパッチを転送します。パッチを特定のフォルダーに入れます。

その結果、分離されたすべての管理サーバーは、現在の管理サーバーに接続されている管理対象デバイスに必要なアップデートの実際のリストを作成します。インターネットにアクセス可能な管理サーバーが必要なアップデートのリストを受信した後、管理サーバーはインターネットからパッチをダウンロードします。パッチが分離された管理サーバー上に現れると、*アップデートのインストールと脆弱性の修正*タスクがパッチを処理します。このように、アップデートが管理対象デバイスにインストールされ、ソフトウェアの脆弱性が修正されます。

*アップデートのインストールと脆弱性の修正*タスクの実行中には、管理サーバーデバイスを再起動しないでください。また、再起動を必要とする*管理サーバーデータのバックアップ*タスクも実行しないでください。*アップデートのインストールと脆弱性の修正*タスクが中断され、アップデートがインストールされません。この場合、このタスクを手動で再開するか、設定されたスケジュールに従って実行されるまで待つ必要があります。

# 分離されたネットワークでのパッチの送信とアップデートのインストールを無効にする

分離されたネットワークから1つまたはそれ以上のサーバーを取り出すことにした場合など、分離された管理サーバーでパッチの送信を無効にすることができます。このように、パッチの数とそれらをダウンロードする時間を削減することができます。

*分離された管理サーバーへのパッチの送信を無効にするには：*

1. 管理サーバーを分離状態から削除するには、インターネットに接続できる管理サーバーのプロパティで、パッチのフォルダーと必要なアップデートのリストからパスを削除してください。分離されたネットワークに特定の管理サーバーをそのまま置いておくには、この手順を省略してください。

   コマンドラインを実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているディレクトリにあります。既定のインストールパスは /opt/kaspersky/ksc64/sbin です。

   コマンドラインで次のコマンドを実行します：

   - パッチのフォルダーのパスを削除するには：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - 必要なアップデートのリストのフォルダーのパスを削除するには：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. フォルダーへのパスを削除した場合は、インターネットにアクセスできる管理サーバーでサービスを再起動します。

3. 分離状態から取り出すそれぞれの管理サーバーのプロパティで、パッチのフォルダーのパスと必要なアップデートのリストのフォルダーのパスを削除してください。

   ルート権限を持つアカウントのコマンドラインで次のコマンドを実行します：

   - パッチのフォルダーのパスを削除するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`

   - 必要なアップデートのリストのフォルダーのパスを削除するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. フォルダーのパスを削除したそれぞれの管理サーバーのサービスを再起動します。

インターネットにアクセス可能な管理サーバーを再設定した場合、パッチは Kaspersky Security Center Linux 経由で送信されなくなります。

特定の管理サーバーのみを再設定し、分離されたネットワークから削除した場合、それらのサーバーは Kaspersky Security Center Linux 経由でパッチを受信しなくなります。分離されたネットワーク内に残っている管理サーバーのみ、引き続きパッチを受信します。

将来、無効になっている分離された管理サーバーの脆弱性の修正を開始する場合は、もう一度これらの管理サーバーとインターネットにアクセスできる管理サーバーを構成する必要があります。

# API リファレンスガイド

この Kaspersky Security Center OpenAPI リファレンスガイドは、次のタスクを支援する目的で作成されています：

- 自動化とカスタマイズ。手動で扱う必要がないタスクを自動化できます。たとえば、管理者として Kaspersky Security Center OpenAPI を使用し、管理グループ構造の作成を支援するスクリプトを作成、実行することで、その構造の最新の状態を維持できます。
- カスタム開発。OpenAPI を使用して、クライアントアプリケーションを開発できます。

画面右側の検索フィールドを使用して OpenAPI リファレンスガイドから必要な情報を見つけることができます。

**OPENAPI リファレンスガイド（英語）**

## スクリプトのサンプル

OpenAPI リファレンスガイドには、次の表に示す Python スクリプトのサンプルが含まれています。これらのサンプルは、OpenAPI メソッドを呼び出して、ネットワークを保護するための様々なタスクを自動的に実行する方法を示しています。たとえば、「プライマリ」と「セカンダリ」の階層の作成、Kaspersky Security Center Linux でのタスクの実行、ディストリビューションポイントの割り当てなどの方法です。サンプルをそのまま実行することも、サンプルを基に独自のスクリプトを作成することもできます。

*OpenAPI メソッドを呼び出してスクリプトを実行するには：*

1. KlAkOAPI.tar.gz アーカイブをダウンロードします。このアーカイブには、KlAkOAPI パッケージとサンプルが含まれています（アーカイブまたは OpenAPI リファレンスガイドからコピーできます）。

2. 管理サーバーがインストールされているデバイス上の KlAkOAPI.tar.gz アーカイブから KlAkOAPI パッケージをインストールします。

   OpenAPI メソッドを呼び出し、サンプルや独自のスクリプトを実行するのは、管理サーバーと KlAkOAPI パッケージがインストールされているデバイスでのみ実行できます。

ユーザーシナリオと Kaspersky Security Center OpenAPI メソッドのサンプルの一致

| サンプル | サンプルの目的 | シナリオ |
| --- | --- | --- |
| KlAkParams のログ記録 | `KlAkParams` データ構造を使用してデータを抽出、処理できます。サンプルには、このデータ構造の使用方法を示しています。<br>サンプル出力は、様々な方法で表示される場合があります。データを取得して HTTP メソッドを送信したり、自分のコードで使用したりできます。 | 監視とレポート |
| プライマリ / セカンダリ階層の作成と削除（英語） | 管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立できます。または、セカンダリ管理サーバーを階層から切断することもできます。 | 管理サーバーの階層の作成、セカンダリ管理サーバーの追加、管理サーバーの階層の削除 |
| 接続ゲートウェイを使用してネットワークリストファイルを指定したホストにダウンロード | 接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に、ネットワークリストを含むファイルをデバイスにダウンロードします。 | ディストリビューションポイントと接続ゲートウェイの調整 |
| プライマリ管理サーバーリポジトリに保存されたライセンスのセカンダリ管理サーバーへのインストール | プライマリ管理サーバーに接続し、そこから必要なライセンスをダウンロードして、このライセンスを階層内のすべてのセカンダリ管理サーバーに送信できます。 | 管理対象アプリケーションのライセンスの管理 |
| 有効なユーザー権限のレポートの作成 | 様々なレポートを作成できます。たとえば、このサンプルを使用して、有効なユーザー権限のレポートを生成できます。このレポートでは、ユーザーのグループと役割に応じて、ユーザーが持つ権限について説明します。<br>レポートは、HTML、PDF、Excel 形式でダウンロードできます。 | レポートの生成と表示 |
| デバイスタスクの開始 | 接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に必要なタスクを実行します。 | タスクの手動での開始 |
| デバイスのディストリビューションポイントのグループへの登録（英語） | 管理対象デバイスをディストリビューションポイント（以前はアップデートエージェントと呼ばれていました）として割り当てることができます。 | 定義データベースとカスペルスキー製品のアップデート |
| すべてのグループの列挙（英語） | 管理グループに対して、様々な処理を実行できます。サンプルでは、次の実行方法を例示しています：<br>• ［管理対象デバイス］ルートグループの識別子の取得<br>• グループ階層の移動<br>• グループの完全な拡張階層を、名前とネスト構造とともに取得 | 管理サーバーの設定 |
| タスクの列挙、タスクの統計のクエリ、タスクの実行（英語） | 参照可能な情報は次の通りです：<br>• タスクの進捗履歴<br>• 現在のタスクステータス<br>• 様々なステータスのタスクの数<br>タスクの実行も可能です。既定では、サンプルは統計の出力後にタスクを実行します。 | タスクの管理 |

| サンプル | サンプルの目的 | シナリオ |
| --- | --- | --- |
| タスクの作成と実行（英語） | タスクを作成できます。サンプルにある次のタスクパラメータを指定します：<br>• 種別<br>• 実行方法<br>• 名前<br>• タスクが使用されるデバイスグループ<br>既定では、サンプルは「メッセージを表示する」種別のタスクを作成します。このタスクは、管理サーバーのすべての管理対象デバイスに対して実行できます。必要に応じて、タスクパラメータを独自に指定できます。 | タスクの作成 |
| ライセンスの列挙（英語） | 管理サーバーが管理するデバイスにインストールされたカスペルスキー製品の、現在のライセンスがすべてリストされた一覧を取得できます。リストには、全ライセンスの詳細データ（名前、種別、有効期限日など）が含まれています。 | 使用中のライセンスに関する情報の表示 |
| 内部ユーザーの作成および検索（英語） | さらなる作業のためにアカウントを作成できます。 | 内部ユーザーのアカウントの追加 |
| カスタムカテゴリの作成（英語） | 必要なパラメータとともに、アプリケーションカテゴリを作成できます。 | コンテンツが手動で追加されるアプリケーションカテゴリの作成 |
| SrvView を使用したユーザーの列挙（英語） | SrvView クラスを使用して、管理サーバーからの詳細な情報をリクエストできます。たとえば、このサンプルを使用してユーザーのリストを取得できます。 | ユーザーとユーザーロールの管理 |

## OpenAPI 経由で Linux Kaspersky Security Center と連携するアプリケーション

一部のアプリケーションは、OpenAPI 経由で Kaspersky Security Center Linux と連携します。Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization などがこのようなアプリケーションに含まれます。また、OpenAPI に基づいて開発されたカスタムクライアントアプリケーションであることもあります。

OpenAPI 経由で Kaspersky Security Center Linux と連携するアプリケーションは管理サービスに接続します。管理サーバーへの接続用に IP アドレスの許可リストを設定している場合は、Kaspersky Security Center Linux の OpenAPI を使用するアプリケーションをインストールしているデバイスの IP アドレスを追加してください。使用しているアプリケーションが OpenAPI によって動作しているかどうかについては、そのアプリケーションのヘルプを参照してください。

# 導入と設定に関する推奨事項

このセクションでは、Kaspersky Security Center Linux の設定方法と使用方法について説明します。

アプリケーションの導入、設定、および使用方法についての推奨事項を確認いただけます。また、アプリケーションの操作に関する一般的な問題を解決する方法についても説明しています。

## Kaspersky Security Center Linux の導入を計画する

組織のネットワークに Kaspersky Security Center Linux コンポーネントを導入する計画がある場合は、プロジェクトのサイズと範囲を考慮する必要があります。特に、次の要素を重視してください：

- デバイスの合計数
- MSP クライアントの数

1 台の管理サーバーで最大 50,000 台のデバイスをサポートできます。組織ネットワーク上に合計で 50,000 台を超えるデバイスが存在する場合は、サービスプロバイダー側で複数の管理サーバーを導入し、階層化して一元的に管理する必要があります

1 台の管理サーバーで最大 500 の仮想サーバーを作成できます。このため、MSP クライアント 500 ごとに管理サーバー 1 台が必要です。

導入計画段階では、管理サーバーに対して特別な X.509 証明書を割り当てることを検討する必要があります。管理サーバーに対する X.509 証明書の割り当てが有効になるのは、次の場合です（部分的なリスト）：

- SSL Termination プロキシを使用して、セキュアソケットレイヤー（SSL）トラフィックをスキャンする場合
- 証明書で必要な値を指定する場合
- 証明書で必要な暗号化強度を指定する場合

## 管理サーバーへのインターネットアクセス

クライアントネットワーク上のデバイスにインターネット経由での管理サーバーへのアクセスを許可するためには、次の管理サーバーのポートを使用できるようにする必要があります：

- 13000 TCP — クライアントネットワークに導入されたネットワークエージェントを接続するための管理サーバーの TLS ポート
- 8061 TCP — Kaspersky Security Center Web コンソールツールを使用してスタンドアロンパッケージを公開するための HTTPS ポート
- 8060 TCP — Kaspersky Security Center Web コンソールツールを使用してスタンドアロンパッケージを公開するための HTTP ポート

- 13292 TCP — 管理が必要なモバイルデバイスがある場合のみ必要とされる TLS ポート
- 8080 TCP — Kaspersky Security Center Web コンソールの HTTPS ポート

# Kaspersky Security Center Linux の標準設定

1 台または複数台の管理サーバーを MSP のサーバーに導入します。管理サーバーの数は、使用可能なハードウェア、MSP クライアントの合計数、または管理対象デバイスの合計数に基づき選択可能です。

1 台の管理サーバーで最大 50,000 台のデバイスをサポートできます。導入後に管理対象デバイスを増やす可能性がある場合は、1 台の管理サーバーに接続するデバイスの数を少なくしておきます。

1 台の管理サーバーで最大 500 の仮想サーバーを作成できます。このため、MSP クライアント 500 ごとに管理サーバー 1 台が必要です。

複数台のサーバーを使用する場合は、1 つの階層に統合してください。管理サーバーの階層を使用することによりポリシーとタスクが重複するのを防ぎ、管理対象デバイスの全セットを 1 台の管理サーバーで管理している場合と同様に処理できます。つまり、デバイスの検索、デバイス選択の構築、レポートの作成などの処理です。

MSP クライアントに対応する各仮想サーバー上で、ディストリビューションポイントを 1 台または複数台、割り当てる必要があります。MSP クライアントと管理サーバーがインターネットを経由して接続されている場合は、ディストリビューションポイントで、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成しておくことが有用な場合があります。これにより、管理サーバーからではなくカスペルスキーのサーバーから直接アップデートをダウンロードできるようになります。

MSP クライアントネットワーク内のデバイスの一部がインターネットに直接アクセスできない場合、ディストリビューションポイントをゲートウェイモード接続に切り替える必要があります。この場合、MSP クライアントネットワーク上のデバイスのネットワークエージェントは、直接ではなくゲートウェイを介して管理サーバーに接続され、緊密に同期します。

たいていの場合、管理サーバーは MSP クライアントネットワークをポーリングできないので、ディストリビューションポイントに対してこの機能をオンにしておくと便利です。

管理サーバーは、MSP クライアントネットワーク上で NAT よりも内側にある管理対象デバイスに対して、ポート 15000 UDP に通知を送信することはできません。この問題は、ディストリビューションポイントとして動作し、接続ゲートウェイモードで実行中のデバイスのプロパティで、管理サーバーへの常時接続モード（[**管理サーバーから切断しない**]）をオンにすることで解決できる場合があります。連続接続モードは、ディストリビューションポイントの合計数が 300 を超えていない場合に使用可能です。

MSP クライアントは、従業員の Android デバイスと iOS デバイスを管理したい場合があります。管理サーバーは、モバイルデバイスを TLS、TCP ポート 13292 を使用して管理します。

# ディストリビューションポイントの概要

ネットワークエージェントがインストールされたデバイスはディストリビューションポイントとして使用できます。このモードでは、ネットワークエージェントは、次の機能を実行できます：

- 次のファイルをクライアントデバイスに転送します：
  - 定義データベースとソフトウェアモジュールのアップデート

    アップデートは管理サーバーまたはカスペルスキーのサーバーから取得できます。後者の場合、ディストリビューションポイントとして機能するデバイスに対して*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成する必要があります。
  - サードパーティ製ソフトウェアのアップデート
  - インストールパッケージ
- その他のデバイスへのソフトウェアのインストール（ネットワークエージェントの初期導入を含む）。
- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。

組織ネットワークにディストリビューションポイントを導入する目的は、次の通りです：

- アップデート元として機能させる場合、管理サーバーの負荷を減らします。
- インターネットのトラフィックを最適化します。この場合、MSP クライアントネットワーク上にある各デバイスがアップデート時にカスペルスキーのサーバーまたは管理サーバーにアクセスする必要がないためです。
- 管理サーバーに、MSP クライアントネットワークの NAT の背後（管理サーバーを基準にして）にあるデバイスへのアクセスを提供し、管理サーバーが次の処理を実行できるようにします：
  - IPv4 または IPv6 ネットワークの UDP を経由したデバイスへの通知の送信
  - IPv4 または IPv6 ネットワークの検索
  - 初期導入の実行
  - プッシュサーバーとしての動作

1つの管理グループに対して、1つのディストリビューションポイントが割り当てられます。この場合、ディストリビューションポイントの範囲には、管理グループとそのすべてのサブグループ内にあるすべてのデバイスが含まれます。ただし、ディストリビューションポイントとして動作しているデバイスは、割り当てられている管理グループに含まれていなくてもかまいません。

ディストリビューションポイントを接続ゲートウェイとして動作させることができます。この場合、ディストリビューションポイントの範囲内のデバイスは、管理サーバーと直接接続されずゲートウェイを介して接続されます。このモードは、ネットワークエージェントをインストールしたデバイスと管理サーバー間を直接には接続できない場合に有効です。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

# 管理サーバーの階層構造

MSP などの一部のクライアント企業は、複数の管理サーバーを実行している場合があります。複数台の別の管理サーバーを管理するのは不便であるため、1つの階層を適用することができます。階層で、Linux ベースの管理サーバーはプライマリサーバーとセカンダリサーバーのどちらとしても機能できます。Linux ベースのプライマリサーバーは、Linux ベースと Windows ベースのセカンダリサーバーの両方を管理できます。プライマリ Windows ベースのサーバーは、セカンダリ Linux ベースのサーバーを管理できます。

2 台の管理サーバーのプライマリおよびセカンダリ設定には、次のオプションがあります：

- セカンダリ管理サーバーは、プライマリ管理サーバーからポリシー、タスク、ユーザーロール、インストールパッケージを継承することにより、設定の重複を防ぎます。
- プライマリ管理サーバーのデバイスには、セカンダリ管理サーバーのデバイスを含めることができます。
- プライマリ管理サーバーのレポートには、セカンダリ管理サーバーのデータ（詳細情報を含む）を含めることができます。
- プライマリ管理サーバーは、セカンダリ管理サーバーのアップデート元として使用できます。

プライマリ管理サーバーは、上記のオプションの範囲内で非仮想セカンダリ管理サーバーからのみデータを受信します。この制限は、プライマリ管理サーバーと定義データベースを共有する仮想管理サーバーには適用されません。

# 仮想管理サーバー

物理管理サーバーに基づいて、複数台の仮想管理サーバーを作成できます。これは、セカンダリ管理サーバーと類似したものです。仮想管理サーバーモデルは、アクセス制御リスト（ACL）に基づいた任意のアクセスモデルと比較した場合、機能性が高く、高度の分離性を実現しています。ポリシーとタスクが存在する割り当て済みデバイスの管理グループ専用の構造に加えて、各仮想管理サーバーにも未割り当てデバイスのグループ、レポート、抽出されたデバイスとイベント、インストールパッケージ、移動ルールなどがあります。各 MSP クライアントを最大限に分離するため、使用する機能に仮想管理サーバーを選択することを推奨します。さらに、各 MSP クライアントに仮想管理サーバーを作成すると、Kaspersky Security Center Web コンソールを介して、クライアントにネットワーク管理の基本オプションを提供することができます。

仮想管理サーバーはセカンダリ管理サーバーと非常に類似していますが、次の相違点があります：

- 仮想管理サーバーには、多数のグローバル設定と独自の TCP ポートが備えられていません。
- 仮想管理サーバーには、セカンダリ管理サーバーはありません。
- 仮想管理サーバーには、他の仮想管理サーバーはありません。
- 物理管理サーバーには、すべての仮想管理サーバーの管理対象デバイスに関するデバイス、グループ、およびオブジェクトが表示されます（隔離中の項目、アプリケーションレジストリなど）。
- 仮想管理サーバーがスキャンできるのは、ディストリビューションポイントが接続されているネットワークのみです。

# 導入と初期セットアップ

Kaspersky Security Center Linux は配信アプリケーションです。Kaspersky Security Center Linux には次のアプリケーションが含まれます：

- 管理サーバー - 組織のデバイスを管理し、DBMS にデータを格納するためのコアコンポーネント。
- Kaspersky Security Center Web コンソールは、基本操作向けに設計された管理サーバー用 Web インターフェイスです。このコンポーネントはシステム要件を満たす任意のデバイスにインストールできます。
- ネットワークエージェント - デバイスにインストールされているセキュリティ製品の管理、およびそのデバイスに関する情報の取得を実行。組織のデバイスには、ネットワークエージェントがインストールされています。

組織ネットワークに Kaspersky Security Center Linux を導入するには、次の作業を実行します：

- 管理サーバーのインストール
- Kaspersky Security Center Web コンソールのインストール
- 企業のデバイスへのネットワークエージェントとセキュリティ製品のインストール

# 管理サーバーのインストールに関する推奨事項

このセクションでは、管理サーバーをインストールする際の推奨事項について説明します。また、管理サーバーデバイスの共有フォルダーを使用して、クライアントデバイスにネットワークエージェントを導入する方法についても説明します。

## フェールオーバークラスターに管理サーバーサービス用のアカウントを作成する

フェールオーバークラスタに Kaspersky Security Center Linux を導入する前に、Kaspersky Security Center Linux サービスのアカウントを作成する必要があります。

これを実行するには、アクティブノード、パッシブノード、およびファイルサーバーで次の手順を実行します：

1. 「kladmins」という名前のグループを作成し、3 つのグループすべてに同じ GID を割り当てます。
2. 「ksc」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。作成したアカウントのプライマリグループを「kladmins」に設定します。
3. 「rightless」という名前のユーザーアカウントを作成し、3 つのユーザーアカウントすべてに同じ UID を割り当てます。作成したアカウントのプライマリグループを「kladmins」に設定します。

# DBMS の選択

次の表に、有効な DBMS オプションとその使用上の推奨事項と制限事項を示します。

DBMS に関する推奨事項と制限事項

| DBMS | 推奨事項と制限事項 |
| --- | --- |
| MySQL（サポートされているバージョンを参照） | 20,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |
| MariaDB（サポートされているバージョンを参照） | 20,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |
| PostgreSQL、Postgres Pro（サポートされているバージョンを参照） | 50,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 |

選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。

PostgreSQL または Postgres Pro DBMS をインストールする場合は、スーパーユーザーのパスワードを指定したことを確認してください。パスワードが指定されていない場合、管理サーバーがデータベースに接続できない可能性があります。

MySQL、MariaDB、PostgreSQL、または Postgres Pro をインストールする場合は、DBMS が適切に機能するように推奨設定を使用してください。

PostgreSQL、MariaDB、または MySQL DBMS を使用する場合、［**イベント**］タブには、選択したクライアントデバイスのイベントの不完全なリストが表示されることがあります。これは、DBMS が非常に大量のイベントを保存する場合に発生します。次のいずれかを実行すると、表示されるイベントの数を増やすことができます：

- 不要なイベントを削除します。
- 不要なイベントの保存期間を短縮します。

デバイスの管理サーバーに記録されたイベントの完全なリストを表示するには、レポートを使用します。

# 管理サーバーのアドレスの指定

管理サーバーのインストール時に、管理サーバーの DNS 名または固定 IP アドレスを指定する必要があります。このアドレスは、ネットワークエージェントのインストールパッケージを作成する際の既定のアドレスとして使用されます。その後、Kaspersky Security Center Web コンソールツールを使用して管理サーバーホストのアドレスを変更できるようになります。この場合、作成済みのネットワークエージェントのインストールパッケージでは、アドレスは自動的には変更されません。

# ネットワークエージェントとセキュリティ製品の導入

組織内のデバイスを管理し、セキュリティの脅威から保護するには、各デバイスにネットワークエージェントとカスペルスキーのセキュリティ製品をインストールする必要があります。

保護の導入の詳細については、［ネットワークエージェントとセキュリティ製品の導入］セクションを参照してください。

モバイルデバイスの保護の詳細については、［モバイルデバイス管理］セクションを参照してください。

Microsoft Windows XP では、ネットワークエージェントがカスペルスキーのサーバーから（ディストリビューションポイントとして）アップデートを直接ダウンロードする操作と、（ディストリビューションポイントとして）KSN プロキシサーバーとして機能する操作を正しく実行しない可能性があります。

# クライアント組織のネットワークでの保護の設定

管理サーバーのインストールが完了すると Kaspersky Security Center Web コンソールが起動し、関連するウィザードを使用して初期セットアップを実行するよう要求されます。クイックスタートウィザードの実行中に、ルート管理グループに次のポリシーとタスクが作成されます：

- Kaspersky Endpoint Security のポリシー
- Kaspersky Endpoint Security をアップデートするグループタスク
- Kaspersky Endpoint Security がインストールされたデバイスをスキャンするグループタスク
- ネットワークエージェントのポリシー
- 脆弱性スキャンタスク（ネットワークエージェントのタスク）
- アップデートのインストールと脆弱性修正タスク（ネットワークエージェントのタスク）

ポリシーとタスクは既定の設定値で作成されますが、組織が最適ではないまたは許容できない状態であることが示されます。この場合、作成したオブジェクトのプロパティを確認し、必要な場合は手動で変更します。

このセクションでは、ポリシー、タスク、および管理サーバーのその他の設定の手動設定、ディストリビューションポイント、管理グループ構造とタスクの階層の構築や、その他の設定について説明します。

## Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、クイックスタートウィザードで作成される、Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項を説明します。ポリシーのプロパティウィンドウで設定を実行できます。

設定を編集する場合、ワークステーション上での設定値の編集を禁止または許可するために、設定をロックまたはロック解除できることに注意してください。

## ［先進の脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

［**先進の脅威対策**］セクションで、Kaspersky Endpoint Security for Windows の Kaspersky Security Network の使用を設定できます。ふるまい検知、脆弱性攻撃ブロック、ホスト侵入防止、修復エンジンなどの Kaspersky Endpoint Security for Windows モジュールを設定することもできます。

［**Kaspersky Security Network**］サブセクションで、［**Kaspersky Security Network**］をオンにすることを推奨します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。［**Kaspersky Security Network**］がオフになっている場合は、KSN サーバーの直接使用をオンにできます。

## ［脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ポリシープロパティウィンドウの［**脅威対策**］セクションで、［**ファイアウォール**］および［**ファイル脅威対策**］サブセクションに追加の設定を指定することを推奨します。

［**ファイアウォール**］サブセクションには、クライアントデバイス上のアプリケーションのネットワークアクティビティを制御できる設定が含まれています。クライアントデバイスは、パブリック、ローカル、信頼済みのいずれかのステータスが割り当てられているネットワークを使用します。ネットワークステータスに応じて、Kaspersky Endpoint Security はデバイスでのネットワークアクティビティを許可または拒否できます。組織に新しいネットワークを追加する時は、適切なネットワークステータスを割り当てる必要があります。たとえば、クライアントデバイスがノート PC の場合、ノート PC は常にローカルネットワークに接続されているとは限らないため、このデバイスではパブリックネットワークまたは信頼できるネットワークを使用することを推奨します。［**ファイアウォール**］サブセクションで、組織で使用するネットワークにステータスを正しく割り当てたことを確認できます。

*ネットワークのリストを確認するには：*

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
2. ［**使用可能なネットワーク**］セクションで、［**設定**］をクリックします。
3. 表示される［**ファイアウォール**］ウィンドウで、［**ネットワーク**］タブに移動してネットワークのリストを表示します。

［**ファイル脅威対策**］サブセクションで、ネットワークドライブのスキャンをオフにできます。ネットワークドライブのスキャンを行うと、ネットワークドライブに大幅な負荷がかかることがあります。ファイルサーバーで間接スキャンを実行するのが有効です。

*ネットワークドライブのスキャンを無効にするには：*

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイル脅威対策**］の順に選択します。
2. ［**セキュリティレベル**］セクションで、［**設定**］をクリックします。
3. ［**ファイル脅威対策**］ウィンドウが開いたら、［**全般**］タブで［**すべてのネットワークドライブ**］をオフにします。

## ［全般設定］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明は、Kaspersky Endpoint Security のヘルプを参照してください。

以下で、詳細なセットアップ操作について説明します。この操作は、Kaspersky Endpoint Security のポリシーのプロパティウィンドウの［**全般設定**］セクションで実行してください。

## ［全般設定］セクション、［レポートと保管領域］サブセクション

［**管理サーバーへのデータ転送**］セクションで、［**起動されたアプリケーションの情報**］をオンにしてください。このチェックボックスをオンにすると、管理サーバー定義データベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報が保存されます。この情報は、Kaspersky Security Center Linux データベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。このため、トップレベルのポリシーで［**起動されたアプリケーションの情報**］がオンになっている場合は、オフにする必要があります。

## ［全般設定］セクション、［インターフェイス］サブセクション

Kaspersky Security Center Web コンソールを使用して、組織のネットワークの脅威対策を集中管理する必要がある場合は、ワークステーション上の Kaspersky Endpoint Security のユーザーインターフェイスの表示をオフにし（［**ユーザーとの対話**］セクションの［**アプリケーションインターフェイスを表示する**］をオフにする）、パスワード保護を有効にする（［**パスワードによる保護**］セクションの［**パスワード保護を有効にする**］をオンにする）必要があります。

## ［イベントの設定］セクションでのポリシーの設定

［**イベントの設定**］セクションで、管理サーバーに関する次の項目以外のすべてのイベントを保存しないように設定する必要があります：

- ［**緊急**］タブ：
  - *コンピューター起動時の自動実行がオフです*
  - *アクセスが拒否されました*
  - *アプリケーションの起動が禁止されました*
  - *駆除できません*
  - *使用許諾契約書違反です*
  - *暗号化モジュールを読み込めません*
  - *2つのタスクを同時に開始できません*
  - *アクティブな脅威が検知されました。特別な駆除を開始してください*
  - *ネットワーク攻撃の検知*
  - *アップデートされていないコンポーネントがあります*
  - *アクティベーションエラー*
  - *ポータブルモードの有効化中にエラーが発生しました*
  - *Kaspersky Security Center との通信中にエラーが発生しました*
  - *ポータブルモードの無効化中にエラーが発生しました*
  - *アプリケーションコンポーネントの変更エラー*
  - *ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました*
  - *ポリシーを適用できません*
  - *プロセスが終了しました*
  - *ネットワーク動作がブロックされました*
- **機能エラー**タブ：*タスク設定が無効です。設定は反映されていません*

- ［**警告**］タブ：
  - *セルフディフェンスがオフです*
  - *予備のライセンスが正しくありません*
  - *ユーザーが暗号化ポリシーを拒否しました*
- ［**情報**］タブ：*アプリケーションの起動がテストモードでブロックされています*

## Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

管理サーバーがアップデート元として動作する場合、Kaspersky Endpoint Security で最適かつ推奨されるスケジュールオプションは、［**新しいアップデートがリポジトリにダウンロードされ次第**］と［**タスクの開始を自動的かつランダムに遅延させる**］をオンにすることです。

カスペルスキーのサーバーからリポジトリにダウンロードをアップデートするローカルタスクが各ディストリビューションポイントで作成される場合、Kaspersky Endpoint Security グループのアップデートタスクに合わせて定期スケジュールを組むことが最適かつ推奨されます。この場合、ランダム化の間隔を 1 時間に設定する必要があります。

## Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ

クイックスタートウィザードにより、デバイススキャン用のグループタスクが作成されます。自動的に指定されたグループスキャンタスクのスケジュールが組織にとって適切でない場合は、組織で採用されている職場のルールに基づいて、このタスクに最も便利なスケジュールを手動で設定する必要があります。

たとえば、このタスクは**金曜日の午後 7 時に実行**するよう設定され、［**未実行のタスクを実行する**］がオフになっています。つまり、組織内のデバイスが、たとえば、金曜日の午後 6 時 30 分にシャットダウンされる場合、そのデバイスのスキャンタスクは一切実行されません。この場合、グループスキャンタスクを手動で設定する必要があります。

## 脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定

クイックスタートウィザードにより、ネットワークエージェントでの*脆弱性とアプリケーションのアップデートの検索*タスクが作成されます。既定では、このタスクは**火曜日の午後 7 時に実行**するよう設定されており、［**未実行のタスクを実行する**］がオンになっています。

組織で採用されている職場のルールによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり水曜日の朝以降に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

# アップデートのインストールと脆弱性の修正用グループタスクの手動セットアップ

クイックスタートウィザードにより、ネットワークエージェントのアップデートのインストールと脆弱性の修正用のグループタスクが作成されます。既定では、このタスクの実行時間は毎日午前1時に設定されており、［**未実行のタスクを実行する**］がオフになっています。

組織の職場のルールにより夜間はデバイスをシャットダウンするように定められている場合、アップデートのインストールは一切実行されません。組織で採用されている職場のルールに基づいて、脆弱性スキャンタスクに対する最も効率的なスケジュールをセットアップする必要があります。また、アップデートのインストール時には、デバイスの再起動を要求される場合があることにも注意してください。

# 管理グループの構造の構築とディストリビューションポイントの割り当て

Kaspersky Security Center Linux の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する一連の設定をデバイスに適用する別の方法は、ポリシーのプロファイルを使用することです。この場合、ポリシーの範囲はたとえばデバイスタグ、ユーザーロールなどで設定されます。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の構造と MSP クライアントによって導入されたネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス

- 複数の小規模な離れているオフィス

## MSP クライアントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

管理グループの構造は、次の方法で構築することが可能です：

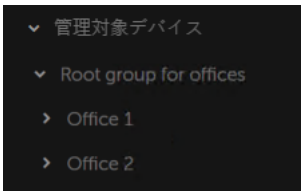
- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。

- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する1台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは、最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティまたは traceroute ユーティリティによって追跡できます。

## MSP クライアントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。




管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

# ポリシーのプロファイルを使用した、ポリシーの階層

このセクションでは、管理グループ内のデバイスにポリシーを適用する方法について説明します。また、ポリシープロファイルについても説明します。

## ポリシーの階層

Kaspersky Security Center Linux では、複数のデバイスに対して単一の一連の設定を定義するためにポリシーを使用します。たとえば、管理グループ G で定義されているアプリケーション P のポリシー範囲には、グループ G とそのすべてのサブグループの、アプリケーション P がインストールされた管理対象デバイスが含まれます。ただし、プロパティで［**親グループから継承する**］がオフになっているサブグループを除きます。

ポリシーは、設定の横にロックアイコン（🔒）がある点で、ローカル設定とは異なります。ポリシープロパティの設定（または設定のグループ）がロックされている場合は、効率的な設定を作成する際に最初にこの設定（または、設定のグループ）を使用し、次に下位のポリシーに対して設定または設定のグループを記述する必要があります。

デバイスに対して効率的な設定を作成する際の説明は次の通りです。ロックされていない設定値をすべてポリシーから取得し、その値をローカル設定値で上書きします。これにより、生成されたコレクションがポリシーから取得したロック済みの設定値により上書きされます。

同じアプリケーションのポリシーは、管理グループの階層を介してお互いに影響を与えます。上位のポリシーのロック済みの設定は、下位のポリシーの同じ設定を上書きします。

モバイルユーザーに対しては、特別なポリシーが存在します。このポリシーは、デバイスがモバイルユーザーモードに切り替わった際に有効になります。モバイルユーザーポリシーが管理グループの階層を介して他のポリシーに影響することはありません。

## ポリシーのプロファイル

多数の環境において、デバイスにポリシーを適用する方法が管理グループの階層を使用するだけというのは適切ではありません。複数の管理グループで 1 つまたは 2 つの設定値が異なる単一ポリシーで複数のインスタンスを作成し、将来これらのポリシーの内容を同期させることが必要になる場合があります。

このような問題を回避するために、Kaspersky Security Center Linux は*ポリシープロファイル*をサポートしています。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、クライアントデバイス（コンピューターまたはモバイルデバイス）でアクティブな「基本」ポリシーとは異なる設定のみです。プロファイルを有効にすると、プロファイルが有効になる前にデバイスで有効になっていたポリシー設定が修正されます。こうした設定により、プロファイルで指定された値が得られます。

現在、ポリシーのプロファイルに適用されている制限事項は次の通りです：

- ポリシーには最大 100 個のプロファイルを含めることができます。
- ポリシーのプロファイルにその他のプロファイルを含めることはできません。
- ポリシーのプロファイルに通知の設定を含めることはできません。

## プロファイルの内容

ポリシーのプロファイルには、次の構成要素が含まれています：

- 名前：同じ名前のプロファイルは、共通のルールが含まれる管理グループの階層によって相互に影響します。
- ポリシー設定のサブセット：すべての設定が含まれているポリシーとは異なり、プロファイルには実際に必要な設定のみが含まれています（ロック済みの設定）。
- アクティベーション条件：デバイスのプロパティを使用した論理式。プロファイルが有効になる（ポリシーを補完する）のは、プロファイルの有効化条件に該当する場合のみです。その他の場合はすべて、プロファイルは非アクティブで無視されます。論理式には、次のデバイスプロパティを含めることができます：
  - モバイルユーザーモードのステータス
  - ネットワーク環境のプロパティ：ネットワークエージェント接続の有効なルールの名前
  - 指定したタグがデバイスに存在するかどうか
  - Active Directory 単位におけるデバイスの場所：明示的（デバイスはまさに指定した OU 内にある）、または暗黙的（デバイスは OU 内にある。ただし、任意のネストレベルで指定した OU 内にある）
  - デバイスが属している Active Directory セキュリティグループ（明示的または暗黙的）
  - デバイス所有者が属している Active Directory セキュリティグループ（明示的または暗黙的）
- プロファイルを無効にする：無効化されたプロファイルは常に無視され、それぞれの有効化条件は検証されません。
- プロファイルの優先度：異なるプロファイルの有効化条件は独立しているため、複数のプロファイルを同時に有効化することができます。アクティブなプロファイルに重複しない一連の設定が含まれている場合、問題は発生しません。ただし、2 つのアクティブなプロファイルで同じ設定の値が異なる場合は、不明確さが発生します。この不明確さを回避するために、プロファイルの優先度が使用されます。不明確な変数の値は、優先度が高い方（プロファイルのリスト内での位置付けが高い方）のプロファイルから取得されます。

## ポリシーが階層を介してお互いに影響を与え合う場合のプロファイルの動作

名前が同じプロファイルは、ポリシー統合ルールに従って統合されます。上位のポリシーのプロファイルは、下位のポリシーのプロファイルよりも優先度が高くなっています。上位のポリシーで設定の編集がブロックされている（ロック状態）場合、下位のポリシーでは上位のポリシーのプロファイルの有効化条件が使用されます。一方、上位のポリシーで設定の編集が許可されている場合は、下位のポリシーのプロファイルの有効化条件が使用されます。

ポリシーのプロファイルの有効化条件には［**オフラインのデバイス**］プロパティが含まれているため、プロファイルではサポートされていないモバイルユーザー用のポリシー機能は完全に置き換えられます。

モバイルユーザー用のポリシーにはプロファイルが含まれていることがありますが、そのプロファイルがアクティブ化されるのは、デバイスがモバイルユーザーモードに切り替えられた後だけです。

# タスク

Kaspersky Security Center Linux は、様々なタスクを作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインがインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次のタスクは管理サーバーで実行されます：

- レポートの自動配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が Kaspersky Security Center Web コンソールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、管理サーバー上の Syslog ログと Kaspersky Security Center Linux のイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

## デバイス移動ルール

*デバイス移動ルール*を使用して、管理グループにデバイスへの割り当てを自動化することを推奨します。デバイス移動ルールは、3 つのメイン部分から構成されます。それは、名前、実行条件（デバイス属性を使用した論理式）、および対象管理グループです。デバイス属性がルールの実行条件を満たしている場合は、このルールによりデバイスが対象管理グループに移動されます。

デバイス移動ルールにはすべて優先度が設定されています。管理サーバーは優先度の昇順に従って、デバイス属性が各ルールの実行条件を満たしているかどうかを確認します。デバイス属性がルールの実行条件を満たしている場合、そのデバイスは対象グループに移動され、このデバイスに対するルール処理が完了します。デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールは暗黙的に作成できます。たとえば、インストールパッケージまたはリモートインストールタスクのプロパティで、ネットワークエージェントをデバイスにインストールした後にそのデバイス移動先の管理グループを指定できます。さらに、［**アセット（デバイス）**］→［**移動ルール**］セクションで Kaspersky Security Center Linux の管理者が、デバイス移動ルールを明示的に作成できます。

既定では、デバイス移動ルールは、管理グループに対してデバイスを最初にワンタイムで割り当てることを目的としています。このルールにより、［未割り当てデバイス］グループから一度だけデバイスが移動されます。デバイスがこのルールによって一度移動されている場合は、デバイスを手動で［未割り当てデバイス］グループに戻したとしても、このデバイスが再度移動されることはありません。これは移動ルールを適用する際に推奨される方法です。

一部の管理グループに割り当て済みであるデバイスを移動できます。これを実行するには、ルールのプロパティで［**どの管理グループにも属していないデバイスのみ移動する**］をオフにします。

一部の管理グループに割り当て済みのデバイスに対して移動ルールを適用すると、管理サーバーの負荷が大幅に増大します。

［**どの管理グループにも属していないデバイスのみ移動する**］は、自動的に作成された移動ルールのプロパティでロックされています。このようなルールは、［*アプリケーションをリモートでインストールする*］タスクを追加するか、スタンドアロンインストールパッケージを作成する時に作成されます。

単一のデバイスに繰り返し適用される移動ルールを作成することができます。

単一のデバイスをあるグループから別のグループに繰り返し移動させないでください（たとえば、該当するデバイスに特別なポリシーを適用するために、特別なグループタスクを実行するか、または特定のディストリビューションポイントを使用してデバイスをアップデートする）。

このような処理は、管理サーバーとネットワークのトラフィックの負荷を極端に増大させるため、サポートされていません。また、Kaspersky Security Center Linux の操作原理と競合する可能性もあります（特に、アクセス権限、イベント、レポートの分野において）。ポリシーのプロファイル、デバイスの抽出のタスク、標準シナリオに従ったネットワークエージェントの割り当てなどを使用して、別のソリューションを見つける必要があります。

## ソフトウェアのカテゴリ分け

アプリケーションの実行状態を監視する主なツールは、*カスペルスキーのカテゴリ*です（以下、*KL カテゴリ*と表記）。KL カテゴリを使用することで、Kaspersky Security Center Linux 管理者によるソフトウェアのカテゴリ分けのサポートを簡略化でき、管理対象デバイスへのトラフィックを最小化できます。

アプリケーションカテゴリは、既存の KL カテゴリのいずれかには分類できないアプリケーションに対してのみ作成する必要があります（たとえば、カスタムメイドソフトウェア用）。また、アプリケーションカテゴリは、アプリケーションのインストールパッケージ（MSI）またはインストールパッケージの置かれているフォルダーに基づいて作成されます。

KL カテゴリによりカテゴリ化されていない大規模セットのソフトウェアが提供されている場合は、自動的に更新されるカテゴリを作成するのが便利です。実行ファイルのチェックサムは、配布パッケージを含むフォルダーが変更されるたびに、自動的にこのカテゴリに追加されます。

# 管理サーバーの設定のバックアップと復元

管理サーバーとそのデータベースの設定のバックアップは、バックアップタスクと klbackup ユーティリティを使用して実行されます。バックアップコピーには、証明書、管理対象デバイスのドライブ暗号化用のプライマリキー、様々なライセンス情報、および内容、タスク、ポリシーのすべてを含む管理グループ構造など、管理サーバーに関係するすべての主要な設定とオブジェクトが含まれています。バックアップコピーを使用すると、数十分から数時間で可能な限り迅速に管理サーバーの操作を復元できます。

バックアップコピーが使用できない場合は、障害が発生して証明書や管理サーバーの設定がすべて失われてしまうことがあります。この場合は、Kaspersky Security Center Linux を最初から再設定し、組織ネットワークで再度ネットワークエージェントの初期導入を実行する必要があります。管理対象デバイスのドライブ暗号化用のプライマリキーもすべて失われ、Kaspersky Endpoint Security がインストールされたデバイスの暗号化されたデータも失われてしまう危険性があります。そのため、必ず標準的なバックアップタスクを実行し、管理サーバーを定期的にバックアップしてください。

クイックスタートウィザードは、管理サーバー設定のバックアップタスクを作成し、このタスクが毎日午前 4 時に実行されるように設定します。既定では、バックアップコピーは［/var/opt/kaspersky/KSC_Backups*］フォルダーに保存されます。

バックアップコピーには重要なデータが含まれているため、バックアップタスクと klbackup ユーティリティではバックアップコピーがパスワードにより保護されます。既定では、作成されるバックアップタスクのパスワードは空白です。このため、バックアップタスクのプロパティでパスワードを設定する必要があります。この要件を無視すると、管理サーバー証明書のすべての鍵、ライセンスの鍵、および管理対象デバイスのドライブ暗号化用のプライマリキーが暗号化されないままになります。

定期的なバックアップの他に、管理サーバーのアップグレードのインストールやパッチ適用などの重要な変更を加える前にも、必ずバックアップコピーを作成する必要があります。

バックアップコピーからの復元を実行するには、インストール済みで、バックアップコピーを作成したのと同じバージョン（またはそれ以降）の管理サーバーの操作可能なインスタンスでユーティリティ klbackup を使用します。

復元を実行する対象の管理サーバーのインスタンスでは、同じ種別で同じバージョンまたはそれ以降のバージョンの DBMS を使用している必要があります。管理サーバーのバージョンは、同じ（同一またはそれ以降のパッチを適用）またはそれ以降にする必要があります。

このセクションでは、管理サーバーの設定とオブジェクトを復元する標準的な方法について説明します。

## 管理サーバーがインストールされているデバイスを操作できない

障害が発生しているため、管理サーバーをインストールしたデバイスが操作できない場合は、次の操作を実行してください：

- 新しい管理サーバーには同じ DNS 名を割り当てる必要があります。

  新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

- 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーをインストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。

- klbackup ユーティリティを実行し、復元を実行します。

## 管理サーバーまたはデータベースの設定が破損している

設定またはデータベースが破損しているため（たとえば、電力サージが原因）、管理サーバーが操作できない場合は、次の復元方法を使用してください：

1. 損傷を受けたデバイスでファイルシステムをスキャンする。
2. 操作できないバージョンの管理サーバーをアンインストールする。
3. 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーを再インストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。
4. klbackup ユーティリティを実行し、復元を実行します。

klbackup ユーティリティ以外の方法で管理サーバーを復元することは禁止されています。

サードパーティ製のソフトウェアを使用して管理サーバーの復元を試行した場合は、配信アプリケーション Kaspersky Security Center Linux のノード上のデータが同期化されなくなり、その結果、本製品が正常に動作しなくなります。

# モバイルユーザー用の接続プロファイルの概要

モバイルユーザー用のノートPC（以降「デバイス」とも表記）では、企業ネットワーク内でのデバイスの現在位置によっては、管理サーバーへの接続方法を変更する、または管理サーバーを切り替える必要があります。

接続プロファイルは、Windowsおよびmacosを実行しているデバイスでのみサポートされます。

## 単一の管理サーバーに対する異なるアドレスの使用

ネットワークエージェントがインストールされたデバイスは、組織の社内ネットワークかイントラネット経由で管理サーバーに接続できます。そのため、ネットワークエージェントは異なるアドレスを使用して管理サーバーに接続することが必要になる場合があります。つまり、インターネット経由で接続された場合は外部管理サーバーアドレス、社内ネットワーク経由で接続された場合は内部管理サーバーアドレスが使用されます。

これを行うには、（インターネット経由で管理サーバーに接続するための）プロファイルを、ネットワークエージェントポリシーに追加する必要があります。ポリシープロパティでプロファイルを追加します（[**接続**]セクション、[**接続プロファイル**]サブセクション）。次に、プロファイル作成ウィンドウで、[**アップデートの受信にのみ使用する**]をオフにし、[**このプロファイルで指定された管理サーバー設定と接続設定を同期する**]をオンにします。接続ゲートウェイを使用して管理サーバーにアクセスする場合（たとえば、「インターネットアクセス：DMZ内でネットワークエージェントを接続ゲートウェイとして使用する」で説明されているようなKaspersky Security Center Linuxの設定の場合）、接続プロファイルの該当フィールドで、接続ゲートウェイのアドレスを指定する必要があります。

## 現在のネットワークに応じた管理サーバーの切り替え

企業に、異なる管理サーバーを使用する複数のオフィスがあり、ネットワークエージェントがインストールされた一部のデバイスが管理サーバー間を移動している場合、現在のデバイスがあるオフィスのローカルネットワークの管理サーバーに、ネットワークエージェントを接続する必要があります。

この場合、各オフィスにおいて、ネットワークエージェントのポリシーのプロパティに、管理サーバーへの接続用プロファイルを作成する必要があります。ただし、独自のホーム管理サーバーがあるホームオフィスは除きます。接続プロファイルで管理サーバーのアドレスを指定し、次のように、[**アップデートの受信にのみ使用する**]をオンまたはオフにする必要があります：

- ローカルサーバーをアップデートのダウンロードのためだけに使用する間、ネットワークエージェントをホーム管理サーバーと同期する必要がある場合は、このオプションをオンにします。
- ネットワークエージェントをローカル管理サーバーで完全に管理する必要がある場合は、このオプションをオフにします。

その後、新たに作成したプロファイルに切り替える条件を設定します。ホームオフィスを除いて、オフィスごとに少なくとも1つの条件を設定する必要があります。各条件は、オフィスのネットワーク環境特有の項目を検出することを目的とします。条件が真の場合、対応するプロファイルがアクティブになります。いずれの条件も真でない場合、ネットワークエージェントはホーム管理サーバーに切り替わります。

# 管理対象デバイスへのリモートアクセス

このセクションでは、管理対象デバイスへのリモートアクセスについて説明します。

## ［管理サーバーから切断しない］オプションを使用して、管理対象デバイスと管理サーバー間の継続的な接続を提供する

プッシュサーバーを使用しない場合、Kaspersky Security Center Linux は、管理対象デバイスと管理サーバー間の継続的な接続を提供しません。管理対象デバイスのネットワークエージェントが、定期的に接続を確立し、管理サーバーと同期させます。同期セッションの間隔は、ネットワークエージェントのポリシーで定義されます。早期の同期実行が必要な場合、管理サーバー（または、使用されているディストリビューションポイント）は署名されたネットワークパケットを、IPv4 または IPv6 ネットワーク経由でネットワークエージェントの UDP ポートへ送信します。既定では、ポート番号は 15000 です。管理サーバーと管理対象デバイスとの間で UDP を使用した接続が確立できない場合、同期間隔の間の次の定期接続時に、ネットワークエージェントと管理サーバー間で同期が実行されます。

一部の動作は、ネットワークエージェントと管理サーバーが事前に接続されていないと実行できません。例：ローカルタスクの実行と停止、管理対象アプリケーションの統計情報の受信など。この問題を解決するには、プッシュサーバーを使用していない場合は、[**管理サーバーから切断しない**］オプションを使用し、管理対象デバイスと管理サーバーの間に継続的な接続があることを確認します。

*クライアントデバイスと管理サーバー間の継続的な接続を確認するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、目的のデバイス名のリンクをクリックします。
3. デバイスのプロパティウィンドウの［**全般**］セクションで、［**管理サーバーから切断しない**］をオンにします。

   継続的な接続が、管理デバイスと管理サーバー間で確立されます。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

## デバイスと管理サーバー間の接続時間の確認について

デバイスのシャットダウン時に、ネットワークエージェントは管理サーバーにシャットダウンを通知します。Kaspersky Security Center Web コンソールでは、そのデバイスはシャットダウン済みとして表示されます。ただし、ネットワークエージェントがすべてのシャットダウンを管理サーバーに通知できるわけではありません。そのため、管理サーバーは、各デバイスの［**管理サーバーへの接続**］属性（この属性の値は、Kaspersky Security Center Web コンソールのデバイスプロパティの［**全般**］セクションに表示されます）を定期的に分析し、ネットワークエージェントの現在の設定の同期間隔と比較します。あるデバイスが連続した同期間隔に 3 回を超えて応答していない場合、そのデバイスはシャットダウンとマーク付けされます。

# 強制同期について

Kaspersky Security Center Linux では、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されますが、場合によっては、現時点において指定されたデバイスで同期が実行されているかどうかを管理者が正確に知る必要があります。

管理対象デバイスのプロパティウィンドウには、［**強制同期**］があります。Kaspersky Security Center Linux が同期化コマンドを実行すると、管理サーバーはデバイスへの接続を試行します。この試行が成功すると、強制同期が実行されます。試行が失敗した場合は、ネットワークエージェントと管理サーバー間の次の定期接続まで待機してから同期が強制的に実行されます。

# サイジングガイド

このセクションでは、Kaspersky Security Center Linux のサイジングについて説明します。

# このガイドの概要

このサイジングガイドは、Kaspersky Security Center Linux（以降、単に「Kaspersky Security Center」とも表記）をインストールおよび管理する担当者、および Kaspersky Security Center を使用するテクニカルサポートをする担当者を対象としています。

カスペルスキー製品がインストールされたデバイスの保護を Kaspersky Security Center によって管理するネットワークに対するすべての推奨事項と計算について説明します。

様々な運用状況で最適なパフォーマンスを実現し維持するには、ネットワークに接続されたデバイスの数、ネットワークのトポロジー、必要な Kaspersky Security Center の機能を考慮する必要があります。

このガイドでは、次の項目について説明します：

- Kaspersky Security Center の制限
- Kaspersky Security Center の主要なコンポーネントに関する計算（管理サーバーとディストリビューションポイント）：
  - 管理サーバーとディストリビューションポイントのハードウェア要件
  - 管理サーバーの数と階層の算出
  - ディストリビューションポイントの数の計算と設定
- ネットワーク上のデバイス数に応じてイベントのデータベースへの記録を設定
- パフォーマンス最適化のための一般的なベストプラクティス
- Kaspersky Security Center のパフォーマンスを最適化するためのタスクの設定
- Kaspersky Security Center 管理サーバーと保護されるデバイスとの間のトラフィックレート（ネットワーク負荷）

このガイドは、以下の場合に参照してください：

- Kaspersky Security Center のインストールに先立ってリソースを計画する時
- Kaspersky Security Center が導入されているネットワークの規模の大幅な変更を計画する時
- テスト環境用の限定されたネットワークセグメントで Kaspersky Security Center を使用する段階から組織のネットワークへ Kaspersky Security Center を全面的に導入する段階へ移行する時
- 使用する Kaspersky Security Center の機能を変更する時

# 管理サーバーの計算

このセクションでは、管理サーバーとして使用するデバイスのソフトウェアおよびハードウェア要件について説明します。また、組織のネットワークの構成に応じた管理サーバーの数と階層を計算する際の推奨事項についても説明します。

# 管理サーバーのハードウェアリソースの計算

このセクションでは、管理サーバー用のハードウェアリソースを計画するための指針となる計算について説明します。

## DBMS および管理サーバーのハードウェア要件

テストによって得られた DBMS および管理サーバーのハードウェア最小要件は、下記の表で示す通りです。サポートされるオペレーティングシステムと DBMS の完全なリストについては、システム要件のリストを参照してください。

### ネットワークには 50,000 台のデバイスが含まれています

管理サーバーがインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 8 コア（12 コアを推奨）、2,500 MHz |
| メモリ | 16 GB |
| ディスク容量 | 300 GB、150 IOPS 以上 |

PostgreSQL DBMS がインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 300 GB、150 IOPS 以上 |

フェールオーバークラスタのノードの設定

| ハードウェア | 値 |
|---|---|
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、300 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 1 Gbps |

管理サーバーと PostgreSQL DBMS の両方がインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 24 コア（28 コアを推奨）、2,500 MHz |
| メモリ | 48 GB |
| ディスク容量 | 600 GB、300 IOPS 以上 |

## ネットワークには 30,000 台のデバイスが含まれています

管理サーバーがインストールされたデバイスの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 6 コア（8 コアを推奨）、2,500 MHz |
| メモリ | 12 GB |
| ディスク容量 | 200 GB、150 IOPS 以上 |

PostgreSQL DBMS がインストールされたデバイスの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 12 コア、2500 MHz |
| メモリ | 24 GB |
| ディスク容量 | 250 GB、150 IOPS 以上 |

フェールオーバークラスタのノードの設定

| ハードウェア | 値 |
| --- | --- |
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、300 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 1 Gbps |

管理サーバーと PostgreSQL DBMS の両方がインストールされたデバイスの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 18 コア（20 コアを推奨）、2,500 MHz |
| メモリ | 36 GB |
| ディスク容量 | 450 GB、300 IOPS 以上 |

## ネットワークには 10,000 台のデバイスが含まれています

管理サーバーがインストールされたデバイスの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 4 コア（6 コアを推奨）、2,500 MHz |
| メモリ | 8 GB |
| ディスク容量 | 100 GB、150 IOPS 以上 |

PostgreSQL DBMS がインストールされたデバイスの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 8 コア、2500 MHz |
| メモリ | 18 GB |
| ディスク容量 | 200 GB、150 IOPS 以上 |

フェールオーバークラスターのノードの構成

| ハードウェア | 値 |
| --- | --- |
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、300 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 1 Gbps |

管理サーバーと PostgreSQL DBMS の両方がインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 12 コア（14 コアを推奨）、2,500 MHz |
| メモリ | 26 GB |
| ディスク容量 | 300 GB、300 IOPS 以上 |

## ネットワークには 1000 台のデバイスが含まれています

管理サーバーがインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 2 コア、2,500 MHz |
| メモリ | 6 GB |
| ディスク容量 | 10 GB、150 IOPS 以上 |

PostgreSQL DBMS がインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 2 コア、2,500 MHz |
| メモリ | 4 GB |
| ディスク容量 | 20 GB、150 IOPS 以上 |

フェールオーバークラスタのノードの設定

| ハードウェア | 値 |
|---|---|
| CPU | 16 コア、2500 MHz |
| メモリ | 32 GB |
| ディスク容量 | 500 GB、300 IOPS 以上 |
| ネットワークインターフェイスコントローラー | 1 Gbps |

管理サーバーと PostgreSQL DBMS の両方がインストールされたデバイスの構成

| ハードウェア | 値 |
|---|---|
| CPU | 4 cores、2500 MHz |
| メモリ | 10 GB |
| ディスク容量 | 30 GB、300 IOPS 以上 |

テストは次の設定で実行されました：

- ディストリビューションポイントの自動割り当てが管理サーバー上で有効になっている、または、ディストリビューションポイントが推奨条件に従って手動で割り当てられている。
- PostgreSQL DBMS には、plpgsql 以外の拡張機能は含まれていません。

DBMS がインストールされているデバイスでは、データベースが約 100 GB のディスク領域を消費し、トランザクションログが約 200 GB のディスク領域を消費します。

# データベースの容量の計算

データベースのために予約する必要のあるディスク容量は次の計算式で計算できます：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

説明：

- C はデバイスの数です。
- E は保存するイベントの数です。
- A は Active Directory オブジェクトの合計数です：
  - デバイスアカウント
  - ユーザーアカウント
  - セキュリティグループのアカウント
  - Active Directory 組織単位

  Active Directory のスキャンを無効化すると、A はゼロになります。
- N は、エンドポイントデバイスでインベントリされた実行可能ファイルの平均数です。
- F は、実行ファイルがインベントリされたエンドポイントデバイスの数です。

Kaspersky Endpoint Security のポリシーの設定で、実行しているアプリケーションに関する管理サーバーの通知を有効にする場合、実行しているアプリケーションについての情報をデータベースに保存するために (0.03 * C) GB を追加する必要があります。

動作中には、データベース内に*未割り当て領域*が常に存在します。したがって、定義データベースファイルの実際のサイズは、データベースで占有されるスペースの量の約 2 倍になることがよくあります。

トランザクションログのサイズを明示的に制限することは推奨しません。MAXSIZE パラメータの既定値を変更せずに使用することが推奨されます。

## ディスク容量の計算

管理サーバーの［/var/opt/kaspersky/klnagent_srv/］フォルダーに必要なディスク容量の見積もりは、次の式で概算できます：

(724 * C + 0.15 * E + 0.17 * A) KB

説明：

- C はデバイスの数です。
- E は保存するイベントの数です。
- A は Active Directory オブジェクトの合計数です：
  - デバイスアカウント
  - ユーザーアカウント
  - セキュリティグループのアカウント
  - Active Directory 組織単位

Active Directory のスキャンを無効化すると、A はゼロになります。

# 管理サーバーの数と構成の算出

プライマリ管理サーバーの負荷を軽減するため、各管理グループに管理サーバーを割り当てることができます。セカンダリ管理サーバーの数は、プライマリ管理サーバーあたり 500 を超えることができません。

組織のネットワークの構成に対応した管理サーバーの構成を作成することを推奨します。

# 動的仮想マシンを Kaspersky Security Center に接続する際の推奨事項

動的仮想マシン（単に「動的 VM」とも表記）は、静的仮想マシンより多くのリソースを消費します。

動的仮想マシンの詳細については、「動的仮想マシンのサポート」を参照してください。

新しい動的 VM が接続されると、Kaspersky Security Center Linux は Kaspersky Security Center Web コンソールにこの動的 VM の記録を作成し、動的 VM を管理グループに移動します。その後、動的 VM が管理サーバーデータベースに追加されます。管理サーバーは、この動的 VM にインストールされたネットワークエージェントと完全に同期されます。

組織のネットワークでは、ネットワークエージェントは動的 VM ごとに次のネットワークリストを作成します：

- ハードウェア
- インストールされたソフトウェア
- 検知された脆弱性
- アプリケーションコントロールコンポーネントのイベントおよび実行可能ファイルのリスト

ネットワークエージェントは、これらのネットワークリストを管理サーバーに転送します。ネットワークリストのサイズは、動的 VM にインストールされているコンポーネントによって決まり、Kaspersky Security Center Linux とデータベース管理システム（DBMS）のパフォーマンスに影響を与える可能性があります。負荷は非線形に増加する可能性があります。

ユーザーが動的 VM の操作を終了してオフにすると、このマシンは仮想インフラストラクチャから削除され、このマシンに関するエントリは管理サーバーデータベースから削除されます。

これらの操作はいずれも、Kaspersky Security Center Linux と管理サーバーデータベースのリソースを大量に消費し、Kaspersky Security Center Linux と DBMS のパフォーマンスを低下させる可能性があります。Kaspersky Security Center Linux に接続する動的 VM は、最大 20,000 台にすることを推奨します。

接続された動的 VM が標準的な操作（定義データベースのアップデートなど）を実行し、メモリの消費が 80% 以内、使用可能なコアの消費が 75 ～ 80% 程度であれば、20,000 台以上の動的 VM を Kaspersky Security Center Linux に接続できます。

動的 VM のポリシー設定、ソフトウェア、またはオペレーティングシステムを変更すると、リソースの消費が増減する可能性があります。80 ～ 95% のリソース消費が最適と判断されます。

# ディストリビューションポイントと接続ゲートウェイの計算

このセクションでは、ディストリビューションポイントとして使用するデバイスのハードウェア要件と、組織のネットワークの構成に応じたディストリビューションポイントおよび接続ゲートウェイの数を計算する際の推奨事項について説明します。

# ディストリビューションポイントの要件

この記事では、Windows および Linux ベースのディストリビューションポイントのハードウェアおよびソフトウェア要件について説明します。

管理サーバー上でリモートインストールタスクが実行を待っている場合、ディストリビューションポイントがあるデバイスには、インストール対象となるインストールパッケージの合計サイズと同等の空き容量が必要です。

管理サーバー上でアップデート（パッチ）のインストールタスクと脆弱性の修正タスクが 1 つ以上保留されている場合、ディストリビューションポイントが動作しているデバイスには、インストールするすべてのパッチの合計サイズの 2 倍の空きディスク容量が追加で必要です。

ディストリビューションポイントがカスペルスキーのアップデートサーバーから直接定義データベースとアプリケーションソフトウェアモジュールのアップデートを受信するスキームを使用する場合は、ディストリビューションポイントがインターネットに接続されている必要があります。

管理サーバーをディストリビューションポイントとして割り当てることは、管理サーバーの負荷が増加するため、推奨されません。

## Windows ベースのディストリビューションポイントのハードウェア要件

**Windows ベースのディストリビューションポイントの最小ハードウェア要件**

| クライアントデバイスの数 | CPU | メモリ | パッチ管理が有効になっている場合の RAM | ディスク容量 |
|---|---|---|---|---|
| 10,000 | 4 cores、2500 MHz | 8 GB | 8 GB | 120 GB |
| 5,000 | 4 cores、2500 MHz | 6 GB | 8 GB | 120 GB |
| 1000 | 2 コア、2,500 MHz | 4 GB | 8 GB | 120 GB |

## Linux ベースのディストリビューションポイントのハードウェア要件

**Windows ベースのディストリビューションポイントの最小ハードウェア要件**

| クライアントデバイスの数 | CPU | メモリ | ディスク容量 |
|---|---|---|---|
| 10,000 | 4 cores、2500 MHz | 10 GB | 120 GB |
| 5,000 | 4 cores、2500 MHz | 8 GB | 120 GB |
| 1000 | 2 コア、2,500 MHz | 6 GB | 120 GB |

# ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ディストリビューションポイントの自動割り当ては、できるだけ使用しないでください。ディストリビューションポイントの自動割り当てが有効になっており、クライアントデバイスの数が非常に多い場合、管理サーバーがディストリビューションポイントの割り当てと設定を行います。

## 用途専用のディストリビューションポイントの使用

特定のデバイスをディストリビューションポイントとして使用する場合（たとえば、この用途専用で割り当てられたサーバー）、ディストリビューションポイントの自動割り当ては使用しないでください。また、ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

| ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 300 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 300 以上 | 許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数） |

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

| 各ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 10 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 10～100 | 1 |
| 100 以上 | 許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数） |

## 通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

| ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 300 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 300 以上 | N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要） |

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

| 各ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
|---|---|
| 10 台未満 | 0（ディストリビューションポイントを割り当てない） |
| 10～30 | 1 |

| 各ネットワークセグメントでのクライアントデバイスの数 | ディストリビューションポイントの数 |
| --- | --- |
| 31～300 | 2 |
| 300 以上 | N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要） |

ディストリビューションポイントがシャットダウンされた（もしくは、何らかの理由により使用できない）場合も、ディストリビューションポイントの対象範囲に含まれる管理対象デバイスは管理サーバーにアクセスしてアップデートを取得できます。

# 接続ゲートウェイの数の計算

接続ゲートウェイを使用する場合、接続ゲートウェイ専用のデバイスを割り当てることを推奨します。

また、接続ゲートウェイに接続できる管理対象デバイスは最大で 10,000 台です。

# タスクおよびポリシーのイベントに関する情報の記録

このセクションでは、管理サーバーのデータベースに保存するイベントに関する計算と、イベントの数を最小限にして管理サーバーの負荷を低減する方法に関する推奨事項について説明します。

既定では、各タスクおよびポリシーのプロパティによって、タスクの実行およびポリシーの適用に関するすべてのイベントが保存されます。

しかし、タスクが頻繁に（週に数回など）多くのデバイス（たとえば 10,000 台以上）に対して実行される場合、イベントの数が多すぎてデータベースの容量を超えてしまうことがあります。この場合、タスクの設定で次のいずれかを選択してください：

- **タスクの進捗に関連したイベントを保存**：この場合、データベースは、タスクの開始、進捗、完了（成功、警告、エラー）に関する情報のみを、タスクが実行されるデバイスから受信します。
- **タスク実行結果のみ保存**：この場合、データベースは、タスクの完了（成功、警告、エラー）に関する情報のみを、タスクが実行されるデバイスから受信します。

ポリシーが多くのデバイス（たとえば 10,000 台以上）に対して定義されている場合も、イベントの数が多すぎてデータベースの容量を超えてしまうことがあります。この場合、ポリシーの設定で、最も緊急イベントのみ記録を有効にしてください。その他のイベントは記録を無効にします。

それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって緊急イベントが上書きされる可能性を低下させることができます。

また、タスクまたはポリシーに関連するイベントの保存期間を短くすることもできます。既定の期間は、タスクに関連するイベントは 7 日、ポリシーに関連するイベントは 30 日です。イベントの保存期間を変更する際は、組織で運用している業務手順と、システム管理者がイベントを分析するのにかかる時間を考慮してください。

次の場合には、イベントの保存期間を変更してください：

- グループタスクの中間状態の変更に関するイベントやポリシー適用に関するイベントが、Kaspersky Security Center Linux データベース内のすべてのイベントの大部分を占める場合。
- データベースに保存できるイベント数の上限を超え、イベントの自動削除に関する項目がオペレーティングシステムログに記録される場合。

1つのデバイスから送信されるイベントの数が1日あたり 20 を超えないように、イベント記録オプションを選択してください。必要に応じて、この上限をわずかに超過することができますが、そのためにはネットワークに接続されたデバイスの数が比較的少数（10,000 未満）である必要があります。

# 多数のデバイスを管理する管理サーバーのベストプラクティス

## DBMS の使用に関するベストプラクティス

特に PostgreSQL DBMS を使用する場合は、**管理サーバーのメンテナンス**タスクが定期的に実行されるように設定します。

［DBMS］フォルダーを IOC スキャンから除外します。

## ポリシーとプロファイルのベストプラクティス

コンポーネント（Kaspersky Endpoint Security for Windows など）に対するアクティブなポリシーの数を減らします。ポリシーをポリシープロファイルに置き換えることができます。

## 多数のデバイスを管理する管理サーバーのベストプラクティス

同時に実行されるタスクの数、特にリモートインストールとパッチの管理の数を減らします。

デバイスの抽出に関連するタスクの数を減らし、スケジュールを最適化します。

ポリシー設定の［**イベントの設定**］セクションで、保存されるイベントタイプの数を最小限に抑えます。

## イベントを保存するためのベストプラクティス

アプリケーションコントロールコンポーネントから単一タイプのイベントの頻度を減らします。詳細については、次のセクションを参照してください：「頻出イベントのブロック」。

コンポーネント（Kaspersky Endpoint Security for Windows など）からのイベントと修正された脆弱性に関する情報イベントの保存期間を短縮します。

アップデートタスクなどの一般的なタスクのタスク設定で、「タスクの進捗に関連したイベントを保存］オプションをオンにします。詳細については、次のトピックを参照してください「：タスクとポリシーのイベントに関する情報のログ記録」。

インベントリタスク設定を最適化します。詳細については、次のトピックを参照してください：「インベントリタスク」。

# タスクごとの考慮事項と最適な設定

タスクによっては、ネットワーク上のデバイスの数に関して特別な考慮事項があります。このセクションでは、そのようなタスクに推奨される最適な設定について説明します。

デバイスの検索、データバックアップタスク、データベースメンテナンスタスク、Kaspersky Endpoint Security をアップデートするグループタスクは、Kaspersky Security Center Linux の基本機能の一部です。

インベントリタスクは脆弱性とパッチ管理機能の一部であり、この機能が有効でない場合使用できません。

## デバイスの検索の頻度

既定のデバイスの検索の頻度を高くすることは推奨されません。ドメインコントローラーに過大な負荷がかかる可能性があります。それよりむしろ、組織の必要に応じてポーリングの頻度をできるだけ低くしてください。最適なスケジュールを算出する際の推奨事項を次の表に示します：

デバイスの検索のスケジュール

| ネットワーク上のデバイスの数 | 推奨されるデバイスの検索の頻度 |
| --- | --- |
| 10,000 台未満 | 既定またはより低い頻度 |
| 10,000 台以上 | 1 日に 1 回またはより低い頻度 |

## 管理サーバーデータのバックアップタスクとデータベースのメンテナンスタスク

管理サーバーは、以下のタスクの実行中は動作を停止します：

- 管理サーバーデータのバックアップ
- 管理サーバーのメンテナンス

これらのタスクの実行中は、データベースがデータを受信できません。

これらのタスクが別の管理サーバータスクと同時に実行されないように、タスクのスケジュールを変更する必要がある場合があります。

# Kaspersky Endpoint Security をアップデートするグループタスク

管理サーバーがアップデート元として動作する場合、Kaspersky Endpoint Security 10 以降のグループアップデートタスクに推奨されるスケジュールオプションは、［**新しいアップデートがリポジトリにダウンロードされ次第**］と［**タスクの開始を自動的かつランダムに遅延させる**］です。

カスペルスキーのサーバーからリポジトリにダウンロードをアップデートするローカルタスクが各ディストリビューションポイントで作成される場合、Kaspersky Endpoint Security のグループアップデートタスクをスケジュールによって定期的に実行することを推奨します。この場合、ランダムに遅延させる時間の範囲を 1 時間に設定する必要があります。

## インベントリタスク

実行ファイルに関する情報を取得しながら定義データベースの負荷を軽減できます。これを行うには、標準的なソフトウェアがインストールされている参照デバイスで、Kaspersky Endpoint Security のインベントリタスクを実行することを推奨します。

管理サーバーが 1 台のデバイスから受信できる実行ファイルは、最大で 150,000 個です。この上限に達すると、Kaspersky Security Center Linux が新しいファイルを受信できなくなります。

通常、一般的なクライアントデバイスのファイルの数は 60,000 を超えません。ファイルサーバー上の実行ファイルの数はそれより大きい場合があり、150,000 の上限を超えることもあります。

# 管理サーバーと保護されるデバイスとの間のネットワーク負荷に関する詳細情報

このセクションでは、ネットワークトラフィックのテスト測定の結果とその測定の実行条件について説明します。組織内（または管理サーバーと管理対象デバイスがある組織との間）のネットワークインフラストラクチャとネットワークチャネルのスループットを計画する際、この情報を参照できます。ネットワークのスループットがわかると、様々なデータ転送操作にかかる時間を見積もることができます。

## 様々なシナリオでのトラフィック

次の表に、様々なシナリオでの管理サーバーと管理対象デバイスとの間のトラフィックに関する測定テストの結果を示します。

既定では、デバイスは 15 分に 1 回またはより長い間隔で管理サーバーと同期します。ただし、管理サーバーでポリシーやタスクの設定を変更した場合、そのポリシーまたはタスクが適用されるデバイスで事前に同期が実行され、新しい設定がデバイスに転送されます。

| シナリオ | 管理サーバーから各管理対象デバイスへのトラフィック | 各管理対象デバイスから管理サーバーへのトラフィック |
|---|---|---|
| アップデートされた定義データベースを使用した Kaspersky Endpoint Security for Linux のインストール | 390 MB | 3.3 MB |
| ネットワークエージェントのインストール | 75 MB | 397 KB |
| ネットワークエージェントと Kaspersky Endpoint Security for Linux の同時インストール | 459 MB | 3.6 MB |
| パッケージ内のデータベースをアップデートしない定義データベースの初回のアップデート（Kaspersky Security Network への参加が無効な場合） | 113 MB | 1.8 MB |
| 定義データベースの定期アップデート（Kaspersky Security Network への参加が有効な場合） | 22 MB | 373 MB |
| デバイス上の定義データベースをアップデートする前の初回の同期（ポリシーとタスクの転送） | 382 KB | 446 KB |
| デバイス上の定義データベースをアップデートした後の初回の同期 | 20 KB | 157 KB |
| 管理サーバーに変更がない場合の同期（定期） | 18 KB | 23 KB |
| グループポリシーで 1 つの設定を変更した時の同期（変更直後） | 19 KB | 20 KB |
| グループタスクで 1 つの設定を変更した時の同期（変更直後） | 14 KB | 11 KB |
| 強制同期 | 110 KB | 109 KB |
| 「**ウイルスの検知**」イベント（1 件のウイルス） | 44 KB | 50 KB |
| 「**ウイルスの検知**」イベント（10 件のウイルス） | 58 KB | 77 KB |
| アプリケーションレジストリリストを有効にした後のワンタイムトラフィック | 最大 10 KB | 最大 12 KB |
| アプリケーションレジストリリストが有効になっている場合の毎日のトラフィック | 最大 840 KB | 最大 1 MB |

# 24 時間あたりの平均トラフィック

管理サーバーと管理対象デバイス間の 24 時間あたりの平均トラフィックは次の通りです：

- 管理サーバーから管理対象デバイスへのトラフィックは 840 KB です
- 管理対象デバイスから管理サーバーへのトラフィックは 1 MB

トラフィックは次の条件下で測定されました：

- 管理対象デバイスにはネットワークエージェントおよび Kaspersky Endpoint Security for Linux がインストールされている
- デバイスはディストリビューションポイントに割り当てられていない
- 脆弱性とパッチ管理が無効
- 管理サーバーとの同期間隔は 15 分

# 既知の問題

Kaspersky Security Center Linux には、本アプリケーションの動作には重大な影響を与えない制限があります：

- 仮想管理サーバーでの認証中に、**一般的な機能：仮想管理サーバー**機能領域でアクセス権を持たないユーザーの資格情報が使用されると、エラーが発生します。資格情報の再入力はできません。この問題を解決するには、Kaspersky Security Center Web コンソールからログアウトします。

- 子ポリシーで［**親ポリシーから設定を継承する**］をオフにし、この変更を保存して、親ポリシーでロックされている設定に移動すると、これらの設定は子ポリシーでもロックされたままになります。この問題を解決し、子ポリシー設定のロックを解除するには、ポリシー設定ウィンドウを閉じてから再度開きます。

- systemd 初期化システムバージョン 232 のオペレーティングシステムを実行しているデバイスに Kaspersky Security Center Linux をインストールしようとすると、エラーが発生します。

  インストール後に Kaspersky Security Center Linux 管理サーバーが起動せず、オペレーティングシステムのログに kladminserver_srv.service に関連するエラー 213/SECUREBITS が含まれている場合は、スーパーユーザーとして次のコマンドを実行します：

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  インストール後に Kaspersky Security Center Web コンソールが起動せず、オペレーティングシステムのログに KSCWebConsole.service に関連するエラー 213/SECUREBITS が含まれている場合は、スーパーユーザーとして次のコマンドを実行します：

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" >
  /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleMessageQueue.service.d
  echo "[Service]" >
  /etc/systemd/system/KSCWebConsoleMessageQueue.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCWebConsoleMessageQueue.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >>
  /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

- ドメインユーザーをグループに追加することはできません。
- ［**アカウント保護**］ウィンドウで［**キャンセル**］をクリックするとエラーが発生します。
- Arm アーキテクチャのオペレーティングシステムを実行し、管理サーバーと時刻が同期されていないデバイスからネットワークエージェントをアンインストールするために、［**アプリケーションのリモートアンインストール**］タスクを実行すると、ネットワークエージェントがデバイスから正常にアンインストールされた後でも、タスクのステータスが［**実行中**］から［**完了**］に変わりません。この問題を解決するには、［**アプリケーションのリモートアンインストール**］を実行する前に、デバイスの時刻とインストールされているネットワークエージェントの時刻、およびデバイスの時刻と管理サーバーの時刻を同期します。
- 名前にキリル記号が含まれるデバイスに Kaspersky Security Center Linux がインストールされている場合、管理対象デバイスは KSN プロキシサービスを介して KSN に接続できません。
- オペレーティングシステムがクローズドソフトウェア環境モードで動作している場合、Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）を実行しているデバイスに Kaspersky Security Center Web コンソールをインストールしても起動しません。
- オペレーティングシステムがクローズドソフトウェア環境モードで動作している場合、Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）を実行しているデバイスに Kaspersky Security Center Linux をインストールすることはできません。
- CentOS 6.6 を実行している管理対象デバイスでプロセスを強制終了した後、ネットワークエージェントが再起動しません。
- Kaspersky Security Center Linux 15.2 Web コンソールで「**N 時間ごと**」および「**曜日別**」のスケジュール設定を使用してタスクを作成し、そのタスクを以前のバージョンの Kaspersky Security Center Web コンソールまたは Kaspersky Security Center Linux 管理コンソールで開くと（たとえば、タスクが Linux ベースと Windows ベースの両方のセカンダリ管理サーバーにも適用されている場合）、スケジュール設定が正しく表示されないか、エラーが発生する可能性があります。
- ユーザーに対して*アカウントのパスワードの変更（Linux のみ）*タスクを作成し、［**ワンタイムパスワードとして設定（ユーザーは初回ログイン時にパスワードを変更する必要があります）**］をオンにすると、ユーザーは Kaspersky Security Center Web コンソールにサインインできなくなります。
- *ディストリビューションポイントのリポジトリにアップデートをダウンロード*または*アップデート検証*タスクをインポートすると、［**タスクが割り当てられるデバイスを選択する**］オプションがオンになります。これらのタスクは、デバイスの抽出または特定のデバイスに割り当てることはできません。*ディストリビューションポイントのリポジトリにアップデートをダウンロードする*か、特定のデバイスに*アップデート検証*タスクを割り当てると、タスクは正しくインポートされません。
- Kaspersky Endpoint Security for Windows は、管理サーバーのプロパティの KSN プロキシ設定で［**HTTPS を使用する**］がオンになっており、管理サーバーのアドレスに非ラテン文字が含まれている場合、KSN プロキシサービスをサポートしません。
- ［**アプリケーションレジストリ**］セクションのアプリケーションが Linux デバイス上で検出された場合、アプリケーションのプロパティには関連する実行ファイルに関する情報が含まれません。
- レター形式のレポートで、改ページによりテキスト行が横方向に切れることがあります。
- 1つ以上のネットワークアダプターを持つ管理対象デバイスが管理サーバーにネットワークアダプターの MAC アドレスに関する情報を送信する際、管理サーバーへの接続に使用されていないものの情報を送信することがあります。
- *スクリプトをリモートで実行*タスクが開始されると、割り当てられているアカウントを変更することはできません。タスクが割り当てられているアカウントを変更するには、タスク設定でタスクを停止し、正しいアカウント詳細で再度作成します。

- ユーザーデバイスで *SELinux* が有効になっている場合、アカウントパスワードの変更タスクが正しく機能しない可能性があります。SELinux を無効にする方法の詳細については、ご使用のオペレーティングシステムの関連ユーザーガイドを参照してください。

- arping パッケージと iputils-arping パッケージの両方、または arping パッケージのみがインストールされている場合、フェールオーバークラスタの導入は失敗します。フェールオーバークラスタの導入前に、両方のノードに iputils-arping パッケージのみがインストールされていることを確認してください。

- Kaspersky Security Center OpenAPI を使用するには、［Kaspersky Security Center Linux インストール］フォルダー内の KlAkOAPI アーカイブを使用する代わりにアップデートされた KlAkOAPI.tar.gz アーカイブをダウンロードしてください。

# テクニカルサポートへの問い合わせ

このセクションでは、サポートを受ける方法および提供条件について説明します。

## テクニカルサポートのご利用方法

Kaspersky Security Center Linux のドキュメントや Kaspersky Security Center Linux の情報源で問題のソリューションが見つからない場合、カスペルスキーのテクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Security Center Linux のインストール方法や使用方法についてのお問い合わせに回答いたします。

カスペルスキーによる Kaspersky Security Center Linux のサポートは、本製品のライフサイクル期間中に提供されます（アプリケーションのサポートライフサイクルページを参照）。テクニカルサポートに連絡する前に、サポートサービス規約をご確認ください。

テクニカルサポートサービスの内容については、サポートセンターのご案内を参照してください。

- テクニカルサポートサイトにアクセスする
- カスペルスキーカンパニーアカウントからテクニカルサポートへリクエストを送信

## カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品を使用する法人向けのポータルです。このポータルは、オンラインリクエストを通じてユーザーとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストの進捗をモニターでき、リクエストの履歴を保存することができます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語

- ポルトガル語
- ロシア語
- フランス語
- 日本語

カスペルスキーカンパニーアカウントについて詳しくは、テクニカルサポートサイトをご覧ください。

# 管理サーバーのダンプファイルの取得

管理サーバーのダンプファイルには、ある時点での管理サーバープロセスに関するすべての情報が含まれています。管理サーバーのダンプファイルは、ディレクトリ /var/lib/systemd/coredump に保存されます。ダンプファイルは、Kaspersky Security Center Linux が使用されている限り保存され、削除されると完全に削除されます。ダンプファイルが自動的にカスペルスキーに送信されることはありません。

管理サーバーがクラッシュした場合は、カスペルスキーのテクニカルサポートにお問い合わせください。サポートの担当者が、カスペルスキーでより詳細な分析を行うために管理サーバーのダンプファイルのご提供をお客様にお願いする場合があります。

ダンプファイルには個人データが含まれている可能性があります。情報をカスペルスキーに送信する前に、不正アクセスから保護することを推奨します。

# 製品の情報源

## カスペルスキー Web サイトの Kaspersky Security Center Linux のページ

カスペルスキー Web サイトの Kaspersky Security Center Linux のページで、本製品と機能、使用に関する一般的な情報を確認できます。

## ナレッジベースの Kaspersky Security Center Linux のページ

カスペルスキーのテクニカルサポートサイトにナレッジベースのセクションがあります。

ナレッジベースの Kaspersky Security Center Linux のページに、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、本製品だけではなく他のカスペルスキー製品に関連した質問にも回答しています。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

## カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーのフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、様々なトピックで意見交換しています。

フォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

> オンラインの情報源を使用するには、インターネット接続が必要です。

問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートまでお問い合わせください。

# 用語解説

## Cloud Discovery

Cloud Discovery は、組織のクラウドインフラストラクチャを保護する Cloud Access Security Broker（CASB）ソリューションのコンポーネントです。Cloud Discovery は、クラウドサービスへのユーザーアクセスを管理します。クラウドサービスには、Microsoft Teams、Salesforce、Microsoft Office 365 などがあります。クラウドサービスは、*データ交換*、*メッセンジャー*、*メール*などのカテゴリにグループ化されています。

## HTTPS

データ転送用のセキュアプロトコル。ブラウザーと Web サーバーの通信に暗号を使用します。HTTPS は、企業データや財務データなどの制限付き情報へのアクセスに使用されます。

## iOS MDM サーバー

クライアントデバイスにインストールされる Kaspersky Security Center のコンポーネントの 1 つ。iOS モバイルデバイスの管理サーバーへの接続と、APNs（Apple Push Notifications Service）による iOS モバイルデバイスの管理を可能にします。

## iOS MDM デバイス

iOS MDM プロトコルを使用して iOS MDM サーバーに接続されたモバイルデバイス。iOS オペレーティングシステムで動作しているデバイスが、iOS MDM プロトコルを使用して接続および管理できます。

## JavaScript

Web ページのパフォーマンスを拡張するプログラミング言語。JavaScript を使用して作成された Web ページでは、Web サーバーからの新しいデータでブラウザーの表示をアップデートすることなく、インターフェイス要素の表示を変更したり、新しいウィンドウを表示したりできます。JavaScript を使用して作成されたページを表示するには、ブラウザーの設定で JavaScript のサポートを有効にします。

## Kaspersky Private Security Network（KPSN）

Kaspersky Private Security Network は、カスペルスキー製品がインストールされたデバイスのユーザーがデバイスから Kaspersky Security Network にデータを送信することなく、Kaspersky Security Network の評価データベースとその他の統計データにアクセスできるようにするソリューションです。Kaspersky Private Security Network は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- デバイスがインターネットに接続されていない。

- 国外や企業 LAN の外へのデータの送信が、法律または社内のセキュリティポリシーで禁止されている。

## Kaspersky Security Center Linux Web サーバー

管理サーバーとともにインストールされる Kaspersky Security Center Linux のコンポーネントの 1 つ。Web サーバーは、スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

## Kaspersky Security Center Linux 管理者

Kaspersky Security Center Linux システムを使用して、アプリケーションの動作をリモートで一元管理する担当者。

## Kaspersky Security Center オペレーター

Kaspersky Security Center システムで管理している保護システムのステータスと動作を監視するユーザー。

## Kaspersky Security Center システム正常性検証ツール（SHV）

Kaspersky Security Center Linux のコンポーネントの 1 つで、Kaspersky Security Center Linuz と Microsoft NAP を同時運用している場合のオペレーティングシステムの操作性をチェックします。

## Network Location Awareness（NLA）

オペレーティングシステムが現在のネットワークを識別するのに役立つ Windows サービス。NLA はネットワークの変更を検出し、デバイスのセキュリティ設定を調整します。

## SSL

インターネットおよびローカルネットワークで使用されるデータ暗号化プロトコル。Secure Sockets Layer（SSL）は Web アプリケーションで使用され、クライアントとサーバーの間のセキュアな接続を確立します。

## アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を置換または追加する処理。

## アプリケーションの一元管理

Kaspersky Security Center が備える管理サービスを使用した、アプリケーションのリモート管理。

## アプリケーションの直接管理

ローカルインターフェイスを使用したアプリケーション管理。

## アプリストア

Kaspersky Security Center Linux のコンポーネント。アプリストアを使用すると、Android デバイスの所有者が自分でアプリケーションをインストールできます。アプリストアでは、アプリケーションの APK ファイルや Google Play のリンクを公開できます。

## アンチウイルスサービスプロバイダー

クライアント組織にカスペルスキー製品に基づくアンチウイルスサービスを提供する組織。

## イベントの重要度

カスペルスキー製品の動作時に発生したイベントのプロパティ。次のレベルに分かれています：

- 緊急
- 機能エラー
- 警告
- 情報

イベント発生の状況によって、同じ種別のイベントで重要度が異なる場合があります。

## イベントリポジトリ

管理サーバーデータベースのうち、Kaspersky Security Center Linux で発生するイベントに関する情報の保管専用の領域です。

## インストールパッケージ

カスペルスキー製品のリモートインストール用に作成されるファイルセット。リモート管理システム Kaspersky Security Center を使用して作成します。インストールパッケージには、アプリケーションをインストールし、インストール後にすぐに実行させるのに必要な設定の範囲が含まれます。設定は、アプリケーションの既定値になります。インストールパッケージは、配布キットに含まれる拡張子が kpd および kud のファイルを使用して作成されます。

## ウイルスアウトブレイク

デバイスをウイルスに感染させるための、一連の意図的な試み。

## カスペルスキーのアップデートサーバー

カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

## 仮想管理サーバー

クライアント組織のネットワークの保護システムを管理する Kaspersky Security Center Linux のコンポーネント。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

## 管理グループ

機能およびインストールされているカスペルスキー製品に応じてデバイスをまとめたグループ。複数のデバイスを1つのグループとして管理できます。1つのグループに下位のグループとして他のグループを含めることができます。グループにインストールされている各アプリケーションに対してグループポリシーやグループタスクを作成することができます。

## 管理コンソール

Windows ベースの Kaspersky Security Center（別名「MMC ベースの管理コンソール」）のコンポーネント。このコンポーネントは、管理サーバーとネットワークエージェントの管理サービスに対してユーザーインターフェイスを提供します。管理コンソールは、 Kaspersky Security Center Web コンソールに類似しています。

## 管理コンピューター

Kaspersky Security Center Web コンソールを開いたデバイス。このコンポーネントにより、Kaspersky Security Center Linux の管理に使用できるインターフェイスが提供されます。

管理コンピューターは、Kaspersky Security Center Linux のサーバー部分の設定と管理に使用されます。管理コンピューターを使用して、カスペルスキー製品に基づいて一元化されたアンチウイルスによる企業内 LAN の保護を構築および管理します。

## 管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center Linux のコンポーネント。製品の管理にも使用できます。

## 管理サーバークライアント（クライアントデバイス）

ネットワークエージェントがインストールされ管理対象のカスペルスキー製品が実行されているデバイス、サーバー、またはワークステーション。

## 管理サーバー証明書

管理サーバーが次の目的で使用する証明書：

- Kaspersky Security Center Web コンソールへの接続時における管理サーバーの認証
- 管理対象デバイスでの管理サーバーとネットワークエージェントとの安全な連携
- プライマリ管理サーバーをセカンダリ管理サーバーに接続する際の管理サーバーの認証

証明書は、管理サーバーをインストールすると自動的に作成され、管理サーバーに保存されます。

## 管理サーバーデータのバックアップ

管理サーバーのデータをバックアップし、後でバックアップユーティリティを使用して復元できるようにコピーすること。ユーティリティで保存できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

## 管理サーバーデータの復元

バックアップユーティリティを使用して、バックアップに保存されている情報から管理サーバーデータを復元すること。ユーティリティで復元できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

## 管理者権限

Exchange 組織内の Exchange オブジェクトの管理に必要な、ユーザー権限および特権のレベル。

## 管理対象デバイス

管理グループに含まれる企業ネットワークデバイス。

## 共有証明書

ユーザーのモバイルデバイスを識別することを目的とした証明書。

## クライアント管理者

クライアント組織のスタッフ。アンチウイルスのステータスを監視します。

## グループタスク

管理グループに定義され、そのグループ内のすべてのクライアントデバイスで実行されるタスク。

## 軽量ナジェント（LWNGT）

モバイルデバイス上の Kaspersky Endpoint Security と対話するためのプロトコル。LWNGT（モバイルプロトコルとも呼ばれます）は、モバイルデバイスにネットワークエージェントを実際にインストールしなくても、ネットワークエージェントとして機能します。

## 現在のライセンス

アプリケーションによって現在使用されているライセンス。

## 互換性がないアプリケーション

サードパーティ製のアンチウイルス製品、または Kaspersky Security Center Linux を使用した管理に対応していないカスペルスキー製品。

## サービスプロバイダーの管理者

アンチウイルスサービスプロバイダーのスタッフ。サービスプロバイダーの管理者は、カスペルスキー製品に基づき、アンチウイルスシステムをインストールおよび管理し、テクニカルサポートを顧客に提供します。

## 手動インストール

配布パッケージからの、企業ネットワーク上のデバイスへのセキュリティ製品のインストール。手動インストールには、管理者または別の IT スペシャリストの参加が必要です。通常、手動インストールは、リモートインストールでエラーが発生した場合に行います。

## 脆弱性

マルウェアの開発者がオペレーティングシステムやプログラムに侵入してその完全性を損なわせるために利用する可能性のあるオペレーティングシステムまたはプログラムの欠陥。オペレーティングシステムに多くの脆弱性があると、機能の信頼性が損なわれます。侵入したウイルスによってオペレーティングシステム自体またはインストールされているアプリケーションで障害が引き起こされる可能性があるためです。

## 接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

## 設定プロファイル

iOS MDM モバイルデバイスの設定と制限事項に関するポリシー。

## タスク

カスペルスキー製品によって実行される機能はタスクとして実装されます。ファイルのリアルタイム保護、デバイスの完全スキャン、定義データベースのアップデートなどのタスクがあります。

## タスク設定

各タスク種別に固有のアプリケーション設定です。

## 追加（または予備）ライセンス

製品を使用する権限を認定する、現在使用されていないライセンス。

## 定義データベース

定義データベースの公開時点で、カスペルスキーが把握しているコンピューターセキュリティへの脅威についての情報を含むデータベース。定義データベース内のエントリによって、スキャンしているオブジェクトで悪意のあるコードを検知できます。定義データベースはカスペルスキーのエキスパートにより作成され、1時間ごとにアップデートされます。

## ディストリビューションポイント

ネットワークエージェントがインストールされており、アップデートの配信やアプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。ディストリビューションポイントは、アップデート配信時の管理サーバーの負荷軽減およびネットワークトラフィックの最適化の目的で設計されています。ディストリビューションポイントは、管理サーバーによって自動的に、または管理者によって手動で割り当てられます。ディストリビューションポイントは、以前のバージョンの製品ではアップデートエージェントという名称でした。

## 適用可能なアップデート

カスペルスキーのソフトウェアモジュールに関する一連のアップデート（一定期間に蓄積された重大なアップデート、アプリケーションのアーキテクチャへの変更を含む）

## デバイスの所有者

デバイスで特定の操作が必要になった際に管理者が連絡できるユーザー。

## 特定のデバイスに対するタスク

任意の管理グループに属する一連のクライアントデバイスに割り当てられ、それらのデバイスで実行されるタスク。

## 内部ユーザー

内部ユーザーのアカウントは、仮想管理サーバーを操作するために使用します。Kaspersky Security Center Linux によって、実際のユーザーの権限がアプリケーションの内部ユーザーに付与されます。

内部ユーザーのアカウントは、Kaspersky Security Center Linux 内でのみ作成および使用されます。内部ユーザーに関するデータは、オペレーティングシステムには送信されません。Kaspersky Security Center Linux が内部ユーザーを認証します。

## 認証エージェント

起動可能なハードディスクの暗号化後に、暗号化されたハードディスクへのアクセス権を取得してオペレーティングシステムを読み込むための認証手順を完了することができるインターフェイス。

## ネットワークエージェント

管理サーバーと特定のネットワークノード（ワークステーションまたはサーバー）にインストールされているカスペルスキー製品との間のやり取りを受け持つ Kaspersky Security Center Linux のコンポーネント。このコンポーネントは、カスペルスキーの Microsoft® Windows® 用の製品に共通した機能です。Unix 系の OS および macOS 用には、それぞれ異なるバージョンのネットワークエージェントがあります。

## ネットワークのアンチウイルスによる保護

組織のネットワークにウイルスやスパムが侵入する危険性を軽減し、ネットワーク攻撃やフィッシングなどの脅威を防ぐ一連の技術的、組織的対策。ネットワークセキュリティは、セキュリティ製品およびサービスを使用して企業のセキュリティポリシーに従い、正しく適用することで向上します。

## ネットワーク保護ステータス

企業ネットワーク内のデバイスのセキュリティレベルを定義する現在の保護ステータス。ネットワーク保護ステータスには、インストール済みセキュリティ製品、ライセンスの使用、検知された脅威の数と種類のような要因を含みます。

## バックアップフォルダー

管理サーバーデータのコピーを保管するための特別なフォルダー。バックアップユーティリティによって作成されます。

## パッチの重要度

パッチの属性の1つ。Microsoft のパッチおよびサードパーティのパッチには、5 つの重要度があります：

- 緊急
- 高
- 中
- 低
- 不明

サードパーティのパッチまたは Microsoft のパッチの重要度は、パッチが修正する脆弱性のうち、最も高い重要度によって決定されます。

## 非武装地帯（DMZ）

非武装地帯は、サーバーを含むローカルネットワークのセグメントで、グローバル Web からの要求に応えます。組織のローカルネットワークのセキュリティを確保するために、非武装地帯から LAN へのアクセスがファイアウォールで保護されます。

## 復元

隔離またはバックアップ内のオブジェクトを、隔離、感染駆除、削除される前の元のフォルダーまたはユーザーが指定したフォルダーに移動すること。

## ブロードキャストドメイン

OSI 基本参照モデル（Open Systems Interconnection Basic Refernce Model）のレベルにおける、ブロードキャストチャネルを使用してすべてのノードがデータ交換を行えるネットワークの論理領域。

## プログラム設定

あらゆる種類のタスクに共通していて、アプリケーションの動作全体を管理するアプリケーション設定（アプリケーションパフォーマンス設定、レポート設定、バックアップ設定など）。

## プロビジョニングプロファイル

iOS モバイルデバイスでのアプリケーションの動作に関する設定の集まり。プロビジョニングプロファイルには、ライセンスに関する情報が書き込まれています。このプロファイルは、特定のアプリケーションにリンクされています。

## プロファイル

Exchange モバイルデバイスに関する一連の設定。Microsoft Exchange サーバーへの接続時の動作を定義します。

## ホーム管理サーバー

ネットワークエージェントのインストール中に指定した管理サーバー。ホーム管理サーバーは、ネットワークエージェントの接続プロファイルを設定するために使用できます。

## 保護ステータス

コンピューターのセキュリティレベルを定義する現在の保護ステータス。

## ポリシー

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピューターにインストールされたアプリケーションを設定する権限を管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピューターにインストールされたアプリケーションについて複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つだけです。

## ライセンス情報ファイル

拡張子が「KEY」のファイル。このファイルを使用することで、カスペルスキー製品を試用版または製品版ライセンスで使用できます。

## ライセンスの有効期間

ユーザーがアプリケーションの機能および追加サービスへのアクセス権を有する期間。使用できるサービスは、ライセンスの種別によって異なります。

## リモートインストール

Kaspersky Security Center Linux を使用した、カスペルスキー製品のインストール。

## ローカルインストール

組織のネットワーク上のデバイスにセキュリティ製品をインストールするには、セキュリティ製品の配布パッケージからインストールを手動で開始する方法、またはコンピューターに事前にダウンロードしておいた公開済みインストールパッケージを手動で起動する方法があります。

## ローカルタスク

1台のクライアントコンピューターを対象として定義、実行されるタスク。

## ロールグループ

同一の管理者権限を許可されている、Exchange ActiveSync モバイルデバイスユーザーのグループ。

# サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、ファイル legal_notices.txt に記載され、カスペルスキー製品のインストールディレクトリに保存されています。

# 商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、PostScript、Shockwaveは、米国および他の国における Adobe の登録商標または商標です。

AMD、AMD64 は、Advanced Micro Devices, Inc. の商標または登録商標です。

Amazon、Amazon Web Services、AWS、Amazon EC2、AWS Marketplace は、Amazon.com, Inc. またはその関連会社の商標です。

Apache は、Apache Software Foundation の登録商標または商標です。

AirPlay、AirDrop、AirPrint、App Store、Apple、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、Tiger、QuickTime、Touch ID は、Apple Inc. の商標です。

Arm は、Arm Limited（またはその子会社）の米国および / またはその他の国における登録商標です。

Bluetooth の表記、マークおよびロゴは、Bluetooth SIG, Inc. に所有権があります。

Ubuntu LTS は Canonical Ltd の登録商標です。

Cisco、Cisco Jabber、Cisco Systems、IOS は、米国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Citrix、XenServer は、米国およびその他の国における Cloud Software Group, Inc. およびその子会社の登録商標または商標です。

Corel は、カナダ、米国およびその他の国における Corel Corporation およびその子会社の商標または登録商標です。

Cloudflare、Cloudflare のロゴ、および Cloudflare Workers は、米国およびその他の法域における Cloudflare, Inc. の商標や登録商標です。

Dropbox は、Dropbox, Inc. の商標です。

Radmin は、Famatech の登録商標です。

Firebird は、Firebird Foundation の登録商標です。

Foxit は、Foxit Corporation の登録商標です。

FreeBSD は、FreeBSD Foundation の登録商標です。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Google Public DNS、Hangouts、YouTube は、Google LLC の商標です。

EulerOS、FusionCompute、FusionSphere は、Huawei Technologies Co., Ltd. の商標です。

Intel、Core、Xeon は、Intel Corporation またはその子会社の商標です。

IBM および QRadar は、世界各国で International Business Machines Corporation が所有する登録商標です。

Node.js は Joyent Inc. の商標です。

Linux は、米国およびその他の国における Linus Torvalds 氏の登録商標です。

Logitech は Logitech の米国および他の国における登録商標または商標です。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、PowerShell、PowerPoint、SharePoint、SQL Server、Office 365、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Server、Windows Phone、Windows Vista、Windows Azure は、Microsoft グループ企業が所有する商標です。

Mozilla、Firefox、Thunderbird は、米国およびその他の国における Mozilla Foundation の商標です。

Novell は、米国およびその他の国における Novell Enterprises Inc. の登録商標です。

OpenSSL は、OpenSSL Software Foundation が所有する商標です。

OpenVPN は、OpenVPN, Inc. の登録商標です。

Oracle、Java、JavaScript、TouchDown は、Oracle とその関連会社の両方またはいずれかの登録商標です。

Parallels、Parallels ロゴ、および Coherence は、Parallels International GmbH の商標または登録商標です。

Chef は、Progress Software Corporation およびその子会社または関連会社の、米国およびその他の国における商標または登録商標です。

Puppet は、Puppet, Inc. の商標または登録商標です。

Python は Python Software Foundation の登録商標または商標です。

Red Hat、CentOS、Fedora、Red Hat Enterprise Linux は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

Ansible は、米国およびその他の国における Red Hat, Inc. の登録商標です。

CentOS は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

BlackBerry は、Research In Motion Limited の米国における登録商標であり、その他の国における登録商標または登録出願中の商標です。

Rocky Linux は、Rocky Enterprise Software Foundation の商標です。

Samsung は、米国およびその他の国における SAMSUNG の登録商標です。

Debian は、Software in the Public Interest, Inc. の登録商標です。

Splunk、SPL は、Splunk, Inc. の米国およびその他の国における登録商標です。

SUSE は、米国およびその他の国における SUSE LLC の登録商標です。

Symbian の商標は Symbian Foundation Ltd. が所有します。

OpenAPI は、Linux Foundation の登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited のライセンス契約の下で排他的に使用されています。

Zabbix は Zabbix SIA の登録商標です。