KASPERSKY

Kaspersky Security for Windows Server

管理者用ガイド

製品バージョン：10.1.0.622

Kaspersky Lab の製品をお使いの皆さまへ

このたびは Kaspersky Lab をセキュリティソフトウェアプロバイダとしてお選びいただき、ありがとうございます。このガイドが当社製品をご利用いただく際の一助となることを願っております。

ガイド改訂日：2018 年 5 月 10 日

https://www.kaspersky.co.jp
https://support.kaspersky.co.jp

目次

このガイドの概要

Kaspersky Security for Windows Server 10.1.0.622（以降「Kaspersky Security 10.1 for Windows Server」）の『管理者用ガイド』は、保護対象の全デバイスにおいて Kaspersky Security 10.1 for Windows Server をインストールおよび管理する担当者と、Kaspersky Security 10.1 for Windows Server を使用する組織のテクニカルサポートを行う担当者向けのガイドです。

このガイドでは、Kaspersky Security 10.1 for Windows Server の設定および使用に関する情報について記載しています。

また、本製品に関する情報の入手先およびテクニカルサポートを受ける方法についても確認できます。

この章の内容

ガイドの内容

Kaspersky Security 10.1 for Windows Server の『管理者用ガイド』には、以下のセクションがあります：

Kaspersky Security 10.1 for Windows Server に関する情報源

このセクションでは、製品の情報源を示します。

Kaspersky Security 10.1 for Windows Server

このセクションでは、Kaspersky Security 10.1 for Windows Server の機能、コンポーネント、および配布キット

について説明し、Kaspersky Security 10.1 for Windows Server のシステム要件のリストを提供します。

Kaspersky Security 10.1 for Windows Server のインストールおよびアンインストール

このセクションでは、Kaspersky Security 10.1 for Windows Server のインストールと削除について、段階的に説明します。

アプリケーションインターフェイス

このセクションでは、Kaspersky Security 10.1 for Windows Server のインターフェイス項目に関する情報について説明します。

ライセンス

このセクションでは、本製品のライセンスに関する主要な概念について説明します。

Kaspersky Security 10.1 for Windows Server の開始と停止

このセクションでは、Kaspersky Security 10.1 for Windows Server の管理プラグイン（以降「Kaspersky Security 10.1 for Windows Server 管理プラグイン」）および Kaspersky Security サービスの開始と停止について説明します。

Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限

このセクションでは、Kaspersky Security 10.1 for Windows Server を管理するための権限およびアプリケーションによって登録される Windows® サービスを管理するための権限に関する情報と、それらの権限の設定方法について説明します。

ポリシーの作成と設定

このセクションでは、Kaspersky Security Center のポリシーによる複数のサーバーの Kaspersky Security 10.1 for Windows Server の管理について説明します。

Kaspersky Security Center を使用したタスクの作成と設定

このセクションでは、Kaspersky Security 10.1 for Windows Server タスク、そのタスクの作成方法と設定方法、およびそのタスクの開始方法と停止方法に関する情報について説明します。

アプリケーション設定の管理

このセクションでは、Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server の全般的な設定についての情報が記載されています。

サーバーのリアルタイム保護

このセクションでは、リアルタイム保護タスク:リアルタイムファイル保護、スクリプト監視、KSN の使用、脆弱性攻撃からの保護に関する情報について説明します。また、リアルタイム保護タスクを設定する手順、および保護対象のサーバーのセキュリティ設定を管理する手順についても説明します。

ローカルアクティビティの管理

このセクションでは、USB 経由で外部デバイスによってアプリケーションの開始と接続をコントロールする Kaspersky Security 10.1 for Windows Server 機能に関する情報について説明します。

ネットワークアクティビティの管理

このセクションでは、ファイアウォール管理とアンチクリプタータスクに関する情報について説明します。

システム監査

このセクションではファイル変更監視タスクと、オペレーティングシステムログを調査する機能に関する情報が含まれています。

監視パフォーマンス Kaspersky Security 10.1 for Windows Server のカウンター

このセクションでは、Kaspersky Security 10.1 for Windows Server のカウンター:システム監視用パフォーマンスカウンター、SNMP カウンターとトラップに関する情報について説明します。

コマンドラインからの Kaspersky Security 10.1 for Windows Server の使用

このセクションでは、コマンドラインからの Kaspersky Security 10.1 for Windows Server の使用について説明します。

テクニカルサポートへのお問い合わせ

このセクションでは、テクニカルサポートを受ける方法と利用条件について説明します。

用語解説

このセクションでは、このガイドで使用されている用語とその定義について説明します。

AO Kaspersky Lab

AO Kaspersky Lab について説明します。

サードパーティ製のコードに関する情報

このセクションでは、アプリケーションで使用されているサードパーティ製のコードに関する情報について説明します。

商標に関する通知

このセクションでは、このガイド内で使用されている、サードパーティ所有者に属する商標について説明します。

索引

このセクションでは、ガイド内の必要な情報をすばやく見つけることができます。

文書規約

このガイドで使用される文書規約について説明します（以下の表を参照）。

表 1. 文書規約

サンプルテキスト	文書規約の説明
...に注意してください	警告は赤色で表示し、枠で囲んで強調します。警告には、良くない結果となる可能性がある操作に関する情報が含まれます。
...を使用してください	注記は枠で強調表示します。注記には補足情報や参考情報が記載されています。
例: …	例は、「例」という見出しで青色の背景のブロックに表記されます。
アップデートとは… [定義データベースの未アップデート]イベントが発生します。	次の要素はテキスト内で太字表記されます: • 新しい用語 • アプリケーションのステータス名とイベント名
ENTER キーを押します。 ALT+F4 キーを押します。	キーボードのキー名は太字で、すべて大文字になっています。 キー名がプラス記号(+)で結合されている場合、キーの組み合わせを示します。これらのキーは同時に押下する必要があります。
[有効にする]をクリックします。	テキストボックス、メニュー項目、ボタンなどの製品インターフェイスの要素名は太字で表記します。
► **タスクスケジュールを設定するには:**	手順は太字表記され、矢印のマークで示されます。

サンプルテキスト	文書規約の説明
コマンドラインに「`help`」と入力してください。 次のメッセージが表示されます: 日付を `dd:mm:yy` の形式で指定してください。	次の種類のテキストの内容は特殊フォントで表記されます: • コマンドラインのテキスト • 画面上に表示されるメッセージテキスト • キーボードによる入力が必要なデータ
<ユーザー名>	変数は山括弧で囲んで表記します。変数の代わりに、それぞれの状況に対応する値を、山括弧なしで挿入する必要があります。

Kaspersky Security 10.1 for Windows Server に関する情報源

このセクションでは、製品の情報源を示します。

問題の重要性や緊急性に応じて、情報の入手先をお選びください。

この章の内容

自分で調査する場合の情報源

Kaspersky Security 10.1 for Windows Server についての情報は、次の場所から入手できます:

- カスペルスキーの Web サイトの Kaspersky Security 10.1 for Windows Server のページ。
- テクニカルサポートサイト（ナレッジベース） - Kaspersky Security 10.1 for Windows Server のページ。
- ガイド。

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（https://support.kaspersky.co.jp/）にお問い合わせください。

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。

カスペルスキーの Web サイトの Kaspersky Security 10.1 for Windows Server のページ

カスペルスキーの Web サイトの Kaspersky Security 10.1 for Windows Server のページ（https://www.kaspersky.co.jp/business-security/windows-server-security）で、本製品とその機能に関する全般的な情報を参照できます。

Kaspersky Security 10.1 for Windows Server のページには、オンラインストアへのリンクがあります。このページでアプリケーションの購入やライセンスの更新ができます。

ナレッジベースの Kaspersky Security 10.1 for Windows Server のページ

ナレッジベースは、テクニカルサポートサイトにあるセクションです。

ナレッジベースの Kaspersky Security 10.1 for Windows Server のページ（https://support.kaspersky.co.jp/ksws10/）には、製品の購入、インストール、使用の方法に関する便利な情報、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、Kaspersky Security 10.1 for Windows Server だけでなく、その他のカスペルスキー製品に関する質問への回答も参照できます。また、テクニカルサポートニュースも含まれます。

Kaspersky Security 10.1 for Windows Server に関する文書

『Kaspersky Security 10.1 for Windows Server 管理者用ガイド』には、アプリケーションのインストール、アンインストール、設定、および使用に関する情報が含まれます。

Web フォーラムの利用

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 Web フォーラム（http://forum.kaspersky.com/）をご利用ください。ここでは、Kaspersky Lab のエキスパートやカスペルスキー製品のユーザーが、さまざま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スレッドの閲覧、コメントの書き込み、新しいスレッドの作成が可能です。

Kaspersky Security 10.1 for Windows Server

このセクションでは、Kaspersky Security 10.1 for Windows Server の機能、コンポーネント、および配布キットについて説明し、Kaspersky Security 10.1 for Windows Server のシステム要件のリストを提供します。

この章の内容

Kaspersky Security 10.1 for Windows Server について

Kaspersky Security 10.1 for Windows Server（以前の製品名は Kaspersky Anti-Virus for Windows Servers Enterprise Edition）は、Microsoft® Windows® オペレーティングシステムで動作するサーバーとネットワークストレージを、ファイル交換を介してサーバーに影響を及ぼすウイルスなどのコンピューターセキュリティの脅威から保護します。Kaspersky Security 10.1 for Windows Server は、中規模から大規模の組織のローカルエリアネットワークでの使用を想定して設計されています。Kaspersky Security 10.1 for Windows Server の対象ユーザーは、企業ネットワークをアンチウイルスによって保護することを責務とする企業のネットワーク管理者お

よびスペシャリストです。

Kaspersky Security 10.1 for Windows Server は次のサーバーにインストールできます:

- ターミナルサーバー
- 印刷サーバー
- アプリケーションサーバー
- ドメインコントローラー
- ネットワーク接続ストレージを保護しているサーバー
- ファイルサーバー - このサーバーは、ユーザーのワークステーションとファイルを交換するため、感染の可能性が他のサーバーよりも高くなります。

Kaspersky Security 10.1 for Windows Server は次の方法で管理できます:

- Kaspersky Security 10.1 と同じサーバーまたは異なるコンピューターにインストールされた Kaspersky Security 10.1 for Windows Server コンソールを使用する方法
- コマンドラインでコマンドを使用する方法
- Kaspersky Security Center の管理コンソールを使用する方法

Kaspersky Security Center アプリケーションを使用して、Kaspersky Security 10.1 for Windows Server を実行している複数のサーバーを一元管理することもできます。

「システム監視」アプリケーション用の Kaspersky Security 10.1 for Windows Server のパフォーマンスカウンターに加えて、SNMP カウンターおよび SNMP トラップを確認することができます。

Kaspersky Security 10.1 for Windows Server のコンポーネントと機能

本製品には、次のコンポーネントが含まれています:

- **リアルタイム保護**:Kaspersky Security 10.1 for Windows Server はオブジェクトがアクセスされたタイミングでスキャンを行います。Kaspersky Security 10.1 for Windows Server は次のオブジェクトをスキャンします:

- ファイル
- 代替のファイルシステムスレッド（NTFS スレッド）
- ローカルハードディスクおよびリムーバブルドライブのマスターブートレコードとブートセクター

- **オンデマンドスキャン**：Kaspersky Security 10.1 for Windows Server は、指定した領域で、ウイルスやその他のコンピューターセキュリティの脅威のスキャンを 1 回実行します。アプリケーションは、保護されたコンピューターでファイル、RAM、およびスタートアップオブジェクトをスキャンします。
- **RPC ネットワークストレージの保護**および **ICAP ネットワークストレージの保護**：Microsoft Windows オペレーティングシステムが実行されているサーバーにインストールされた Kaspersky Security 10.1 for Windows Server は、ファイル交換によってサーバーに侵入するウイルスやその他のセキュリティの脅威からネットワーク接続ストレージシステムを保護します。
- **アプリケーション起動コントロール**：ユーザーによるアプリケーションの起動の試行を追跡し、アプリケーションの起動を制御します。
- **デバイスコントロール**：大容量記憶デバイスと CD / DVD ドライブの登録と使用を制御し、USB 接続フラッシュドライブやその他の種別の外部デバイスとファイルを交換している際に発生する可能性のあるセキュリティ脅威からコンピューターを保護します。
- **アンチクリプター**および **NetApp のアンチクリプター**：悪意のある動作を示すコンピューターをブロックして、サーバーおよびネットワーク接続ストレージ上の共有フォルダーを悪意のある暗号化から保護します。
- **スクリプト監視**：Microsoft Windows スクリプトテクノロジーを使用して作成されたスクリプトの実行を制御します。
- **トラフィックのセキュリティ**：既知のコンピューターと保護対象サーバーのその他の脅威を検知するため、Web トラフィック（メールを含む）を介して転送されるオブジェクトをインターセプトおよびスキャンします。
- **ファイアウォール管理**：Windows ファイアウォールを管理する機能を提供します。設定およびオペレーティングシステムのファイアウォールのルールを設定し、ファイアウォールを設定する他の方法をすべて

ブロックします。

- **ファイル変更監視**：Kaspersky Security 10.1 for Windows Server では、タスク設定で指定された監視範囲内のファイルの変更が検出されます。これらの変更は、保護対象のコンピューターでのセキュリティ侵害を示している場合があります。

- **Windows イベントログ監視**：このコンポーネントは、Windows イベントログの検査の結果に基づいて、保護された環境の整合性を監視します。

この製品で実装されている機能は次のとおりです：

- **定義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アップデート**：Kaspersky Security 10.1 for Windows Server は、Kaspersky Lab の FTP または HTTP アップデートサーバー、Kaspersky Security Center 管理サーバー、またはその他のアップデート元から定義データベースやモジュールのアップデートをダウンロードします。

- **隔離**：Kaspersky Security 10.1 for Windows Server は、感染の可能性があるオブジェクトを、元の場所から**隔離**に移動することで隔離します。セキュリティ上の理由から、オブジェクトは暗号化形式で隔離に保存されます。

- **バックアップ**：Kaspersky Security 10.1 for Windows Server では、**感染**または**感染の可能性あり**に分類されたオブジェクトの暗号化されたコピーが、駆除または削除の前に**バックアップ**に保存されます。

- **管理者およびユーザーの通知**：保護対象のコンピューターにアクセスする管理者とユーザーに対して Kaspersky Security 10.1 for Windows Server の動作におけるイベントとコンピューター上のアンチウイルスによる保護のステータスを通知するように、本製品を設定できます。

- **設定のインポートとエクスポート**：Kaspersky Security 10.1 for Windows Server の設定を XML 設定ファイルにエクスポートしたり、設定ファイルから Kaspersky Security 10.1 for Windows Server に設定をインポートしたりすることができます。設定ファイルには、すべてのアプリケーション設定または個別のコンポーネント設定のみを保存できます。

- **テンプレートの適用**：コンピューターのファイルリソースのツリー内またはリスト内のフォルダーのセキュリティ設定を手動で設定し、その設定値をテンプレートとして保存できます。その後、そのテンプレートを使用して、Kaspersky Security 10.1 for Windows Server の保護やスキャンタスクで、他のフォルダーのセキュリティ設定を行うことができます。

- **Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限の管理**：アプリケーションに登録されているユーザーやグループユーザーに対して Kaspersky Security 10.1 for Windows Server サービスおよび Windows サービスを管理する権限を設定できます。
- **アプリケーションイベントログへのイベントの書き込み**：Kaspersky Security 10.1 for Windows Server はソフトウェアコンポーネントの設定や、タスクの現在の状態、タスクの実行中に発生したイベント、Kaspersky Security 10.1 for Windows Server 管理に関連付けられたイベントなどの情報や、Kaspersky Security 10.1 for Windows Server におけるエラーの診断に必要な情報を記録します。
- **階層型ストレージ**：Kaspersky Security 10.1 for Windows Server は、階層型ストレージ管理モード（HSM システム）で実行できます。HSM システムにより、高速なローカルドライブと長期データ保管領域の低速なデバイスとの間で、データを再配置できます。
- **信頼ゾーン**：Kaspersky Security 10.1 for Windows Server がオンデマンドおよびリアルタイム保護タスクで適用する、保護またはスキャン範囲から除外する対象のリストを生成できます。
- **脆弱性攻撃ブロック**：プロセスにエージェントを注入するエクスプロイトから、プロセスメモリを保護できます。
- **ブロック対象コンピューター**：悪意のある動作が検知された場合、サーバーのネットワーク共有フォルダーにアクセスしようとするリモートコンピューターをブロックできます。

新機能

Kaspersky Security 10.1 for Windows Server は、企業サーバーとデータ保存システムを保護するソリューションです。保護範囲（Windows、データ保存システムを稼動しているサーバー）と一連の機能コンポーネントは、購入されたライセンスの種別によって異なります。

Kaspersky Security 10.1 for Windows Server は前バージョンのプログラム機能を改善および完全に維持しながら、同時に新しい保護コンポーネントが追加されました。

新しい Kaspersky Security 10.1 for Windows Server は次のメリットを提供します：

- 新たに追加されたトラフィックセキュリティコンポーネント（311 ページのセクション「トラフィックセキュリティ」を参照）：メール経由で送り込まれる脅威に加えて、HTTP または HTTPS トラフィック経由で送り込まれる Web の脅威からサーバーを保護できるようになりました。この新しいコンポーネントは次の保護シナリオをサポートします：
  - Kaspersky Security 10.1.0.622 を使用した、メールトラフィックのウイルス対策とフィッシング対策 Microsoft Outlook® アドイン（以降「Kaspersky Security 10.1 Microsoft Outlook アドイン」）
  - Web 対策トラフィックのウイルス対策とフィッシング対策
  - 悪意のある Web サイトアドレスのデータベースを使用したリンク検証
  - 悪意のある Web サイトアドレスのクラウドベースのデータベースを使用したリンク検証
  - リンクルールと認証ルールを使用したウェブコントロール
  - カテゴリに基づいた Web リソースコントロール
  - 接続時の Web サーバー認証の検証

トラフィックは、3 つの設定のうちの 1 つの ICAP サービスを使用して保護されます：

- 外部プロキシ：外部プロキシサーバーからリダイレクトされるトラフィックの分析（ネットワークドライバーなし）。
- リダイレクター：ターミナルセッションで起動するブラウザーからリダイレクトされるトラフィックの分析（ネットワークドライバーなし）。プログラムは内部システムプロキシを使用します。
- ドライバーインターセプター：ターミナルセッション内のネットワークドライバーを使用して、トラフィックがインターセプトされます。

- NetApp 用の新しいアンチクリプターコンポーネント：接続された NetApp ネットワーク接続トストレージを悪意ある暗号化から保護するため、Kaspersky Security 10.1 for Windows Server がインストールされたサーバーを使用できるようになりました。

『**Network Attached Storage Implementation Guide（英語）**』を参照してください。

- 新しいデバイスコントロールコンポーネント（381 ページのセクション「ネットワークコンピューターに接続された外部デバイスに関するシステムデータに基づくルール作成」を参照）：外部データストレージデバイス（USB および MTP 接続の大容量記憶デバイス、CD/DVD デバイス）とのファイル交換を許可またはブロックするためプログラムで使用されるルールリストを作成できるようになりました。

- 新しい脆弱性攻撃ブロックコンポーネント（298 ページのセクション「脆弱性攻撃ブロック」を参照）：衝撃を弱める技術を使用して、プロセスを脆弱性攻撃から保護する設定ができるようになりました。

- 新しいファイル変更監視コンポーネント（408 ページのセクション「ファイル変更監視」を参照）：整合性を監視するオブジェクトを提示できるようになりました。

- 新しい Windows イベントログ監視コンポーネント（420 ページのセクション「Windows イベントログ監視」を参照）：Windows イベントログの監査ルールの作成と、Windows イベントログに対してヒューリスティックアナライザーを使用する設定ができるようになりました。

- 外部の SIEM システムと統合する新しい機能（259 ページのセクション「SIEM 統合設定」を参照）：syslog プロトコルを使用して、外部のイベント集計システムへのアプリケーションログのエクスポートを設定できるようになりました。

- 保護対象デバイスへの USB 接続を追跡する新しい機能（377 ページのセクション「デバイスコントロールタスクについて」を参照）：各種デバイスによって行われる、保護対象コンピューターへの USB 接続に関わる通知を設定できるようになりました。

- セキュリティイベントログ（259 ページ）の実装：製品コンポーネントによってログに記録された、保護対象システムが危険にさらされている可能性を示すすべてのイベントを 1 つのログで表示できるようになりました。

- 新しいファイアウォール管理コンポーネント（389 ページのセクション「ファイアウォール管理」を参照）：Kaspersky Security 10.1 for Windows Server のグラフィカルユーザーインターフェイスを介して Windows ファイアウォールルールを管理できるようになりました。

- USB 大容量記憶デバイスをスキャンする新しい機能（243 ページのセクション「リムーバブルドライブスキャン」を参照）：保護対象コンピューターへの接続時に大容量記憶デバイスをスキャンできるようになり

ました。

- アプリケーション管理のパスワード保護を有効にする新しい機能（163 ページのセクション「Kaspersky Security 10.1 for Windows Server 機能へのパスワードで保護されたアクセス」を参照）：Kaspersky Security 10.1 for Windows Server の保護と、重要な操作へのアクセス制限を設けるためパスワードの使用が可能になりました。

- 信頼する配布パッケージからのアプリケーション起動開始を自動的に許可する新しい機能（360 ページのセクション「ソフトウェア配信管理の設定」を参照）：ソフトウェアのインストール時またはアップデート時のファイル起動プロセスを簡素化するため、アプリケーション起動コントロールタスクの設定で配布パッケージの除外を追加できるようになりました。

- Microsoft Windows Server 2016 コンテナーに対してウイルススキャンと保護を実行する新しい機能（269 ページのセクション「ファイルのリアルタイム保護タスクについて」を参照）が追加されました。

- 簡素化された信頼しないコンピューターのブロック（250 ページの「信頼しないコンピューターのブロック：ブロック対象コンピューター」を参照）：アンチクリプターとファイルのリアルタイム保護により、攻撃しているコンピューターの識別番号をブロック対象コンピューターの保管領域に追加できるようになりました。ブロック対象コンピューターの保管領域の追加は、保護タスク設定でオフにできます。ブロックされたすべてのコンピューターをまとめたリストは、管理サーバーのコンソールで確認することもできます。

- 信頼ゾーンに対して信頼するプロセスのルールのリストを生成するための最適化された機能（239 ページのセクション「信頼されたプロセスの追加」を参照）：チェックサム、パスのみ、またはパスとチェックサムの両方に基づいてプロセスを除外できるようになりました。

- アプリケーション起動コントロールルールの追加リストのメカニズム簡素化および展開（367 ページのセクション「全コンピューターに対する Kaspersky Security Center でのアプリケーション起動コントロールルールの作成について」を参照）：ローカルコンピューター上とポリシー内で設定されたルールリストを同時に使用する機能、および Kaspersky Security Center 内のタスクイベントに基づいてルールを生成する新しいメカニズムが新たに追加されました。

配布キット

配布キットには、次のことを実行できる開始アプリケーションが含まれます:

- Kaspersky Security 10.1 for Windows Server インストールウィザードの起動
- Kaspersky Security 10.1 コンソールのインストールウィザードの起動
- Kaspersky Security Center を介して本製品を管理するための Kaspersky Security 10.1 for Windows Server 管理プラグインをインストールするインストールウィザードの起動
- 『管理者用ガイド』をお読みください。
- 『ユーザーガイド』をお読みください。
- 『ネットワークストレージ保護導入ガイド』をお読みください。
- カスペルスキー Web サイトの Kaspersky Security 10.1 for Windows Server のページ（https://www.kaspersky.co.jp/business-security/windows-server-security）をご覧ください。
- テクニカルサポートサイト https://support.kaspersky.co.jp/にアクセスしてください。
- 最新バージョンの Kaspersky Security 10.1 for Windows Server に関する情報をお読みください。

フォルダー ¥client には、Kaspersky Security 10.1 コンソール（コンポーネントの「Kaspersky Security 10.1 for Windows Server 管理ツール」のセット）をインストールするためのファイルが含まれています。

フォルダー ¥server には、以下のファイルが含まれています:

- 32 ビット版または 64 ビット版の Microsoft Windows オペレーティングシステムが稼働しているコンピューター上に Kaspersky Security 10.1 for Windows Server のコンポーネントをインストールするためのファイル。

- Kaspersky Security Center によって Kaspersky Security 10.1 for Windows Server を管理するプラグインをインストールするためのファイル。
- 製品のリリース時点で最新の定義データベースのアーカイブファイル。
- 使用許諾契約書およびプライバシーのテキストが記載されたファイル。
- KSN 声明ファイル。

フォルダー ¥setup には、ファイル起動用の構成プログラムが含まれています。

フォルダー ¥email_plugin には、Kaspersky Security 10.1 Microsoft Outlook アドインのインストールパッケージが含まれています。

配布キットファイルは、使用目的によって異なるフォルダーに保存されています（下表を参照）。

表 2. Kaspersky Security 10.1 for Windows Server 配布キットファイル

ファイル	目的
autorun.inf	リムーバブルメディアからインストールする場合の Kaspersky Security 10.1 for Windows Server インストールウィザードの自動実行ファイル。
ks4ws_admin_guide_en.pdf	管理者用ガイド。
ks4ws_user_guide_en.pdf	ユーザーガイド。
release_notes.txt	このファイルにはリリース情報が含まれています。
setup.exe	ファイル起動用の構成プログラム（setup.hta の起動）。
¥client¥ks4wstools_x86(x64).msi	Windows Installer インストールパッケージ。Kaspersky Security 10.1 コンソールを保護対象サーバーにインストールします。

¥client¥setup.exe	コンポーネントの「管理ツール」のセット（Kaspersky Security コンソールを含む）用セットアップウィザードを起動するファイル。このセットアップウィザードで指定した設定を使用して、インストールパッケージファイル ks4wstools.msi を起動します。
¥server¥bases.cab	製品のリリース時点で最新の定義データベースのアーカイブファイル。
¥server¥setup.exe	保護対象のサーバーに Kaspersky Security 10.1 for Windows Server をインストールするためのウィザードを起動するファイル。このウィザードで指定されたインストールの設定を使用してインストーラーパッケージファイル ks4ws.msi を起動します。
¥server¥ks4ws_x86(x64).msi	Windows Installer インストールパッケージ。Kaspersky Security 10.1 for Windows Server を保護対象サーバーにインストールします。
¥server¥ks4ws.kpd	Kaspersky Security Center を経由した Kaspersky Security 10.1 for Windows Server のインストールパッケージのリモートインストールの説明が含まれる Kaspersky Unicode Definition フォーマット内のファイル。
¥server¥klcfginst.exe	Kaspersky Security 10.1 for Windows Server を Kaspersky Security Center 経由で管理するプラグイン用インストーラー。これを使用して Kaspersky Security 10.1 for Windows Server を管理する場合、Kaspersky Security Center の管理コンソールがインストールされた各サーバーに管理プラグインをインストールします。
¥server¥license.txt	使用許諾契約書およびプライバシーポリシーのテキスト。
¥server¥ksn.txt	KSN 声明のテキスト。

¥setup¥setup.hta	ファイル起動用の構成プログラム。
¥email_plugin¥ksmail_x86(x64).msi	Windows Installer インストールパッケージ。Kaspersky Security 10.1 Microsoft Outlook アドインを保護対象サーバーにインストールします。

配布キットファイルはインストール CD から実行できます。事前に配布パッケージファイルをローカルディスクにコピーしていた場合は、配布キットファイルの構造が維持されていることを確認してください。

システム要件

このセクションでは、Kaspersky Security 10.1 for Windows Server のシステム要件について説明します。

この章の内容

Kaspersky Security 10.1 for Windows Server を導入するサーバーの要件

Kaspersky Security 10.1 for Windows Server をインストールする前に、その他のアンチウイルス製品をサーバーからアンインストールする必要があります。

Kaspersky Security 10.1 for Windows Server は、Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition または Kaspersky Security 10 for Windows Server をアンインストールせずにインストールできます。

サーバーのハードウェア要件

一般要件:

- x86 - x64 互換のシングルコアまたはマルチコアシステム
- 空きディスク容量の要件:
  - すべてのアプリケーションコンポーネントのインストール:70 MB

- アプリケーションの定義データベースのダウンロードおよび保管：2 GB（推奨）
- ［隔離］および［バックアップ］へのオブジェクトの保管：400 MB（推奨）
- ログ保管：1 GB（推奨）

最小構成：

- プロセッサ：シングルコア 1.4 GHz
- RAM：1 GB
- ハードディスクサブシステム：空き容量 4 GB

推奨構成：

- プロセッサ：クアッドコア 2.4 GHz
- RAM：2 GB
- ハードディスクサブシステム：空き容量 4 GB

サーバーのソフトウェア要件

Kaspersky Security 10.1 for Windows Server は、32 ビット版または 64 ビット版の Microsoft Windows オペレーティングシステムが稼働しているサーバー上にインストールできます。

Kaspersky Security 10.1 for Windows Server をインストールして運用する場合、Microsoft Windows Installer 3.1 がサーバーにインストールされている必要があります。

Kaspersky Security 10.1 for Windows Server は、次のいずれかの 32 ビット版 Microsoft Windows オペレーティングシステムが稼働しているサーバー上にインストールできます：

- Windows Server® 2003 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 以降
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 以降

Kaspersky Security 10.1 for Windows Server は、次のいずれかの 64 ビット版 Microsoft Windows オペレーティングシステムが稼働しているサーバー上にインストールできます:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 以降
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 以降
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 以降
- Windows Hyper-V® Server 2008 R2 SP1 以降
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server
- Windows Server 2012 Core / Standard / Datacenter
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Core / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server

- Windows Server 2016 Core / Standard / Datacenter
- Windows Storage Server 2016
- Windows Hyper-V Server 2016

以下のオペレーティングシステムはすでに Microsoft Windows でサポートされていません：Windows Server 2003 Standard / Enterprise / Datacenter SP2、Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2（32 ビット / 64 ビット）。カスペルスキーでは、これらのオペレーティングシステムで稼働しているサーバーのテクニカルサポートが制限される場合があります。

Kaspersky Security 10.1 for Windows Server は、以下のターミナルサーバーにインストールできます：

- Windows Server 2008 ベースの Microsoft リモートデスクトップサービス
- Windows Server 2008 R2 ベースの Microsoft リモートデスクトップサービス
- Windows Server 2012 ベースの Microsoft リモートデスクトップサービス
- Windows Server 2012 R2 ベースの Microsoft リモートデスクトップサービス
- Windows Server 2016 ベースの Microsoft リモートデスクトップサービス
- Citrix XenApp 6.0、6.5、7.0、7.5 ～ 7.9、7.15
- Citrix XenDesktop 7.0、7.1、7.5 ～ 7.9、7.15

保護対象のネットワークストレージの要件

Kaspersky Security 10.1 for Windows Server は、次のネットワーク接続ストレージの保護に使用できます:

- NetApp(次のいずれかのオペレーティングシステムで使用):
  - 7 モードの Data ONTAP 7.x および Data ONTAP 8.x
  - クラスターモードの Data ONTAP 8.2.1 以降
- Dell™ EMC™ Celerra™ /VNX™(次のソフトウェアを搭載):
  - EMC DART 6.0.36 以降
  - Celerra(CAVA)Anti-Virus Agent 4.5.2.3 以降
- Dell EMC Isilon™(オペレーティングシステム OneFS™ 7.0 以降で使用)
- Hitachi NAS(次のプラットフォームのいずれかで使用):
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080
- IBM NAS シリーズ IBM System Storage N シリーズ
- Oracle® NAS Systems シリーズ Oracle ZFS Storage Appliance
- Dell Compellent™ FS8600 プラットフォーム上の Dell NAS

Kaspersky Security 10.1 コンソールをインストールするコンピューターの要件

コンピューターハードウェア要件

推奨される RAM 容量:128 MB 以上

空きディスク容量:30 MB

コンピューターのソフトウェア要件

Kaspersky Security 10.1 for Windows Server コンソールは、32 ビット版または 64 ビット版の Microsoft Windows オペレーティングシステムが稼働しているコンピューター上にインストールできます。

Kaspersky Security 10.1 コンソールのインストールおよび動作をサポートするために、Microsoft Windows Installer 3.1 がコンピューターにインストールされている必要があります。

Kaspersky Security 10.1 コンソールは、次のいずれかの 32 ビット版 Microsoft Windows オペレーティングシステムが稼働しているコンピューター上にインストールできます:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 以降
- Microsoft Windows XP Professional SP2 以降
- Microsoft Windows Vista® の各エディション
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Kaspersky Security 10.1 コンソールは、次のいずれかの 64 ビット版 Microsoft Windows オペレーティングシステムが稼働しているコンピューター上にインストールできます:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 以降
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 以降
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint™ Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server
- Windows Storage Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server
- Windows Storage Server 2016
- Microsoft Windows XP Professional Edition SP2 以降
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1

- Microsoft Windows 10

機能要件および制限事項

このセクションでは、Kaspersky Security 10.1 for Windows Server コンポーネントの追加の機能要件および既存の制限事項について説明します。

このセクションの内容

インストールとアンインストール

- Kaspersky Security 10.1 for Windows Server のインストールフォルダーの新しいパスに 150 以上の記号が含まれる場合、製品のインストール時に警告が表示されます。この警告はインストールプロセスには影響ありません。Kaspersky Security 10.1 for Windows Server は正常にインストールされ、稼働します。

- SNMP プロトコルサポートのインストールでは、SNMP サービスが実行中の場合、このサービスを再起動する必要があります。

- 組み込みオペレーティングシステムによって管理されているデバイス上に Kaspersky Security 10.1 for Windows Server をインストールして機能させるには、Filter Manager がインストールされている必要があります。

- Kaspersky Security 10.1 for Windows Server 管理ツールのインストールを、Microsoft Active Directory® グループポリシーから行うことはできません。
- 定期的なアップデートを受け取ることができない古いオペレーティングシステムで稼働しているコンピューターに製品をインストールする場合は、次のルート証明書を確認する必要があります：DigiCert Assured ID Root CA、DigiCert_High_Assurance_EV_Root_CA、DigiCertAssuredIDRootCA。指定された証明書がないと、製品が正しく機能しないことがあります。可能な方法で指定された証明書をインストールしてください。
- Kaspersky Security 10.1 コンソールをスタートメニューからアンインストールすることはできません。Kaspersky Security 10.1 コンソールは[**プログラムの追加と削除**]ウィンドウにあるリンクを使用してアンインストールできます。

トラフィックセキュリティ

- このコンポーネントは、Microsoft Windows Server 2008 R2 以降のオペレーティングシステムで稼働しているサーバーでのみ使用できます。
- 暗号化トークンを使用して Web 接続が行われた場合、トラフィックを検証することはできません。
- 保護範囲に VPN トラフィックを含めないでください（ポート 1723）。
- IPv6 形式の IP アドレスによる操作はできません。
- タスクの設定で[**証明書が無効の Web サーバーを信頼しない**]がオンになっている場合、本製品は自己署名証明書を無効と見なし、その接続をブロックします。
- 本製品が処理するのは、TCP パケットのみです。
- 脅威からのメールの保護では、送信メールトラフィックはスキャンされません。
- 管理サーバーのネットワークエージェントは、本製品への接続時にトラフィックセキュリティを検出するため、トラフィックセキュリティを導入する前に、管理プラグインをインストールしてください。管理プラグイン

をインストールする前に、トラフィックセキュリティをインストールしてタスクを開始した場合、トラフィックセキュリティタスクを再起動してください。

- トラフィックセキュリティは Yandex.Disk、Dropbox では機能しません。
- VPN 制限事項：Microsoft VPN 接続プロトコルを使用している場合、問題が発生する可能性があります。
- インストールが KSC からドライバーインターセプターモードで実行される場合、そのような接続種別は信頼できない証明書を使用するため、トラフィックセキュリティは MMC コンソールから Kaspersky Security Center サーバーへの接続をブロックします。
- コンポーネントは、たとえば sha1 証明書など、ルート証明書の生成に古い技術を使用するサイトへの接続をブロックします。
- [**次のサイズより大きいオブジェクトはスキャンしない（MB）**]は、100 MB 以下に指定する必要があります。インターネットの接続速度が遅い場合、大きな値を指定すると、容量の大きなファイルの受信時に問題が発生する可能性があります。推奨値は 20 MB です。
- 以下の条件を満たす場合、HTTPS 接続を危険と認識し、ブロックします：
  - タスクが**ドライバーインターセプター**モードで実行されている。
  - トラフィックが外部デバイスからリダイレクトされる。
  - トラフィックのリダイレクト元であるデバイスが、Kaspersky Security 10.1 for Windows Server によって保護され、設定済みのトラフィックセキュリティタスクが 1 回以上実行されたことがある。

外部コンピューターからリダイレクトされたトラフィックのチェックに**リダイレクター**モードを使用しないでください。前述の誤検知の他に、サーバーの負荷を増大させ、アプリケーションのパフォーマンスを低下させる可能性があります。

ファイル変更監視

既定では、システムフォルダーの変更やファイルシステムの状態監視ファイルの変更は、ファイル変更監視による監視の対象になっていません。オペレーティングシステムによって絶えず行われるファイル変更に関する情報が、タスクレポートに記録されないようにするためです。こうしたフォルダーを監視範囲に手動で含めることはできません。

監視範囲から除外されるフォルダーおよびファイルは、次の通りです:

- ファイル ID が 0 ～ 33 の NTFS の状態監視ファイル
- %SystemRoot%¥Prefetch¥
- %SystemRoot%¥ServiceProfiles¥LocalService¥AppData¥Local¥
- %SystemRoot%¥System32¥LogFiles¥Scm¥
- %SystemRoot%¥Microsoft.NET¥Framework¥v4.0.30319¥
- %SystemRoot%¥Microsoft.NET¥Framework64¥v4.0.30319¥
- %SystemRoot%¥Microsoft.NET¥
- %SystemRoot%¥System32¥config¥
- %SystemRoot%¥Temp¥
- %SystemRoot%¥ServiceProfiles¥LocalService¥
- %SystemRoot%¥System32¥winevt¥Logs¥
- %SystemRoot%¥System32¥wbem¥repository¥
- %SystemRoot%¥System32¥wbem¥Logs¥
- %ProgramData%¥Microsoft¥Windows¥WER¥ReportQueue¥
- %SystemRoot%¥SoftwareDistribution¥DataStore¥

- %SystemRoot%¥SoftwareDistribution¥DataStore¥Logs¥
- %ProgramData%¥Microsoft¥Windows¥AppRepository¥
- %ProgramData%¥Microsoft¥Search¥Data¥Applications¥Windows¥
- %SystemRoot%¥Logs¥SystemRestore¥
- %SystemRoot%¥System32¥Tasks¥Microsoft¥Windows¥TaskScheduler¥

最上位のフォルダーは除外されます。

ReFS または NTFS ファイルシステムをバイパスするファイル変更（BIOS、LiveCD などを使用したファイル変更）は監視の対象外となります。

ファイアウォール管理

- 適用されるルール範囲が 1 つのアドレスで構成されている場合、IPv6 形式の IP アドレスは使用できません。
- 設定済みのファイアウォールのポリシールールによって、ローカルコンピューターと管理サーバー間のやり取りの基本的なシナリオの実行が可能になります。Kaspersky Security Center の機能を十分に活用するには、ポートに対してルールを手動で設定する必要があります。ポート番号、プロトコル、機能に関する情報は、Kaspersky Security Center のナレッジベース（記事 ID：9297）を参照してください。
- 本製品のインストール時に、Windows ファイアウォールルールがタスク設定に追加されていない場合、ファイアウォール管理タスクで常時実行されている照会処理中に加えられるこれらのルールやルールグループの変更は、管理の対象外となります。ステータスを更新し、これらのルールを含めるには、ファイアウォール管理タスクを再起動する必要があります。
- Microsoft Windows Server ファミリーの 2008 以降のオペレーティングシステムでは、ファイアウォール管理をインストールする前に Windows ファイアウォールサービスを開始しておく必要があります（既定で起動されます）。

- ファイアウォール管理タスクを開始すると、オペレーティングシステムのファイアウォール設定から次の種別のルールが自動的に削除されます:
  - 拒否ルール
  - 送信トラフィックの監視ルール

その他の制限事項

オンデマンドスキャン、ファイルのリアルタイム保護:

- MTP 接続のデバイスのスキャンは使用できません。
- アーカイブのスキャンを実行する場合、SFX アーカイブをスキャン対象から外すことはできません。Kaspersky Security 10.1 for Windows Server の保護設定でアーカイブのスキャンを有効にすると、アーカイブ内および SFX アーカイブ内のオブジェクトが自動的にスキャンされます。通常のアーカイブをスキャンせずに、SFX アーカイブのみをスキャンすることは可能です。

コンピューターコントロールと診断:

- 保護対象のコンピューターが Microsoft Windows Server 2008 R2 以降のオペレーティングシステムで稼働している場合、デバイスコントロールタスクの保護範囲には、MTP 接続のデバイスが含まれます。
- ドメインコントローラー(アップデートがインストール済み)として Windows Server 2008 以降で稼働しているコンピューターの場合、Windows イベントログ監視タスクが検知する攻撃は、Kerberos 認証の脆弱性(MS14-068)を悪用した攻撃のみです。

ライセンス:

- ライセンス情報が SUBST コマンドで作成したディスクに保存されている場合、またはライセンス情報ファイルへのネットワークパスが指定されている場合、セットアップウィザードからライセンス情報を使用した製品のアクティベーションを行うことはできません。

アップデート:

- Kaspersky Security 10.1 for Windows Server の重要なモジュールのアップデートをインストールしたあと、製品のアイコンは既定で非表示になります。
- KLRAMDISK は、Windows XP または Windows 2003 オペレーティングシステムで稼働しているコンピューターではサポートされません。

インターフェイス:

- Kaspersky Security 10.1 コンソールを使用して、隔離、バックアップ、システム監査ログ、実行ログでフィルタリングを使用する場合、大文字と小文字を区別する必要があります。
- Kaspersky Security 10.1 コンソール で保護およびスキャンの範囲を設定する場合、1 つのパスに対して使用できるマスクは 1 つのみで、マスクを指定できる場所はパスの末尾のみです。正しいマスクの使用例:「C:¥Temp¥Temp*」、「C:¥Temp¥Temp???.doc」、「C:¥Temp¥Temp*.doc」。制限事項は信頼ゾーン設定には影響しません。

セキュリティ:

- オペレーティングシステムの設定でユーザーアカウント制御が有効な場合、タスクバーの通知領域にある製品のアイコンをダブルクリックして Kaspersky Security 10.1 コンソールが開くようにするには、ユーザーアカウントを KAVWSEE Administrators グループに追加する必要があります。その他の場合は、[製品情報]ウィンドウが開きます。
- ユーザーアカウント制御を有効にすると、Microsoft Windows の[プログラムと機能]ウィンドウから製品をアンインストールすることはできません。

Kaspersky Security Center との統合:

- 管理サーバーは、アップデートパッケージを受け取るときと、ネットワークコンピューターにアップデートを送信する前に、定義データベースのアップデートの有効性を確認します。管理サーバーは、取得したソフトウェアモジュールのアップデートの有効性を確認しません。

- ネットワークリストを利用して Kaspersky Security Center に動的に変更されたデータを送信するコンポーネントを使用する場合、管理サーバーとの対話設定で必要なチェックボックスがオンになっていることを確認してください（隔離、バックアップ）。

脆弱性攻撃ブロック:

- 現在の環境設定に apphelp.dll ライブラリが読み込まれていない場合、脆弱性攻撃ブロックは使用できません。
- 脆弱性攻撃ブロックは、Microsoft Windows 10 オペレーティングシステムで稼働しているコンピューターに実装されている Microsoft の EMET ユーティリティと競合します。EMET が実装されたコンピューターに脆弱性攻撃ブロックがインストールされている場合、Kaspersky Security 10.1 for Windows Server は EMET をブロックします。

NetApp のアンチクリプター:

- 新しいオペレーティングシステム ONTAP 9 以降で稼働しているの NAS で、FlexGroup コンテナーを使用している場合、アンチクリプターによる保護は提供されません。
- 7 モードでの NetApp ネットワーク接続ストレージで、ファイルに対する脅威を検知する機能は制限されます。
- NetApp のアンチクリプターは、クラスターモードでのみ使用できます。
- サーバーが使用できるネットワークインターフェイスと IP v4 アドレスは、それぞれ 1 つのみです。

ブロック対象コンピューターの保管領域：アンチクリプターまたはファイルのリアルタイム保護が有効になっている場合に、継続的に実行されます。

ICAP ネットワークストレージの保護：保護対象の保管領域のコンテンツの管理は、保管領域の設定によって異なります。たとえば、感染したオブジェクトが検知されても、保管領域の設定で許可されていなければ、これらのオブジェクトは削除されません。HP 3Par ストレージはアクセスブロックモードでのみ機能します。信頼ゾーンは使用できません。

RPC ネットワークストレージの保護：クラスターモードの場合は、Active Directory が必要です。

KSN の使用：Windows Vista 以前のオペレーティングシステムの場合、このコンポーネントでは、ウェブアンチウイルスおよびメールアンチウイルスの統計情報はサポートされません。

アプリケーションのインストールと削除

このセクションでは、Kaspersky Security 10.1 for Windows Server のインストールと削除について、段階的に説明します。

この章の内容

Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントと Windows インストーラーサービスで使用する各コンポーネントのコード

既定では、¥server¥ks4ws_x86(x64).msi ファイルを使用すると、すべての Kaspersky Security 10.1 for Windows Server コンポーネントをインストールします。スクリプト監視をインストールするには、カスタムインストールでインストール対象として追加します。

ファイル ¥client¥ks4wstools_x86(x64).msi により、すべてのソフトウェアコンポーネントが「管理ツール」セットからインストールされます。

次のセクションでは、Windows インストーラーサービスで使用する Kaspersky Security 10.1 for Windows Server コンポーネントのコードをリストにまとめています。これらのコードを使用して、コマンドラインから Kaspersky Security 10.1 for Windows Server をインストールする際に、インストールするコンポーネントのリストを定義することができます。

このセクションの内容

Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネント

Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントのコードとその説明を次の表に示します。

表 3. Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントについて

コンポーネント	コード	実行される機能
基本機能	core	製品の基本的な機能のセットが含まれており、それら機能を実行します。
アプリケーション起動コントロール	AppCtrl	ユーザーによるアプリケーションの実行の試行を監視し、設定されたアプリケーション起動コントロールルールに従ってアプリケーションの起動を許可または拒否します。 これは、アプリケーション起動コントロールタスクに実装されています。
デバイスコントロール	DevCtrl	このコンポーネントは、保護されたサーバーの USB 大容量記憶デバイスへの接続試行を追跡し、指定したデバイスコントロールルールに従ってこれらのデバイスの使用を許可または拒否します。 コンポーネントは、デバイスコントロールタスクに実装されます。
トラフィックセキュリティ	WebGW	このコンポーネントは Web トラフィックを処理し(メールサービス経由で受信するトライフィックを含む)、既知のコンピューターと保護対象サーバーのその他の脅威を検知するため、Web トラフィックを介して転送されるオブジェクトをインターセプトおよびスキャンします。

コンポーネント	コード	実行される機能
アンチウイルスによる保護	AVProtection	アンチウイルスによる保護を実行します。このコンポーネントには、次のコンポーネントが含まれます: • オンデマンドスキャン • ファイルのリアルタイム保護
オンデマンドスキャン	Ods	Kaspersky Security 10.1 for Windows Server システムファイルとオンデマンドスキャンタスク(要求に基づいた保護対象サーバーにあるオブジェクトのスキャン)をインストールします。 コマンドラインから Kaspersky Security 10.1 for Windows Server をインストールする際に、Core コンポーネントを指定せずに他の Kaspersky Security 10.1 for Windows Server コンポーネントを指定した場合、Core コンポーネントは自動でインストールされます。
ファイルのリアルタイム保護	Oas	保護対象サーバーにあるファイルにアクセスした際に、それらのファイルに対してアンチウイルススキャンを実行します。 このコンポーネントにより、ファイルのリアルタイム保護タスクが実装されます。
Kaspersky Security Network (KSN)の使用	KSN	カスペルスキーのクラウド技術を基に、保護を提供します。 このコンポーネントにより、KSN の使用タスクが実装されます(Kaspersky Security

コンポーネント	コード	実行される機能
		Network サービスへの要求の送信および同サービスからの判定の受信)。
ファイル変更監視	Fim	このコンポーネントは、指定された監視範囲にあるファイル上で実行された操作を記録します。 このコンポーネントにより、ファイル変更監視タスクが実装されます。
脆弱性攻撃ブロック	AntiExploit	このコンポーネントは、保護されたサーバーのメモリにあるプロセスが使用するメモリを保護する設定の管理を可能にします。
ファイアウォール管理	ファイアウォール	このコンポーネントは、Kaspersky Security 10.1 for Windows Server のグラフィカルユーザーインターフェイスを介したWindows ファイアウォールの管理を可能にします。 このコンポーネントにより、ファイアウォール管理タスクが実装されます。

コンポーネント	コード	実行される機能
Kaspersky Security Center ネットワークエージェントとの統合モジュール	AKIntegration	Kaspersky Security 10.1 for Windows Server と Kaspersky Security Center ネットワークエージェント間の接続と提供します。 Kaspersky Security Center を使用して製品を管理する場合、保護対象サーバーにこのコンポーネントをインストールできます。
Windows イベントログ監視	LogInspector	このコンポーネントは、Windows イベントログの検査の結果に基づいて、保護された環境の整合性を監視します。
RPC ネットワークストレージの保護	RPCProt	このコンポーネントは、ファイル交換によってサーバーに侵入するウイルスなどのコンピューターセキュリティの脅威から RPC ネットワークストレージ（NetApp ネットワーク接続ストレージなど）を保護します。
ICAP ネットワークストレージの保護	ICAPProt	このコンポーネントは、ファイル交換によってサーバーに侵入するウイルスなどのセキュリティの脅威から ICAP ネットワークストレージ（EMC Isilon など）を保護します。

コンポーネント	コード	実行される機能
NetApp のアンチクリプター	AntiCryptorNAS	このコンポーネントは、ネットワーク接続ストレージのフォルダーに対して暗号化保護を提供します。悪意のある暗号化が検知された場合、Kaspersky Security 10.1 for Windows Server は保護対象のネットワーク接続ストレージのフォルダーに対するアクセスをブロックします。
「システム監視」パフォーマンスカウンターのセット	PerfMonCounters	一連のシステム監視用パフォーマンスカウンターがインストールされます。Kaspersky Security 10.1 for Windows Server をその他のプログラムと一緒に使用する際、パフォーマンスカウンターにより、Kaspersky Security 10.1 for Windows Server のパフォーマンスが測定され、コンピューターの潜在的なボトルネックが特定されます。
SNMP カウンターと SNMP トラップ	SnmpSupport	Microsoft Windows の Simple Network Management Protocol（SNMP）から、Kaspersky Security 10.1 for Windows Server のカウンターとトラップを公開します。このコンポーネントは、Microsoft SNMP が保護されたサーバーにインストールされている場合にのみ、そのサーバーにインストールできます。

コンポーネント	コード	実行される機能
通知領域内の Kaspersky Security 10.1 for Windows Server アイコン	TrayApp	保護対象のサーバーのタスクトレイの通知領域に Kaspersky Security 10.1 for Windows Server アイコンを表示します。Kaspersky Security 10.1 for Windows Server アイコンは、コンピューターのファイル保護のステータスを示します。また、このアイコンを使用して、MMC の Kaspersky Security 10.1 コンソール（インストールされている場合）と、[製品情報]ウィンドウを開くことができます。
コマンドラインユーティリティ	Shell	保護対象サーバーのコマンドラインから Kaspersky Security 10.1 for Windows Server を管理できるようになります。

ソフトウェアコンポーネントの「管理ツール」セット

ソフトウェアコンポーネントの「管理ツール」セットのコードとその説明を次の表に示します。

表 4.　「管理ツール」ソフトウェアコンポーネントの説明

コンポーネント	コード	コンポーネントの機能
Kaspersky Security 10.1 for Windows Server スナップイン	MmcSnapin	Kaspersky Security 10.1 コンソールから Microsoft 管理コンソールをインストールします。 コマンドラインから「管理ツール」をインストールするときに、MmcSnapin コンポーネントを指定せずに他のコンポーネントを指定した場合、MmcSnapin コンポーネントは自動でインストールされます。
Help	Help	Kaspersky Security 10.1 for Windows Server 管理ツールファイルと同じフォルダーに保存される CHM ヘルプファイルです。ヘルプファイルは、[**スタート**]メニューを使用するか、Kaspersky Security Console 10.1 ウィンドウが表示された状態で **F1** キーを押して開くことができます。
ガイド	Docs	Kaspersky Security 10.1 for Windows Server では、『Implementation Guide for Network Attached Storage Protection（英語）』、『管理者用ガイド』、および『ユーザーガイド』が、保護されたサーバーに PDF 形式で保存されています。ガイドはすべて、[**スタート**]メニューから開けます。

Kaspersky Security 10.1 for Windows Server インストール後のシステム変更

Kaspersky Security 10.1 for Windows Server と Kaspersky Security 10.1 コンソール（「管理ツール」のセッ

ト）が一緒にインストールされると、Windows インストーラーサービスにより、次の変更がサーバーに加えられます：

- 保護対象サーバーおよび Kaspersky Security 10.1 コンソールがインストールされているサーバーでの Kaspersky Security 10.1 for Windows Server フォルダーの作成
- Kaspersky Security 10.1 for Windows Server サービスの登録
- Kaspersky Security 10.1 for Windows Server ユーザーグループの作成
- Kaspersky Security 10.1 for Windows Server キーのシステムレジスタ内での登録

以下の表に、これらの変更点を示します。

Kaspersky Security 10.1 for Windows Server フォルダー

表 5. 保護対象サーバー上の Kaspersky Security 10.1 for Windows Server フォルダー

フォルダー	Kaspersky Security 10.1 for Windows Server ファイル
フォルダー %Kaspersky Security 10.1 for Windows Server%（既定）: Microsoft Windows 32 ビット版 – %ProgramFiles%¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Server¥ Microsoft Windows 64 ビット版 - %ProgramFiles(x86)%¥Kaspersky Security 10.1 for Windows Server¥	Kaspersky Security 10.1 for Windows Server 実行ファイル（インストール中に指定された宛先フォルダー）
%Kaspersky Security 10.1 for Windows Server%¥mibs フォルダー	管理情報ベース（MIB）ファイル。SMNP プロトコルを使用して Kaspersky Security 10.1 for Windows Server により公開されるカウンターとフックが含まれます。
%Kaspersky Security 10.1 for Windows Server%¥x64 フォルダー	64 ビット版の Kaspersky Security 10.1 for Windows Server の実行ファイル（フォルダーは、64 ビット版の Microsoft Windows に Kaspersky Security 10.1 for Windows Server がインストールされるときにのみ作成されます）。

フォルダー	Kaspersky Security 10.1 for Windows Server ファイル
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Data¥ %ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Settings¥ %ALLUSERSPROFILE%¥Application Data¥Kaspersky Security 10.1 for Windows Server¥Dskm¥	Kaspersky Security 10.1 for Windows Server サービスファイル

フォルダー	Kaspersky Security 10.1 for Windows Server ファイル
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Update¥	アップデート元設定のファイル
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Update¥Distribution¥	アップデートのコピータスクを使用してダウンロードされた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（フォルダーは、初めてアップデートのコピータスクを使用してアップデートがダウンロードされたときに作成されます）
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Reports¥	実行ログとシステム監査ログ
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Bases¥Current¥	現在使用されている定義データベースのセット
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Bases¥Backup¥	定義データベースのバックアップコピー。定義データベースがアップデートされるたびに上書きされます。
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Bases¥Temp¥	アップデートタスクの実行時に作成される一時的なファイル
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Quarantine¥	隔離されたオブジェクト（既定のフォルダー）
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Backup¥	バックアップされたフォルダー（既定のフォルダー）

フォルダー	Kaspersky Security 10.1 for Windows Server ファイル
%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Restored¥	バックアップおよび隔離から復元されたオブジェクト（復元されたオブジェクトの既定のフォルダー）

表 6. Kaspersky Security 10.1 コンソールのインストール時に作成されるフォルダー

フォルダー	Kaspersky Security 10.1 for Windows Server ファイル
フォルダー %Kaspersky Security 10.1 for Windows Server%（既定）: • Microsoft Windows 32 ビット版 – %ProgramFiles%¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Server¥ Microsoft Windows 64 ビット版 - %ProgramFiles(x86)%¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Server¥	「管理ツール」ファイル（保存先フォルダーは Kaspersky Security 10.1 コンソールのインストール時に指定）。

Kaspersky Security 10.1 for Windows Server サービス

Kaspersky Security 10.1 for Windows Server サービスでは、ローカルシステム（SYSTEM）アカウントを使用します。

表 7. Kaspersky Security 10.1 for Windows Server サービス

サービス	目的
Kaspersky Security サービス(KAVFS)サービス	Kaspersky Security 10.1 for Windows Server タスクとワークフローを管理する、重要な Kaspersky Security 10.1 for Windows Server サービス
Kaspersky Security 管理サービス(KAVFSGT)	Kaspersky Security 10.1 コンソールを介した Kaspersky Security 10.1 for Windows Server のアプリケーション管理を対象としたサービス。
Kaspersky Security ブローカーサービス (KAVFSWH)	セキュリティ設定を外部セキュリティエージェントに送信し、セキュリティイベントについてのデータを受信する通信を仲介するサービス。
Kaspersky Security スクリプトチェッカー (KAVFSSCS)	このサービスはスクリプト監視タスクと一緒に開始され、Microsoft Windows スクリプトテクノロジーを使用して作成されたスクリプトの実行を制御できます。

Kaspersky Security 10.1 for Windows Server グループ

表 8. Kaspersky Security 10.1 for Windows Server グループ

グループ	目的
KAVWSEE Administrators	保護対象サーバー上のグループで、グループのユーザーには、Kaspersky Security Windows Server 管理サービスと Kaspersky Security 10.1 for Windows Server の全機能にアクセスできる権限があります。

システムレジストリキー

表 9.　システムレジストリキー

ライセンス	目的
[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥KAVFS]	Kaspersky Security 10.1 for Windows Server サービスプロパティ。
[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Kaspersky Security]	Kaspersky Security 10.1 for Windows Server イベントログ設定（Kaspersky Event Log）。
[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥KAVFSGT]	Kaspersky Security 10.1 for Windows Server 管理サービスプロパティ。
Microsoft Windows 32 ビット版: [HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Kaspersky Security¥Performance] Microsoft Windows 64 ビット版: [HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Kaspersky Security x64¥Performance]	パフォーマンスカウンターの設定
Microsoft Windows 32 ビット版: [HKEY_LOCAL_MACHINE¥SOFTWARE¥KasperskyLab¥WSEE¥10.1¥SnmpAgent] Microsoft Windows 64 ビット版: [HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥KasperskyLab¥WSEE¥10.1¥SnmpAgent]	SNMP プロトコルサポートの設定
Microsoft Windows 32 ビット版: HKEY_LOCAL_MACHINE¥SOFTWARE¥KasperskyLab¥WSEE¥10.1	ダンプファイル書き込み設定。

¥CrashDump¥ Microsoft Windows 64 ビット版: HKEY_LOCAL_MACHINE¥Software¥Wow6432Node¥KasperskyLab¥WSEE¥10.1¥CrashDump¥	
Microsoft Windows 32 ビット版: HKEY_LOCAL_MACHINE¥Software¥KasperskyLab¥WSEE¥10.1¥Trace¥ Microsoft Windows 64 ビット版: HKEY_LOCAL_MACHINE¥Software¥Wow6432Node¥KasperskyLab¥WSEE¥10.1¥Trace¥	トレースログの設定
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥KasperskyLab¥WSEE¥10.1¥Environment]	製品のタスクと機能の設定

Kaspersky Security 10.1 for Windows Server プロセス

Kaspersky Security 10.1 for Windows Server が下表に記載されたプロセスを開始します。

表 10. Kaspersky Security 10.1 for Windows Server プロセス

ファイル名	目的
kavfswp.exe	Kaspersky Security 10.1 for Windows Server ワークフロー。
kavtray.exe	Kaspersky Security 10.1 for Windows Server タスクバーアイコンのプロセス。
kavshell.exe	コマンドラインユーティリティのプロセス

ファイル名	目的
kavfsrcn.exe	Kaspersky Security 10.1 for Windows Server リモート管理プロセス
kavfs.exe	Kaspersky Security のサービスプロセス
kavfsgt.exe	Kaspersky Security 管理サービスプロセス
kavfswh.exe	Kaspersky Security ブローカーコンピューターサービス外部制御プロセス
kavfsscs.exe	Kaspersky Security スクリプトチェッカーサービス

インストールおよびアンインストールの設定と Windows インストーラーサービスで使用するコマンドラインオプション

次の表では、Kaspersky Security 10.1 for Windows Server をインストールおよびアンインストールするための設定と、各設定の既定値、インストールの設定値を変更するためのキーと、設定可能な値について説明します。これらのキーは、コマンドラインから Kaspersky Security 10.1 for Windows Server をインストールするときに Windows インストーラーサービスのコマンド msiexec で使用する標準のキーと一緒に使用できます。

表 11. インストールのパラメータと Windows インストーラーでのコマンドラインオプション

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
使用許諾契約書の条件に同意	使用許諾契約書の条件を拒否	EULA=<値> 0 - 使用許諾契約書の条件を拒否する。 1 - 使用許諾契約書の条件に同意する。	Kaspersky Security 10.1 for Windows Server をインストールするには、使用許諾契約書の条件に同意する必要があります。
プライバシーポリシーの条項に同意	プライバシーポリシーの条項を拒否	PRIVACYPOLICY=<値> 0 – プライバシーポリシーの条項を拒否します。 1 – プライバシーポリシーの条項に同意します。	Kaspersky Security 10.1 for Windows Server をインストールするには、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。

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
インストール先フォルダー	Kaspersky Security 10.1 for Windows Server：%Program Files%¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Server 管理ツール：%ProgramFiles%¥Kaspersky Lab¥ Kaspersky Security 10.1 for Windows Server Admins Tools Microsoft Windows 64 ビット版：%ProgramFiles(x86)%	INSTALLDIR=<フォルダーの完全パス>	インストールのときに Kaspersky Security 10.1 for Windows Server のファイルが保存されるフォルダー。 別のフォルダーも指定できます。
Kaspersky Security 10.1 for Windows Server の開始時にリアルタイム保護タスクを起動（**製品インストール後にリアルタイム保護を有効にする**）	開始する	RUNRTP=<値> 1 - 開始する 0 - 開始しない	Kaspersky Security 10.1 for Windows Server の起動時にファイルのリアルタイム保護とスクリプト監視を開始する場合は、この設定をオンにします（推奨）。

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
Microsoft Corporation が推奨するファイルとしてスキャンから除外（**Microsoft によって推奨されているファイルを除外リストに追加する**）	除外する	ADDMSEXCLUSION=<値> 1 – 除外する 0 – 除外しない	ファイルのリアルタイム保護タスクで、Microsoft Corporation によって除外が推奨されているオブジェクトを、サーバーの保護範囲から除外します。 サーバーにある一部のアプリケーションによって使用されているファイルが、アンチウイルス製品によってインターセプトまたは変更されると、これらのアプリケーションが不安定になる場合があります。たとえば、Microsoft Corporation は、一部のドメインコントローラアプリケーションをそのようなオブジェクトのリストに含めています。

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
Kaspersky Lab の推奨事項に従ってスキャン範囲から除外されるオブジェクト（**Kaspersky Lab によって推奨されているファイルを除外リストに追加する**）	除外する	ADDKLEXCLUSION=<値> 1 – 除外する 0 – 除外しない	ファイルのリアルタイム保護タスクで、Kaspersky Lab によって除外が推奨されているオブジェクトを、サーバーの保護範囲から除外します。
Kaspersky Security 10.1 コンソールへのリモート接続を許可する	拒否	ALLOWREMOTECON=<値> 1 - 許可 0 - 拒否	既定では、保護対象サーバーにインストールされた Kaspersky Security 10.1 コンソールへはリモート接続できません。インストール時に接続を許可できます。Kaspersky Security 10.1 for Windows Server は、すべてのポートについて、TCP プロトコルを使用してプロセス kavfsgt.exe の許可ルールを作成します。

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
ライセンス情報ファイルのパス（**ライセンスキー**）	配布キットのディレクトリ server	LICENSEKEYPATH=<ライセンス情報ファイル名>	既定では、配布キットの ¥server フォルダーにある、拡張子が .key のファイルをインストーラーが探そうとします。 ¥server フォルダーに複数のライセンス情報ファイルがある場合、有効期限が最も先のライセンス情報ファイルが、インストーラーに選ばれます。 ライセンス情報ファイルはあらかじめフォルダー server に保存できます。また［**ライセンス情報ファイルの追加**］設定を使用して、別のパスをライセンス情報ファイルに指定して保存することもできます。 Kaspersky Security 10.1 for Windows Server がインストールされた後、Kaspersky Security 10.1 コンソールなどの管理ツールを使用してライセンスを追加できます。製品のインストール時にライセンスを追加しない場合、Kaspersky Security 10.1 for Windows Server は機能しません。

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
設定ファイルのパス	指定されていません	CONFIGPATH=<設定ファイルの名前>	Kaspersky Security 10.1 for Windows Server は、製品に作成された指定の設定ファイルから各設定をインポートします。 タスクの起動に使用するアカウントのパスワードやプロキシサーバーに接続するためのパスワードなどのパスワードは、設定ファイルからインポートされません。設定のインポートが完了すると、すべてのパスワードを手動で入力する必要があります。 設定ファイルを指定しない場合、セットアップの完了後、既定の設定が使用されます。
コンソールに対するネットワーク接続の有効	無効	ADDWFEXCLUSION=<値> **1** - 許可 **0** – 拒否	別のサーバーに Kaspersky Security 10.1 for Windows Server をインストールするにはこのオプションを使用します。Kaspersky Security 10.1 コンソールがインストールされた別のデバイスからサーバー保護をリモート管理できます。 Microsoft Windows ファイア

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
			ウォールでポート 135（TCP）が開き、Kaspersky Security 10.1 for Windows Server のリモート管理の実行ファイル kavfsrcn.exe に対してネットワーク接続が許可されます。また、DCOM アプリケーションへのアクセス権が付与されます。 サーバーが Microsoft Windows Server 2008 で動作している場合、インストールが完了したらユーザーを KAVWSEE 管理者グループに追加して、リモートからのアプリケーション管理と、サーバーの Kaspersky Security 管理サービス（kavfsgt.exe ファイル）へのネットワーク接続を許可します。 別のコンピューターに Kaspersky Security 10.1 コンソールをインストールした場合の追加設定については詳細情報が用意されています（89 ページのセクション

設定	既定値	Windows インストーラーのコマンドラインオプションと使用できる値	説明
			「Kaspersky Security 10.1 コンソールを別のコンピューターにインストールした後の詳細設定」を参照）。
非互換ソフトウェアのチェックの無効化	チェックを実行する	SKIPINCOMPATIBLESW = <値> 0 - 非互換ソフトウェアのチェックを実行する 1 - 非互換ソフトウェアのチェックを実行しない	この設定を使用すると、デバイスへのアプリケーションのバックグラウンドインストール時に非互換ソフトウェアのチェックを有効化または無効化できます。 Kaspersky Security 10.1 for Windows Server のインストール時には、アプリケーションの他のバージョンがデバイスにインストールされている場合、この設定の値に関係なく常に警告します。

表 12. Windows インストーラーのアンインストール設定とコマンドラインオプション

設定	既定値	説明、Windows インストーラーのコマンドラインオプション、および使用できる値
隔離されたオブジェクトの復元	削除	RESTOREQTN =<値> **0** – 隔離されたコンテンツを削除する。 **1** – 隔離されたコンテンツをパラメータ RESTOREPATH で指定したフォルダーに復元する。
バックアップのコンテンツの復元	削除	RESTOREBCK =<値> **0** – バックアップされたコンテンツを削除する。 **1** – バックアップされたコンテンツをパラメータ RESTOREPATH で指定したフォルダーに復元する。
現在のパスワードの入力による削除の確認（パスワード保護が有効の場合）	指定されていません	UNLOCK_PASSWORD=<指定されたパスワード>

設定	既定値	説明、Windows インストーラーのコマンドラインオプション、および使用できる値
復元されたオブジェクトのフォルダー	%ALLUSERSPROFILE%¥Application Data¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Restored	RESTOREPATH=<フォルダーの完全パス> 復元したオブジェクトは、この設定で指定されるフォルダーに保存されます: 隔離のオブジェクトの保存先 - サブフォルダー Quarantine。 バックアップのオブジェクトの保存先 - サブフォルダー Backup。

Kaspersky Security 10.1 for Windows Server のインストールログとアンインストールログ

インストール(アンインストール)ウィザードを使用して Kaspersky Security 10.1 for Windows Server をインストールまたはアンインストールした場合、Windows インストーラーサービスによってインストール(アンインストール)のログが作成されます。ログファイル ks4ws_v10.1_install_<UID>.log(<UID> - 6 文字からなる一意のログ識別子)が、ファイル setup.exe を起動したアカウントのユーザーのフォルダー %temp% に保存されます。

Kaspersky Security 10.1 for Windows Server がコマンドラインからインストールまたはアンインストールされた場合、既定では、インストールファイルのログは作成されません。

► **Kaspersky Security 10.1 for Windows Server のインストールの際にドライブ C:¥ にログファイル ks4ws.log を作成するには:**

- `msiexec /i ks4ws_x86.msi /l*v C:¥log.txt /qn EULA=1`
- `msiexec /i ks4ws_x64.msi /l*v C:¥log.txt /qn EULA=1`

インストールの計画

このセクションでは、Kaspersky Security 10.1 for Windows Server 管理ツールセットの説明と、ウィザード（81 ページのセクション「ウィザードを使用した製品のインストールとアンインストール」を参照）、コマンドライン（103 ページのセクション「コマンドラインによる製品のインストールとアンインストール」を参照）、Kaspersky Security Center（111 ページのセクション「Kaspersky Security Center を使用した製品のインストールとアンインストール」を参照）、および Active Directory® グループポリシーを介した Kaspersky Security 10.1 for Windows Server インストールおよびアンインストール（119 ページのセクション「Active Directory のグループポリシーを使用したインストールとアンインストール」を参照）の特殊事情について説明します。

Kaspersky Security 10.1 for Windows Server のインストールを開始する前に、インストールの主要な段階について計画しましょう。

1. Kaspersky Security 10.1 for Windows Server の管理と設定に使用する管理ツールを決定します。
2. インストールに必要な製品コンポーネントを選択します（50 ページのセクション「Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントと Windows インストーラーサービスで使用する各コンポーネントのコード」を参照）。
3. インストール方法を選択します。

このセクションの内容

管理ツールの選択

Kaspersky Security 10.1 for Windows Server の設定および管理に使用する管理ツールを決定します。

Kaspersky Security 10.1 for Windows Server の管理には、Kaspersky Security 10.1 コンソール、コマンドラインユーティリティ、Kaspersky Security Center 管理コンソールが使用できます。

Kaspersky Security 10.1 コンソール

Kaspersky Security 10.1 コンソールは、Microsoft 管理コンソールに追加される独立したスナップインです。Kaspersky Security 10.1 for Windows Server は、企業ネットワーク上の保護対象サーバーやその他のコンピューターにインストールされた Kaspersky Security 10.1 コンソール経由で管理できます。

複数の Kaspersky Security 10.1 for Windows Server スナップインを、権限モードで開かれた 1 つの Microsoft 管理コンソールに追加できます。これにより、Microsoft 管理コンソールを使用して、Kaspersky Security 10.1 for Windows Server がインストールされている複数のサーバーに対する保護を管理できます。

Kaspersky Security 10.1 コンソールは、「管理ツール」製品コンポーネントセットに含まれます。

コマンドラインユーティリティ

保護対象サーバーのコマンドラインを使用して Kaspersky Security 10.1 for Windows Server を管理できます。

コマンドラインユーティリティは、Kaspersky Security 10.1 for Windows Server のソフトウェアコンポーネントグループに含まれます。

Kaspersky Security Center

Kaspersky Security Center アプリケーションを使用してアンチウイルスによるコンピューターの保護を一元管理している場合、Kaspersky Security Center 管理コンソールを使用して Kaspersky Security 10.1 for Windows Server を管理できます。

次のコンポーネントがインストールされます:

- **Kaspersky Security Center ネットワークエージェントとの統合モジュール**：Kaspersky Security 10.1 for Windows Server のソフトウェアコンポーネントグループに含まれます。Kaspersky Security 10.1 for Windows Server とネットワークエージェントとの通信を確実にします。Kaspersky Security Center ネットワークエージェントとの統合モジュールは保護対象サーバーにインストールします。
- **Kaspersky Security Center ネットワークエージェント**：各保護対象サーバーにインストールします。このコンポーネントでは、サーバーにインストールされている Kaspersky Security 10.1 for Windows Server と Kaspersky Security Center 管理コンソールのやり取りがサポートされます。ネットワークエージェントのインストールファイルは、Kaspersky Security Center の配布キットフォルダーに含まれます。
- **Kaspersky Security 10.1 for Windows Server プラグイン**：管理コンソールを使用して、Kaspersky Security Center の管理サーバーがインストールされているコンピューターに Kaspersky Security 10.1 for Windows Server の管理プラグインをインストールすることもできます。これで、Kaspersky Security Center を通した、アプリケーションの管理インターフェイスの利用が可能になります。プラグインインストールファイル server¥klcfginst.exe は、Kaspersky Security 10.1 for Windows Server の配布キットに含まれます。

インストール方法の選択

Kaspersky Security 10.1 for Windows Server でインストールするソフトウェアコンポーネントを指定したら（50 ページのセクション「Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントと Windows インストーラーサービスで使用する各コンポーネントのコード」を参照）、製品のインストール方法を選択する必要があります。

ネットワークアーキテクチャと次の条件に従って、インストール方法を選択します：

- 特別な Kaspersky Security 10.1 for Windows Server インストール設定が必要なのか、それとも推奨のインストール設定が使用されるのか（66 ページのセクション「インストールおよびアンインストールの設定と Windows インストーラーサービスで使用するコマンドラインオプション」を参照）。
- すべてのサーバーに対して同じインストール設定を使用するか、各サーバーによって異なるインストール設定を使用するか。

Kaspersky Security 10.1 for Windows Server は、セットアップウィザードを使用してインタラクティブに、または

サイレントモードでユーザーの介在なしでインストールできます。また、コマンドラインからセットアップ設定を指定してインストールパッケージファイルを実行し、起動することもできます。Active Directory のグループポリシーまたは Kaspersky Security Center のリモートインストールタスクを使用すると、Kaspersky Security 10.1 for Windows Server を一元的にリモートでインストールできます。

Kaspersky Security 10.1 for Windows Server を 1 つのサーバーにインストールし、運用のための設定をした後、設定を設定ファイルに保存したら、Kaspersky Security 10.1 for Windows Server を他のサーバーにインストールする際にその設定ファイルを使用できます（Active Directory のグループポリシーを使用して製品をインストールした場合は使用できません）。

セットアップウィザードの起動

セットアップウィザードでは次の操作を実行できます：

- 配布キットに含まれる ¥server¥setup.exe ファイルからの保護対象サーバーの Kaspersky Security コンポーネント（50 ページのセクション「Kaspersky Security 10.1 for Windows Server のソフトウェアコンポーネント」を参照）。
- 保護対象サーバーまたは別の LAN コンピューターの配布キットの ¥client¥setup.exe ファイルからの Kaspersky Security 10.1 コンソール（87 ページのセクション「Kaspersky Security 10.1 コンソールのインストール」を参照）。

コマンドラインで必要なインストール設定を指定してインストールパッケージファイルを実行する

コマンドラインオプションを設定せずにインストールパッケージファイルを開始した場合、Kaspersky Security 10.1 for Windows Server は既定の設定でインストールされます。Kaspersky Security 10.1 for Windows Server のオプションを使用してインストールの設定を変更できます。

Kaspersky Security 10.1 コンソールは、保護対象サーバーまたは管理者のワークステーションにインストールできます。

Kaspersky Security 10.1 for Windows Server および Kaspersky Security コンソールのインストールのためのサンプルコマンドは、セクション「コマンドラインによる製品のインストールとアンインストール」にあります（103 ページのセクション「コマンドラインによる製品のインストールとアンインストール」を参照）。

Kaspersky Security Center による一括インストール

お使いのネットワークで Kaspersky Security Center を使用してアンチウイルスによるネットワークコンピューターの保護を管理している場合、Kaspersky Security Center のリモートインストールタスクを使用して複数のサーバーに Kaspersky Security 10.1 for Windows Server をインストールできます。

Kaspersky Security Center を使用して Kaspersky Security 10.1 for Windows Server をインストールする場合（111 ページのセクション「Kaspersky Security Center を使用した製品のインストールとアンインストール」を参照）、インストール先となるサーバーは、Kaspersky Security Center と同じドメインに存在していても異なるドメインに存在していてもかまいません。また、属するドメインがなくてもかまいません。

Active Directory のグループポリシーによる一括インストール

Active Directory のグループポリシーを使用して、保護対象サーバーに Kaspersky Security 10.1 for Windows Server をインストールできます。Kaspersky Security 10.1 コンソールは、保護対象サーバーまたは管理者のワークステーションにインストールできます。

Active Directory のグループポリシーを使用して Kaspersky Security 10.1 for Windows Server をインストールする場合、推奨されているインストール設定でしかインストールできません。

Active Directory グループポリシーを使用して Kaspersky Security 10.1 for Windows Server をインストールするサーバーは（119 ページのセクション「Active Directory のグループポリシーを使用したインストールとアンインストール」を参照）、同じドメインおよび同じ組織単位に存在している必要があります。コンピューターの起動時、Microsoft Windows にログインする前にインストールが実行されます。

ウィザードを使用した製品のインストールとアンインストール

このセクションでは、インストールウィザードによる Kaspersky Security 10.1 for Windows Server および Kaspersky Security 10.1 コンソールのインストールおよびアンインストールプロセスと、Kaspersky Security

10.1 for Windows Server の追加の設定に関する情報、およびインストール時に実行される処理について説明します。

このセクションの内容

セットアップウィザードを使用したインストール

このセクションでは、Kaspersky Security 10.1 for Windows Server と Kaspersky Security 10.1 コンソールのインストールの情報について説明します。

► **Kaspersky Security 10.1 for Windows Server をインストールして使用するには、次の手順を実行します:**

2. Kaspersky Security 10.1 for Windows Server を保護対象サーバーにインストールします。
3. Kaspersky Security 10.1 コンソールは、Kaspersky Security 10.1 for Windows Server を管理する予定のコンピューターにインストールしてください。
4. Kaspersky Security 10.1 コンソールがネットワーク上の(保護対象サーバー以外の)いずれかのコンピューターにインストールされている場合、コンソールユーザーが Kaspersky Security 10.1 for Windows Server をリモート管理できるようにするには、追加調整を実行してください。
5. Kaspersky Security 10.1 for Windows Server インストール後に、処理を実行します。

このセクションの内容

Kaspersky Security 10.1 for Windows Server のインストール

Kaspersky Security 10.1 for Windows Server インストール前に、次の手順を行います:

- サーバーに他のアンチウイルス製品がインストールされていないことを確認します。Kaspersky Security 10.1 for Windows Server は、Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition または Kaspersky Security 10 for Windows Server を削除しないでインストールできます。
- セットアップウィザードの起動に使用するアカウントが、保護対象サーバーの管理グループに登録されていることを確認します。

上記の確認が完了したら、インストールの手順に進んでください。セットアップウィザードの説明に続いて、Kaspersky Security 10.1 for Windows Server をインストールするための設定を指定します。Kaspersky Security 10.1 for Windows Server のインストールプロセスは、セットアップウィザードのどの段階でも中断できます。それには、[セットアップウィザード]ウィンドウで[**キャンセル**]を押してください。

インストール(アンインストール)の設定については詳細情報があります(66 ページのセクション「インストールおよびアンインストールの設定と Windows インストーラーサービスで使用するコマンドラインオプション」を参照)。

► **インストールウィザードを使用して Kaspersky Security 10.1 for Windows Server をインス**

トールするには:

1. サーバーでランチャーの実行ファイル setup.exe を起動します。
2. 表示されるウィンドウの[インストール]セクションで、[**Kaspersky Security 10.1 for Windows Server のインストール**]をクリックします。
3. Kaspersky Security 10.1 for Windows Server のセットアップウィザードの開始スクリーンで[**次へ**]をクリックします。

   [**使用許諾契約書とプライバシーポリシー**]ウィンドウが表示されます。
4. 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ます。
5. 使用許諾契約書とプライバシーポリシーの条項に同意する場合、[使用許諾契約書の条件]と[**データの取り扱いについて記載されているプライバシーポリシー**]をオンにして、インストールを続行します。

   使用許諾契約書とプライバシーポリシーに同意しない場合は、インストールは中止されます。
6. [**次へ**]をクリックします。

   サーバーに互換性のあるバージョンのアプリケーションがインストールされている場合、[**以前のバージョンのアプリケーションが見つかりました**]ウィンドウが表示されます。

   以前のバージョンのアプリケーションが検知されなかった場合は、この説明の手順 8 に進んでください。
7. 以前のバージョンのアプリケーションからアップグレードするには、[**インストール**]をクリックします。セットアップウィザードが Kaspersky Security 10.1 for Windows Server にアプリケーションをアップグレードし、互換性のある設定を新しいバージョンで保存します。アップグレードが完了すると、[**インストールの完了**]ウィンドウが表示されます(この説明の手順 15 に進んでください)。

   [**インストール前のコンピューターの簡易スキャン**]ウィンドウが表示されます。
8. ローカルのサーバードライブのシステムメモリとブートセクターをスキャンして脅威の有無を確認する場合は、[**インストール前のコンピューターの簡易スキャン**]ウィンドウで[**コンピューターのウイルスをス**

キャンする]をオンにします。[**次へ**]を押します。スキャンが完了すると、スキャン結果のウィンドウが表示されます。

このウィンドウには、スキャンしたサーバーのオブジェクトの情報として次の結果が表示されます:スキャンしたオブジェクトの合計、検知された脅威の種別の数、検知された感染したオブジェクトまたは感染の可能性があるオブジェクトの数、Kaspersky Security 10.1 for Windows Server によってメモリから削除された危険なプロセスまたは疑わしいプロセスの数、削除できなかった危険なプロセスまたは疑わしいプロセスの数。

スキャンされたオブジェクトの詳細を確認するには、[**処理されたオブジェクトのリスト**]をクリックします。

9. [**インストール前のコンピューターの簡易スキャン**]ウィンドウで[**次へ**]をクリックします。

   [**カスタムインストール**]ウィンドウが開きます。

10. インストールするコンポーネントを選択します。

    既定では、ファイアウォール管理とスクリプト監視を除くすべての Kaspersky Security 10.1 for Windows Server コンポーネントが推奨インストールセットに含まれています。

    > Kaspersky Security 10.1 for Windows Server の SNMP プロトコルサポートは、Microsoft Windows SNMP サービスがサーバーにインストールされている場合にのみ、インストールするコンポーネントのリストに表示されます。

11. すべての変更をキャンセルするには、[**カスタムインストール**]ウィンドウで[**リセット**]をクリックします。[**次へ**]をクリックします。

12. [**インストール先フォルダーの選択**]ウィンドウで次のように操作します:

    - 必要に応じて、Kaspersky Security 10.1 for Windows Server のファイルのコピー先のフォルダーを指定します。
    - 必要に応じて、[**ディスク**]をクリックして、ローカルディスクの使用可能な容量の情報を確認します。

[**次へ**]をクリックします。

13. [**インストールの詳細設定**]ウィンドウで、次のインストール設定を行います:

- **製品インストール後にリアルタイム保護を有効にする**
- **Microsoft によって推奨されているファイルを除外リストに追加する**
- **Kaspersky Lab によって推奨されているファイルを除外リストに追加する**

[**次へ**]をクリックします。

14. [**設定ファイルからのインポートの設定**]ウィンドウが開きます:

a. 互換性のある以前のバージョンのアプリケーションで作成された既存の設定ファイルから Kaspersky Security 10.1 for Windows Server の設定をインポートする場合は、設定ファイルを指定します。

b. [**次へ**]を押します。

15. [**製品のアクティベーション**]ウィンドウで、次のいずれかを行います:

- 製品をアクティベーションする場合は、アクティベーションに使用する Kaspersky Security 10.1 for Windows Server のライセンス情報ファイルを指定します。
- 製品を後でアクティベーションする場合は、[**次へ**]をクリックします。
- ライセンス情報ファイルがあらかじめ配布キットのフォルダー server に保存されている場合は、このファイルの名前が[**ライセンス**]に表示されます。
- 別のフォルダーに保存されているライセンス情報ファイルを使用してライセンスを追加する場合は、そのライセンス情報ファイルを指定します。

> セットアップウィザードからは、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ことはできません。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ションする場合は、インストール後にアクティベーションコードを入力する必要があります。

ライセンス情報ファイルが追加されると、ライセンス情報がウィンドウに表示されます。Kaspersky Security 10.1 for Windows Server がライセンス有効期限日を計算および表示します。ライセンスの有効期間は、ライセンスが追加された時間から実行され、ライセンス情報ファイルの有効期限日まで有効です。

[**次へ**]をクリックして、ライセンスを製品に適用します。

16. [**インストールの準備完了**]ウィンドウで、[インストール]をクリックします。Kaspersky Security 10.1 for Windows Server のコンポーネントのインストールが開始します。

17. インストールが完了すると[**インストールの完了**]ウィンドウが表示されます。

18. セットアップウィザードの完了後にリリースに関する情報を確認する場合は、[**リリースノートの表示**]をオンにします。

19. [**OK**]をクリックします。

セットアップウィザードのウィンドウが閉じます。アクティベーションコードを入力している場合、インストールが完了すると Kaspersky Security 10.1 for Windows Server が使用できるようになります。

Kaspersky Security 10.1 コンソールのインストール

セットアップウィザードの指示に従い、Kaspersky Security 10.1 コンソールのインストール設定を調整します。インストールプロセスは、セットアップウィザードのどの段階でも中断できます。それには、ウィザードのウィンドウで[**キャンセル**]を押してください。

► **Kaspersky Security 10.1 コンソールをインストールするには、次の手順を実行します:**

1. セットアップウィザードを実行するアカウントが、コンピューターの管理グループに含まれていることを確認します。

2. コンピューターの上でランチャーの実行ファイル setup.exe を実行します。

   プログラムの開始ウィンドウが表示されます。

3. [**Kaspersky Security 10.1 コンソールのインストール**]をクリックします。

   セットアップウィザードの開始ウィンドウが表示されます。[**次へ**]をクリックします。

4. 表示されるウィンドウ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、[**使用許諾契約書の条件**]と[**データの取り扱いについて記載されているプライバシーポリシー**]をオンにして、インストールを続行します。[**次へ**]をクリックします。

5. [**インストールの詳細設定**]ウィンドウで次のように操作します:

   - Kaspersky Security 10.1 コンソールを使用してリモートのコンピューターにインストールされている Kaspersky Security 10.1 for Windows Server を管理する場合は、[**リモートアクセスを許可する**]をオンにします。
   - [**カスタムインストール**]ウィンドウを開いてコンポーネントを選択するには:

     a. [**詳細設定**]をクリックします。

     [**カスタムインストール**]ウィンドウが開きます。

     b. リストから「管理ツール」セットのコンポーネントを選択します。

     既定では、すべてのコンポーネントがインストールされます。

     c. [**次へ**]をクリックします。

   > Kaspersky Security 10.1 for Windows Server コンポーネントに関する詳細情報があります(50 ページのセクション「Kaspersky Security 10.1 for Windows Server ソフトウェアコンポーネントと Windows インストーラーサービスで使用する各コンポーネントのコード」を参照)。

6. [**インストール先フォルダーの選択**]ウィンドウで次のように操作します:

   c. 必要に応じて、インストールするファイルの保存先として別のフォルダーを指定します。

   d. [**次へ**]をクリックします。

7. [**インストールの準備完了**]ウィンドウで、[**インストール**]をクリックします。

   選択したコンポーネントのインストールが開始します。

8. [**OK**]をクリックします。

セットアップウィザードのウィンドウが閉じます。Kaspersky Security 10.1 コンソールが、保護対象サーバーにインストールされます。

「管理ツール」セットが、ネットワーク上の、保護対象サーバー以外のサーバーにインストールされた場合、詳細設定を行ってください（89 ページのセクション「Kaspersky Security 10.1 コンソールを別のコンピューターにインストールした後の詳細設定」を参照）。

Kaspersky Security 10.1 コンソールを別のコンピューターにインストールした後の詳細設定

Kaspersky Security 10.1 コンソールを、ネットワーク上の、保護対象サーバー以外のコンピューターにインストールした場合、次の操作を実行してリモートで Kaspersky Security 10.1 for Windows Server を管理できるようにします：

- 保護対象サーバーの KAVWSEE Administrators グループに Kaspersky Security 10.1 for Windows Server のユーザーを追加します。
- 保護対象サーバーが Windows ファイアウォールまたはサードパーティのファイアウォールを使用している場合、Kaspersky Security 管理サービス（kavfsgt.exe）のネットワーク接続を許可してください。
- Microsoft Windows が動作しているコンピューターへの Kaspersky Security 10.1 コンソールのインストール時に[**リモートアクセスを許可する**]をオンにしない場合、コンピューターのファイアウォールを経由する Kaspersky Security 10.1 コンソールのネットワーク接続を手動で許可してください。

このセクションの内容

Kaspersky Security 管理サービスのアクセス権限について

Kaspersky Security 10.1 for Windows Server サービスのリストを確認できます。

Kaspersky Security 10.1 for Windows Server はインストール時に Kaspersky Security 10.1 for Windows Server 管理サービス(KAVFSGT)を登録します。別のコンピューターにインストールされた Kaspersky Security 10.1 コンソールから本製品を管理するには、Kaspersky Security 10.1 for Windows Server への接続に使用される権限を持つアカウントが、保護対象サーバーの Kaspersky Security 10.1 for Windows Server 管理サービスへのフルアクセス権を持っている必要があります。

既定では、保護対象サーバーの管理者グループのユーザーと、Kaspersky Security 10.1 for Windows Server のインストール時に保護対象サーバーに作成された[KAVWSEE Administrators]グループのユーザーに、すべての Kaspersky Security 管理サービスへのアクセス権が付与されます。

Kaspersky Security 管理サービスは、Microsoft Windows の**サービス**スナップインでのみ管理できます。

Kaspersky Security 10.1 for Windows Server の設定では、Kaspersky Security 10.1 for Windows Server 管理サービスへのユーザーアクセスを許可またはブロックできません。

名前とパスワードが同じアカウントが保護対象のサーバーに登録されている場合、ローカルアカウントから Kaspersky Security 10.1 for Windows Server に接続できます。

Kaspersky Security 10.1 コンソールのネットワーク接続を許可する

Windows オペレーティングシステムによって、設定名が異なる場合があります。

リモートコンピューター上の Kaspersky Security 10.1 コンソールは、DCOM プロトコルを使用して、Kaspersky Security 10.1 for Windows Server イベントに関する情報(スキャンされたオブジェクトや完了したタスクなど)を保護対象サーバーの Kaspersky Security 10.1 for Windows Server 管理サービスから受信します。Kaspersky Security 10.1 コンソールと Kaspersky Security 10.1 for Windows Server 管理サービス間の接続を確立するために、Windows ファイアウォールの設定で Kaspersky Security 10.1 コンソールに対してネットワーク接続を許可する必要があります。

次の操作を行います:

- COM アプリケーションへの匿名リモートアクセスが許可されていることを確認します(COM アプリケーションの遠隔起動とアクティベーションは許可しません)。
- Windows ファイアウォールで、TCP ポート 135 を開き、Kaspersky Security 10.1 for Windows Server リモート管理プロセスの実行ファイル(kavfsrcn.exe)に対してネットワーク接続を許可します。

  Kaspersky Security 10.1 コンソールがインストールされているクライアントコンピューターでは、保護対象サーバーへのアクセスと応答の受信に、ポート TCP 135 が使用されます。

保護対象サーバーと Kaspersky Security 10.1 コンソールがインストールされているサーバー間の接続を設定したときにコンソールが開かれた場合、Kaspersky Security 10.1 コンソールを閉じ、Kaspersky Security 10.1 for Windows Server リモート管理プロセス(kavfsrcn.exe)が終了するまで待機し、コンソールを再起動します。新しい接続設定が適用されます。

► COM アプリケーションへの匿名リモートアクセスを許可するには、次の手順を実行します:

1. Kaspersky Security 10.1 コンソールがインストールされたサーバーで、コンポーネントサービスコンソールを開きます。

2. **[スタート]-[実行]**の順に選択します。

3. `dcomcnfg` コマンドを入力します。

4. [**OK**]をクリックします。

5. サーバーのコンポーネントサービスコンソールで[**コンピューター**]を展開します。

6. [**マイ コンピューター**]のコンテキストメニューを開きます。

7. [**プロパティ**]を選択します。

8. [**プロパティ**]ウィンドウの[**COM セキュリティ**]タブで、[**アクセス許可**]設定グループの[**編集**]をクリックします。

9. [**リモートアクセスを許可する**]ウィンドウで、ANONYMOUS LOGON ユーザーに対して[**リモートアクセスを許可する**]になっていることを確認します。

10. [**OK**]をクリックします。

► **Windows ファイアウォールで TCP ポート 135 を開き、Kaspersky Security 10.1 for Windows Server リモート管理プロセスの実行ファイルに対してネットワーク接続を許可するには:**

1. リモートコンピューターで Kaspersky Security 10.1 コンソールを閉じます。

2. 次のいずれかの処理を実行します:

   - Microsoft Windows XP または Microsoft Windows Vista の場合:

     d. Microsoft Windows XP SP2 以降の場合は、**[スタート]-[Windows ファイアウォール]**の順に選択します。

     Microsoft Windows Vista の場合は、**[スタート]-[コントロール パネル]-[Windows ファイアウォール]**の順に選択し、[**Windows ファイアウォール**]ウィンドウで[**設定の変更**]を選択します。

     e. [Windows ファイアウォール]ウィンドウ(または[Windows ファイアウォールの設定])の[**除外**]タブで、[**ポートの追加**]をクリックします。

     f. [**名前**]にポート名「RPC (TCP/135)」を指定するか、他の名前(「Kaspersky Security 10.1

for Windows Server DCOM」など）を入力し、[**ポート番号**]にポート番号（135）を指定します。

g. [**TCP**]プロトコルを選択します。

h. [**OK**]をクリックします。

i. [**除外**]タブで、[**追加**]をクリックします。

- Microsoft Windows 7 以降の場合：

a. **[スタート]-[コントロール パネル]-[Windows ファイアウォール]**の順に選択します。[**Windows ファイアウォール**]ウィンドウで、[**Windows ファイアウォールを介したプログラムまたは機能を許可する**]を選択します。

b. [**Windows ファイアウォール経由の通信をプログラムに許可します**]ウィンドウで、[**別のプログラムの許可**]をクリックします。

3. [**プログラムの追加**]ウィンドウでファイル kavfsrcn.exe を指定します。このファイルは、MMC を使用して Kaspersky Security 10.1 コンソールをインストールしたときにインストール先フォルダーとして指定したフォルダー内にあります。

4. [**OK**]をクリックします。

5. [**Windows ファイアウォール**]（[**Windows ファイアウォールの設定**]）ウィンドウで、[**OK**]をクリックします。

Kaspersky Security 管理サービスのネットワーク接続の有効化

Windows オペレーティングシステムによって、設定名が異なる場合があります。

Kaspersky Security 10.1 コンソールと Kaspersky Security 管理サービス間の接続を確立するには、保護対象サーバーのファイアウォールから管理サービスのネットワーク接続を許可する必要があります。

Kaspersky Security が Microsoft Windows Server 2003、Microsoft Windows Server 2008、Microsoft Windows Server 2012 または Microsoft Windows Server 2012 R2 で動作している場合、ネットワーク接続を設定する必要があります。

► **Kaspersky Security 管理サービスのネットワーク接続を許可するには:**

1. Microsoft Windows Server を実行する保護対象サーバーで、**[スタート]-[コントロール パネル]-[セキュリティ]-[Windows ファイアウォール]**の順に選択します。
2. [**Windows ファイアウォールの設定**]ウィンドウで、[**設定の変更**]を選択します。
3. [**除外**]タブ上の定義済み除外リストで、フラグをチェックします:[**COM + ネットワークアクセス**]、[**Windows Management Instrumentation(WMI)**]、[**リモート管理**]。
4. [**プログラムの追加**]をクリックします。
5. [**プログラムの追加**]ダイアログウィンドウでファイル kavfsgt.exe を指定します。このファイルは、MMC を使用して Kaspersky Security 10.1 for Windows Server をインストールしたときにインストール先フォルダーとして指定したフォルダー内にあります。
6. [**OK**]をクリックします。
7. [**Windows ファイアウォールの設定**]ダイアログウィンドウで[**OK**]をクリックします。

Kaspersky Security 管理サービスのネットワーク接続が有効になります。

Kaspersky Security 10.1 for Windows Server インストール後に実行する処理

製品をすでにアクティベーションしている場合、インストールが完了すると保護タスクとスキャンタスクがただちに開始されます。Kaspersky Security 10.1 for Windows Server のインストール時に[**製品インストール後にリアルタイム保護を有効にする**]をオンにしていた場合(既定のオプション)、サーバーファイルのシステムオブジェクトにアクセスした際にそれらのオブジェクトをスキャンします。カスタムインストールでスクリプト監視をインストー

ルした場合、スクリプトの実行時にすべてのスクリプトのプログラムコードをスキャンします。毎週金曜日の 20:00 に重要領域のスキャンタスクが実行されます。

Kaspersky Security 10.1 for Windows Server のインストール後に、次の手順を実行してください:

- Kaspersky Security 10.1 for Windows Server データベースのアップデートタスクを開始します。インストール後、製品の配布キットに含まれる定義データベースを使用してオブジェクトがスキャンされます。

  > 定義データベースは最新のものでない可能性があるため、ただちにアップデートしてください。

  その後定義データベースは、タスクで設定されている既定のスケジュールに従って 1 時間ごとにアップデートされます。

- Kaspersky Security 10.1 for Windows Server をインストールする前にファイルのリアルタイム保護機能のあるアンチウイルス製品が保護対象サーバーにインストールされていなかった場合、重要領域のスキャンをサーバーで実行します。

- Kaspersky Security 10.1 for Windows Server イベントに関する管理者への通知を設定します。

このセクションの内容

Kaspersky Security 10.1 for Windows Server データベースのアップデートタスクの開始と設定

► **インストール後に定義データベースをアップデートするには、次の操作を行います:**

1. 定義データベースのアップデートタスクの設定で、アップデート元である Kaspersky Lab の HTTP アップデートサーバーまたは FTP アップデートサーバーとの接続を設定します。

2. 定義データベースのアップデートタスクを開始します。

► **Kaspersky Lab のアップデートサーバーとの接続を設定するには、定義データベースのアップデートタスクで次の手順を実行します:**

1. 次のいずれかの方法で Kaspersky Security 10.1 コンソールを開始します:

   - 保護対象サーバーで Kaspersky Security 10.1 コンソールを開きます。それには、**[スタート]-[すべてのプログラム]-[Kaspersky Security 10.1 for Windows Server]-[管理ツール]-[Kaspersky Security for Windows Server 10.1 コンソール]**の順に選択します。

   - 保護対象サーバー以外で Kaspersky Security 10.1 コンソールを起動した場合、次の手順で保護対象サーバーに接続します:

     a. Kaspersky Security 10.1 コンソールのツリーで[**Kaspersky Security**]フォルダーのコンテキストメニューを開きます。

     b. [**別のコンピューターに接続**]を選択します。

     c. [**コンピューターの選択**]ウィンドウで[**他のコンピューター**]を選択し、入力欄に保護対象サーバーのネットワーク名を入力します。

   > Microsoft Windows のサインインに使用したユーザーアカウントが Kaspersky Security 管理サービスへのアクセス権を持っていない場合、必要なアクセス権のあるユーザーアカウントを指定します(90 ページのセクション「Kaspersky Security 管理サービスのアクセス権限について」を参照)。

   Kaspersky Security 10.1 コンソールが開きます。

2. Kaspersky Security 10.1 コンソールツリーで、[**アップデート**]フォルダーを展開します。

3. [**定義データベースのアップデート**]サブフォルダーを選択します。

4. 詳細ペインで[**プロパティ**]をクリックします。

5. 表示される[**タスクの設定**]ウィンドウで、[**接続設定**]タブを開きます。

6. 次の操作を行います:

    a. LAN でのプロキシサーバー設定の自動検知用に、お使いのサーバーで Web Proxy Auto-Discovery Protocol(WPAD)が設定されていない場合、次の手順でプロキシサーバーの設定を指定します。[**Kaspersky Security**]フォルダーを展開し、詳細ペインの[**アプリケーションのプロパティ**]をクリックします。[**アプリケーションのプロパティ**]ウィンドウの[**接続設定**]タブを選択し、[**プロキシサーバーの設定**]セクションで[**指定したプロキシサーバー設定を使用する**]をオンにし、[**アドレス**]にアドレスを、[**ポート**]にプロキシサーバーのポート番号を入力します。

    b. プロキシサーバーへのアクセス時にネットワークにより認証が要求される場合、[**プロキシサーバーの認証設定**]セクションのドロップダウンリストより、必要な認証方法を選択してください:

- **NTLM 認証**:プロキシサーバーによって組み込みの Microsoft Windows NTLM 認証がサポートされている場合に選択します。タスクの設定で指定されているユーザーアカウントを使用して、プロキシサーバーにアクセスします(既定では、タスクは**ローカルシステム**(**SYSTEM**)ユーザーアカウントで実行されます)。
- **ユーザー名とパスワードを指定して NTLM 認証を使用する**:プロキシサーバーによって組み込みの Microsoft Windows NTLM 認証がサポートされている場合に選択します。指定されたアカウントを使用してプロキシサーバーにアクセスします。ユーザー名とパスワードを入力するか、リストからユーザーを選択します。
- **ユーザー名とパスワード**:基本認証を選択できます。ユーザー名とパスワードを入力するか、リストからユーザーを選択します。

7. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

定義データベースのアップデートタスクでのアップデート元との接続設定の内容が保存されます。

► **定義データベースのアップデートタスクを実行するには:**

1. Kaspersky Security 10.1 コンソールツリーで、[**アップデート**]フォルダーを展開します。
2. [**定義データベースのアップデート**]サブフォルダーのコンテキストメニューを開き、[**開始**]を選択します。

定義データベースのアップデートタスクが開始されます。

タスクが正常に完了すると、インストールされた定義データベースの最新のアップデートの公開日が[**Kaspersky Security**]フォルダーの詳細ペインで確認できます。

重要領域のスキャン

Kaspersky Security 10.1 for Windows Server の定義データベースのアップデートが完了したら、重要領域のスキャンタスクを使用してサーバーをスキャンしマルウェアの有無を確認します。

► **重要領域のスキャンタスクを実行するには、次の手順を実行します:**

1. Kaspersky Security 10.1 コンソールツリーで、[**オンデマンドスキャン**]フォルダーを展開します。
2. [**重要領域のスキャン**]サブフォルダーのコンテキストメニューで、[**開始**]を選択します。

タスクが開始し、タスクのステータスが[**実行中**]として作業領域に表示されます。

► **タスクの実行ログを確認するには:**

[**重要領域のスキャン**]フォルダーの詳細ペインで、[**実行ログを開く**]をクリックします。

コンポーネントセットの変更と Kaspersky Security 10.1 for Windows Server の復元

Kaspersky Security 10.1 for Windows Server コンポーネントは追加と削除ができます。ファイルのリアルタイム保護を削除する場合は、事前にファイルのリアルタイム保護タスクを停止する必要があります。それ以外の状況では、ファイルのリアルタイム保護タスクや Kaspersky Security サービスを停止する必要はありません。

アプリケーション管理アクセス権がパスワードで保護されている場合、セットアップウィザードの追加手順でコンポーネントセットを削除または変更しようとすると、パスワードを求められます。

► **Kaspersky Security 10.1 for Windows Server のコンポーネントセットを変更するには:**

1. [**スタート**]メニューで、[**すべてのプログラム**] - [**Kaspersky Security 10.1 for Windows Server**] - [Kaspersky Security for Windows Server の変更または削除]の順に選択します。

   セットアップウィザードの[**インストールの変更、修復、または削除**]ウィンドウが表示されます。

2. [**コンポーネントセットの変更**]を選択します。[**次へ**]をクリックします。

   [**カスタムインストール**]ウィンドウが開きます。

3. [**カスタムインストール**]ウィンドウの、選択可能なコンポーネントのリストで Kaspersky Security 10.1 for Windows Server に追加するコンポーネントまたは削除するコンポーネントを選択します。それには、次の操作を実行します:

   - コンポーネントのセットを変更するには選択したコンポーネント名の隣にあるボタンをクリックし、コンテキストメニューで次の項目を選択します:

     - **コンポーネントをローカルハードディスクにインストール**:1 つのコンポーネントをインストールする場合
     - **コンポーネントとサブコンポーネントをローカルハードディスクにインストール**:コンポーネントのグループをインストールする場合

   - 以前インストールしたコンポーネントを削除する場合は、選択したコンポーネント名の隣にあるボタンをクリックし、コンテキストメニューで[**コンポーネントを使用しない**]をオンにします。

   [**次へ**]をクリックします。

4. [**インストールの準備完了**]ウィンドウで[インストール]をクリックし、ソフトウェアコンポーネントのセットの変更を確定します。

5. インストールの完了後に表示されるウィンドウで、[**OK**]をクリックします。

指定の設定に基づいて、Kaspersky Security 10.1 for Windows Server のコンポーネントのセットが変更されます。

Kaspersky Security 10.1 for Windows Server の実行中に問題が発生した場合(タスクのクラッシュや、タスクが開始しないなどの Kaspersky Security 10.1 for Windows Server のクラッシュ)、Kaspersky Security 10.1 for Windows Server の復元を試みることができます。復元は、Kaspersky Security 10.1 for Windows Server の現在の設定の保存中に行えます。または、Kaspersky Security 10.1 for Windows Server のすべての設定を既定値にリセットするオプションを選択できます。

► **アプリケーションまたはタスクのクラッシュ後に Kaspersky Security 10.1 for Windows Server を復元するには次の手順を実行します:**

1. [**スタート**]メニューで、[**すべてのプログラム**] - [**Kaspersky Security 10.1 for Windows Server**] - [**Kaspersky Security for Windows Server の変更または削除**]の順に選択します。

   セットアップウィザードの[**インストールの変更、修復、または削除**]ウィンドウが表示されます。

2. [**インストール済みコンポーネントの修復**]をオンにします。[**次へ**]をクリックします。

   [**インストール済みコンポーネントの修復**]ウィンドウが表示されます。

3. 編集したアプリケーションの設定をリセットし Kaspersky Security 10.1 for Windows Server を既定値で復元する場合は、[**インストール済みコンポーネントの修復**]ウィンドウで[**製品の推奨設定を復元する**]をオンにします。[**インストール**]をクリックします。

4. [**修復準備完了**]ウィンドウで[**次へ**]をクリックし、修復操作を確定します。

5. 修復操作の完了後に表示されるウィンドウで、[**OK**]をクリックします。

指定の設定に基づいて、Kaspersky Security 10.1 for Windows Server が復元されます。

セットアップウィザードを使用したアンインストール

このセクションでは、セットアップウィザードを使用した保護対象サーバーからの Kaspersky Security 10.1 for Windows Server および Kaspersky Security 10.1 コンソールの削除方法について説明します。

このセクションの内容

Kaspersky Security 10.1 for Windows Server のアンインストール

Windows オペレーティングシステムによって、設定名が異なる場合があります。

セットアップおよびアンインストールウィザードを使用して、保護対象サーバーから Kaspersky Security 10.1 for Windows Server をアンインストールできます。

保護対象サーバーから Kaspersky Security 10.1 for Windows Server をアンインストールした後、再起動が必要になる場合があります。再起動は、後から実施することもできます。

オペレーティングシステムが UAC 機能（ユーザーアカウント制御）を使用しているか、アプリケーションへのアクセスがパスワードで保護されている場合、Windows コントロール パネルからのアプリケーションのアンインストール、復元およびインストールはできません。

アプリケーション管理アクセス権がパスワードで保護されている場合、セットアップウィザードの追加手順でコンポーネントセットを削除または変更しようとすると、パスワードを求められます。

► **Kaspersky Security 10.1 for Windows Server をアンインストールするには:**

1. ［**スタート**］メニューで、［**すべてのプログラム**］ - ［**Kaspersky Security 10.1 for Windows Server**］ -

[**Kaspersky Security for Windows Server の変更または削除**]の順に選択します。

セットアップウィザードの[**インストールの変更、修復、または削除**]ウィンドウが表示されます。

2. [**ソフトウェアコンポーネントの削除**]をオンにします。[**次へ**]をクリックします。

   [**アンインストールの詳細設定**]ウィンドウが表示されます。

3. 必要に応じて[**アンインストールの詳細設定**]ウィンドウで次の操作を実行します:

   a. 隔離されたオブジェクトをエクスポートする場合は、[**隔離されたオブジェクトをエクスポートする**]をオンにします。既定では、このチェックボックスはオフです。

   b. Kaspersky Security 10.1 for Windows Server のバックアップからオブジェクトをエクスポートする場合は、[**バックアップされたオブジェクトをエクスポートする**]をオンにします。既定では、このチェックボックスはオフです。

   c. [**保存**]をクリックし、復元するオブジェクトのエクスポート先のフォルダーを選択します。既定では、オブジェクトは次のフォルダーにエクスポートされます: %ProgramData%¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Servers¥10.1¥Uninstall

   [**次へ**]をクリックします。

4. [**アンインストールの準備完了**]ウィンドウで[**アンインストール**]をクリックし、アンインストールを確定します。

5. アンインストールの完了後に表示されるウィンドウで、[**OK**]をクリックします。

Kaspersky Security 10.1 for Windows Server が保護対象サーバーからアンインストールされます。

Kaspersky Security 10.1 コンソールのアンインストール

Windows オペレーティングシステムによって、設定名が異なる場合があります。

セットアップおよびアンインストールウィザードを使用して、サーバーから Kaspersky Security 10.1 コンソールをアンインストールできます。

Kaspersky Security 10.1 コンソールのアンインストール後、サーバーを再起動する必要はありません。

► **Kaspersky Security 10.1 コンソールをアンインストールするには:**

1. [**スタート**]メニューで、[**すべてのプログラム**] - [**Kaspersky Security 10.1 for Windows Server**] - [**管理ツール**] - [**Kaspersky Security for Windows 管理ツールの変更または削除**]の順に選択します。

2. ウィザードの[**インストールの変更、修復、または削除**]ウィンドウが表示されます。

   [**ソフトウェアコンポーネントの削除**]をオンにして[**次へ**]をクリックします。

3. [**アンインストールの準備完了**]ウィンドウが表示されます。[**アンインストール**]をクリックします。

   [**アンインストールの完了**]ウィンドウが表示されます。

4. [**OK**]をクリックします。

削除が完了し、セットアップウィザードが終了します。

コマンドラインによる製品のインストールとアンインストール

このセクションでは、コマンドラインを使用して Kaspersky Security 10.1 for Windows Server をインストールおよびアンインストールする方法について説明します。コマンドラインから Kaspersky Security 10.1 for Windows Server をインストールおよびアンインストールするためのコマンドの例や、コマンドラインから Kaspersky Security 10.1 for Windows Server のコンポーネントを追加または削除するためのコマンドの例も記載されています。

このセクションの内容

コマンドラインからの Kaspersky Security 10.1 for Windows Server のインストールとアンインストール

キーによるインストール設定の指定後、コマンドラインからインストールパッケージ server¥ks4ws_x86(x64).msi を実行することで、Kaspersky Security 10.1 for Windows Server のインストールやアンインストール、および Kaspersky Security コンポーネントの追加や削除が行えます。

「管理ツール」セットは、保護対象サーバーまたはネットワークにある別のコンピューターにインストールして、ローカルまたはリモートで Kaspersky Security 10.1 コンソールを使用できます。それには、インストールパッケージ client¥ks4wstools.msi を使用します。

インストールは、製品がインストールされているサーバーの管理グループに登録されているアカウントの権限を使用して実行します。

ファイル ¥server¥ks4ws_x86(x64).msi のうち、予備のライセンスがない状態で、保護対象サーバーで実行されているファイルがある場合、Kaspersky Security 10.1 for Windows Server は、推奨されているインストール設定でインストールされます。

ADDLOCAL コマンドラインオプションを使用して、選択したコンポーネントやコンポーネントセットのコードをリストすることで、インストールする一連のコンポーネントを割り当てることができます。

Kaspersky Security 10.1 for Windows Server のインストールで使用するコマンド事例

このセクションでは、Kaspersky Security 10.1 for Windows Server のインストールに使用するコマンドの例を紹介します。

> 32 ビット版の Microsoft Windows を実行するサーバーでは、配布キットに含まれる接尾語が「x86」のファイルを実行します。64 ビット版の Microsoft Windows を実行するサーバーでは、配布キットに含まれる接尾語が「x64」のファイルを実行します。

Windows インストーラーの標準的なコマンドとコマンドラインオプションの使用についての詳細な情報については、Microsoft から提供されるガイドを参照してください。

ファイル setup.exe からの Kaspersky Security 10.1 for Windows Server のインストール事例

► **ユーザーとのやり取りを必要としないモードを使用して推奨されているインストール設定で Kaspersky Security 10.1 for Windows Server をインストールするには、次のコマンドを実行します:**

¥server¥setup.exe /s/p EULA=1 PRIVACYPOLICY=1

► **Kaspersky Security 10.1 for Windows Server を次の設定でインストールするには:**

- ファイルのリアルタイム保護とオンデマンドスキャンのみをインストールする。
- Kaspersky Security 10.1 for Windows Server の開始時にリアルタイム保護を実行しない。

- Microsoft Corporation によって除外が推奨されているスキャンファイルを除外しない。

次のコマンドを実行します:

```
¥server¥setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

インストールで使用するコマンドの例:インストールパッケージの msi ファイルを実行

► **ユーザーとのやり取りを必要としないモードを使用して推奨されているインストール設定で Kaspersky Security 10.1 for Windows Server をインストールするには、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► **推奨されているインストール設定に基づき、インストールインターフェイスを表示して Kaspersky Security 10.1 for Windows Server をインストールするには、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

► **ライセンス情報ファイル C:¥0000000A.key を使用して Kaspersky Security 10.1 for Windows Server をアクティベートした状態でインストールするには:**

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:¥0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

► **実行中のプロセスとローカルドライブのブートセクターを事前にスキャンしてから Kaspersky Security 10.1 for Windows Server をインストールするには、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

► **保存先フォルダー C:¥WSEE にファイルを保存する際に Kaspersky Security 10.1 for Windows Server をインストールするには、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi INSTALLDIR=C:¥WSEE /qn EULA=1 PRIVACYPOLICY=1
```

► **Kaspersky Security 10.1 for Windows Server をインストールするには、Kaspersky Security 10.1 for Windows Server インストールパッケージの MSI ファイルが保存されているフォルダーにインストールのログファイルを「ksws.log」という名前で保存して、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

► **Kaspersky Security 10.1 コンソールをインストールするには、次のコマンドを実行します:**

```
msiexec /i ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

► **Kaspersky Security 10.1 for Windows Server をインストールしてキーファイル C:¥0000000A.key を使用してアクティベートし、設定ファイル C:¥settings.xml の記述に従って Kaspersky Security 10.1 for Windows Server を設定するには、次のコマンドを実行します:**

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:¥0000000A.key
CONFIGPATH=C:¥settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Security 10.1 for Windows Server インストール後に実行する処理

製品をすでにアクティベーションしている場合、インストールが完了すると保護タスクとスキャンタスクがただちに開始されます。Kaspersky Security 10.1 for Windows Server のインストール時に[**製品インストール後にリアルタイム保護を有効にする**]をオンにしていた場合、サーバーファイルのシステムオブジェクトにアクセスした際にそれらのオブジェクトをスキャンします。カスタムインストールでスクリプト監視をインストールした場合、スクリプトの実行時にすべてのスクリプトのプログラムコードをスキャンします。毎週金曜日の午後 8 時に重要領域のスキャンタスクが実行されます。

Kaspersky Security 10.1 for Windows Server のインストール後に、次の手順を実行してください:

- Kaspersky Security 10.1 for Windows Server データベースのアップデートタスクを開始します。インストール後、製品の配布キットに含まれる定義データベースを使用してオブジェクトがスキャンされます。Kaspersky Security 10.1 for Windows Server データベースをすぐにアップデートすることを推奨します。それには、定義データのアップデートタスクを実行する必要があります。その後定義データベースは、既定のスケジュールに従って 1 時間ごとにアップデートされます。

  例として、定義データベースのアップデートタスクは、次のコマンドを使用して実行できます:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  この場合、Kaspersky Security 10.1 for Windows Server の定義データベースのアップデートは Kaspersky Lab のアップデートサーバーからダウンロードされます。アップデート元への接続は、プロキシサーバーを経由し(プロキシサーバーアドレス:proxy.company.com、ポート:8080)、ビルトイン Windows NTLM 認証を使用して、アカウント下のサーバー(ユーザー名:inetuser、パスワード:

123456）にアクセスして確立します。

- Kaspersky Security 10.1 for Windows Server をインストールする前にファイルのリアルタイム保護機能のあるアンチウイルス製品が保護対象サーバーにインストールされていなかった場合、コンピューターの重要領域のスキャンを実行します。

► **コマンドラインを使用して重要領域のスキャンタスクを開始するには：**

KAVSHELL SCANCRITICAL /W:scancritical.log

このコマンドでは、現在のフォルダーに含まれるファイル scancritical.log に実行ログを保存します。

- Kaspersky Security 10.1 for Windows Server イベントに関する管理者への通知を設定します。

コンポーネントの追加および削除：サンプルコマンド

オンデマンドスキャンは自動でインストールされます。Kaspersky Security 10.1 for Windows Server のコンポーネントを追加または削除して、ADDLOCAL キーの値のリストでオンデマンドスキャンを指定する必要はありません。

► **すでにインストールされているコンポーネントにアプリケーション起動コントロールを追加するには、次のコマンドを実行します：**

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn EULA=1 PRIVACYPOLICY=1
```

または

```
¥server¥setup.exe /s /p "ADDLOCAL=Oas,AppCtrl EULA=1 PRIVACYPOLICY=1"
```

インストールするコンポーネントとすでにインストールされているコンポーネントを列挙すると、既存のコンポーネントが再インストールされます。

► **インストールされたコンポーネントを削除するには、次のコマンドを実行します：**

```
msiexec /i ks4ws.msi REMOVE=AppCtrl,WiFiControl /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Security 10.1 for Windows Server のアンインストール：サンプルコマンド

► **保護対象サーバーから Kaspersky Security 10.1 for Windows Server をアンインストールするには、次のコマンドを実行します：**

```
msiexec /x ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► **Kaspersky Security コンソールをアンインストールするには、次のコマンドを実行します：**

```
msiexec /x ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

または

- 32 ビットオペレーティングシステムの場合：

```
msiexec /x {232497F6-6572-4934-A6AF-24986952598B} /qn
```

- 64 ビットオペレーティングシステムの場合：

```
msiexec /x {F96C7F1F-9B03-480D-A8F3-19D43CA89090} /qn
```

► **パスワード保護が有効である保護対象サーバーから Kaspersky Security 10.1 for Windows Server をアンインストールするには、次のコマンドを実行します：**

- 32 ビットオペレーティングシステムの場合：

```
msiexec /x {DD1532DD-387B-43C5-8968-7E8130CC8A5E}
UNLOCK_PASSWORD=*** /qn
```

- 64 ビットオペレーティングシステムの場合：

```
msiexec /x {D025308B-AA7E-42D6-8058-B2B79A3D71F5}
UNLOCK_PASSWORD=*** /qn
```

► **パスワード保護が有効である保護対象サーバーから Kaspersky Security 10.1 for Windows Server プラグインをアンインストールするには、次のコマンドを実行します：**

```
msiexec.exe /x {DA15CF4A-75FF-4C92-AFC2-0A16DC645D2E}
UNLOCK_PASSWORD=*** /qn
```

リターンコード

コマンドラインのリターンコードのリストを次の表に示します。

表 13. リターンコード

コード	説明
1324	インストール先のフォルダー名に無効な文字が含まれています。
25001	Kaspersky Security 10.1 for Windows Server をインストールする権限が不十分な場合。アプリケーションをインストールするには、ローカル管理者権限でインストールウィザードを開始してください。
25003	このバージョンの Microsoft Windows を実行しているコンピューターには Kaspersky Security 10.1 for Windows Server をインストールできません。64 ビットバージョンの Microsoft Windows 用のインストールウィザードを開始してください。
25004	互換性のないソフトウェアが検知されました。インストールを続けるには、次のソフトウェアをアンインストールします:<非互換ソフトウェアのリスト>。
25010	指定したパスは、隔離されたオブジェクトの保存に使用できません。
25011	隔離されたオブジェクトを保存するフォルダーの名前に無効な文字が含まれています。
26251	パフォーマンスカウンター DLL をダウンロードできません。
26252	パフォーマンスカウンター DLL をダウンロードできません。
27300	ドライバーをインストールできません。
27301	ドライバーをアンインストールできません。

27302	ネットワークコンポーネントをインストールできません。フィルタリングされたデバイス数の、サポートされる最大値に達しました。
27303	定義データベースがありません。

Kaspersky Security Center を使用した製品のインストールとアンインストール

このセクションでは、Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server のインストールについての全般的な情報が記載されています。Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server のインストールおよびアンインストール方法と、製品のインストール後の処理についても説明します。

このセクションの内容

Kaspersky Security Center を使用したインストールに関する全般的な情報

リモートインストールタスクを使用することで、Kaspersky Security Center を介して Kaspersky Security 10.1 for Windows Server をインストールできます。

リモートインストールタスクが完了すると、Kaspersky Security 10.1 for Windows Server は同じ設定で複数のサーバーにインストールされます。

すべてのサーバーを 1 つの管理グループに統合し、このサーバーグループに対して Kaspersky Security 10.1 for Windows Server のインストールを実行するためのグループタスクを作成できます

同じ管理グループに含まれていない一部のサーバーに対して、Kaspersky Security 10.1 for Windows Server をリモートでインストールするタスクを作成できます。このタスクを作成する際、Kaspersky Security 10.1 for Windows Server をインストールする個別のサーバーのリストを生成する必要があります。

リモートインストールタスクの詳細な情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

Kaspersky Security 10.1 for Windows Server をインストールまたはアンインストールする権限

リモートインストール（削除）タスクで指定されたアカウントは、あらゆる場合において各保護対象サーバーの管理グループに含まれている必要があります。ただし、以下で説明する場合を除きます：

- Kaspersky Security 10.1 for Windows Server のインストール先となるコンピューターに Kaspersky Security Center ネットワークエージェントがすでにインストールされている場合（コンピューターのドメインや、コンピューターがドメインに属しているかは問わない）。

  > ネットワークエージェントがサーバー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タスクを使用して、Kaspersky Security 10.1 for Windows Server と一緒にインストールできます。ネットワークエージェントをインストールする前に、タスクで指定するアカウントが各サーバーの管理グループに含まれていることを確認してください。

- Kaspersky Security 10.1 for Windows Server のインストール先となるすべてコンピューターが管理サーバーと同じドメインにあり、**ドメイン管理者**のアカウントで管理サーバーが登録されている場合（このアカウントが、そのドメイン内のコンピューターに対してローカルの管理者権限を持っている場合）。

既定では、**強制インストール**の方法を使用する場合、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るアカウントから実行されます。

強制インストール（アンインストール）モードでグループタスクまたは特定のコンピューターに対するタスクを使用する場合、アカウントはクライアントコンピューターに対して次の権限を持っている必要があります：

- リモートアプリケーションを実行する権限
- **Admin$** リソースに対する権限
- ［**サービスとしてのログオン**］権限

Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server のインストール手順

> インストールパッケージの生成およびリモートインストールタスクの作成の詳細な情報については『Kaspersky Security Center 導入ガイド』を参照してください。

今後、Kaspersky Security Center を介して Kaspersky Security 10.1 for Windows Server を管理する場合、次の条件を満たす必要があります:

- Kaspersky Security Center の管理サーバーがインストールされているサーバーに、Kaspersky Security 10.1 for Windows Server の管理プラグインもインストールされていること(Kaspersky Security 10.1 for Windows Server 配布キットのファイル ¥server¥klcfginst.exe)。
- Kaspersky Security Center ネットワークエージェントが保護対象サーバーにインストールされていること。Kaspersky Security Center ネットワークエージェントが保護対象サーバー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タスクを使用して Kaspersky Security 10.1 for Windows Server と一緒にインストールできます。

後で Kaspersky Security Center のポリシーとグループタスクを使用して保護設定を管理するために、複数のサーバーをあらかじめ 1 つの管理グループにまとめることができます。

► リモートインストールタスクを使用して Kaspersky Security 10.1 for Windows Server をインストールするには:

1. Kaspersky Security Center の管理コンソールを開始します。
2. Kaspersky Security Center で[**詳細**]フォルダーの下にある[**リモートインストール**]フォルダーを展開し、[**インストールパッケージ**]サブフォルダーで[**インストールパッケージの作成**]をクリックします。[**インストールパッケージの種別の選択**]ウィンドウで[**カスペルスキー製品の新しいインストールパッケージを作成する**]を選択します。
3. インストールパッケージ名を入力します。

4. インストールパッケージファイルとして、Kaspersky Security 10.1 for Windows Server 配布キットから ks4ws.kud ファイルを指定します。

   [**使用許諾契約書とプライバシーポリシー**]ウィンドウが表示されます。

5. 使用許諾契約書とプライバシーポリシーの条項に同意する場合、[使用許諾契約書の条件]と[**データの取り扱いについて記載されているプライバシーポリシー**]をオンにして、インストールを続行します。

   > インストールを続行するには、使用許諾契約とプライバシーポリシーに同意する必要があります。

6. インストールする Kaspersky Security 10.1 for Windows Server コンポーネントのセット(98 ページのセクション「Kaspersky Security 10.1 for Windows Server のコンポーネントのセットの変更と復元」を参照)と、インストールパッケージの既定のインストール設定(66 ページのセクション「Windows Installer サービスのインストールおよびアンインストールの設定とコマンドラインオプションを参照)を変更するには:

   Kaspersky Security Center で[**詳細**]フォルダーの下にある[**リモートインストール**]フォルダーを展開し、[**インストールパッケージ**]サブフォルダーの作業領域で、作成した Kaspersky Security 10.1 for Windows Server インストールパッケージのコンテキストメニューを開いて[**プロパティ**]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の[**設定**]セクションで、次の操作を行います:

   a. [**インストールするコンポーネント**]グループの設定で、インストールする Kaspersky Security コンポーネントの名前の隣にあるチェックボックスをオンにします。

   b. インストール先のフォルダーを既定のものではなく指定する場合、フォルダーの名前とパスを[**インストール先フォルダー**]に指定します。

   インストール先フォルダーのパスには、システム環境変数を含むことができます。フォルダーがサーバーに存在しない場合、フォルダーが作成されます。

   c. [**インストールの詳細設定**]グループで次の設定を構成します:

   - インストールの前にコンピューターをスキャンする

- 製品インストール後にリアルタイム保護を有効にする
- Microsoft によって推奨されているファイルを除外リストに追加する
- Kaspersky Lab によって推奨されているファイルを除外リストに追加する

d. 旧バージョンの Kaspersky Security 10.0 for Windows Server で作成された設定ファイルから設定をインポートする場合は、必要な設定ファイルを指定します。

e. インストールパッケージのプロパティウィンドウで[**OK**]をクリックします。

7. [**インストールパッケージ**]フォルダーで、選択したサーバー(管理グループ)に Kaspersky Security 10.1 for Windows Server をリモートでインストールするタスクを作成します。タスクの設定を編集します。

   リモートインストールタスクの作成と設定の詳細は、『**Kaspersky Security Center ヘルプ**』を参照してください。

8. Kaspersky Security 10.1 for Windows Server のリモートインストールタスクを実行します。

タスクで指定したサーバーに Kaspersky Security 10.1 for Windows Server がインストールされます。

Kaspersky Security 10.1 for Windows Server インストール後に実行する処理

Kaspersky Security 10.1 for Windows Server をインストールしたら、サーバーにある Kaspersky Security 10.1 for Windows Server の定義データベースをアップデートしてください。また、Kaspersky Security 10.1 for Windows Server のインストール前に、リアルタイム保護機能が有効になっているアンチウイルス製品がサーバーにインストールされていなかった場合は、サーバーの重要領域のスキャンを実行してください。

Kaspersky Security 10.1 for Windows Server がインストールされたサーバーが、Kaspersky Security Center で 1 つの管理グループにまとめられている場合、次の方法を使用してこれらのタスクを実行できます:

1. Kaspersky Security 10.1 for Windows Server がインストールされたサーバーのグループに対して、定義データベースのアップデートタスクを作成します。アップデート元として Kaspersky Security Center 管理サーバーを指定します。

2. ステータスを重要領域のスキャンタスクに設定したオンデマンドスキャンのグループタスクを作成します。重要領域のスキャンタスクの結果ではなく、このタスクの実行結果に基づいて、グループの各コンピューターのセキュリティレベルが Kaspersky Security Center によって診断されます。

3. サーバーのグループに対して新しいポリシーを作成します。作成したポリシーのプロパティで、[**タスク管理**]タブで必要に応じてシステムスキャンタスクのスケジュールによる開始と、管理グループサーバーでの定義データベースのアップデートタスクを無効にします。

Kaspersky Security 10.1 for Windows Server イベントに関する管理者への通知を設定することもできます。

Kaspersky Security Center を使用した Kaspersky Security 10.1 コンソールのインストール

インストールパッケージおよびリモートインストールタスクの作成の詳細な情報については『**Kaspersky Security Center 導入ガイド**』を参照してください。

► **リモートインストールタスクを使用して Kaspersky Security 10.1 コンソールをインストールするには:**

1. Kaspersky Security Center の管理コンソールで[**詳細**]フォルダーの下にある[**リモートインストール**]フォルダーを展開し、[**インストールパッケージ**]サブフォルダーでファイル client¥setup.exe を基に新たにインストールパッケージを作成します。新しいインストールパッケージの作成で、次の操作を行います:

   - [**インストールパッケージの種別の選択**]ウィンドウで[**指定した実行ファイルのインストールパッケージを作成する**]を選択し、[**インストールする配布パッケージの選択**]で Kaspersky Security 10.1 for Windows Server 配布キットのフォルダーから client¥setup.exe ファイルを選択し、[**すべてのフォルダーをインストールパッケージへコピー**]をオンにします。

- 必要な場合、[**実行ファイルのコマンドライン（オプション）**]で ADDLOCAL コマンドラインオプションを使用してインストールするコンポーネントのセットを変更し、インストール先のフォルダーを変更します。

  例として、ヘルプファイルやガイドはインストールせずに、フォルダー C:¥KasperskyConsole にある Kaspersky Security 10.1 コンソールのみをインストールする場合は、次のコマンドを入力します：

  ```
  /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:¥KasperskyConsole EULA=1 PRIVACYPOLICY=1"
  ```

2. [インストールパッケージ]フォルダーで、選択したコンピューター（管理グループ）に Kaspersky Security 10.1 コンソールをリモートでインストールするタスクを作成します。タスクの設定を編集します。

   > リモートインストールタスクの作成と設定の詳細は、『**Kaspersky Security Center ヘルプ**』を参照してください。

3. 作成したリモートインストールタスクを実行します。

タスクで指定したコンピューターに Kaspersky Security 10.1 コンソールがインストールされます。

Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server のアンインストール

> ネットワークコンピューターでの Kaspersky Security 10.1 for Windows Server 管理アクセス権がパスワードで保護されている場合、複数のアプリケーションアンインストールタスク作成時にパスワードを入力します。パスワード保護が Kaspersky Security Center ポリシーにより集中管理されていない場合、Kaspersky Security 10.1 for Windows Server は、入力したパスワードが設定値に適合したアクセス保護されたサーバーから正常にアンインストールされます。Kaspersky Security 10.1 for Windows Server は、その他のコンピューターからはアンインストールされません。

► **Kaspersky Security 10.1 for Windows Server をアンインストールするには、Kaspersky Security Center の管理コンソールで次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールで、アプリケーションを削除するタスクを作成し、開始します。

2. タスクで、アンインストール方法を選択し(インストール方法の選択と同様。前のセクションを参照)、管理サーバーがサーバーをアドレシングするために権限を使用するアカウントを指定します。Kaspersky Security 10.1 for Windows Server のアンインストールで使用できるのは、既定のアンインストール設定のみです(66 ページのセクション「インストールおよびアンインストールの設定と Windows インストーラーサービスのコマンドラインオプション」を参照)。

Active Directory のグループポリシーを使用したインストールとアンインストール

このセクションでは、Active Directory のグループポリシーを使用した Kaspersky Security 10.1 for Windows Server のインストールとアンインストールについて説明します。グループポリシーを使用して製品をインストールした後の処理についても説明します。

このセクションの内容

Active Directory のグループポリシーを使用した

Kaspersky Security 10.1 for Windows Server のインストール

Active Directory のグループポリシーを使用して複数のサーバーに Kaspersky Security 10.1 for Windows Server をインストールできます。同じ方法で Kaspersky Security 10.1 コンソールもインストールできます。

Kaspersky Security 10.1 for Windows Server または Kaspersky Security 10.1 コンソールのインストール先となるすべてのサーバーが、同じドメインおよび同じ組織単位内に存在している必要があります。

Active Directory のグループポリシーを使用して Kaspersky Security 10.1 for Windows Server をインストールするすべてのサーバーのオペレーティングシステムが、同じバージョンである必要があります（32 ビットまたは 64 ビット）。

ドメイン管理者権限で実行する必要があります。

Kaspersky Security 10.1 for Windows Server をインストールするには、インストールパッケージ ks4ws_x86(x64).msi を使用します。Kaspersky Security 10.1 コンソールをインストールするには、インストールパッケージ ks4wstools.msi を使用します。

> Active Directory のグループポリシーの使用についての詳細な情報は、Microsoft が提供するガイドを参照してください。

► **Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 コンソール）をインストールするには：**

1. インストールされている Microsoft Windows オペレーティングシステムのバージョンのワードサイズ（32 ビットまたは 64 ビット）に対応するインストールパッケージの MSI ファイルを、ドメインコントローラーのパブリックフォルダーに保存します。
2. ドメインコントローラーで、サーバーが所属するグループに対して新しいポリシーを作成します。
3. **グループポリシーオブジェクトのエディター**を使用して、[**コンピューターの構成**]フォルダーで新しいインストールパッケージを作成します。Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 コンソール）のインストールパッケージの MSI ファイルのパスを UNC（ユニバーサルネーミング規約）形式で指定します。

4. Windows インストーラーで、選択したグループの[**コンピューターの構成**]フォルダーと[**ユーザーの構成**]フォルダーの両方で、[**常にシステム特権でインストールする**]を選択します。

5. `gpupdate / force` コマンドで変更を適用します。

グループのコンピューターを再起動すると、Microsoft Windows へのログイン前に Kaspersky Security 10.1 for Windows Server がインストールされます。

Kaspersky Security 10.1 for Windows Server インストール後に実行する処理

保護対象サーバーへの Kaspersky Security 10.1 for Windows Server のインストールが完了したら、ただちに定義データベースをアップデートし、重要領域のスキャンを実行してください。これらの処理(94 ページのセクション「Kaspersky Security 10.1 for Windows Server インストール後に実行する処理」を参照)は、Kaspersky Security 10.1 コンソールから実行できます。

Kaspersky Security 10.1 for Windows Server イベントに関する管理者への通知を設定することもできます。

Active Directory のグループポリシーを使用した Kaspersky Security 10.1 for Windows Server のアンインストール

Active Directory のグループポリシーを使用してグループ内のサーバーに Kaspersky Security 10.1 for Windows Server(または Kaspersky Security 10.1 コンソール)をインストールした場合、Active Directory のグループポリシーを使用して Kaspersky Security 10.1 for Windows Server(または Kaspersky Security 10.1 コンソール)をアンインストールすることもできます。

この方法で Kaspersky Security 10.1 for Windows Server をアンインストールする場合、使用できるのは既定のアンインストール設定だけです。

Active Directory のグループポリシーの使用についての詳細な情報は、Microsoft が提供するガイドを参照してください。

アプリケーション管理アクセス権がパスワード保護されている場合、Active Directory グループポリシーを使用して Kaspersky Security 10.1 for Windows Server をアンインストールすることはできません。

► **Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 コンソール）をアンインストールするには:**

1. Kaspersky Security 10.1 for Windows Server または Kaspersky Security 10.1 コンソールを削除するサーバーのドメインコントローラーで、組織単位を選択します。

2. Kaspersky Security 10.1 for Windows Server のインストール用に作成したポリシーを選択し、**グループポリシーエディター**の［**ソフトウェア インストール**］フォルダー（［**コンピューターの構成**］ - ［**ソフトウェア設定**］ - ［**ソフトウェア インストール**］）で Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 コンソール）のインストールパッケージのコンテキストメニューを開き、［**すべてのタスク**］ - ［**削除**］コマンドを選択します。

3. ［**直ちに、ソフトウェアをユーザーとサーバーからアンインストールする**］のアンインストール方法を選択します。

4. `gpupdate / force` コマンドで変更を適用します。

サーバーを再起動すると、Microsoft Windows へのログイン前に Kaspersky Security 10.1 for Windows Server がコンピューターから削除されます。

Kaspersky Security 10.1 for Windows Server 機能チェック:テスト用ウイルス EICAR の使用

このセクションでは、テスト用ウイルス EICAR について、またこのテスト用ウイルスを使用して Kaspersky Security 10.1 for Windows Server のリアルタイム保護機能およびオンデマンドスキャン機能を検証する方法について説明します。

このセクションの内容

テスト用ウイルス EICAR について

EICAR はアンチウイルス製品の動作検証を目的としたテスト用ウイルスです。European Institute for Computer Antivirus Research(EICAR)により開発されました。

> このテスト用ウイルスはウイルスではなく、お使いのコンピューターに損害を与える可能性のあるプログラムコードは含まれていません。それにもかかわらず多くの製造元のアンチウイルス製品によって、脅威として検知されます。

このテスト用ウイルスを含むファイルは eicar.com と呼ばれます。EICAR の Web サイトからダウンロードできます(http://www.eicar.org/anti_virus_test_file.htm)。

コンピューターのハードディスクにファイルを保存する前に、そのディスクのファイルのリアルタイム保護が無効になっていることを確認してください。

eicar.com ファイルには、1 行のテキストが含まれています。このファイルをスキャンする際、Kaspersky Security 10.1 for Windows Server がこの文字列の中でテスト用の脅威を検知し、このファイルに対し「**感染**」のステータスを割り当て、ファイルを削除します。ファイルで検知された脅威に関する情報は、Kaspersky Security 10.1 コンソールおよびタスク実行ログに表示されます。

ファイル eicar.com を使用して、Kaspersky Security 10.1 for Windows Server が感染したオブジェクトをどのようにして駆除するか、また Kaspersky Security 10.1 for Windows Server がどうやって感染の可能性があるオブジェクトを検知するかを確認できます。それには、テキストエディタを使用してファイルを開き、ファイル内のテキスト行の先頭に、次の表にリストされた接頭辞の 1 つを追加して、新しい名前（たとえば eicar_cure.com）でファイルを保存します。

接頭辞を追加したファイル eicar.com が Kaspersky Security 10.1 for Windows Server によって問題なく処理されることを確認するには、［**オブジェクトの保護**］セキュリティ設定セクションで、Kaspersky Security 10.1 for Windows Server のファイルのリアルタイム保護タスク既定のオンデマンドスキャンタスクに対して［**すべてのオブジェクト**］の値を設定します。

表 14. EICAR ファイルの接頭辞

接頭辞	スキャンおよび Kaspersky Security 10.1 for Windows Server 処理後のファイルステータス
接頭辞なし	Kaspersky Security 10.1 for Windows Server によって「**感染**」のステータスが割り当てられ、オブジェクトが削除されます。
SUSP-	Kaspersky Security 10.1 for Windows Server によって「**感染の可能性あり**」のステータスが割り当てられ、オブジェクト（ヒューリスティックアナライザーによって検知）が削除されます（感染の可能性があるオブジェクトは駆除されません）。
WARN-	Kaspersky Security 10.1 for Windows Server によって「**感染の可能性あり**」のステータスが割り当てられ、オブジェクト（オブジェクトのコードが既知の脅威のコードと部分的に一致）が削除されます（感染の可能性があるオブジェクトは駆除されません）。
CURE-	Kaspersky Security 10.1 for Windows Server によって「**感染**」のステータスが割り当てられ、オブジェクトが駆除されます。駆除に成功した場合、ファイル全体のテキストが「CURE」という単語に置き換わります。

リアルタイム保護テストとオンデマンドスキャンテスト

Kaspersky Security 10.1 for Windows Server のインストール後、Kaspersky Security 10.1 for Windows Server による悪意あるコードが含まれるオブジェクト検出を確認できます。確認は、テスト用ウイルス EICAR を使用して行えます（「テスト用ウイルス EICAR について」（123 ページ）を参照）。

► **リアルタイム保護機能を確認するには、次の手順を実行します：**

1. EICAR の Web サイト（http://www.eicar.org/anti_virus_test_file.htm）からファイル eicar.com をダウンロードします。ネットワークにある任意のコンピューターのローカルドライブのパブリックフォルダーに

保存します。

> パブリックフォルダーに保存する前に、このフォルダーのファイルのリアルタイム保護が無効になっていることを確認してください。

2. ネットワークユーザー通知の動作を確認する場合は、保護対象サーバーとファイル eicar.com を保存したコンピューターの両方で、Microsoft Windows のメッセージングサービスが無効になっていることを確認してください。

3. Kaspersky Security 10.1 コンソールを開く

4. 次のいずれかの方法を使用して、保存したファイル eicar.com を保護対象サーバーのローカルドライブにコピーします:

   - ターミナルサービスのウィンドウを通して通知のテストを行う場合、リモートデスクトップ接続ユーティリティを使用してサーバーに接続してから、ファイル eicar.com をサーバーにコピーします。

   - Microsoft Windows Messenger サービスを使用して通知をテストするには、eicar.com ファイルを保存したコンピューターのネットワークの場所を使用してファイルをコピーします。

次に条件を満たすと、ファイルのリアルタイム保護が正常に機能していることになります:

- ファイル eicar.com が、保護対象サーバーから削除されている。

- Kaspersky Security 10.1 コンソールで、タスク実行ログに「**緊急**」のステータスが割り当てられている。ファイル eicar.com 内の脅威に関する情報がログの行に表示されます。(実行ログを確認するには、Kaspersky Security 10.1 コンソールで[**サーバーのリアルタイム保護**]フォルダーを展開し、ファイルのリアルタイム保護タスクを選択します。詳細パネルで[**実行ログを開く**]をクリックします)。

  - 次の Microsoft Windows Messenger Service メッセージが、ファイルのコピー元のコンピューターに表示されます:`Kaspersky Security 10.1 for Windows Server blocked access to <path to file on the computer>¥eicar.com on computer <network name of computer> at <time that event occurred>` (`Kaspersky Security 10.1 for Windows Server` は `<`イベント発生時`>` にコンピューター `<`コンピューターのネットワーク名`>` の `<`コンピューター上のファイルへのパス`>¥eicar.com` へのアクセスをブロックし

ました。) Reason: Threat detected.(理由:脅威の検出。) Virus: EICAR-Test-File.(ウイルス:EICAR-Test-File。) User name: <user name>.(ユーザー名:<ユーザー名>。) Computer name: <network name of the computer from which you copied the file>.(コンピューター名:<ファイルのコピー元であるコンピューターのネットワーク名>。)

ファイル eicar.com のコピー元であるコンピューターで、Microsoft Windows Messenger サービスが機能していることを確認してください。

► **オンデマンドスキャン機能を確認するには、次の手順を実行します:**

1. EICAR の Web サイト(http://www.eicar.org/anti_virus_test_file.htm)からファイル eicar.com をダウンロードします。ネットワークにある任意のコンピューターのローカルドライブのパブリックフォルダーに保存します。

   パブリックフォルダーに保存する前に、このフォルダーのファイルのリアルタイム保護が無効になっていることを確認してください。

2. Kaspersky Security 10.1 コンソールを開く

3. 次の操作を行います:

   a. Kaspersky Security 10.1 コンソールツリーで、[**オンデマンドスキャン**]フォルダーを展開します。

   b. [**重要領域のスキャン**]サブフォルダーを選択します。

   c. [**スキャン範囲の設定**]タブで、[**ネットワーク**]フォルダーのコンテキストメニューを開いて、[**ネットワークファイルの追加**]を選択します。

   d. リモートコンピューターで、ファイル eicar.com のネットワークパスを UNC(ユニバーサルネーミング規約)形式で入力します。

e. チェックボックスをオンにして、追加したネットワークのパスをスキャン範囲に含めます。

f. 重要領域のスキャンタスクを実行します。

次の条件を満たすと、オンデマンドスキャンが正常に機能していることになります:

- ファイル eicar.com が、コンピューターのハードディスクから削除されている。
- Kaspersky Security 10.1 コンソールで、実行ログに「**緊急**」のステータスが割り当てられている。重要領域のスキャンタスクの実行ログに、ファイル eicar.com 内の脅威に関する情報の行が表示されます(実行ログを確認するには、Kaspersky Security 10.1 コンソールで[**オンデマンドスキャン**]フォルダーを展開し、重要領域のスキャンタスクを選択します。詳細パネルで[**実行ログを開く**]をクリックします。

アプリケーションインターフェイス

ローカルコンソールや Kaspersky Security Center 管理プラグインを介して Kaspersky Security 10.1 for Windows Server を管理できます。ローカルコンソールでの処理については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』で説明されています。Kaspersky Security Center 管理コンソールのインターフェイスを使用して、管理プラグインで処理できます。Kaspersky Security Center インターフェイスの詳細情報は、Kaspersky Security Center のガイドに記載されています。

ライセンス

このセクションでは、本製品のライセンスに関する主要な概念について説明します。

この章の内容

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 との間で締結される拘束力のある契約であり、製品の使用条件を規定しています。

製品の使用を開始する前に、使用許諾契約書の条件をよくお読みください。

使用許諾契約書の条件は、次のような方法で確認できます:

- Kaspersky Security 10.1 for Windows Server インストール時
- ファイル license.txt で確認できます。使用許諾契約書は、本製品の配布キットに含まれています。

本製品のインストール中に使用許諾契約書に同意すると、使用許諾契約書の条件に同意したことになります。使用許諾契約書の条件に同意しない場合は、製品のインストールを終了するか、製品の使用を中止する必要があります。

ライセンスについて

ライセンスは、使用許諾契約書に基づいて提供される、製品を使用する期限付きの権利です。

有効なライセンスを取得すると、次のサービスを利用できます:

- 使用許諾契約書の条件に基づいた製品の使用
- テクニカルサポート

サービスの範囲と製品の使用期間は、アクティベーションに使用したライセンスの種別によって異なります。

次のライセンスの種別があります:

- **試用版**ライセンスは、製品の試用を目的とした無償のライセンスです。

試用版ライセンスは短期間有効です。試用版ライセンスの有効期間が終了すると、Kaspersky Security 10.1 for Windows Server の機能が制限されます。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。

試用版ライセンスで製品をアクティベートできるのは 1 回だけです。

- **製品版ライセンス**は、製品の購入時に提供される有償のライセンスです。

  製品版ライセンスの有効期間が終了した場合、製品は継続して機能しますが、一部の機能が使用できなくなります（Kaspersky Security の定義データベースをアップデートできないなど）。Kaspersky Security 10.1 for Windows Server のすべての機能を継続して使用するには、製品版ライセンスを更新する必要があります。

セキュリティ脅威からコンピューターを最大限に保護するために、有効期間が終了する前にライセンスを更新するようにしてください。

Kaspersky Security 10.1 for Windows Server はライセンスの有効期限日の追跡を継続的に行いません。有効期限切れのライセンスでプログラムをもう一度アクティブにする場合（初回のアクティベーションコードがアクティブな間に）、有効なライセンスを使用してアクティベーションコードを再度追加する必要があります。

ライセンス証明書について

ライセンス証明書は、ライセンス情報ファイルやアクティベーションコードと一緒に提供されるドキュメントです。

ライセンス証明書には、提供されるライセンスに関する次の情報が含まれます：

- 注文番号
- ライセンスを付与されたユーザーに関する情報
- 提供されるライセンスでアクティベートできる製品に関する情報
- ライセンス単位数の上限（たとえば、提供されるライセンスの下でアプリケーションを使用できるデバイス）

- ライセンスの有効期間の開始日
- ライセンス有効期限またはライセンス期間
- ライセンスの種別

ライセンスの種別について

Kaspersky Security 10.1 for Windows Server は、企業を保護する各種ソリューションの一部です。Kaspersky Security 10.1 for Windows Server で利用できる機能は、選択するソリューションによって異なります。次の表に、提供されているソリューションのタイプと、各ソリューションで利用できる製品機能を示します。

Kaspersky Endpoint Security for Business Basic	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理

Kaspersky Endpoint Security for Business Select	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理
Kaspersky Endpoint Security for Business Advanced	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 アプリケーション起動コントロール デバイスコントロール トラフィックセキュリティ

Kaspersky Endpoint Security for Business Total	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 アプリケーション起動コントロール デバイスコントロール トラフィックセキュリティ
Kaspersky Security for File Servers	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 アプリケーション起動コントロール デバイスコントロール ファイル変更監視 Windows イベントログ監視 トラフィックセキュリティ（外部プロキシモードは使用できません）

Kaspersky Security for Data Storage Systems	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 アプリケーション起動コントロール デバイスコントロール ファイル変更監視 Windows イベントログ監視 トラフィックセキュリティ NAS 保護（ストレージ） + NAS 用アンチクリプター
Kaspersky Security for Virtualization	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 デバイスコントロール トラフィックセキュリティ

Kaspersky Security for xSP	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック ファイアウォール管理 トラフィックセキュリティ
Kaspersky Hybrid Cloud Security	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 デバイスコントロール トラフィックセキュリティ

Kaspersky Hybrid Cloud Security Enterprise	
定額制サービスによって使用可能	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 ファイル変更監視 Windows イベントログ監視 アプリケーション起動コントロール デバイスコントロール トラフィックセキュリティ
AWS プリペイド定額制サービス	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック アンチクリプター（共有フォルダー用） ファイアウォール管理 ファイル変更監視 Windows イベントログ監視 アプリケーション起動コントロール トラフィックセキュリティ デバイスコントロール
Kaspersky Security Internet Gateway	

Kaspersky Security Internet Gateway	
コンポーネント	ファイルウイルス対策 脆弱性攻撃ブロック ファイアウォール管理 トラフィックセキュリティ

ライセンス情報について

ライセンスは、使用許諾契約書の条件に従って本製品をアクティベートして利用するのに使用する数値列です。ライセンスはカスペルスキーが生成します。

本製品にライセンスを追加するには、ライセンス情報ファイルを使用します。本製品にライセンスを追加すると、ライセンスは製品インターフェイスに一意の英数字文字列として表示されます。

カスペルスキーは、使用許諾契約書に違反したライセンスをブラックリストに掲載します。ライセンスがブロックされた場合、本製品を動作させるためには、別のライセンス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」と「予備のライセンス」があります。

現在のライセンスは、製品が機能するために現在使われているライセンスです。試用版または製品版のライセンスを現在のライセンスとして追加できます。本製品で使用できる現在のライセンスは、1 つのみです。

予備のライセンスは、製品を使用する権限を確認する、現在使用されていないライセンスです。現在のライセンスの有効期間が終了した場合、自動的に予備のライセンスがアクティブになります。予備のライセンスは、現在のライセンスが適用されている場合のみ追加できます。

試用版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。

アクティベーションコードについて

アクティベーションコードは、Kaspersky Security 10.1 for Windows Server の商用ライセンス購入後に受け取るコードです。このコードは、ライセンスファイルを受け取り、ライセンスファイルをインストールしてアプリケーションをアクティベートするために必要です。

アクティベーションコードは xxxxx-xxxxx-xxxxx-xxxxx という形式の 20 桁の数字およびアルファベットの列です。

ライセンスの使用期間は、アプリケーションをアクティベートしたときに開始されます。複数のコンピューターで Kaspersky Security 10.1 for Windows Server を使用するライセンスを購入した場合、ライセンス使用期間は、アプリケーションが 1 台目のコンピューター上でアクティベートされたときに始まります。

アクティベーションコードを紛失したかうっかり削除した場合、復元するには Kaspersky Lab テクニカルサポートにリクエストを送信する必要があります。

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、カスペルスキーから受信する .key という拡張子の付いたファイルです。ライセンス情報ファイルを使って、ライセンスを追加して製品をアクティベートします。

ライセンス情報ファイルは、Kaspersky Security 10.1 for Windows Server の購入時、または Kaspersky Security 10.1 for Windows Server の試用版の注文時に入力したメールアドレス宛に送信されます。

ライセンス情報ファイルで製品をアクティベートする際に、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

ライセンス情報ファイルは、誤って削除しても復元できます。カスペルスキーカンパニーアカウントへの登録に、ライセンス情報ファイルが必要となる場合があります。

ライセンス情報ファイルを復元するには、次のいずれかの操作を行います:

- テクニカルサポートへのお問い合わせ（https://support.kaspersky.co.jp/）

- 既存のアクティベーションコードに基づき、カスペルスキーの Web サイトからライセンス情報ファイルを取得する。

データの提供について

Kaspersky Security 10.1 for Windows Server の使用許諾契約の「データ処理の条件」という項には、このガイドに記載されているデータの送信および処理に関する諸条件、責任、手順が明記されています。使用許諾契約に同意する前に、その条項ならびに使用許諾契約にリンクされているすべての文書を慎重に確認してください。

お客様から Kaspersky Lab に送信されるデータは、プライバシーポリシーに（www.kaspersky.com/Products-and-Services-Privacy-Policy）に従って保護され、処理されます。

使用許諾契約の条項に同意することにより、お客様は次の情報を Kaspersky Lab に自動的に送信することに同意するものとします：

- アップデートを受信するメカニズムをサポートするため - インストールされている製品とライセンス証明書に関する情報：インストールされている製品の識別子と完全なバージョン（ビルド番号、種別、ライセンス識別子、インストール識別子、一意のアップデートタスク識別子など）。

- アプリケーションエラーが発生したときにナレッジベースの記事を参照する機能を使用するため（リダイレクターサービス） - 製品とリンク種別に関する情報：具体的には、製品の名前、ロケール、完全バージョン番号、リダイレクトリンクの種別、エラー識別子。

- データ処理についての承認を管理するための情報 - データ転送に関する条項を定めた使用許諾契約書やその他のドキュメントの承認状態に関する情報：
  使用許諾契約書やその他のドキュメントの識別子またはバージョン（データの処理に関する条項を承認または拒否した部分）、属性、ユーザー動作での表示（条件承認の確認）、データの処理に関する条項の承認に関するステータス変更の日時。

ローカルでのデータ処理

このガイドで説明している製品の主要な機能を実行しているときに、Kaspersky Security 10.1 for Windows

Server は、一連のデータをローカルで処理し、保護対象サーバーに保存します:

- スキャンしたファイルと検知したオブジェクトに関する情報(処理したファイルの名前と属性、スキャンしたメディア上での処理したファイルの完全パス、スキャンしたファイルに対して実行された処理、保護対象のネットワークや保護対象のサーバー上で処理を実行するユーザーのアカウント、スキャンしたデバイスの名前とデータ、システム上で実行中のプロセスに関する情報など)。
- オペレーティングシステムの動作と設定に関する情報(Windows ファイアウォール設定、Windows イベントログのエントリー、ユーザーアカウントの名前、開始された実行ファイルのインスタンス、およびこれらのファイルの種別、名前、チェックサム、属性など)。
- Web アクティビティに関する情報(処理した URL、割り当てたカテゴリ、ダウンロードされたオブジェクトに関するデータ、処理したデジタル証明書の属性、処理したメールに関するデータ(送信者、受信者、件名、メッセージの本文、添付ファイルなどを含む)など)。
- ネットワークアクティビティに関する情報(ブロックしたクライアントコンピューターの IP アドレスなど)。

Kaspersky Security 10.1 for Windows Server は、製品イベントの記録や診断データの受信などの製品の基本機能の一部として、データの処理と保存を行います。ローカルで処理されたデータは、設定して適用された製品設定に従って処理および保護されます。

Kaspersky Security 10.1 for Windows Server では、ローカルで処理されたデータに対して保護レベルを設定できます。たとえば、処理するデータへのアクセスに関するユーザー権限の変更、そのようなデータの保存期間の変更、データの記録を伴う機能全体または一部の無効化、データが記録されているドライブのフォルダーのパスと属性の変更などができます。

データ処理を含む製品機能の設定の詳細は、本ガイドの該当するセクションを参照してください。

ライセンスによるアプリケーションのアクティベーション

キーを適用して Kaspersky Security 10.1 for Windows Server をアクティベートできます。

Kaspersky Security 10.1 for Windows Server に現在のライセンスがすでに追加されている場合、別のライセンスを現在のライセンスとして追加すると、新しいライセンスが以前に追加されたライセンスと置き換わります。以前にインストールした現在のライセンスは削除されます。

Kaspersky Security 10.1 for Windows Server に予備のライセンスがすでに追加されている場合、別のライセンスを予備として追加すると、新しいライセンスが以前に追加されたライセンスと置き換わります。以前にインストールした予備のライセンスは削除されます。

Kaspersky Security 10.1 for Windows Server に現在のライセンスと予備のライセンスがすでに追加されている場合、新しいライセンスを現在のライセンスとして追加すると、新しいライセンスが以前に追加された現在のライセンスと置き換わって予備のライセンスが削除されます。

► **ライセンスを使用して Kaspersky Security 10.1 for Windows Server をアクティベートするには、次の手順を実行します:**

1. Kaspersky Security 10.1 コンソールツリーで、[**ライセンス**]フォルダーを展開します。
2. [**ライセンス**]フォルダーの詳細ペインで、[**ライセンス情報ファイルの追加**]をクリックします。
3. 表示されるウィンドウで[**参照**]をクリックし、拡張子が .key のライセンス情報ファイルを選択します。

   予備のライセンスとして追加することもできます。ライセンスを予備として追加するには、[**予備のライセンスとして使用する**]をオンにします。

4. [**OK**]をクリックします。

選択したライセンスが適用されます。追加されるライセンスに関する情報は[**ライセンス**]フォルダーにあります。

現在のライセンスに関する情報の表示

ライセンス情報の表示

現在のライセンスの情報は、Kaspersky Security 10.1 コンソールにある[**Kaspersky Security**]フォルダーの詳細ペインに表示されます。ライセンスのステータスには、次の値が使用されます:

- **ライセンスのステータスを確認しています** - Kaspersky Security 10.1 for Windows Server は、追加されたライセンス情報ファイル、または適用されたアクティベーションコードをチェックして、現在のライセンスのステータスに関する対応を待ちます。
- **ライセンスの有効期限** - Kaspersky Security 10.1 for Windows Server は指定された日時までアクティベートされています。次の場合にライセンスのステータスが黄色で表示されます:
  - ライセンスの有効期間の残り日数が 14 日で、予備のライセンスまたはアクティベーションコードが追加されていない
  - 追加されたライセンスがブラックリストに含まれていて、ブロックされる予定である
- **製品がアクティベートされていません** - ライセンスが追加されていないか、アクティベーションコードが適用されていないため、Kaspersky Security 10.1 for Windows Server はアクティベートされていません。ステータスは赤色で表示されます。
- **ライセンスの有効期間が終了しました** - ライセンスの有効期間が終了したため、Kaspersky Security 10.1 for Windows Server はアクティベートされていません。ステータスは赤色で表示されます。
- **使用許諾契約書に違反しています** - 使用許諾契約書の条件に違反しているため、Kaspersky Security 10.1 for Windows Server はアクティベートされていません(131 ページのセクション「使用許諾契約書について」を参照)。ステータスは赤色で表示されます。
- **ライセンスがブラックリストに掲載されています** - ライセンス情報ファイルが第三者によって不正にアクティベートするために使用されたなどの理由から、追加されたライセンスがブロックされ、カスペルスキーによってブラックリストに登録されています。ステータスは赤色で表示されます。

- **定額制サービスを一時停止しました** - 定額制サービスが一時的に停止されています。ステータスは赤色で表示されます。定額制サービスはいつでも更新できます。

現在のライセンスに関する情報の表示

► **現在のライセンスに関する情報を表示するには:**

Kaspersky Security 10.1 コンソールツリーで、[**ライセンス**]フォルダーを展開します。

現在のライセンスの全般的な情報が、[**ライセンス**]フォルダーの詳細ペインに表示されます(次の図を参照)。

表 15. [ライセンス]フォルダーで表示されるライセンスの全般的な情報

フィールド	説明
アクティベーションコード	アクティベーションコードの番号。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した場合に、表示されます。
アクティベーションステータス	製品のアクティベーションのステータス情報。[ライセンス]フォルダーのコントロール パネル内にある[アクティベーションステータス]に表示される情報は、次の値を含みます: • **適用済み** – アクティベーションコードまたはライセンスを使用して製品をアクティベートした場合。 • **アクティベーション** – アクティベーションコードを適用してアプリケーションをアクティベートしたが、アクティベーションのプロセスがまだ完了していない場合。製品のアクティベートが完了し、フォルダーの詳細ペインの内容が更新されると、ステータスの値は[適用済み]に変更します。 • **アクティベーションエラー** – 製品がアクティベーションできなかった場合。アクティベーションエラーの原因は、タスク実行ログで確認できます。
ライセンス	製品をアクティベートする際に使用したライセンスの番号。
ライセンスの種別	ライセンスの種別:製品版または試用版。
有効期限	現在のライセンスの有効期限の日時。

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ステータス	アクティベーションコードのステータス、またはキーステータス：アクティブまたは追加。

► **ライセンスの詳細情報を確認するには：**

[**ライセンス**]フォルダーの、展開するライセンスデータの文字列上でコンテキストメニューを開き、[**プロパティ**]を選択します。

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プロパティウィンドウの[**全般**]タブでは、現在のライセンスの詳細情報が表示されます。[**詳細設定**]タブでは、お客様の情報と、カスペルスキーまたは Kaspersky Security 10.1 for Windows Server を購入した販売店の問い合わせ先の詳細が表示されます（下の表を参照）。

表 16. ライセンス情報ファイルのプロパティウィンドウで表示されるライセンスの詳細情報

フィールド	説明
[全般]タブ	
識別 ID	製品をアクティベートする際に使用したライセンスの番号。
ライセンス追加日	本製品にライセンスが追加された日付。
ライセンスの種別	ライセンスの種別：製品版または試用版。
有効期間終了までの日数	現在のライセンスの有効期限までの残り日数。
有効期限	現在のライセンスの有効期限の日時。無制限の定額制サービスで製品をアクティベートした場合、値は**無制限**と表示されます。ライセンスの有効期限が特定できない場合、値は**不明**と設定されます。

アプリケーション	そのライセンスでアクティベートされたアプリケーションの名前または追加されたアクティベーションコード。
機能制限	ライセンス使用の制限（存在する場合）。
テクニカルサポート利用可能	使用許諾契約書に従ってカスペルスキーまたはいずれかのパートナー企業からお客様向けにテクニカルサポートが提供されるかどうかに関する情報。
［詳細設定］タブ	
ライセンス情報	現在のライセンスの名前と種別。
サポート情報	カスペルスキーまたはテクニカルサポートを提供するパートナーの連絡先の詳細。テクニカルサポートが提供されていない場合は空欄のことがあります。
所有者情報	ライセンス所有者のお客様情報：お客様の名前およびライセンスを取得している組織の名前。

ライセンスの有効期限が切れた場合の機能の制限

現在のライセンスの有効期限が切れた場合、機能コンポーネントの操作に以下の制限が適用されます：

- ファイルのリアルタイム保護タスク、オンデマンドスキャンタスク、およびアプリケーションの整合性チェックタスク以外のすべてのタスクが停止します。
- リアルタイム保護タスク、オンデマンドスキャンタスク、およびアプリケーションの整合性チェックタスク以外のタスクの起動は、拒否されます。これらのタスクは、古い定義データベースで引き続き実行されます。

- 脆弱性攻撃ブロックが制限されます:
  - プロセスは再起動されるまで保護されます。
  - 新しいプロセスを保護範囲に追加することはできません。

その他の機能(保管領域、ログ、診断情報)は引き続き利用可能です。

ライセンスの更新

既定で、ライセンスの有効期限までの日数が 14 日になると、Kaspersky Security 10.1 for Windows Server より通知が表示されます。この場合、[**Kaspersky Security**]ノードの詳細ペインのステータス[**ライセンスの有効期限**]が黄色で表示されます。

予備ライセンスまたはアクティベーションコードを使用して、切れる前にライセンスの有効期限を更新できます。これにより、既存のライセンスの有効期限が切れてから新しいライセンスで製品をアクティベートするまでのあいだ、コンピューターは保護された状態を保つことができます。

► ライセンスを更新するには、次の手順を実行します:

1. 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新たに購入します。
2. Kaspersky Security 10.1 コンソールツリーで、[**ライセンス**]フォルダーを開きます。
3. [**ライセンス**]フォルダーの詳細ペインで、次のいずれかの処理を実行します:
   - 予備のライセンスを使用して更新する場合:
     a. [**ライセンス情報ファイルの追加**]をクリックします。
     b. 表示されるウィンドウで[**参照**]をクリックし、拡張子が .key の新しいライセンス情報ファイルを選択します。
     c. [**予備のアクティベーションコードとして使用する**]をオンにします。
   - アクティベーションコードを使用して更新する場合:
     a. [**アクティベーションコードの追加**]をクリックします。
     b. 表示されるウィンドウで、購入済みのアクティベーションコードを入力します。

c. [**予備のアクティベーションコードとして使用する**]をオンにします。

アクティベーションコードを適用するには、インターネット接続が必要です。

4. [**OK**]をクリックします。

予備のライセンスまたはアクティベーションコードは、現在のライセンスの有効期限が切れると自動的に適用されます。

ライセンスの削除

追加されたライセンスを削除できます。

Kaspersky Security 10.1 for Windows Server に予備のライセンスが追加されている場合、現在のライセンスを削除すると、予備のライセンスが自動的に現在のライセンスになります。

追加されたライセンスを削除した場合、ライセンス情報ファイルを再度適用しないと削除したライセンスを復元できません。

► **追加されたライセンスを削除するには:**

1. Kaspersky Security 10.1 コンソールツリーで、[**ライセンス**]フォルダーを選択します。
2. [**ライセンス**]フォルダーの詳細ペインにある追加されているライセンスに関する情報の表で、削除するライセンスを選択します。
3. 選択したライセンスの情報が表示されている行のコンテキストメニューで[**削除**]を選択します。
4. 確認ウィンドウで[**はい**]をクリックしてライセンスを削除することを確認します。

選択したライセンスが削除されます。

Kaspersky Security 10.1 for Windows Server の開始と停止

このセクションでは、Kaspersky Security 10.1 for Windows Server 管理プラグインおよび Kaspersky Security サービスの開始と停止について説明します。

この章の内容

Kaspersky Security Center 管理プラグインの開始

Kaspersky Security 10.1 for Windows Server の作業を実行する Kaspersky Security Center プラグインの開始に、追加の処理は必要ありません。管理者のコンピューターにインストールされたプラグインは Kaspersky Security Center と同時に開始されます。Kaspersky Security Center の開始についての詳細情報は、『**Kaspersky Security Center ヘルプ**』を参照してください。

Kaspersky Security サービスの開始と停止

既定では、Kaspersky Security サービスはオペレーティングシステムの起動時に自動で開始します。Kaspersky Security サービスは、リアルタイム保護、ローカルアクティビティの管理、ネットワーク接続ストレージの保護、オンデマンドスキャン、およびアップデートタスクが実行されるときの処理プロセスを管理します。

既定では、Kaspersky Security 10.1 for Windows Server の開始時に、ファイルのリアルタイム保護タスク、スクリプト監視タスク（インストールされている場合）、オペレーティングシステムの起動時のスキャンタスク、および

アプリケーションの整合性チェックタスクが開始されます。さらに、**アプリケーションの起動時**に開始するようにスケジュールされたその他のタスクも開始されます。

Kaspersky Security サービスが停止されると、実行中のすべてのタスクが停止されます。Kaspersky Security サービスの再起動後には、スケジュールで起動の頻度が[**アプリケーションの起動時**]に設定されたタスクのみが自動的に開始されます。それ以外のタスクは手動で開始する必要があります。

Kaspersky Security サービスは、[**Kaspersky Security**]フォルダーのコンテキストメニューまたは Microsoft Windows の[**サービス**]スナップインを使用して開始および停止することもできます。

保護対象のサーバーの管理者グループのメンバーは、Kaspersky Security 10.1 for Windows Server を開始および停止することができます。

► **管理コンソールを使用してアプリケーションを停止または開始するには、次の手順を実行します:**

1. Kaspersky Security 10.1 コンソールツリーで、[**Kaspersky Security**]フォルダーのコンテキストメニューを開きます。
2. 次のいずれかの項目を選択します:
   - **サービスの停止**
   - **サービスの起動**

Kaspersky Security サービスが開始または停止します。

Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限

このセクションでは、Kaspersky Security 10.1 for Windows Server を管理するための権限およびアプリケーションによって登録される Windows サービスを管理するための権限に関する情報と、それらの権限の設定方法について説明します。

この章の内容

Kaspersky Security 10.1 for Windows Server を管理するための権限について

既定では、保護対象サーバーの管理者グループのユーザー、Kaspersky Security 10.1 for Windows Server のインストール時に保護対象サーバーに作成された KAVWSEE Administrators グループのユーザー、および SYSTEM システムグループに、Kaspersky Security 10.1 for Windows Server の全機能に対するアクセス権が付与されます。

Kaspersky Security 10.1 for Windows Server の[**編集**]権限機能へのアクセス権を持つユーザーは、保護対象サーバーに登録された他のユーザー、またはドメイン内の他のユーザーに対し、Kaspersky Security 10.1 for Windows Server の各種機能へのアクセス権を付与することができます。

Kaspersky Security 10.1 for Windows Server ユーザーのリストに登録されていないユーザーは、Kaspersky Security コンソールを開くことができません。

ユーザーまたはユーザーのグループに対し、次のいずれかの設定済み Kaspersky Security 10.1 for Windows Server アクセス権限レベルを選択できます:

- **フルコントロール** - 製品のすべての機能に対するアクセス。Kaspersky Security 10.1 for Windows Server の全般設定、コンポーネント設定、および Kaspersky Security 10.1 for Windows Server ユーザーの権限を表示および編集でき、Kaspersky Security 10.1 for Windows Server の統計情報を表示できます。

- **編集** - ユーザー権限の編集以外のすべてのアプリケーションの機能へのアクセス。Kaspersky Security 10.1 for Windows Server および Kaspersky Security コンポーネント設定の全般的な設定を表示、編集できます。

- **読み取り** - Kaspersky Security 10.1 for Windows Server 全般設定、Kaspersky Security 10.1 for Windows Server コンポーネント設定、Kaspersky Security 10.1 for Windows Server 統計、Kaspersky Security 10.1 for Windows Server ユーザー権限を表示できます。

詳細なアクセス権限を設定して(159 ページの「Kaspersky Security 10.1 for Windows Server と Kaspersky Security サービスを管理するためのアクセス権限の設定」を参照)、特定の Kaspersky Security 10.1 for Windows Server の機能へのアクセスを許可またはブロックすることもできます。

ユーザーまたはグループのアクセス権限を手動で設定した場合、該当のユーザーまたはグループには[**高度なアクセス許可**]のアクセスレベルが設定されます。

表 17. Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限

ユーザー権限	説明
タスク管理	Kaspersky Security 10.1 for Windows Server タスクを開始、停止、一時停止、または再開できます。
オンデマンドスキャンタスクの作成および削除	オンデマンドスキャンタスクを作成および削除できます。
設定の編集	以下の操作を実行できます: • 設定ファイルからの Kaspersky Security 10.1 for Windows Server の設定のインポート。 • 製品設定の編集。
設定の読み取り	以下の操作を実行できます: • Kaspersky Security 10.1 for Windows Server 全般設定とタスク設定の表示。 • Kaspersky Security 10.1 for Windows Server 設定の設定ファイルのエクスポート。 • 実行ログ、システム監査ログ、および通知に関する設定の表示
保管領域の管理	以下の操作を実行できます: • オブジェクトの隔離への移動 • 隔離およびバックアップからのオブジェクトの削除 • 隔離およびバックアップからのオブジェクトの復元
ログの管理	タスク実行ログとシステム監査ログを削除できます。
ログの読み取り	タスク実行ログとシステム監査ログのアンチウイルスイベントを表示できます。

統計情報の読み取り	各 Kaspersky Security 10.1 for Windows Server タスクの統計を表示できます。
ライセンス	Kaspersky Security 10.1 for Windows Server はアクティベートまたは非アクティベートできます。
アプリケーションのアンインストール	Kaspersky Security 10.1 for Windows Server をアンインストールできます。
権限の読み取り	Kaspersky Security 10.1 for Windows Server ユーザーのリストと、各ユーザーのアクセス権限を表示できます。
権限の編集	以下の操作を実行できます: • アプリケーション管理のアクセス権を持つユーザーリストの編集 • Kaspersky Security 10.1 for Windows Server の各種機能に対するユーザーアクセス権限を編集します。

Kaspersky Security サービスを管理するための権限について

Kaspersky Security 10.1 for Windows Server はインストール中に Kaspersky Security サービス(KAVFS)を Windows に登録し、オペレーティングシステムの起動時に機能コンポーネントを内部で起動できるようにします。Kaspersky Security サービスの管理を介して第三者によって保護対象サーバーのアプリケーション機能やセキュリティ設定にアクセスされるリスクを低下させるために、ローカルの Kaspersky Security 10.1 コンソールや Kaspersky Security Center Administration プラグインから Kaspersky Security サービスを管理する権限を制限することができます。

既定では、Kaspersky Security サービスを管理するためのアクセス権限は、保護対象サーバーで「管理者」グ

ループに登録されているユーザー、読み取り権限を持つ SERVICE および INTERACTIVE のグループ、および読み取りと実行権限を持つ SYSTEM のグループに付与されます。

> SYSTEM ユーザーアカウントを削除したり、このアカウントの権限を編集したりすることはできません。SYSTEM ユーザーアカウント権限を編集する場合、変更を保存するときに、最大限の権限が回復されます。

[編集権限]レベルの機能へのアクセス権限を持つユーザーは(152 ページのセクション「Kaspersky Security 10.1 for Windows Server を管理するための権限について」を参照)、保護対象サーバーに登録されているその他のユーザー、またはドメインに含まれているユーザーに対して、Kaspersky Security サービスを管理するためのアクセス権を付与できます。

Kaspersky Security サービスの管理のため、Kaspersky Security 10.1 for Windows Server のユーザーまたはユーザーのグループに対し、次のいずれかの設定済み Kaspersky Security 10.1 for Windows Server アクセス権限レベルを選択できます:

- **フルコントロール**:Kaspersky Security サービスの全般設定とユーザー権限を表示および編集でき、さらに Kaspersky Security サービスの開始と停止ができます。
- **読み取り**:Kaspersky Security サービスの全般的な設定とユーザー権限を表示できます。
- **変更**:Kaspersky Security サービスの全般的な設定とユーザー権限を表示、変更できます。
- **実行**:Kaspersky Security サービスの開始と停止ができます。

特定の Kaspersky Security 10.1 for Windows Server 機能へのアクセスを許可または拒否するように、高度なアクセス権限を指定することもできます(以下の表を参照)。

ユーザーまたはグループのアクセス権限を手動で設定した場合、該当のユーザーまたはグループには[**高度なアクセス許可**]のアクセスレベルが設定されます。

表 18. Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限の限界設定

機能	説明
サービスの設定の表示	Viewing（表示）：Kaspersky Security サービスの全般的な設定とユーザー権限を表示できます。
Service Control Manager からのサービスステータスの要求	Microsoft Windows のサービスコントロールマネージャーから Kaspersky Security サービスの実行ステータスを要求できます。
サービスからのステータスの要求	Kaspersky Security サービスからサービス実行ステータスを要求できます。
依存するサービスのリストの読み込み	Kaspersky Security サービスが依存するサービス、および Kaspersky Security サービスに依存するサービスのリストを表示できます。
サービスの設定の編集	Kaspersky Security サービスの全般的な設定とユーザー権限を表示、変更できます。
サービスの開始	Kaspersky Security サービスを開始できます。
サービスの停止	Kaspersky Security サービスを停止できます。
サービスの一時停止 / 再開	Kaspersky Security サービスの一時停止と再開ができます。
権限の読み取り	Kaspersky Security サービスのユーザーのリストと、各ユーザーのアクセス権限を表示できます。
権限の編集	以下の操作を実行できます： • Kaspersky Security サービスユーザーの追加と削除 • Kaspersky Security サービスに対するユーザーのアクセス権限の編集

機能	説明
サービスの削除	Microsoft Windows のサービスコントロールマネージャーで Kaspersky Security サービスを登録解除できます。
サービスへのユーザー定義要求	Kaspersky Security サービスへユーザー要求を作成して送信できます。

Kaspersky Security 管理サービスのアクセス権限について

Kaspersky Security 10.1 for Windows Server サービスのリストを確認できます。

Kaspersky Security 10.1 for Windows Server はインストール時に Kaspersky Security 10.1 for Windows Server 管理サービス(KAVFSGT)を登録します。別のコンピューターにインストールされた Kaspersky Security 10.1 コンソールから本製品を管理するには、Kaspersky Security 10.1 for Windows Server への接続に使用される権限を持つアカウントが、保護対象サーバーの Kaspersky Security 10.1 for Windows Server 管理サービスへのフルアクセス権を持っている必要があります。

既定では、保護対象サーバーの管理者グループのユーザーと、Kaspersky Security 10.1 for Windows Server のインストール時に保護対象サーバーに作成された[KAVWSEE Administrators]グループのユーザーに、すべての Kaspersky Security 管理サービスへのアクセス権が付与されます。

Kaspersky Security 管理サービスは、Microsoft Windows の**サービス**スナップインでのみ管理できます。

Kaspersky Security 10.1 for Windows Server の設定では、Kaspersky Security 10.1 for Windows Server 管理サービスへのユーザーアクセスを許可またはブロックできません。

名前とパスワードが同じアカウントが保護対象のサーバーに登録されている場合、ローカルアカウントから Kaspersky Security 10.1 for Windows Server に接続できます。

Kaspersky Security 10.1 for Windows Server と Kaspersky Security サービスを管理するためのアクセス権限の設定

Kaspersky Security 10.1 for Windows Server の機能へのアクセスが許可されたユーザーとユーザーグループのリストを編集し、Kaspersky Security サービスを管理できます。さらに、それらのユーザーとユーザーグループのアクセス権限も編集することができます。

► **リストでユーザーまたはグループを追加または削除するには:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーション設定を設定するサーバーがある管理グループを展開します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループのポリシー設定を編集する場合は、[**ポリシー**]タブを選択して[**<ポリシー名>**]-[**プロパティ**]の順に開きます。

   - 単一のサーバーのアプリケーションを設定する場合、Kaspersky Security Center の[**アプリケーションのプロパティ**]ウィンドウで必要な設定を開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

3. [**詳細設定**]セクションで、次のいずれかの手順を実行します:

   - Kaspersky Security 10.1 for Windows Server の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、[**アプリケーション管理用のユーザーアクセス権限**]の[**設定**]をクリックします。

- Kaspersky Security サービスを介してアプリケーションを管理するためのアクセス権限を持つユーザーのリストを編集する場合は、[**Kaspersky Security サービス管理用のユーザーアクセス権限**]の[**設定**]をクリックします。

  [**Kaspersky Security 10.1 for Windows Server のアクセス許可**]ウィンドウが開きます。

4. 表示されたウィンドウで、次の操作を行います:

   - ユーザーまたはグループをリストに追加するには、[**追加**]をクリックして権限を付与するユーザーまたはグループを選択します。

   - ユーザーまたはグループをリストから削除するには、アクセスを制限するユーザーまたはグループを選択して、[**削除**]をクリックします。

5. [**適用**]をクリックします。

選択されたユーザー(グループ)が追加または削除されます。

► Kaspersky Security 10.1 for Windows Server または Kaspersky Security サービスを管理するユーザーまたはグループの権限を編集するには:

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーション設定を設定するサーバーがある管理グループを展開します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - ポリシーを設定するには、Kaspersky Security Center 管理コンソールのコンピューターグループで[**ポリシー**]タブを選択し、[**<ポリシー名>**]-[**オプション**]の順に開きます。

   - 単一のサーバーのアプリケーションを設定する場合、Kaspersky Security Center の[**アプリケーションのプロパティ**]ウィンドウで必要な設定を開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

3. [**詳細設定**]セクションで、次のいずれかの手順を実行します:

- Kaspersky Security 10.1 for Windows Server の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、[**アプリケーション管理用のユーザーアクセス権限**]の[**設定**]をクリックします。
- Kaspersky Security サービスを介してアプリケーションを管理するためのアクセス権限を持つユーザーのリストを編集する場合は、[**Kaspersky Security サービス管理用のユーザーアクセス権限**]の[**設定**]をクリックします。

  [**Kaspersky Security 10.1 for Windows Server のアクセス許可**]ウィンドウが開きます。

4. 表示されたウィンドウにある[**グループ名またはユーザー名**]リストで、権限を変更するユーザーまたはユーザーのグループを選択します。
5. 次のアクセスレベルに対して、[**アクセス許可**]セクションにある[**許可**]または[**拒否**]を選択します:
   - **フルコントロール**:Kaspersky Security 10.1 for Windows Server または Kaspersky Security サービスを管理する権限のフルセット。
   - **読み取り**:
     - 次の権限で Kaspersky Security 10.1 for Windows Server を管理します:[**統計情報の取得**]、[**設定の読み取り**]、[**ログの読み取り**]、[**読み取り権限**]。
     - 次の権限で Kaspersky Security サービスを管理します:[**サービスの設定の読み込み**]、[**Service Control Manager からのサービスステータスの要求**]、[**サービスからのステータスの要求**]、[**依存するサービスのリストの読み込み**]、[**読み取り権限**]。
   - **変更**:
     - [**編集権限**]を除く、Kaspersky Security 10.1 for Windows Server を管理するための権限すべて。
     - 次の権限で Kaspersky Security サービスを管理します:[**サービス設定の編集**]、[**読み取り権限**]。
   - **実行**:次の権限で Kaspersky Security サービスを管理します:[**サービスを開始しています**]、

［**サービスを停止しています**］、［**サービスの一時停止 / 再開**］、［**読み取り権限**］、［**サービスへのユーザー定義要求**］。

6. ユーザーまたはグループの権限の詳細設定を行うには（**高度なアクセス許可**）、［**詳細設定**］をクリックします。

    a. 表示された［**Kaspersky Security 10.1 for Windows Server のセキュリティの詳細設定**］ウィンドウで、必要なユーザーまたはグループを選択します。

    b. ［**編集**］をクリックします。

    c. 表示されたウィンドウで、［**高度なアクセス許可を表示する**］をクリックします。

    d. ウィンドウの上部にあるドロップダウンリストで、アクセスコントロールの種別を選択します（**［許可］または［拒否］**）。

    e. 選択したユーザーまたはグループに対して許可または拒否する機能の横にあるチェックボックスをオンにします。

    f. ［**OK**］をクリックします。

    g. ［**Kaspersky Security 10.1 for Windows Server のセキュリティの詳細設定**］ウィンドウで、［**OK**］をクリックします。

7. ［**Kaspersky Security 10.1 for Windows Server のアクセス許可**］ウィンドウで、［**適用**］をクリックします。

Kaspersky Security 10.1 for Windows Server または Kaspersky Security サービスを管理するために設定された権限が保存されます。

Kaspersky Security 10.1 for Windows Server 機能へのパスワードで保護されたアクセス

ユーザー権限の設定によって、アプリケーション管理や登録されたサービスへのアクセスを制限できます（152 ページのセクション「Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限」を参照）。Kaspersky Security 10.1 for Windows Server 設定でパスワード保護を設定して、重要な操作の実行をさらに保護することもできます。

次のアプリケーション機能にアクセスしようとすると、Kaspersky Security 10.1 for Windows Server はパスワードを要求します：

- ローカルの Kaspersky Security 10.1 コンソールへの接続
- Kaspersky Security 10.1 for Windows Server のアンインストール
- Kaspersky Security 10.1 for Windows Server コンポーネントの変更

Kaspersky Security 10.1 for Windows Server インターフェイスでは、指定したパスワードは画面にそのまま表示されません。パスワードを指定するとチェックサムが計算され、パスワードが保存されます。

パスワードで保護するアプリケーションの設定をエクスポートおよびインポートできます。保護対象アプリケーション設定をエクスポートすると作成される設定ファイルには、パスワードチェックサムおよびパスワード文字列の空白を埋めるために使用される修飾子の値が含まれています。

設定ファイルのチェックサムや修飾子は変更しないでください。手動で変更されたパスワード設定をインポートすると、アプリケーションへのアクセスが完全にブロックされる場合があります。

► **Kaspersky Security 10.1 for Windows Server 機能へのアクセスを保護するには、次の手順を実行します：**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。

アプリケーション設定を設定するサーバーがある管理グループを展開します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループのポリシー設定を編集する場合は、[**ポリシー**]タブを選択して**[<ポリシー名>]-[プロパティ]**の順に開きます。
   - 単一のサーバーのアプリケーションを設定する場合、Kaspersky Security Center の[**アプリケーションのプロパティ**]ウィンドウで必要な設定を開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

3. [**アプリケーションの設定**]セクションの[[**セキュリティ**]セクションで、[**設定**]をクリックします。

   [**セキュリティ設定**]ウィンドウが表示されます。

4. [**パスワード保護設定**]セクションで、[**パスワード保護を適用する**]をオンにします。

   [**パスワード**]および[**パスワードの確認**]がアクティブになります。

5. [**パスワード**]で、Kaspersky Security 10.1 for Windows Server 機能へのアクセスを保護するために使用する値を入力します。

6. [**パスワードの確認**]にもう一度パスワードを入力します。

7. [**OK**]をクリックします。

指定された設定が保存されます。保護対象機能へのアクセスに、指定したパスワードが要求されるようになります。

このパスワードは復元できません。パスワードを紛失すると、アプリケーションをまったくコントロールできなくなります。また、保護対象サーバーからアプリケーションをアンインストールできなくなります。

指定したパスワードは、アプリケーション設定でいつでも変更またはリセットできます。

► **パスワードをリセットするには、次の操作を行います。**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーション設定を設定するサーバーがある管理グループを展開します。
2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループのポリシー設定を編集する場合は、[**ポリシー**]タブを選択して[**<ポリシー名>**]-[**プロパティ**]の順に開きます。
   - 単一のサーバーのアプリケーションを設定する場合、Kaspersky Security Center の[**アプリケーションのプロパティ**]ウィンドウで必要な設定を開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。
3. [**アプリケーションの設定**]セクションの[**セキュリティ**]セクションで、[**設定**]をクリックします。

   [**セキュリティ設定**]ウィンドウが表示されます。
4. [**パスワード保護設定**]セクションで、[**パスワード保護を適用する**]をオフにします。

   [**パスワード**]および[**パスワードの確認**]がクリアされ、アクティブでなくなります。
5. [**OK**]をクリックします。

パスワード保護が無効になります。元のパスワードチェックサムがアプリケーション設定から削除されます。

Kaspersky Security 管理サービスのネットワーク接続の有効化

Windows オペレーティングシステムによって、設定名が異なる場合があります。

► **保護されたサーバーで Kaspersky Security 管理サービスのネットワーク接続を許可するには、**

次の手順を行います。

1. Microsoft Windows Server を実行する保護対象サーバーで、**[スタート] - [コントロール パネル] - [セキュリティ] - [Windows ファイアウォール]**の順に選択します。
2. [**Windows ファイアウォールの設定**]ウィンドウで、[**設定の変更**]を選択します。
3. [**除外**]タブ上の定義済み除外リストで、次のチェックボックスをオンにします：[**COM + ネットワークアクセス**]、[**Windows Management Instrumentation（WMI）**]。
4. [**別のアプリの許可**]をクリックします。
5. [**アプリの追加**]ウィンドウでファイル kavfsgt.exe を選択します。このファイルは、Kaspersky Security 10.1 コンソールのインストール時に保存先として指定したフォルダーに保存されます。
6. [**OK**]をクリックします。
7. [**Windows ファイアウォールの設定**]ウィンドウで[**OK**]をクリックします。

保護されたコンピューターで Kaspersky Security 管理サービスのネットワーク接続が許可されます。

ポリシーの作成と設定

このセクションでは、Kaspersky Security Center のポリシーによる複数のサーバーの Kaspersky Security 10.1 for Windows Server の管理について説明します。

この章の内容

ポリシーの概要

Kaspersky Security Center のグローバルポリシーは、Kaspersky Security 10.1 for Windows Server がインストールされている複数のサーバーでの保護を管理するために作成できます。

ポリシーは、1 つの管理グループに所属するすべての保護対象サーバーに対して、指定された Kaspersky Security 10.1 for Windows Server の設定、機能、およびタスクを適用するものです。

1 つの管理グループに対して複数のポリシーを作成して適用できます。管理コンソールでは、グループに対して現在アクティブなポリシーのステータスは、「**アクティブ**」と示されます。

ポリシー適用に関 l する情報は、Kaspersky Security 10.1 for Windows Server システム監査ログに記録されます。この情報は、Kaspersky Security 10.1 コンソールの[**システム監査ログ**]フォルダーで参照できます。

Kaspersky Security Center では、ローカルのコンピューターにポリシーを適用する方法として、**設定の変更の禁止**があります。ポリシーの適用後、Kaspersky Security 10.1 for Windows Server では、ポリシーの適用前に有効であった設定の値の代わりに、ローカルのコンピューターのポリシーのプロパティで 🔒 アイコンを選択した設定の値が使用されます。ポリシーのプロパティで選択されている 🔓 アイコンの横のアクティブポリシーの設

定値は適用されません。

ポリシーが有効の場合、ポリシーで 🔒 アイコンが付いている設定の値が Kaspersky Security 10.1 コンソールに表示されますが、編集はできません。その他の設定（ポリシーで 🔓 アイコンが付いている設定）の値は、Kaspersky Security 10.1 コンソールで編集できます。

また、アクティブポリシーで編集し、🔒 アイコンが付いている設定は、コンピューターのプロパティウィンドウで、各コンピューターの Kaspersky Security Center での変更がブロックされます。

指定され、アクティブなポリシーを使用してローカルコンピューターに送信された設定は、アクティブなポリシーが無効になるとローカルタスク設定に保存されます。

ポリシーでリアルタイム保護タスクのいずれかの設定や、ネットワーク接続ストレージの保護タスクの設定を定義しており、そのタスクが現在実行中の場合、ポリシーによって定義された設定は、ポリシーの適用後すぐに変更されます。タスクが実行中でない場合は、タスクの開始時に設定が適用されます。

ポリシーの作成

ポリシーの作成プロセスには、次の手順が含まれます：

1. ポリシーウィザードを使用したポリシーの作成：ウィザードダイアログを使用して、リアルタイム保護の設定を行うことができます。
2. ポリシーの設定：ポリシーのプロパティウィンドウで、リアルタイム保護設定、Kaspersky Security 10.1 for Windows Server の全般設定、隔離とバックアップの設定、実行ログの詳細レベル、および Kaspersky Security 10.1 for Windows Server のイベントに関するユーザー通知と管理者の通知を定義することができます。

► **インストールした Kaspersky Security 10.1 for Windows Server を実行するサーバーのグループのポリシーを作成するには、次の手順を実行します：**

1. 管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、ポリシーを作成するサーバーが含まれる管理グループを選択します。

2. 選択した管理グループの詳細ペインで[**ポリシー**]タブを選択し、[**ポリシーの作成**]をクリックして、ウィザードを開始してポリシーを作成します。

3. [**グループポリシー作成対象のアプリケーションを選択**]ウィンドウの[**アプリケーション**]リストで、[Kaspersky Security 10.1 for Windows Server]を選択します。

4. [**グループポリシーの名前を入力**]ウィンドウの[**名前**]に、作成するポリシーの名前を入力します。次の記号をポリシー名に含めることはできません:" * < : > ? ¥ / |。

5. [**処理の選択**]ウィンドウで、次の値のいずれかを選択します:

   - **新規**:設定に新しいポリシーを作成し、既定で、新しく作成されたポリシーセットに対して設定します。
   - **Kaspersky Security for Windows Server バージョン 8.* または 10 で作成したポリシーをインポート**:このバージョンのポリシーをテンプレートとして使用します。

     [**参照**]をクリックして、既存のポリシーが保存されている設定ファイルを選択します。

6. [**サーバーのリアルタイム保護**]ウィンドウで、必要に応じてファイルのリアルタイム保護タスクとKSN の使用タスクの設定を行います。ネットワークにあるローカルのコンピューターでの設定済みのポリシータスクの使用を許可またはブロックします:

   - をクリックすると、ネットワークコンピューターのタスク設定の変更を許可し、ポリシーで編集されたタスク設定の適用をブロックします。
   - をクリックすると、ネットワークコンピューターのタスク設定の変更を拒否し、ポリシーで編集されたタスク設定の適用を許可します。

   新たに作成されたポリシーでは、リアルタイム保護タスクの既定の設定を使用します。

   - ファイルのリアルタイム保護タスクの既定の設定を編集するには、[**ファイルのリアルタイム保護**]セクションの[**設定**]をクリックします。表示される[**サーバーのリアルタイム保護**]ウィンドウで、要件に応じてタスクの設定を行います。[**OK**]をクリックします。
   - KSN の使用タスクの既定の設定を編集するには、[**KSN の使用**]セクションの[**設定**]をクリッ

クします。表示される[**KSN の使用**]ウィンドウで、要件に応じてタスクの設定を行います。[**OK**]をクリックします。

KSN の使用タスクは、KSN 声明に同意をすると使用可能になります。

7. [**アプリケーションのグループポリシーを作成**]ウィンドウで、次のいずれかのポリシーステータスを選択します:

   - **アクティブポリシー** - ポリシーの作成後、すぐに適用する場合。アクティブポリシーがすでにグループに存在する場合は、この既存のポリシーが非アクティブになり、作成するポリシーがアクティベートされます。
   - **非アクティブポリシー** - 作成するポリシーをすぐには適用しない場合。この場合、ポリシーは後でアクティベートできます。

8. [**完了**]をクリックします。

作成したポリシーが、選択した管理グループの[**ポリシー**]タブのポリシーのリストに表示されます。ポリシーのプロパティウィンドウで、Kaspersky Security 10.1 for Windows Server のその他の設定、タスク、機能を設定できます。

リシーの設定

既存のポリシーの[**<ポリシー名>:プロパティ**]ウィンドウでは、Kaspersky Security 10.1 for Windows Server の全般設定、隔離とバックアップの設定、信頼ゾーンの設定、リアルタイム保護の設定、ローカルアクティビティの管理の設定、実行ログの詳細レベルの設定、Kaspersky Security 10.1 for Windows Server イベントに関するユーザーや管理者への通知設定、製品および Kaspersky Security サービスを管理するためのアクセス権の設定、ポリシーのプロファイルの適用設定が行えます。

► **ポリシー設定を行うには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開します。
2. 関連するポリシー設定を行う管理グループを展開して、詳細ペインで[**ポリシー**]タブを開きます。

3. 次の方法の 1 つを使用して、設定するポリシーを選択し、[**<ポリシー名>:プロパティ**]ウィンドウを開きます:

   - ポリシーのコンテキストメニューで[**プロパティ**]オプションを選択する。
   - 選択したポリシーの右の詳細ペインで、[**ポリシーの設定**]をクリックする。
   - 選択されたポリシーをダブルクリックする。

4. [**全般**]セクションの[**ポリシーのステータス**]で、ポリシーを有効または無効にします。それには、次のいずれかのオプションを選択します:

   - **アクティブポリシー** - 選択した管理グループ内のすべてのサーバーにポリシーを適用する場合に選択します。
   - **非アクティブポリシー** - 選択したグループ内のすべてのサーバーにポリシーを適用しない場合に選択します。

   > **モバイルユーザーポリシー**は、Kaspersky Security 10.1 for Windows Server を管理している場合は使用できません。

5. [**イベント通知**]、[**アプリケーションの設定**]、[**ログと通知の設定**]、[**詳細設定**]、[**変更履歴**]の各セクションで、アプリケーション設定を変更できます(次の表を参照)。

6. [**サーバーのリアルタイム保護**]、[**ローカルアクティビティの管理**]、[**ネットワークアクティビティの管理**]、および[**システム監査**]の各セクションで、アプリケーション設定およびアプリケーション起動設定を設定します(次の表を参照)。

   > Kaspersky Security Center のポリシーを使用して、管理グループ内のすべてのサーバーに対するタスクの実行を有効または無効にできます。
   >
   > 個別のソフトウェアコンポーネントに対して、すべてのネットワークコンピューターにポリシー設定を適用するかどうかを指定できます。

7. ［**OK**］をクリックします。

設定の内容がポリシーに適用されます。

Kaspersky Security 10.1 コンソールでのタスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

Kaspersky Security 10.1 for Windows Server ポリシー設定のセクション

全般

［**全般**］セクションでは、次のポリシー設定を行うことができます：

- ポリシーのステータスの指定。
- 親ポリシーから子ポリシーへ継承する設定の指定。

イベント通知

［**イベント通知**］セクションでは、次のイベントカテゴリの設定を行えます：

- **緊急イベント**
- **機能エラー**
- **警告**
- **情報**

［**プロパティ**］を使用して、選択したイベントに対して次の設定を行えます：

- 記録したイベントの保管場所と保管期間の指定。
- 記録したイベントの通知方法の指定。

アプリケーションのプロパティ

表 19. [アプリケーションの設定]セクションの設定

セクション	オプション
スケーラビリティとインターフェイス	[**スケーラビリティとインターフェイス**]セクションで[**設定**]をクリックして、次の設定を行います: • スケーラビリティ設定を自動と手動のいずれで設定するかを選択 • 製品アイコンの表示設定
セキュリティ	[**セキュリティ**]セクションで[**設定**]をクリックして、次の設定を行います: • タスク実行の設定 • UPS 電源によるサーバーの実行時のアプリケーションの挙動の指定 • アプリケーション機能のパスワード保護の有効化または無効化
接続	[**接続**]セクションで[**設定**]を使用して、アップデートサーバー、アクティベーションサーバー、および KSN に接続するためのプロキシサーバーの次の設定を行えます: • プロキシサーバーの設定 • プロキシサーバーの認証設定の指定
システムタスクの実行	[**システムタスクの実行**]セクションで[**設定**]をクリックして、ローカルのコンピューターで設定されているスケジュールに応じた次のシステムタスクの起動を許可またはブロックします: • オンデマンドスキャンタスク • アップデートタスクおよびアップデートのコピータスク

詳細設定

表 20.　［詳細設定］セクションの設定

セクション	オプション
信頼ゾーン	［**信頼ゾーン**］セクションの［**設定**］をクリックして、次の信頼ゾーンの設定を編集します： • 信頼ゾーンの除外リストの作成 • ファイルのバックアップ処理のスキャンの有効化または無効化 • 信頼するプロセスのリストの作成
リムーバブルドライブスキャン	［**リムーバブルドライブスキャン**］セクションで［**設定**］をクリックして、リムーバブル USB ドライブのスキャンを設定できます。
アプリケーション管理用のユーザーアクセス権限	［**アプリケーション管理用のユーザーアクセス権限**］セクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky Security 10.1 for Windows Server を管理できます。

Security サービス管理用のユーザーアクセス権限	[**Security サービス管理用のユーザーアクセス権限**]セクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky Security サービスを管理できます。
保管領域	[**保管領域**]セクションで[**設定**]をクリックして、次の隔離設定、バックアップ設定、ブロック対象コンピューターの設定を編集します: • 隔離オブジェクトまたはバックアップオブジェクトを配置するフォルダーのパスの指定 • バックアップと隔離の最大サイズの設定および空き容量のしきい値の指定 • 隔離またはバックアップから復元するオブジェクトの配置先となるフォルダーのパスの指定 • 隔離オブジェクトおよびバックアップオブジェクトに関する情報の管理サーバーへの送信設定 • コンピューターのブロック期間の設定

サーバーのリアルタイム保護

表 21. ［サーバーのリアルタイム保護］セクションの設定

セクション	オプション
ファイルのリアルタイム保護	［**ファイルのリアルタイム保護**］セクションで［**設定**］をクリックすると、次のタスク設定を行えます： • 保護範囲の指定 • ヒューリスティックアナライザーの使用設定 • 信頼ゾーンの使用設定 • 保護範囲の指定 • 選択した保護範囲のセキュリティレベルの設定（定義済みのセキュリティレベルの選択または手動によるセキュリティレベルの設定） • タスク開始を設定します。
KSN の使用	［**KSN の使用**］セクションで［**設定**］をクリックして、次のタスク設定を行います： • KSN の信頼しないオブジェクトの処理の指定 • タスクのパフォーマンス設定 • KSN プロキシサーバーとしての Kaspersky Security Center の使用設定 • KSN 声明への同意 • タスク開始を設定します。
脆弱性攻撃ブロック	［**脆弱性攻撃ブロック**］セクションで［**設定**］をクリックして、次のタスク設定を行います： • プロセスメモリの保護モードを選択 • 脆弱性攻撃リスクを低下させる処理を指定 • 保護対象プロセスのリストを追加して編集

スクリプト監視	**スクリプト監視**タスクで[**設定**]をクリックし、次のタスク実行設定を行います: • 危険な可能性のあるスクリプトの実行の許可またはブロック • ヒューリスティックアナライザーの使用の設定 • 信頼ゾーンの適用設定 • タスク実行の設定

ローカルアクティビティの管理

表 22. [ローカルアクティビティの管理]セクションの設定

セクション	オプション
アプリケーション起動コントロール	[**アプリケーション起動コントロール**]セクションで[**設定**]を使用して、次のタスク設定を行います: • タスク操作モードの選択 • 次回以降のアプリケーション起動を管理する設定を行います。 • アプリケーション起動コントロールルールの範囲を指定します。 • KSN の使用設定 • タスク開始を設定します。
デバイスコントロール	[**デバイスコントロール**]セクションで[**設定**]をクリックして、次のタスク設定を行います: • タスク操作モードの選択 • タスク開始を設定します。

ネットワークアクティビティの管理

表 23. ［ネットワークアクティビティの管理］セクションの設定

セクション	オプション
ファイアウォール管理	［**ファイアウォール管理**］セクションで［**設定**］をクリックして、次のタスク設定を行います： • ファイアウォールのルールの設定 • タスク開始を設定します。
アンチクリプター	［**アンチクリプター**］セクションで［**設定**］をクリックして、次のタスク設定を行います： • アンチクリプター保護範囲の設定 • タスク開始を設定します。

システム監査

表 24. ［システム監査］セクションの設定

セクション	オプション
ファイル変更監視	［**ファイル変更監視**］セクションで、保護対象サーバーにおける、セキュリティ侵害の可能性があるファイル変更の管理を設定できます。
Windows イベントログ監視	［**Windows イベントログ監視**］セクションで、Windows イベントログ分析の結果に基づいて、保護対象サーバーの整合性管理を設定できます。

ログと通知の設定

表 25. [ログと通知の設定]セクションの設定

セクション	オプション
実行ログ	[**実行ログ**]セクションで[**設定**]をクリックして、次の設定を行います: • 選択したソフトウェアコンポーネントの記録されたイベントに対する重要度の指定 • 実行ログのストレージ設定の指定 • Kaspersky Security Center 設定と SIEM との統合の指定
イベント通知	[**イベント通知**]セクションで[**設定**]をクリックして、次の設定を行います: • [**オブジェクトが検知されました**]イベントのユーザーへの通知設定の指定 • [**通知の配信設定**]セクションのイベントリストで選択したイベントの管理者への通知設定の指定
管理サーバーとのインタラクション	[**管理サーバーとのインタラクション**]セクションで、[**設定**]をクリックして、Kaspersky Security 10.1 for Windows Server が管理サーバーに報告するオブジェクトの種別を選択できます。

ネットワーク接続ストレージの保護

表 26.　［ネットワーク接続ストレージの保護］セクションの設定

セクション	オプション
ファイルのリアルタイム保護（RPC）	［**ファイルのリアルタイム保護（RPC）**］セクションで［**設定**］をクリックして、次の設定を行います： • ヒューリスティックアナライザーの使用 • ネットワーク接続ストレージの接続設定 • タスクの保護範囲
ファイルのリアルタイム保護（ICAP）	［**ファイルのリアルタイム保護（ICAP）**］セクションで［**設定**］をクリックして、次の設定を行います： • ICAP サービス接続設定 • 他のコンポーネントとの統合 • セキュリティレベル
NetApp のアンチクリプター	［**NetApp のアンチクリプター**］セクションで［**設定**］をクリックして、次の設定を行います： • タスクモード。 • ヒューリスティックアナライザーの使用 • 接続と認証の設定 • 保護範囲からの除外の指定

ネットワーク接続ストレージの保護タスクの詳細情報を確認するには、『**Kaspersky Security 10.1 for Windows Server Implementation Guide for Network Storages Protection（英語）**』を参照してください。

変更履歴

[**変更履歴**]セクションでは、次のようにしてリビジョンを管理できます:現在のリビジョンや他のポリシーとの比較、リビジョンの説明の追加、ファイルへのリビジョンの保存、ロールバックの実行など。

ローカルのシステムタスクのスケジュールによる開始の設定

ポリシーを使用して、管理グループの各サーバーで、ローカルで設定されたスケジュールに基づくローカルシステムのオンデマンドスキャンタスクおよびアップデートタスクの起動を許可またはブロックできます。

- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって禁止される場合、これらのタスクはローカルコンピューター上でスケジュールどおりに実行されません。ローカルシステムタスクは手動で開始できます。
- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって許可されている場合、これらのタスクは、このタスクに対してローカルに設定されたスケジュールパラメータに従って実行されます。

既定では、ローカルシステムタスクの開始はポリシーによって禁止されています。

> アップデートまたはオンデマンドスキャンが Kaspersky Security Center グループタスクによって管理されている場合、ローカルシステムタスクの開始を許可しないことをお勧めします。

グループアップデートまたはオンデマンドスキャンタスクを使用しない場合は、ポリシーでローカルシステムタスクの開始を許可します。Kaspersky Security 10.1 for Windows Server は既定のスケジュールに従って定義データベースおよびモジュールのアップデートを実行し、すべてのローカルシステムのオンデマンドスキャンタスクを開始します。

ポリシーを使用して、次のローカルのシステムタスクに対するスケジュールによる開始を許可またはブロックできます:

- オンデマンドスキャンタスク：重要領域のスキャン、隔離のスキャン、オペレーティングシステムの起動時にスキャン、ソフトウェアモジュールの整合性チェック。
- アップデートタスク：定義データベースのアップデート、ソフトウェアモジュールのアップデート、アップデートのコピー。

保護対象サーバーが管理グループから除外される場合、システムタスクのスケジュールは自動的に有効になります。

► **Kaspersky Security 10.1 for Windows Server のシステムタスクのスケジュールによる開始をポリシーで許可またはブロックするには、次の手順を実行します：**

1. 管理コンソールツリーの[**管理対象デバイス**]フォルダーで、必要なグループを展開し、[**ポリシー**]タブを選択します。
2. [**ポリシー**]タブで、サーバーのグループでの Kaspersky Security 10.1 for Windows Server システムタスクのスケジュールによる開始を設定するポリシーのコンテキストメニューを開き、[**プロパティ**]コマンドを選択します。
3. [**<ポリシー名>：プロパティ**]ウィンドウで、[**アプリケーションの設定**]セクションを開きます。[**システムタスクの実行**]セクションで[**設定**]をクリックして、次のように実行します：
   - [**オンデマンドスキャンタスクの実行を許可**]と[**アップデートタスクとアップデートのコピータスクの実行を許可**]をオンにし、リストのタスクに対するスケジュールによる開始を許可します。
   - [**オンデマンドスキャンタスクの実行を許可**]と[**アップデートタスクとアップデートのコピータスクの実行を許可**]をオフにし、リストのタスクに対するスケジュールによる開始を無効にします。

   チェックボックスをオンにしてもオフにしても、この種のローカルカスタムタスクの開始設定に影響はありません。
4. 設定するポリシー（167 ページのセクション「ポリシーの概要」を参照）がアクティブで、管理サーバーのグループに適用されることを確認します。
5. [**OK**]をクリックします。

スケジュールによるタスクの開始設定の内容が、選択したタスクに適用されます。

Kaspersky Security Center を使用したタスクの作成と設定

このセクションでは、Kaspersky Security 10.1 for Windows Server タスク、そのタスクの作成方法と設定方法、およびそのタスクの開始方法と停止方法に関する情報について説明します。

この章の内容

Kaspersky Security Center でのタスクの作成について

管理グループと特定のコンピューターに対してグループタスクを作成できます。次のタスクの種別が作成できます:

- 製品のアクティベーション

- アップデートのコピー
- 定義データベースのアップデート
- ソフトウェアモジュールのアップデート
- 定義データベースのロールバック
- オンデマンドスキャン
- アプリケーションの整合性チェック
- アプリケーション起動コントロールルールの自動作成
- デバイスコントロールルールの自動作成

次の方法で、ローカルタスクおよびグループタスクを作成できます:

- 1 台のコンピューターの場合、コンピューターのプロパティウィンドウの[タスク]セクションから作成します。
- 管理グループの場合、選択されたコンピューターのグループのフォルダーの詳細ペインの[**タスク**]タブから作成します。
- 一連のコンピューターの場合、[**デバイスの抽出**]フォルダーの詳細ペインから作成します。

ポリシーを使用し、すべての保護対象サーバー上で同じ管理グループから、アップデートとオンデマンドスキャンのローカルシステムタスクのスケジュール(181 ページのセクション「ローカルのシステムタスクのスケジュールによる開始の設定」を参照)を無効にできます。

Kaspersky Security Center のタスクの一般的な情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

Kaspersky Security Center を使用したタスクの作成

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **Kaspersky Security Center の管理コンソールで新しいタスクを作成するには:**

1. 次のいずれかの方法でタスクウィザードを開始します:

   - ローカルタスクを作成するには:

     a. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、保護対象サーバーが所属するグループを選択します。

     b. 詳細ペインの[**デバイス**]タブで、保護対象のサーバーの情報が含まれる行でコンテキストメニューを開き、[**プロパティ**]を選択します。

     c. 表示されるウィンドウの[**タスク**]セクションで[**追加**]をクリックします。

   - グループタスクを作成するには:

     a. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、タスクを作成するグループを選択します。

     b. 詳細ペインで[**タスク**]タブのコンテキストメニューを開き、[**作成**]-[**タスク**]を選択します。

   - カスタムセットのコンピューターにタスクを作成するには、Kaspersky Security Center の管理コンソールツリーで[**デバイスの抽出**]-[**タスクの作成**]を選択します。

   タスクウィザードのウィンドウが開きます。

2. [**タスク名の定義**]ウィンドウで、タスク名を入力します(100 文字以内とし、**¥"*<>?¥¥:|**は使用できませ

ん）。タスク名にタスク種別（「共有フォルダーのオンデマンドスキャン」など）を追加してください。

3. ［**タスク種別の選択**］ウィンドウの［**Kaspersky Security 10.1 for Windows Server**］ヘッダーで、作成するタスクの種別を選択します。

4. アプリケーションの整合性チェック、製品のアクティベーション、定義データベースのロールバック以外のタスク種別を選択した場合、［**設定**］ウィンドウが開きます。作成したタスクの種別によって、次のいずれかの処理を実行します：

   - **オンデマンドスキャンタスクを作成**するには：

     a. ［**スキャン範囲**］ウィンドウでスキャン範囲を作成します。

     既定では、サーバーの重要な領域がスキャン範囲に含まれます。スキャン範囲は、表では ☑ アイコンのマークが付きます。

     スキャン範囲は変更できます。特定の事前に設定されたスキャン範囲、ディスク、フォルダー、ネットワークオブジェクトおよびファイルを追加し、追加した範囲ごとに特定のセキュリティ設定を割り当てます。

   - すべての重要な領域をスキャン対象から除外するには、各行のコンテキストメニューを開いて［**範囲の削除**］を選択します。
   - 定義済みのスキャン範囲、ディスク、フォルダー、ネットワークオブジェクト、またはファイルをスキャン範囲に含めるには、［**スキャン範囲**］の表を右クリックして［範囲の追加］を選択します。［**スキャン範囲にオブジェクトの追加**］の［**定義済み範囲**］リストで定義済みの範囲を選択し、サーバーまたはその他のネットワークコンピューターのサーバーディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定して［**OK**］をクリックします。
   - サブフォルダーやファイルをスキャン対象から除外するには、ウィザードの［**スキャン範囲**］ウィンドウで追加したフォルダー（ディスク）を選択し、コンテキストメニューを開いて［**設定**］を選択します。さらに、［セキュリティレベル］タブで［**設定**］をクリックし、［**オンデマンドスキャンの設定**］ウィンドウの［**全般**］タブで［**サブフォルダー**］と［**サブファイル**］をオフにします。
   - スキャン範囲のセキュリティ設定を変更するには、設定を行う範囲のコンテキストメニューを開き、［**設定**］を選択します。［**オンデマンドスキャンの設定**］ウィンドウで、定義済みのセキュリティレベルから 1 つを選択するか、［設定］をクリックしてセキュリティ設定を手動で設定します。Kaspersky Security 10.1 コンソールと同じ方法でセキュリティ設定が実行されます。

- 追加したスキャン範囲から埋め込みオブジェクトをスキップするには、[**スキャン範囲**]の表でコンテキストメニューを開き、[**除外の追加**]を選択して、除外するオブジェクトを指定します。[定義済みの範囲]リストで定義済みのスキャン範囲を選択し、サーバーまたはその他のネットワークコンピューターのコンピューターディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定して、[**OK**]をクリックします。
- 除外するスキャン範囲には、表で ☐ アイコンのマークが付きます。

a. [**オプション**]ウィンドウで、次の操作を行います。

Kaspersky Security 10.1 for Windows Server の信頼ゾーンに記載されているオブジェクトをタスクのスキャン範囲から除外するには、[**信頼ゾーンを適用する**]をオンにします。

重要領域のスキャンタスクとして作成したタスクを使用する場合、[**オプション**]ウィンドウで[**バックグラウンドモードでタスクを実行する**]をオンにします。Kaspersky Security Center は、[**重要領域のスキャン**]システムタスクの実行結果だけでなく、**重要領域のスキャン**のステータスを持つタスクの実行結果によって、サーバーのセキュリティを評価します。ローカルのオンデマンドスキャンタスクを作成する場合は、このチェックボックスを使用できません。

タスクが実行される処理対象プロセスに基本の優先度[**低**]を割り当てるには、[**オプション**]ウィンドウで[**バックグラウンドモードでタスクを実行する**]をオンにします。既定では、Kaspersky Security 10.1 for Windows Server タスクが実行される処理対象プロセスは、優先度[**中**]([**標準**])です。プロセスの優先度を下げると、タスクの実行に必要な時間が長くなりますが、他のアクティブなプログラムのプロセスの実行速度は上がる可能性があります。

- **アップデートタスクを作成するには**、要件に基づいてタスク設定を行います:

a. [**アップデート元**]ウィンドウでアップデート元を選択します。

b. [**LAN の設定**]をクリックします。[**接続設定**]ウィンドウが表示されます。

c. **接続**設定:

保護対象サーバーに接続するための FTP サーバーモードを指定します。

必要に応じて、アップデート元に接続する際の接続のタイムアウトを変更します。

アップデート元に接続する際のプロキシサーバーアクセス設定を行います。

保護対象サーバーの場所を指定し、アップデートのダウンロードを最適化します。

- **ソフトウェアモジュールのアップデートタスクを作成するには**、[**ソフトウェアモジュールのアップデートの設定**]ウィンドウで、必要なプログラムモジュールのアップデート設定を行います:

  a. ダウンロードを選択してソフトウェアモジュールの重要なアップデートをインストールするか、その可用性のチェックのみを行います。

  b. [**ソフトウェアモジュールの重要なアップデートをコピーしインストールする**]を選択すると、インストールされたソフトウェアモジュールを適用するために、サーバーの再起動が必要になることがあります。タスクの完了時にサーバーが自動的に再起動するようにしたい場合は、[**システムの再起動を許可する**]をオンにします。タスクの完了時にサーバーが自動的に再起動しないようにするには、[**システムの再起動を許可する**]をオフにします。

  c. Kaspersky Security 10.1 for Windows Server のモジュールのアップグレードに関する情報を入手するには、[**適用可能になったソフトウェアモジュールの定期アップデートの情報を受信する**]をオンにします。

  Kaspersky Lab は、自動インストール用の定期的なアップデートパッケージをアップデートサーバーで公開していません。これらのパッケージは、Kaspersky Lab の Web サイトから手動でダウンロードできます。[**ソフトウェアモジュールの新しい定期アップデートが適用可能です**]イベントに関する管理者の通知を設定できます。これには、定期アップデートをダウンロードできる Kaspersky Lab の Web サイトの URL が含まれます。

- **アップデートのコピータスク**を作成するには、[**アップデートのコピーの設定**]ウィンドウでアップデートとインストール先フォルダーを指定します。

- **製品のアクティベーションタスクを作成する場合**は、[**アクティベーション設定**]ウィンドウで製品のアクティベーションに使用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を適用します。ライセンスを更新するタスクを作成するには[**予備のアクティベーションコードまたはライセンスとして使用する**]をオンにします。

- **アプリケーション起動コントロールルールの自動作成タスクまたはデバイスコントロールルールの自動作成タスクを作成する場合**は、[**設定**]ウィンドウで許可ルールのリスト作成の基となる設定を指定します。

  a. ルール名の接頭辞を指定します(アプリケーション起動コントロールルールの自動作成タスクの場合のみ)。

  b. 許可ルールの使用範囲を設定します(アプリケーション起動コントロールルールの自動作成

タスクの場合のみ)。[**次へ**]をクリックします。

c. 許可ルール作成時(アプリケーション起動コントロールルールの自動作成タスクの場合のみ)およびタスク完了後に許可タスクが実行する処理を指定します。

5. タスクスケジュールを設定します(定義データベースのロールバック以外のすべてのタスク種別のスケジュールを設定できます)。[**スケジュール**]ウィンドウで、次の操作を行います:

a. スケジュールを有効化する場合は、[**スケジュールに従って実行する**]をオンにします。

b. タスク開始頻度を指定します:[**頻度**]リストから次の値のいずれかを選択します:[**時間単位**]、[**日単位**]、[**週単位**]、[**アプリケーションの起動時**]、[**定義データベースのアップデート後**([**管理サーバーがアップデートを取得した後**]の開始頻度も次のタスクを除いたグループタスクで指定できます:定義データベースのアップデートおよびソフトウェアモジュールのアップデート):

- [**時間単位**]を選択した場合は、[**タスクの開始設定**]設定グループの[**<数字>時間ごと**]で時間数を指定します。
- [**日単位**]を選択した場合は、[**タスクの開始設定**]設定グループの[**<数字>日ごと**]で日数を指定します。
- [**週単位**]を選択した場合は、[**タスクの開始設定**]設定グループの[**<数字>週ごと**]で週数を指定します。タスクを開始する曜日を指定します(既定では月曜日です)。

c. [**開始時刻**]でタスクの開始時刻を指定し、[**開始日**]でスケジュールが有効になる日付を指定します。

d. 必要に応じて残りのスケジュール設定も行います。[**詳細設定**]をクリックし、[**スケジュールの詳細設定**]ウィンドウで、次の操作を行います:

- タスク実行の最長実行時間を指定します。[**タスクの停止設定**]グループの[**経過時間**]に時間数と分数を入力します。
- 24 時間のうちで、タスクの実行を一時停止する 24 時間以内の時間間隔を指定する場合は、[**タスクの停止設定**]値グループで、[**一時停止**]と[**から**]に時間間隔の開始する値と終了する値を入力します。

- スケジュールを無効にする日付を指定する場合は、[**スケジュール終了日**]をオンにし、[**カレンダー**]ウィンドウを使用して、スケジュールを無効にする日付を指定します。
- 未実行のタスクの開始を有効にする場合は、[**スキップしたタスクを実行する**]をオンにします。
- 開始時刻の配信設定を有効にする場合は、[**タスク開始を次の期間内でランダム化する**]をオンにし、値を分単位で指定します。

e. [**OK**]をクリックします。

6. 作成したタスクが複数のコンピューターグループ用である場合は、タスクを実行するネットワーク(グループ)コンピューターを選択します。
7. [**タスクを実行するアカウントの選択**]ウィンドウで、タスクを実行するアカウントを指定します。
8. [**タスクの作成を終了**]ウィンドウで、作成後ただちにタスクを開始する場合は[**ウィザード完了後にタスクを実行する**]をオンにします。[**完了**]をクリックします。

[**タスク**]のリストに作成したタスクが表示されます。

Kaspersky Security Center のアプリケーションを設定するウィンドウでのローカルタスクの設定

► **アプリケーションを設定するウィンドウでネットワークサーバー 1 台のローカルタスクまたはアプリケーション設定全般を設定するには、次のタスクを実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、保護対象サーバーが所属するグループを選択します。
2. 結果ペインで、[**デバイス**]タブを選択します。
3. 次のいずれかの方法で、コンピューターのプロパティウィンドウを開きます:
   - 保護対象サーバーの名前をダブルクリックする。

- 保護対象サーバー名のコンテキストメニューを開き、[**プロパティ**]を選択する。

コンピューターのプロパティウィンドウが開きます。

4. ローカルタスクを設定するには、次の手順を実行します:

   a. [**タスク**]セクションに進みます。

   - タスクのリストで、設定するローカルタスクを選択します。
   - タスクのリストで、タスク名をダブルクリックします。
   - タスク名を選択して[**プロパティ**]をクリックします。
   - 選択されたタスクのコンテキストメニューで、[**プロパティ**]を選択します。

5. アプリケーションの設定を行うには、次の手順を実行します:

   a. [**アプリケーション**]セクションに進みます。

   - インストール済みのアプリケーションのリストで、設定するアプリケーションを選択します。
   - インストール済みのアプリケーションのリストで、アプリケーション名をダブルクリックします。
   - インストール済みのアプリケーションのリストで、アプリケーション名を選択して[**プロパティ**]をクリックします。
   - インストール済みのアプリケーションのリストで、アプリケーション名のコンテキストメニューを開き、[**プロパティ**]を選択します。

   > アプリケーションが Kaspersky Security Center ポリシーに従っており、このポリシーでアプリケーション設定の変更が禁止されている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

Kaspersky Security Center でのグループタスクの設定

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **複数のコンピューターに対してグループタスクを設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。
2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。次のいずれかの方法で、タスクのプロパティウィンドウを開きます:
   - 作成済みのタスクのリストで、タスク名をダブルクリックする。
   - 作成済みのタスクのリストでタスク名を選択し、詳細ペインの[**タスクの設定**]をクリックする。
   - 作成済みのタスクのリストからタスク名の上でコンテキストメニューを開き、[**プロパティ**]を選択する。
4. [**通知**]セクションで、タスクイベントの通知設定を行います。

このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

5. 設定したタスクの種別に従って、次のいずれかの処理を実行します:

   - オンデマンドスキャンタスクを設定するには:

     a. [**スキャン範囲**]セクションで、スキャン範囲を生成します。

     b. [**オプション**]セクションで、タスクの優先度とソフトウェアのその他のコンポーネントとの統合を設定します。

   - アップデートタスクを設定するには、要件に基づいてタスク設定を行います:

     a. [**アップデート元**]セクションで、アップデート元の設定とディスクサブシステムの使用の最適化を設定します。

     b. [**接続設定**]をクリックして、全般的な接続設定とアップデート元の接続設定を行います。

   - ソフトウェアモジュールのアップデートタスクを設定する場合は、[**ソフトウェアモジュールのアップデートの設定**]で、ソフトウェアモジュールの重要なアップデートをコピーしインストールするか、ソフトウェアモジュールの重要なアップデートの有無のみを確認します。

   - アップデートのコピータスクを設定する場合は、[**アップデートのコピーの設定**]セクションでアップデートとインストール先フォルダーを指定します。

   - **製品のアクティベーション**タスクを設定する場合は、[**アクティベーション設定**]セクションで製品のアクティベーションに使用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を適用します。ライセンスの更新に使用するアクティベーションコードまたはライセンスを追加する場合は、[予備の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として使用する]をオンにします。

   - アプリケーション起動コントロールルールの自動作成タスクを設定する場合は、[**設定**]セクションで許可ルールのリスト作成の基となる設定を指定します。

6. [**スケジュール**]セクションで、タスクのスケジュールを設定します(定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます)。

7. ［**アカウント**］セクションで、タスクの実行で使用する権限を持つアカウントを指定します。このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

8. 必要に応じて、［**タスク範囲からの除外**］セクションで、タスクの範囲から除外するオブジェクトを指定します。このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

9. タスクのプロパティウィンドウで、［**OK**］をクリックします。

新たに設定したグループタスクの内容が保存されます。

設定可能なグループタスクについて、次の表に概要を示します。

表 27. Kaspersky Security 10.1 for Windows Server グループタスクの設定

Kaspersky Security 10.1 for Windows Server タスクの種別	タスクのプロパティウィンドウ内のセクション	タスクの設定
自動ルール作成(アプリケーション起動コントロールルールの自動作成タスクおよびデバイスコントロールルールの自動作成タスク)。	**設定**	アプリケーション起動コントロールルールの自動作成タスクの設定時に、次を実行できます: • 自動生成されるルールによって起動が許可されるフォルダーのパスの追加や削除をしたり、ファイルの種別を指定したりすることで、保護範囲を変更できます。 • 現在実行中のアプリケーションを考慮してください。

•	**オプション**	アプリケーション起動コントロール許可ルールの作成中に実行する処理を指定できます: **デジタル証明書を使用する** このオプションをオンにすると、アプリケーション起動コントロールに対して新しく生成された許可ルールの設定で、デジタル証明書の存在がルールの適用基準として指定されます。デジタル証明書が指定されたファイルを使用して起動されるプログラムの開始が許可されます。オペレーティングシステムで信頼されているすべてのアプリケーションの起動を許可する場合は、このオプションをオンにしてください。 **デジタル証明書の件名とサムプリントを使用する** アプリケーション起動コントロールの許可ルールを適用する基準として、ファイルのデジタル証明書の件名とサムプリントの使用を有効または無効にします。このチェックボックスをオンにすると、デジタル証明書の確認条件をより厳しく指定できます。このチェックボックスをオンにすると、ルールを生成したファイルのデジタル証明書の件名とサムプリントの値が、アプリケーション起動コントロールの許可ルールを適用するための基準として設定されます。指定されたサムプリントとデジタル証明書を含むファイルを使用して起動されるアプリケーションが許可されます。 サムプリントはデジタル証明書の一意の識別子であり偽造できないため、このチェックボックスをオンにすると、デジタル証明書に基づく許可ルールの適用の制限が厳しくなります。このチェックボックスをオフにすると、オペレーティングシステムで信頼されているすべてのデジタル証明書の存在が、アプリケーション起動コントロールの許可ルールを適用するための基準として設定されます。このチェックボックスは、[**デジタル証明書を使用する**]をオンにすると使用可能になります。 既定では、このチェックボックスはオンです。 **証明書がない場合に使用** ルールの作成に使用されるファイルにデジタル証明書がない場合に、アプリケーション起動コントロールの許可ルールを適用する基準を選択できるドロップダウンリスト。 **SHA256 ハッシュを使用する** このオプションをオンにすると、ルールの作成に使用されるファイルのチェックサムの値が、アプリケーション起動コントロールに対して新しく作成された許可ルールの設定でルールの適用基準として指定されます。指定されたチェックサムの値を持つファイルを使用して起動されるプログラムの開始が許可されます。このオプションは生成されたルールが最高のセキュリティレベルを満たすことを要求される場合:SHA256 チェックサムがユニークなファイル ID として適用される可能性がある場合に推奨されます。ルール有効化の条件として SHA256 チェックサムを使用すると、ルール使用範囲を 1 つのファイルに制限します。既定では、このオプションはオンです。 **ユーザーまたはユーザーグループに対するルールを作成** ユーザーまたはユーザーのグループを表示するフィールド。指定されたユーザーまたはユーザーグループによって実行されるアプリケーションを監視します。 既定の選択項目は[**すべて**]です。 Kaspersky Security 10.1 for Windows Server がタスク完了時に作成する許可ルールリストで、設定ファイルの設定ができます。

	スケジュール	スケジュールによるタスクの開始について設定できます。
製品のアクティベーション	**アクティベーション設定**	製品のアクティベーションや有効期間の更新用にアクティベーションコードまたはライセンスを追加できます。
	スケジュール	スケジュールによるタスクの開始について設定できます。
アップデートのコピー	**アップデート元**	アプリケーションのアップデート元として、Kaspersky Security Center 管理サーバーまたは Kaspersky Lab のアップデートサーバーを指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。 手動でカスタマイズしたサーバーが使用できない場合、Kapersky Lab のアップデートサーバーの使用を指定できます。
	［**接続設定**］ウィンドウ	［**アップデート元への接続設定**］セクションでは、Kaspersky Lab のアップデートサーバーまたはその他のサーバーへの接続をプロキシサーバーを介して確立するかを指定できます。 ► **［接続設定］ウィンドウを開くには、［アップデート元］セクションで［接続設定］をクリックします。**

	アップデートのコピーの設定	コピーするアップデートを指定できます。 [**コピーしたアップデートのローカル用保存フォルダー**]で、コピーしたアップデートの保存先として使用するフォルダーのパスを指定します。
	スケジュール	スケジュールによるタスクの開始について設定できます。
定義データベースのアップデート	**アップデート元**	[**アップデート元**]セクションで、アプリケーションのアップデート元として、Kaspersky Security Center 管理サーバーまたは Kaspersky Lab のアップデートサーバーを指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。 手動でカスタマイズしたサーバーが使用できない場合、Kapersky Lab のアップデートサーバーの使用を指定できます。 [ディスク I/O 使用の最適化]セクションで、ディスクサブシステムの負荷を軽減する機能を設定できます: • **ディスク I/O の負荷の低減** このチェックボックスでは、RAM の仮想ドライブへのアップデートファイルの保管によるディスクサブシステムの最適化の機能を有効または無効にします。 このチェックボックスをオンにすると、この機能が有効になります。 既定では、このチェックボックスはオフです。 • **最適化に使用するメモリ(MB)**

アプリケーションがアップデートファイルの保存に使用する RAM のサイズ（MB）。 既定の RAM のサイズは 512 MB です	［**接続設定**］ウィンドウ	［**アップデート元への接続設定**］セクションでは、Kaspersky Lab のアップデートサーバーまたはその他のサーバーへの接続をプロキシサーバーを介して確立するかを指定できます。 ► **［接続設定］ウィンドウを開くには、** ［**アップデート元**］セクションで［**接続設定**］をクリックします。
	スケジュール	スケジュールによるタスクの開始について設定できます。
ソフトウェアモジュールのアップデート	**アップデート元**	アプリケーションのアップデート元として、Kaspersky Security Center 管理サーバーまたは Kaspersky Lab のアップデートサーバーを指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。 手動でカスタマイズしたサーバーが使用できない場合、Kapersky Lab のアップデートサーバーの使用を指定できます。
	［**接続設定**］ウィンドウ	［**アップデート元への接続設定**］セクションでは、Kaspersky Lab のアップデートサーバーまたはその他のサーバーへの接続をプロキシサーバーを介して確立するかを指定できます。 ► **［接続設定］ウィンドウを開くには、** ［**アップデート元**］セクションで［**接続設定**］をクリックします。

	ソフトウェアモジュールのアップデートの設定	ソフトウェアモジュールの重要なアップデートが適用可能な場合またはすでにインストール済みの場合に実行する処理を指定できます。定期アップデートに関する情報を受信するかどうかの指定も行えます。
	スケジュール	スケジュールによるタスクの開始について設定できます。
オンデマンドスキャン	**スキャン範囲**	オンデマンドスキャンタスクのスキャン範囲を指定し、セキュリティレベルを設定できます。
	[**オンデマンドスキャンの設定**]ウィンドウ	定義済みのセキュリティレベルから 1 つを選択するか、セキュリティレベルを手動でカスタマイズできます。 ► **[オンデマンドスキャンの設定]ウィンドウを開くには、** [**スキャン範囲**]セクションで[**設定**]をクリックします。
	オプション	[**ヒューリスティックアナライザー**]セクションで、オンデマンドスキャンタスクでのヒューリックアナライザーの使用をアクティベートまたはアクティベート解除できます。また、スライダーを使用して分析レベルを設定できます。 [**オプション**]セクションでは、次の設定を行うことができます: • オンデマンドスキャンタスクでの信頼ゾーンの適用 • オンデマンドスキャンタスクでの KSN の使用の適用 • オンデマンドスキャンタスクの優先度の設定:バックグラウンドモードでのタスクの実行(優先度「低」)またはタスクを重要領域のスキャンとします。
	スケジュール	スケジュールによるタスクの開始について設定できます。

アプリケーションの整合性チェック	**スケジュール**	スケジュールによるタスクの開始について設定できます。

定義データベースのロールバックなどのタスクでは、標準のタスク設定のみ、Kaspersky Security Center によって制御される[**通知**]セクションおよび[**タスク範囲からの除外**]セクションで設定できます。このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

このセクションの内容

アプリケーション起動コントロールルールの自動作成タスクおよびデバイスコントロールルールの自動作成タスク

► **デバイスコントロールルールの自動作成タスクまたはアプリケーション起動コントロールルールの自動作成タスクを設定するには、以下の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。

2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。

3. 以前作成したグループタスクのリストで、設定するタスクを選択します。タスクのコンテキストメニューを開いて、[**プロパティ**]を選択します。

   タスクのプロパティウィンドウが開きます。

4. [**通知**]セクションで、タスクイベントの通知設定を行います。

5. このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

6. [**設定**]セクションでは、次の設定を行うことができます:

   - 自動生成されるルールによって起動が許可されるフォルダーのパスを追加や削除をしたり、ファイルの種別を指定したりすることで、保護範囲を変更できます。

   - 現在実行中のアプリケーションを考慮してください。

7. [**オプション**]セクションでは、アプリケーション起動コントロールの許可ルール作成時に実行する処理を指定できます:

   - **デジタル証明書を使用する**

     このオプションをオンにすると、アプリケーション起動コントロールに対して新しく生成された許可ルールの設定で、デジタル証明書の存在がルールの適用基準として指定されます。デジタル証明書が指定されたファイルを使用して起動されるプログラムの開始が許可されます。オペレーティングシステムで信頼されているすべてのアプリケーションの起動を許可する場合は、このオプションをオンにしてください。

   - **デジタル証明書の件名とサムプリントを使用する**

     アプリケーション起動コントロールの許可ルールを適用する基準として、ファイルのデジタル証明書の件名とサムプリントの使用を有効または無効にします。このチェックボックスをオンにすると、デジタル証明書の確認条件をより厳しく指定できます。

     このチェックボックスをオンにすると、ルールを生成したファイルのデジタル証明書の件名とサムプリントの値が、アプリケーション起動コントロールの許可ルールを適用するための基準として設定されます。指定されたサムプリントとデジタル証明書を含むファイ

ルを使用して起動されるアプリケーションが許可されます。

サムプリントはデジタル証明書の一意の識別子であり偽造できないため、このチェックボックスをオンにすると、デジタル証明書に基づく許可ルールの適用の制限が厳しくなります。

このチェックボックスをオフにすると、オペレーティングシステムで信頼されているすべてのデジタル証明書の存在が、アプリケーション起動コントロールの許可ルールを適用するための基準として設定されます。

このチェックボックスは、[**デジタル証明書を使用する**]をオンにすると使用可能になります。

既定では、このチェックボックスはオンです。

- **証明書がない場合に使用**

  ルールの作成に使用されるファイルにデジタル証明書がない場合に、アプリケーション起動コントロールの許可ルールを適用する基準を選択できるドロップダウンリスト。

  - **SHA256 ハッシュ**ルールの作成に使用されるファイルのチェックサムの値が、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。指定されたチェックサムを持つファイルを使用して起動されるプログラムの開始が許可されます。
  - **ファイルのパス**ルールの作成に使用されるファイルのパスが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。[設定]セクションの[次のフォルダーにあるアプリケーションに対する許可ルールを作成する]テーブルのタブで指定されたフォルダーにあるファイルを使用して起動されるプログラムの開始が許可されます。

- **SHA256 ハッシュを使用する**

  このオプションをオンにすると、ルールの作成に使用されるファイルのチェックサムの値が、アプリケーション起動コントロールに対して新しく作成された許可ルールの設定でルールの適用基準として指定されます。指定されたチェックサムの値を持つファイルを使用して起動されるプログラムの開始が許可されます。

  このオプションは生成されたルールが最高のセキュリティレベルを満たすことを要求さ

れる場合：SHA256 チェックサムがユニークなファイル ID として適用される可能性がある場合に推奨されます。ルール有効化の条件として SHA256 チェックサムを使用すると、ルール使用範囲を 1 つのファイルに制限します。

既定では、このオプションはオフです。

- **ユーザーまたはユーザーグループに対するルールを作成**

  ユーザーまたはユーザーのグループを表示するフィールド。指定されたユーザーまたはユーザーグループによって実行されるアプリケーションを監視します。

  既定の選択項目は［**Everyone**］です。

Kaspersky Security 10.1 for Windows Server がタスク完了時に作成する許可ルールリストで、設定ファイルの設定ができます。

8. ［**スケジュール**］セクションで、タスクのスケジュールを設定します（定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます）。
9. ［**アカウント**］セクションで、タスクの実行で使用する権限を持つアカウントを指定します。
10. 必要に応じて、［**タスク範囲からの除外**］セクションで、タスクの範囲から除外するオブジェクトを指定します。

> これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

11. タスクのプロパティウィンドウで、［**OK**］をクリックします。

新たに設定したグループタスクの内容が保存されます。

製品のアクティベーションタスク

► **製品のアクティベーションタスクを設定するには、次の手順を実行します：**

1. Kaspersky Security Center の管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。

2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。タスクのコンテキストメニューを開いて、[**プロパティ**]を選択します。

   タスクのプロパティウィンドウが開きます。
4. [**通知**]セクションで、タスクイベントの通知設定を行います。
5. このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。
6. [**アクティベーション設定**]セクションでは、製品のアクティベーションに使用するライセンス情報ファイルを適用します。ライセンスを延長するためにライセンスを追加するときは、[**予備のアクティベーションコードまたはライセンスとして使用する**]をオンにします。
7. [**スケジュール**]セクションで、タスクのスケジュールを設定します(定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます)。
8. [**アカウント**]セクションで、タスクの実行で使用する権限を持つアカウントを指定します。
9. 必要に応じて、[**タスク範囲からの除外**]セクションで、タスクの範囲から除外するオブジェクトを指定します。

   > これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。
10. タスクのプロパティウィンドウで、[**OK**]をクリックします。

    新たに設定したグループタスクの内容が保存されます。

アップデートタスク

アップデートのコピー、定義データベースのアップデート、またはソフトウェアモジュールのアップデートの各タスク

を設定するには、次の手順を実行します:

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。

2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。

3. 以前作成したグループタスクのリストで、設定するタスクを選択します。タスクのコンテキストメニューを開いて、[**プロパティ**]を選択します。

   タスクのプロパティウィンドウが開きます。

4. [**通知**]セクションで、タスクイベントの通知設定を行います。

   > このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

5. 設定したタスクの種別に従って、次のいずれかの処理を実行します:

   - [**アップデート元**]セクションで、アップデート元の設定とディスクサブシステムの使用の最適化を設定します。

     a. [**アップデート元**]セクションで、アプリケーションのアップデート元として、Kaspersky Security Center 管理サーバーまたは Kaspersky Lab のアップデートサーバーを指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。

     手動でカスタマイズしたサーバーが使用できない場合、Kapersky Lab のアップデートサーバーの使用を指定できます。

     b. 定義データベースのアップデートタスクの[**ディスク I/O 使用の最適化**]セクションで、ディスクサブシステムの負荷を軽減する機能を設定できます:

        - **ディスク I/O の負荷の低減**

     このチェックボックスでは、RAM の仮想ドライブへのアップデートファイルの保管によるディスクサブシステムの最適化の機能を有効または無効にします。

     このチェックボックスをオンにすると、この機能が有効になります。

既定では、このチェックボックスはオフです。

- **最適化に使用するメモリ(MB)**

アプリケーションがアップデートファイルの保存に使用する RAM のサイズ(MB)。既定の RAM のサイズは 512 MB です。

c. [**接続設定**]をクリックすると、[**接続設定**]ウィンドウが開くので、そこで Kaspersky Lab のアップデートサーバーとその他のサーバーへの接続にプロキシサーバーを使用するように設定します。

- ソフトウェアモジュールのアップデートタスクの[**ソフトウェアモジュールのアップデートの設定**]セクションでは、重要なソフトウェアモジュールのアップデートが適用可能なときまたは定期アップデートに関する情報があるときに Kaspersky Security 10.1 for Windows Server が実行する処理と、重要なアップデートがインストールされるときに Kaspersky Security 10.1 for Windows Server が実行する処理を指定できます。

- [**アップデートのコピー**]タスクの[**アップデートのコピーの設定**]セクションで、アップデートのセットと宛先フォルダーを指定します。

6. [**スケジュール**]セクションで、タスクのスケジュールを設定します(定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます)。

7. [**アカウント**]セクションで、タスクの実行で使用する権限を持つアカウントを指定します。

8. 必要に応じて、[**タスク範囲からの除外**]セクションで、タスクの範囲から除外するオブジェクトを指定します。

> これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

9. タスクのプロパティウィンドウで、[**OK**]をクリックします。

新たに設定したグループタスクの内容が保存されます。

定義データベースのロールバックタスクについては、[**通知**]内の Kaspersky Security Center および[**タスク範**

囲からの除外]セクションによってコントロールされる標準タスク設定のみを設定できます。これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

アプリケーションの整合性チェック

► **アプリケーションの整合性チェックタスクを設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。
2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。タスクのコンテキストメニューを開いて、[**プロパティ**]を選択します。

   タスクのプロパティウィンドウが開きます。
4. [**通知**]セクションで、タスクイベントの通知設定を行います。

   > このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。
5. [**スケジュール**]セクションで、タスクのスケジュールを設定します(定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます)。
6. [**アカウント**]セクションで、タスクの実行で使用する権限を持つアカウントを指定します。
7. 必要に応じて、[**タスク範囲からの除外**]セクションで、タスクの範囲から除外するオブジェクトを指定します。

   > これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。
8. タスクのプロパティウィンドウで、[**OK**]をクリックします。

新たに設定したタスクの内容が保存されます。

オンデマンドスキャンタスクの作成

► **Kaspersky Security Center の管理コンソールで新しいタスクを作成するには:**

1. 次のいずれかの方法でタスクウィザードを開始します:

   - ローカルタスクを作成するには:

     a. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、保護対象サーバーが所属するグループを選択します。

     b. 詳細ペインの[**デバイス**]タブで、保護対象のサーバーの情報が含まれる行でコンテキストメニューを開き、[**プロパティ**]を選択します。

     c. 表示されるウィンドウの[**タスク**]セクションで[**追加**]をクリックします。

   - グループタスクを作成するには:

     a. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、ポリシーを作成するグループを選択します。

     b. 詳細ペインで[**タスク**]タブのコンテキストメニューを開き、[**作成**] - [**タスク**]の順に選択します。

   - カスタムセットのコンピューターにタスクを作成するには、Kaspersky Security Center の管理コンソールツリーで[**デバイスの抽出**]-[**タスクの作成**]を選択します。

   タスクウィザードのウィンドウが開きます。

2. [**タスク名の定義**]ウィンドウで、タスク名を入力します(100 文字以内とし、**¥"*<>?¥¥:|**は使用できません)。タスク名にタスク種別(「共有フォルダーのオンデマンドスキャン」など)を追加してください。

3. [**タスク種別の選択**]ウィンドウの[**Kaspersky Security 10.1 for Windows Server**]ヘッダーで[**オンデマンドスキャン**]タスクを選択し、[**次へ**]をクリックします。

4. [**スキャン範囲**]ウィンドウでスキャン範囲を作成します:

既定では、サーバーの重要な領域がスキャン範囲に含まれます。スキャン範囲は、表では ☑ アイコンのマークが付きます。除外するスキャン範囲には、表で ☐ アイコンのマークが付きます。

スキャン範囲は変更できます。特定の事前に設定されたスキャン範囲、ディスク、フォルダー、ネットワークオブジェクトおよびファイルを追加し、追加した範囲ごとに特定のセキュリティ設定を割り当てます。

- すべての重要な領域をスキャン対象から除外するには、各行のコンテキストメニューを開いて[**範囲の削除**]を選択します。
- 定義済みのスキャン範囲、ディスク、フォルダー、ネットワークオブジェクト、またはファイルをスキャン範囲に含めるには:
    a. [**スキャン範囲**]テーブルを右クリックし、[**範囲の追加**]を選択します。
    b. [**スキャン範囲にオブジェクトを追加**]の[**定義済みの範囲**]リストで定義済みの範囲を選択し、サーバーまたはその他のネットワークコンピューターのサーバーディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定して[**OK**]をクリックします。
- サブフォルダーまたはファイルをスキャンから除外するには、ウィザードの[**スキャン範囲**]ウィンドウで追加されたフォルダー(ディスク)を選択します。
    a. コンテキストメニューを開いて、[**設定**]を選択します。
    b. [**セキュリティレベル**]タブの[**設定**]をクリックします。
    c. [**オンデマンドスキャン**の設定]ウィンドウの[**全般**]タブで、[**サブフォルダー**]と[**サブファイル**]をオフにします。
- スキャン範囲のセキュリティ設定を変更するには:
    a. 設定を行う範囲のコンテキストメニューを開き、[**設定**]を選択します。
    b. [**オンデマンドスキャンの設定**]ウィンドウで、定義済みのセキュリティレベルから 1 つを選択するか、[**設定**]をクリックしてセキュリティ設定を手動で設定します。

    Kaspersky Security 10.1 コンソールと同じ方法でセキュリティ設定が実行されます。
- 追加されたスキャン範囲内で埋め込みオブジェクトをスキップするには:
    a. [**スキャン範囲**]テーブルのコンテキストメニューを開き、[**除外の追加**]を選択します。

b. 除外するオブジェクトを指定します：[**定義済みの範囲**]リスト内で定義済み範囲を選択し、サーバーまたは別のネットワークコンピューター上のコンピューターディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定します。

c. [**OK**]をクリックします。

5. [**オプション**]ウィンドウで、ヒューリスティックアナライザーと、他のコンポーネントとの統合を設定します。

- ヒューリスティックアナライザーの使用を設定します（274 ページのセクション「ヒューリスティックアナライザーの使用」を参照）。

- Kaspersky Security 10.1 for Windows Server の信頼ゾーンに記載されているオブジェクトをタスクのスキャン範囲から除外するには、[**信頼ゾーンを適用する**]をオンにします。

  このチェックボックスにより、タスクに対する信頼ゾーンの使用を有効または無効にします。

  このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、信頼されたプロセスのファイル操作が、タスクの設定で指定されたスキャンの除外対象に追加されます。

  チェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、ファイルのリアルタイム保護タスクの保護範囲を作成するときに信頼されたプロセスのファイル操作を無視します。

  既定では、このチェックボックスはオンです。

- Kaspersky Security Network クラウドサービスをタスクに使用するには、[**スキャンに KSN を使用する**]をオンにします。

  タスクの Kaspersky Security Network（KSN）のクラウドサービスの使用を有効または無効にします。

  このチェックボックスをオンにすると、KSN サービスから受信したデータを使用して、新しい脅威に対する応答時間を迅速化し、誤検知の可能性を減少させます。

  このチェックボックスをオフにすると、オンデマンドスキャンタスクは KSN サービスを使用しません。

既定では、このチェックボックスはオンです。

- タスクが実行される処理対象プロセスに基本の優先度[**低**]を割り当てるには、[**オプション**]ウィンドウで[**バックグラウンドモードでタスクを実行する**]をオンにします。

  タスクの優先度が変更されます。

  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でのタスクの優先度が低くなります。他の Kaspersky Security 10.1 for Windows Server タスクおよびアプリケーションによる CPU とコンピューターファイルシステムに対する負荷に応じて、タスクを実行するためのリソースがオペレーティングシステムから提供されます。これにより、負荷が高いときはタスクの実行速度が低下し、負荷が低いときは実行速度が速くなります。

  このチェックボックスをオフにすると、他の Kaspersky Security 10.1 for Windows Server タスクおよびアプリケーションと同じ優先度でタスクが開始および実行されます。この場合、タスクの実行速度が速くなります。

  既定では、このチェックボックスはオフです。

既定では、Kaspersky Security 10.1 for Windows Server タスクが実行される処理対象プロセスは、優先度[**中**]([**標準**])です。

- 重要領域のスキャンタスクとして作成したタスクを使用する場合、[**オプション**]ウィンドウで[**タスクを重要領域のスキャンとする**]をオンにしてください。

  このチェックボックスでは、**重要領域のスキャン**イベントの記録およびサーバー保護のステータスの更新を有効または無効にし、タスクの優先度を変更します。Kaspersky Security Center では、**重要領域のスキャン**のステータスを持つタスクの実行結果によって、サーバーのセキュリティを評価します。Kaspersky Security 10.1 for Windows Server のローカルのシステムタスクおよびカスタムタスクのプロパティでは、このチェックボックスは利用できません。この設定は、Kaspersky Security Center 側でのみ編集できます。

  このチェックボックスをオンにすると、管理サーバーにより、完了した重要領域のスキャンイベントが記録され、タスクの実行結果に基づいてサーバーの保護ステータスが更

新されます。このスキャンタスクの優先度は「高」です。

このチェックボックスをオフにすると、タスクは優先度「低」で実行されます。

簡易スキャンタスクでは、このチェックボックスは既定でオンになります。

6. [**次へ**]をクリックします。
7. [**スケジュール**]ウィンドウで、タスクのスケジュールをセットアップします(221 ページのセクション「タスク開始スケジュールの設定」を参照)。
8. タスクの実行とタスク名の定義を行うユーザーアカウントを指定します。
9. [**完了**]をクリックします。

選択したサーバーまたはサーバーグループに新規オンデマンドスキャンタスクが作成されます。

オンデマンドスキャンタスクの設定

► **既存のオンデマンドスキャンタスクを設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。アプリケーションタスク設定を行うコンピューターの管理グループを展開します。
2. 選択した管理グループの結果ペインで[**タスク**]タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。タスクのコンテキストメニューを開いて、[**プロパティ**]を選択します。

   タスクのプロパティウィンドウが開きます。
4. [**通知**]セクションで、タスクイベントの通知設定を行います。

   このセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

5. [**設定**]セクションでは、次の処理を行うことができます:

   a. [**スキャン範囲**]セクションでは、スキャン範囲に含めるファイルリソース隣のチェックボックスをオンにします。

   b. [**設定**]をクリックして、セキュリティレベルを選択します。

   定義済みのセキュリティレベルから 1 つを選択するか、セキュリティレベルを手動でカスタマイズできます。セキュリティレベルを手動で設定するには、[**オンデマンドスキャンの設定**]ウィンドウで[**設定**]をクリックします。

6. [**オプション**]セクションで、次の処理を実行できます:

   a. [**ヒューリスティックアナライザー**]の使用を有効または無効にする、[**ヒューリスティックアナライザー**]ブロック内のスライダーを使用して分析レベルを設定する。

   b. [**他のコンポーネントとの統合**]を設定します(209 ページのセクション「**オンデマンドスキャンタスクの作成**」を参照)。

7. [**スケジュール**]セクションで、タスクのスケジュールを設定します(定義データベースのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます)。

8. [**アカウント**]セクションで、タスクの実行で使用する権限を持つアカウントを指定します。

9. 必要に応じて、[**タスク範囲からの除外**]セクションで、タスクの範囲から除外するオブジェクトを指定します。

   > これらのセクションでの設定の詳細情報については、『**Kaspersky Security Center ヘルプ**』を参照してください。

10. タスクのプロパティウィンドウで、[**OK**]をクリックします。

    新たに設定したタスクの内容が保存されます。

オンデマンドスキャンタスクへの重要領域のスキャンタスクのステータスの割り当て

既定では、重要領域のスキャンタスクの実行頻度が Kaspersky Security 10.1 for Windows Server のイベント生成しきい値の[**重要領域のスキャンが長期間実行されていません**]設定より低い場合に、Kaspersky Security Center によりサーバーに対して**警告**の状態が割り当てられます。

► **1 つの管理グループですべてのサーバーのスキャンを設定するには、次の手順を実行します**:

1. グループのオンデマンドスキャンタスクを作成します。
2. タスクウィザードの[**オプション**]ウィンドウで、[**タスクを重要領域のスキャンとする**]をオンにします。指定したタスク設定(スキャン範囲およびセキュリティ設定)が、グループ内のすべてのコンピューターに適用されます。タスクのスケジュールを設定します。

   [**タスクを重要領域のスキャンとする**]は、コンピューターのグループまたはコンピューターのセットに対してオンデマンドスキャンタスクを作成するときにオンにするか、後でタスクのプロパティウィンドウでオンにします。

3. 新しいポリシーまたは既存のポリシーを使用して、システムスキャンタスクのスケジュールによる開始を無効にします(「181 ページのセクションローカルのシステムタスクのスケジュールによる開始の設定」を参照)。

Kaspersky Security Center 管理サーバーによって、保護対象サーバーのセキュリティの状態が評価され、**重要領域のスキャン**のシステムタスクの結果ではなく、前回のタスク実行結果と重要領域のスキャンの状態に基づいて、その状態が通知されます。

重要領域のスキャンタスクの状態は、グループのオンデマンドスキャンタスクと、特定のコンピューターのタスクの両方に割り当てることができます。

Kaspersky Security 10.1 コンソールを使用して、オンデマンドスキャンタスクが重要領域のスキャンタスクであるかを確認できます。

Kaspersky Security 10.1 コンソールでは、タスク設定に[**タスクを重要領域のスキャンとする**]が表示されますが、この設定を編集することはできません。

Kaspersky Security Center でのクラッシュの診断設定

Kaspersky Security 10.1 for Windows Server の使用中に Kaspersky Security 10.1 for Windows Server のクラッシュなどの問題が発生し、その問題を診断する場合、Kaspersky Security 10.1 for Windows Server プロセスのトレースファイルおよびダンプファイルの作成を有効にし、それらのファイルを解析するために Kaspersky Lab テクニカルサポートに送信することができます。

Kaspersky Security 10.1 for Windows Server からは、トレースファイルまたはダンプファイルは自動的に送信されません。診断データは、該当する権限を持つユーザーのみが送信できます。

Kaspersky Security 10.1 for Windows Server では、暗号化されていない形式でトレースファイルとダンプファイルに情報を書き込みます。ファイルが保存されるフォルダーはユーザーが選択し、オペレーティングシステムの設定と Kaspersky Security 10.1 for Windows Server の設定によって管理されます。アクセス権限を設定して(152 ページのセクション「Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限」を参照)、ログファイルやトレースファイル、ダンプファイルへのアクセスを必要なユーザーに対してのみ許可することができます。

► **Kaspersky Security Center でクラッシュの診断を設定するには:**

1. Kaspersky Security Center の管理コンソールで、[**アプリケーションのプロパティ**]ウィンドウを開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

2. [**トラブルシューティング**]セクションで次の操作を実行します:

- デバッグ情報をファイルに書き込む場合は、[**デバッグ情報をトレースファイルに書き込む**]をオンにします。

  - 下にあるフィールドで、トレースファイルを保存するフォルダーを指定します。
  - デバッグ情報の詳細レベルを設定します。

    このドロップダウンリストでは、Kaspersky Security 10.1 for Windows Server によってトレースファイルに保存されるデバッグ情報の詳細レベルを選択できます。

    次のいずれかの詳細レベルを選択できます:

    - **緊急イベント** - Kaspersky Security 10.1 for Windows Server により、緊急イベントに関する情報のみがトレースファイルに保存されます。
    - **エラー** - Kaspersky Security 10.1 for Windows Server により、緊急イベントとエラーに関する情報がトレースファイルに保存されます。
    - **注意が必要なイベント** - Kaspersky Security 10.1 for Windows Server により、緊急イベント、エラー、および注意が必要なイベントに関する情報がトレースファイルに保存されます。
    - **情報イベント** - Kaspersky Security 10.1 for Windows Server により、緊急イベント、エラー、注意が必要なイベント、および情報イベントに関する情報がトレースファイルに保存されます。
    - **すべてのデバッグ情報** - Kaspersky Security 10.1 for Windows Server により、すべてのデバッグ情報がトレースファイルに保存されます。

    発生した問題を解決するために設定する必要がある詳細レベルは、テクニカルサポートが判断します。

    既定の詳細レベルは、[**すべてのデバッグ情報**]に設定されています。

    このドロップダウンリストは、[**デバッグ情報をトレースファイルに書き込む**]をオンにすると使用可能になります。

  - トレースファイルの最大サイズを指定します。
  - デバッグするコンポーネントを指定します。コンポーネントコードを複数指定する場合は、セミコロ

ンで区切る必要があります。コードは大文字と小文字が区別されます（次の表を参照）。

表 28. Kaspersky Security 10.1 for Windows Server サブシステムコード

コンポーネントコード	コンポーネントの名前
*	すべてのコンポーネント
gui	ユーザーインターフェイスサブシステム、Microsoft 管理コンソール形式の Kaspersky Security 10.1 for Windows Server スナップイン
ak_conn	ネットワークエージェントと Kaspersky Security Center の統合のためのサブシステム
bl	コントロールプロセス、Kaspersky Security 10.1 for Windows Server コントロールタスクの実装
wp	アンチウイルスによる保護タスクを処理する処理対象プロセス
blgate	Kaspersky Security 10.1 for Windows Server リモート管理プロセス
ods	オンデマンドスキャンサブシステム
oas	ファイルのリアルタイム保護サブシステム
qb	隔離およびバックアップのサブシステム
scandll	アンチウイルススキャンのための補助モジュール
core	アンチウイルス基本機能のためのサブシステム
avscan	アンチウイルス処理サブシステム
avserv	アンチウイルスのカーネルの管理のためのサブシステム
prague	基本機能のためのサブシステム
updater	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ためのサブシステム

snmp	SNMP プロトコルサポートサブシステム
perfcount	パフォーマンスカウンターサブシステム

Kaspersky Security 10.1 for Windows Server スナップインのトレース設定（gui）および Kaspersky Security Center の Kaspersky Security 10.1 for Windows Server プラグインのトレース設定（ak_conn）は、それらのコンポーネントが再起動された後に適用されます。SNMP プロトコルサポートサブシステムのトレース設定（snmp）は、SNMP サービスが再起動された後に適用されます。パフォーマンスカウンターサブシステムのトレース設定（perfcount）は、パフォーマンスカウンターを使用するすべてのプロセスが再起動された後に適用されます。その他の Kaspersky Security 10.1 for Windows Server サブシステムのトレース設定は、クラッシュの診断設定が保存されるとすぐに適用されます。

既定値で、Kaspersky Security 10.1 for Windows Server は、すべての Kaspersky Security 10.1 for Windows Server コンポーネントのデバック情報をログに記録します。

この入力フィールドは、[**デバッグ情報をトレースファイルに書き込む**]をオンにすると使用可能になります。

- ダンプファイルを作成する場合は、[**ダンプファイルの作成**]をオンにしてください。
    - 下にあるフィールドで、メモリダンプファイルを保存するフォルダーを指定します。

3. [**OK**]をクリックします。

アプリケーションの設定内容が保護対象サーバーに適用されます。

タスクスケジュールの管理

Kaspersky Security 10.1 for Windows Server タスクの開始スケジュールを設定して、スケジュールによってタスクを実行するための設定を行うことができます。

このセクションの内容

タスク開始スケジュールの設定

Kaspersky Security 10.1 コンソールでは、ローカルのシステムタスクとカスタムタスクの開始スケジュールを設定することができます。グループタスクの開始スケジュールを設定することはできません。

► **タスクの開始スケジュールを設定するには、次の手順を実行します:**

1. Kaspersky Security Center コンソールツリーで、[**管理対象デバイス**]フォルダーを展開して、次の手順を実行します。

   - ポリシーを設定するには、コンピューターグループで[**ポリシー**]-[**ポリシー名**]-[**セクション**]-[**設定**]-[**タスク管理**]を選択します。
   - Kaspersky Security Center を使用して単一のコンピューターのアプリケーションを設定する場合、Kaspersky Security Center で[**タスクのプロパティ**]ウィンドウを開きます(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     [**タスクのプロパティ**]ウィンドウが開きます。

2. 表示されたウィンドウの[**スケジュール**]タブで、[**スケジュールに従って実行する**]をオンにします。

オンデマンドスキャンタスクとアップデートタスクのスケジュール設定に使用するフィールドは、スケジュールによる開始が Kaspersky Security Center のポリシーによってブロックされている場合、使用できません。

3. 要件に従ってスケジュールを設定します。それには、次の操作を実行します:

   a. [**頻度**]リストでは、次の値のいずれかを選択します:

   - [**時間単位**]:指定された時間間隔でタスクを実行する場合は、[**<数字> 時間**ごと]で時間数を指定します。
   - [**日単位**]:指定された日間隔でタスクを実行する場合は、[**<数字> 日**ごと]で日数を指定します。
   - [**週単位**]:指定された週間隔でタスクを実行する場合は、[**<数字> 週**ごと]で週数を指定します。タスクが開始される曜日を指定します(既定では、タスクは月曜日に実行されます)。
   - [**アプリケーションの起動時**]:Kaspersky Security 10.1 for Windows Server が起動するたびにタスクを実行します。
   - [**定義データベースのアップデート後**]:定義データベースのアップデート後にタスクを実行します。

   b. [**開始時刻**]にタスクを最初に開始する時刻を指定します。

   c. [**開始日**]にスケジュールの適用を開始する日付を指定します。

   タスクの開始頻度、タスクが最初に開始される時刻、およびスケジュールの適用開始日を指定したら、ウィンドウ上部の[**次回開始**]に、計算された次回のタスク開始時間に関する情報が表示されます。[**タスク**]の設定ウィンドウの[**スケジュール**]タブを開くたびに、次回タスクが開始される予定の日時に関する情報が更新されて、表示されます。

   Kaspersky Security Center のアクティブなポリシー設定により、システムタスクのスケジュールによる開始がブロックされている場合、[**次回開始**]に[**ポリシーによりブロック**]の値が表示されます(181 ページのセクション「ローカルのシステムタスクのスケジュールによる開始の設定」を参照)。

4. [**詳細設定**]タブを使用して、要件に従って以下のスケジュール設定を指定します:

   - [**タスクの停止設定**]セクション:

     a. [**経過時間**]をオンにして、右側のフィールドにタスク実行の最大経過時間を指定するために

必要な時間と分の数値を入力します。

b. [**一時停止**]をオンにして、右側のフィールドにタスクの実行が一時停止される間隔を 24 時間で指定するために開始と終了の値を入力します。

- [**詳細設定**]セクション:

a. [**スケジュール終了日**]をオンにして、スケジュールの起動を停止する日付を指定します。

b. [**スキップしたタスクを実行する**]をオンにして、スキップしたタスクの開始を有効にします。

c. [**タスク開始を次の期間内でランダム化する**]をオンにして、値を分で指定します。

5. [**適用**]をクリックして、タスク開始の設定を保存します。

スケジュールに従ったタスクの有効化と無効化

スケジュール設定を行う前、または行った後で、スケジュールに従ったタスクを有効または無効にできます。

► **タスクの開始スケジュールを有効化または無効化するには、次の手順を実行します:**

1. Kaspersky Security 10.1 コンソールツリーで、開始スケジュールを設定するタスク名でコンテキストメニューを開きます。

2. [**プロパティ**]を選択します。

   [**タスクのプロパティ**]ウィンドウが表示されます。

3. 表示されたウィンドウの[**スケジュール**]タブで、次のいずれかの操作を行います:

   - スケジュール設定されたタスクの開始を有効にする場合は、[**スケジュールに従って実行する**]をオンにします。

   - スケジュール設定されたタスクの開始を無効にする場合は、[**スケジュールに従って実行する**]をオフにします。

> 設定されたタスク開始のスケジュール設定は削除されず、次回のタスク開始スケジュールで適用されます。

4. ［**適用**］をクリックします。

タスク開始スケジュールの設定が保存されます。

アプリケーション設定の管理

このセクションでは、Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server の全般的な設定についての情報が記載されています。

この章の内容

Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server の管理方法について

インストールされ、管理グループに含まれた Kaspersky Security 10.1 for Windows Server を使用すると、Kaspersky Security Center プラグインにより複数のサーバーを集中管理できます。Kaspersky Security Center も別々に管理グループに含まれる各サーバーの操作設定を設定させます。

管理グループは、Kaspersky Security Center 側で手動で作成され、Kaspersky Security 10.1 for Windows Server がインストールされている複数のサーバーが含まれます。それらのサーバーに対して、同じ管理設定や保護設定を行えます。管理グループの使用の詳細については、『**Kaspersky Security Center ヘルプ**』を参照

してください。

> サーバーにインストールされている Kaspersky Security 10.1 for Windows Server の動作が Kaspersky Security Center のアクティブポリシーによって制御されている場合、各コンピューターに対するアプリケーションの設定は行えません。

Kaspersky Security Center から Kaspersky Security 10.1 for Windows Server を管理するには、次の方法を実行します:

- **Kaspersky Security Center のポリシーを使用する**:Kaspersky Security Center のポリシーでは、サーバーグループに対して同じ保護設定をリモートで行うことができます。アクティブポリシーで指定されるタスク設定は、Kaspersky Security 10.1 コンソールでローカルで指定されるタスク設定や Kaspersky Security Center のコンピューターのプロパティウィンドウでリモートで指定されるタスク設定よりも優先度が高いです。

  ポリシーを使用して、アプリケーションの全般的な設定、リアルタイム保護タスクの設定、ローカルアクティビティの管理タスクの設定、ネットワーク接続ストレージの保護タスクの設定、スケジュールによるシステムタスクの開始設定、およびプロファイルの使用設定が行えます。

- **Kaspersky Security Center のグループタスクを使用する**:Kaspersky Security Center のグループタスクでは、サーバーグループに対して、有効期限があるタスクの共通設定をリモートで編集できるようになります。

  グループタスクを使用して、製品のアクティベーション、オンデマンドスキャンタスクの設定、アップデートタスクの設定、アプリケーション起動コントロールルールの自動作成タスクの設定が行えます。

- **特定のデバイスのタスクを使用する**:特定のデバイスのタスクを使用すると、どの管理グループにも属していないサーバーに対する、有効期限付きの共通のタスク設定がリモートで行えます。

- **単一のコンピューターのプロパティウィンドウの使用**:コンピューターのプロパティウィンドウで、管理グループに含まれるサーバー 1 台に対して、タスクをリモートで設定できます。選択したサーバーが、Kaspersky Security Center のアクティブポリシーによって制御されていない場合、アプリケーションの全般的な設定とすべての Kaspersky Security 10.1 for Windows Server タスクの設定の両方を編集できます。

Kaspersky Security Center を使用すると、アプリケーションや高度な機能を設定し、ログや通知を利用できます。個別のサーバーだけでなく、サーバーのグループに対してもこれらの設定ができます。

Kaspersky Security Center での全般的なアプリケーション設定

Kaspersky Security Center から、サーバーグループまたは 1 つのサーバーに対して Kaspersky Security 10.1 for Windows Server の全般的な設定を行えます。

このセクションの内容

Kaspersky Security Center でのスケーラビリティおよびインターフェイスの設定

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **スケーラビリティ設定およびアプリケーションインターフェイスを設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**アプリケーションの設定**]セクションの[**スケーラビリティとインターフェイス**]ブロックで、[**設定**]をクリックします。

4. [**製品の詳細設定**]ウィンドウの[**全般**]タブで、次の設定を行います:

   - [**スケーラビリティ設定**]セクションで、Kaspersky Security 10.1 for Windows Server で使用される処理対象プロセスの数を定義する設定を行います:

     - **スケーラビリティ設定を自動的に検出する**

       Kaspersky Security 10.1 for Windows Server は、使用されるプロセス数を自動的に調整します。

       これが既定値です。

     - **処理対象プロセスの数を手動で設定する**

       Kaspersky Security 10.1 for Windows Server で、指定した値に従ってアクティブな処理対象プロセスの数が調整されます。

- **実行中プロセスの最大数。**

  Kaspersky Security 10.1 for Windows Server が使用するプロセスの最大数。この入力フィールドは、[**処理対象プロセスの数を手動で設定する**]をオンにすると使用可能になります。

- **リアルタイム保護の対象プロセスの数**

  リアルタイム保護タスクが使用するプロセスの最大数。この入力フィールドは、[**処理対象プロセスの数を手動で設定する**]をオンにすると使用可能になります。

- **バックグラウンドのオンデマンドスキャンタスクの対象プロセスの数。**

  バックグラウンドでオンデマンドスキャンタスクを実行しているときに、オンデマンドスキャンで使用されるプロセスの最大数。この入力フィールドは、[**処理対象プロセスの数を手動で設定する**]をオンにすると使用可能になります。

- [**ユーザーとの対話設定**]セクションで、[**タスクバーにアプリケーションアイコンを表示する**]をオンまたはオフにして、タスクバーの通知領域に表示される Kaspersky Security 10.1 for Windows Server のアイコンの設定を行います。

5. [**階層型ストレージ**]タブで、階層ストレージへのアクセスに関する次のオプションのいずれかを選択します:

- **HSM システムを使用しない**

  オンデマンドスキャンタスクの実行時には、HSM システムの設定が使用されません。

  既定では、このオプションはオンです。

- **HSM システムで再解析ポイントを使用する**

  オンデマンドスキャンタスクの実行時に、再解析ポイントを使用してリモート保管領域のファイルがスキャンされます。

- **HSM システムで拡張ファイル属性を使用する**

  UNC(ユニバーサルネーミング規約)フォーマットのオブジェクトの復元用フォルダーの

パス。

既定では、次のパスです: C:¥ProgramData¥Kaspersky Lab¥Kaspersky Security for Windows Server¥10.1¥Restored¥

- **不明な HSM システム**

  オンデマンドスキャンタスクの実行時に、すべてのファイルが、リモート保管領域にあるファイルとしてスキャンされます。

  このオプションは推奨されません。

> HSM システムを使用しない場合は、[HSM システムの設定]の既定値([HSM システムを使用しない])を変更しないようにします。

6. [**OK**]をクリックします。

アプリケーションの設定内容が保存されます。

Kaspersky Security Center でのセキュリティ設定

> Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **手動でセキュリティ設定を行うには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

- サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

  > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**アプリケーションの設定**]セクションで、[**セキュリティ**]設定の下の[**設定**]をクリックします。

4. [**セキュリティ設定**]ウィンドウで、次の設定を行います:

   - [**信頼性設定**]セクションで、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合の、Kaspersky Security 10.1 for Windows Server のタスクの復元を設定します。

     - **タスク復元を実行する**

       このチェックボックスにより、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合の、Kaspersky Security 10.1 for Windows Server タスクの復元を有効または無効に設定できます。

       このチェックボックスをオンにすると、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合に、Kaspersky Security 10.1 for Windows Server によって Kaspersky Security 10.1 for Windows Server タスクが自動的に復元されます。

       このチェックボックスをオフにすると、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合に、Kaspersky Security 10.1 for Windows Server タスクは自動的に復元されません。

       既定では、このチェックボックスはオンです。

- **オンデマンドスキャンタスクの復元回数上限**

アプリケーションでエラーが返された後に、オンデマンドスキャンタスクの復元を試行する回数。この入力フィールドは、[**タスク復元を実行する**]をオンにすると使用可能になります。

- [**バックアップ電源を UPS に切り替える場合の処理**]セクションで、UPS 電源への切り替え後における、Kaspersky Security 10.1 for Windows Server によるサーバーの負荷に対する制限を指定できます。

  - **スケジュール設定済みのスキャンタスクを開始しない**

    このチェックボックスにより、コンピューターで UPS 電源に切り替えられてから標準の電源モードが復元されるまでの間における定期スキャンタスクの開始を有効にするか、無効にするかを設定できます。

    このチェックボックスをオンにすると、コンピューターで UPS 電源に切り替えられてから標準の電源モードが復元されるまで、定期スキャンタスクは開始されません。

    このチェックボックスをオフにすると、電源モードに関係なく、Kaspersky Security 10.1 for Windows Server により定期スキャンタスクが開始されます。

    既定では、このチェックボックスはオンです。

  - **現在のスキャンタスクを中止する**

    このチェックボックスにより、コンピューターで UPS 電源に切り替えられた後のスキャンタスクの実行を有効または無効に設定できます。

    このチェックボックスをオンにすると、コンピューターで UPS 電源に切り替えられた後で、Kaspersky Security 10.1 for Windows Server によりスキャンタスクの実行が一時停止されます。

    このチェックボックスをオフにすると、コンピューターで UPS 電源に切り替えられた後でも、Kaspersky Security 10.1 for Windows Server により引き続きスキャンタスクが実行されます。

    既定では、このチェックボックスはオンです。

- [**パスワード保護設定**]セクションで、Kaspersky Security 10.1 for Windows Server 機能へのアクセスを保護するパスワードを入力します。

5. [**OK**]をクリックします。

スケーラビリティと信頼性の設定内容が保存されます。

Kaspersky Security Center を使用した接続の設定

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

接続設定は、Kaspersky Security 10.1 for Windows Server がアップデートサーバーおよびアクティベーションサーバーに接続するのに使用します。また、アプリケーションを KSN サービスと統合する際にも使用します。

► **接続設定を行うには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**アプリケーションの設定**]セクションで、[**接続**]ブロックの[**設定**]をクリックします。

   [**接続設定**]ウィンドウが表示されます。

4. [**接続設定**]ウィンドウで、次の設定を行います:

   - [**プロキシサーバーの設定**]セクションで、プロキシサーバーの使用設定を選択します:

     - **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、Kaspersky Security 10.1 for Windows Server はプロキシサーバーを使用せずに KSN サービスに直接接続します。

       既定では、このオプションはオンです。

     - **指定したプロキシサーバー設定を使用する**

       このオプションを選択すると、Kaspersky Security 10.1 for Windows Server は手動で指定されたプロキシサーバー設定を使用して KSN に接続します。

     - プロキシサーバーの IP アドレスまたはシンボル名(ホスト名または FQDN 名)およびポート番号

     - **ローカルアドレスへの接続時はプロキシサーバーを使用しない**

       このチェックボックスにより、Kaspersky Security 10.1 for Windows Server がインストールされているコンピューターと同じネットワークにあるコンピューターに接続する際のプロキシサーバーの使用を有効または無効にします。

       このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server がインストールされているコンピューターをコンピューターするネットワークから直接コンピューターにアクセスします。プロキシサーバーは使用されません。

       チェックボックスがオフになっている場合、そのプロキシサーバーがローカルコンピューターに接続するために適用されます。

既定では、このチェックボックスはオンです。

- [**プロキシサーバーの認証設定**]セクションで、認証設定を指定します:
  - ドロップダウンリストより認証設定を選択します。
    - **認証を使用しない** - 認証は試行されません。既定では、このモードが選択されます。
    - **NTLM 認証を使用する** - Microsoft が開発した NTLM ネットワーク認証プロトコルを使用して認証が試行されます。
    - **ユーザー名とパスワードを指定して NTLM 認証を使用する** - 名前とパスワードを使用して、Microsoft が開発した NTLM ネットワーク認証プロトコルを通して認証が試行されます。
    - **ユーザー名とパスワードを適用する** - ユーザー名とパスワードを使用して認証が試行されます。
  - 必要に応じて、ユーザー名とパスワードを入力します。
- [**ライセンス**]セクションで、[**アプリケーションのアクティベーション時に Kaspersky Security Center をプロキシサーバーとして使用する**]をオンまたはオフにします。

5. [**OK**]をクリックします。

接続設定の内容が保存されます。

高度な機能の設定

コンピューターのグループまたは単一のコンピューターに対して Kaspersky Security Center から Kaspersky Security 10.1 for Windows Server の高度な機能を設定できます。

このセクションの内容

Kaspersky Security Center での信頼ゾーンの設定

既定では、新しく作成されたポリシーとタスクに信頼ゾーンが適用されます。

► **信頼ゾーンを設定するには：**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します：

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**（170 **ページのセクション「ポリシーの設定」を参照**）。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください（190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照）。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**詳細設定**]セクションの[**信頼ゾーン**]ブロックで[**設定**]をクリックします。

   [**信頼ゾーン**]ウィンドウが開きます。

4. [**除外リスト**]タブで、スキャンをスキップするオブジェクトを指定します:

   - 推奨除外リストを作成するには、[**推奨除外リストを追加**]をクリックします。

     このボタンをクリックすると、Microsoft により推奨されている除外リストと Kaspersky Lab により推奨されている除外リストが追加され、リストを拡張できます。

   - 除外リストをインポートするには、[**インポート**]をクリックして表示されるウィンドウで、Kaspersky Security 10.1 for Windows Server によって信頼するとみなされるファイルを選択します。

   - ファイルを信頼するとみなす条件を手動で指定するには、[**追加**]をクリックします。表示されたウィンドウで、次の設定を指定します:

     - **スキャン対象オブジェクト**

       ファイル名、ファイル名マスク、ローカルまたはリムーバブルのコンピュータードライブ、ローカルフォルダーまたはネットワークフォルダー、事前定義された範囲など。

     - **検知対象オブジェクト**

       検知可能なオブジェクト名のリストについては、ウイルス百科事典

       の Web サイト(http://www.securelist.com)を参照してください。

       このチェックボックスをオンにすると、スキャン時に指定した検知可能なオブジェクトがスキップされます。

       このチェックボックスをオフにすると、指定されたオブジェクトが既定ですべて検知されます。

既定では、このチェックボックスはオフです。

- **ルールの適用範囲**

  ルールが使用される Kaspersky Security 10.1 for Windows Server タスクの名前。

- 必要に応じて、除外対象について説明する追加情報を[**コメント**]に指定します。

5. [**信頼ゾーン**]ウィンドウの[**信頼するプロセス**]タブで、スキャンの際に Kaspersky Security 10.1 for Windows Server によってスキップされるプロセスを指定します:

   - **ファイルのバックアップ処理を確認しない**

     このチェックボックスにより、サーバーにインストールされたバックアップツールによってファイルの読み取り操作が実行される場合に、その操作のスキャンを有効または無効に設定できます。

     このチェックボックスをオンにすると、サーバーにインストールされたバックアップツールによって実行されるファイルの読み取り操作に対する、Kaspersky Security 10.1 for Windows Server によるスキャンがスキップされます。

     このチェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、サーバーにインストールされたバックアップツールによって実行されるファイルの読み取り操作がスキャンされます。

     既定では、このチェックボックスはオンです。

   - **指定した処理でのファイル動作を確認しない**

     このチェックボックスにより、信頼するプロセスのファイル操作のスキャンを有効または無効に設定できます。

     このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server によるスキャンで、信頼するプロセスの操作がスキップされます。

     このチェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server で、信頼するプロセスのファイル操作がスキャンされます。

     既定では、このチェックボックスはオフです。

6. 必要に応じて[**追加**]をクリックし、スキャンしないファイル操作のプロセスを追加します(239 ページのセクション「信頼されたプロセスの追加」を参照)。

7. [**信頼ゾーン**]ウィンドウの[**OK**]をクリックして変更を保存します。

信頼されたプロセスの追加

► **信頼されたプロセスのリストにプロセスを 1 つまたは複数追加するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます(170 ページのセクション「ポリシーの設定」を参照)**。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**詳細設定**]セクションの[**信頼ゾーン**]ブロックで[**設定**]をクリックします。

   [**信頼ゾーン**]ウィンドウが開きます。

4. [**信頼するプロセス**]タブで[**指定した処理でのファイル動作を確認しない**]をオンにします。

5. [**追加**]をクリックします。

6. ボタンコンテキストメニューから、次のいずれかを選択します:

- **複数のプロセス**

  表示された[**信頼するプロセスの追加**]ウィンドウで、次を設定します:

  a. **信頼対象と見なすためにディスク上でフルプロセスパスを使用する**

     チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server はファイルの完全パスを使用してプロセスの信頼ステータスを決定します。

     チェックボックスがオフの場合、プロセスの信頼ステータスを決定する基準として、ファイルのパスは考慮されません。

     既定では、このチェックボックスはオンです。

  b. **信頼対象と見なすためにプロセスファイルハッシュを使用する**

     チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server は選択したファイルのハッシュを使用してプロセスの信頼ステータスを決定します。

     チェックボックスがオフの場合、プロセスの信頼ステータスを決定する基準として、ファイルのハッシュは考慮されません。

     既定では、このチェックボックスはオンです。

  c. 実行可能プロセスに基づいてデータを追加するには、[**参照**]をクリックします。

  d. 表示されたウィンドウで、実行ファイルを選択します。

  > 一度に追加できる実行ファイルは 1 つのみです。他の実行ファイルを追加するには手順 c と d を繰り返してください。

  e. 実行中のプロセスに基づいてデータを追加するには、[**プロセス**]をクリックします。

  f. 表示されたウィンドウで、プロセスを選択します。複数のプロセスを選択するには、[**CTRL**]を押したまま選択します。

  g. [**OK**]をクリックします。

実行中のプロセスのリストを表示できるようにするには、ファイルのリアルタイム保護タスクが実行されたアカウントに、Kaspersky Security 10.1 for Windows Server がインストールされているサーバーの管理者権限が必要です。実行中のプロセスのリスト内のプロセスは、ファイル名、PID、またはローカルサーバー上のプロセスの実行ファイルのパスで並べ替えることができます。実行中のプロセスを選択するには、ローカルサーバーで Kaspersky Security 10.1 コンソールのみを使用するか、あるいは Kaspersky Security Center から指定されたコンピューター設定内で、[**プロセス**]をクリックします。

- **名前とパスに基づく 1 つのプロセス。**

  [**信頼するプロセスを手動で追加**]ウィンドウで、次を設定します:

  a. 実行ファイルへのパスを入力します(ファイル名を含む)。

  b. [**OK**]をクリックします。

- **オブジェクトのプロパティに基づく 1 つのプロセス。**

  [**信頼するプロセスを追加**]ウィンドウで、次を設定します:

  a. [**参照**]をクリックしてプロセスを選択します。

  b. **信頼対象と見なすためにディスク上でフルプロセスパスを使用する**

  チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server はファイルの完全パスを使用してプロセスの信頼ステータスを決定します。

  チェックボックスがオフの場合、プロセスの信頼ステータスを決定する基準として、ファイルのパスは考慮されません。

  既定では、このチェックボックスはオンです。

  c. 信頼対象と見なすためにプロセスファイルハッシュを使用する

  チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server は選択したファイルのハッシュを使用してプロセスの信頼ステータスを決定します。

  チェックボックスがオフの場合、プロセスの信頼ステータスを決定する基準として、ファ

イルのハッシュは考慮されません。

既定では、このチェックボックスはオンです。

d. ［**OK**］をクリックします。

> 選択したプロセスを信頼できるプロセスのリストに追加するには、少なくとも 1 つの信頼の基準を選択する必要があります。

7. ［**信頼するプロセスを追加**］ウィンドウで［**OK**］をクリックします。

選択したファイルまたはプロセスが、［**信頼ゾーン**］ウィンドウの信頼するプロセスのリストに追加されます。

not-a-virus（非ウイルス）マスクの適用

not-a-virus（非ウイルス）マスクを使用すると、スキャン時に有害とみなされる可能性がある合法的なソフトウェアのファイルや Web リソースをスキップできます。マスクが影響を与えるタスクは、次の通りです：

- ファイルのリアルタイム保護
- オンデマンドスキャン
- スクリプト監視
- RPC ネットワークストレージの保護
- トラフィックセキュリティ

マスクが除外リストに追加されていない場合、Kaspersky Security 10.1 for Windows Server はこのカテゴリに分類されるソフトウェアまたは Web リソースに対して、タスク設定に指定された処理を適用します。

► not-a-virus（非ウイルス）マスクを適用するには：

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**詳細設定**]セクションの[**信頼ゾーン**]ブロックで[**設定**]をクリックします。

   [**信頼ゾーン**]ウィンドウが開きます。

4. チェックボックスがオフの場合、[**除外リスト**]タブでリストをスクロールして、「**not-a-virus:***」という値の行を選択します。

5. [**OK**]をクリックします。

新しい設定が適用されます。

リムーバブルドライブスキャン

USB ポートを介して保護対象サーバーに接続されているリムーバブルドライブのスキャンを設定できます。

Kaspersky Security 10.1 for Windows Server では、オンデマンドスキャンタスクを使用してリムーバブルドライブをスキャンします。リムーバブルドライブが接続されると、アプリケーションは自動的に新しいオンデマンドスキャンタスクを作成し、スキャンの完了後にタスクを削除します。作成されたタスクは、リムーバブルドライブスキャンに対してあらかじめ定義されたセキュリティレベルで実行されます。一時オンデマンドスキャンタスクの設

定は変更できません。

> Kaspersky Security 10.1 for Windows Server を定義データベースなしでインストールする場合、リムーバブルドライブスキャンは利用できません。

> Kaspersky Security 10.1 for Windows Server は、オペレーティングシステムに USB 大容量記憶デバイスとして登録されている場合、接続したリムーバブル USB ドライブをスキャンします。 デバイスコントロールタスクによって接続がブロックされている場合はリムーバブルドライブをスキャンしません。MTP 接続したモバイルデバイスはスキャンしません。

Kaspersky Security 10.1 for Windows Server は、スキャン中のリムーバブルディスクへのアクセスを許可します。

リムーバブルドライブの接続時に作成される、各リムーバブルドライブのオンデマンドスキャンタスクのスキャン結果はログにあります。

リムーバブルドライブスキャンの設定は変更できます（次の表を参照）。

表 29. リムーバブルドライブスキャンの設定

設定	既定値	説明
USB 経由の接続でリムーバブルドライブをスキャンする	チェックボックスはオフです	USB 経由での保護対象サーバーへの接続時のリムーバブルドライブのスキャンは、オンにもオフにもできます。

格納データ容量がこの値以下ならリムーバブルドライブをスキャンする（MB）	1024 MB	スキャンされたドライブ上の最大データ容量を設定することによって、コンポーネントの範囲を縮小することができます。 格納データ容量が指定した値を上回る場合、Kaspersky Security 10.1 for Windows Server はリムーバブルドライブスキャンを実行しません。
次のセキュリティレベルでスキャンする	最大の保護	3 つのセキュリティレベルのいずれかを選択することによって、作成されたオンデマンドスキャンタスクを設定できます： • 最大の保護 • 推奨 • 最高のパフォーマンス 感染したオブジェクト、感染した可能性が高いオブジェクト、およびその他のオブジェクトが検知された場合に使用されるアルゴリズムや、各セキュリティレベルに対するその他のスキャン設定は、オンデマンドスキャンタスクであらかじめ定義されたセキュリティレベルに対応しています。

リムーバブルドライブの接続時スキャンを設定するには、次の処理を実行します：

6. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

7. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

8. [**詳細設定**]セクションで、[**リムーバブルドライブスキャン**]ブロックの[**設定**]をクリックします。

   [**リムーバブルドライブスキャン**]ウィンドウが開きます。

9. [**接続時スキャン**]セクションで次の操作を行います:

   - 接続時に自動的にリムーバブルドライブをスキャンする場合、[**USB 経由の接続でリムーバブルドライブをスキャンする**]をオンにします。

   - 必要な場合は、[**格納データ容量がこの値以下ならリムーバブルドライブをスキャンする(MB)**]をオンにし、右側のフィールドに最大値を指定します。

   - [**次のセキュリティレベルでスキャンする**]ドロップダウンリストで、リムーバブルドライブスキャンに必要な設定を持つセキュリティレベルを指定します。

10. [**OK**]をクリックします。

    指定された設定が保存、適用されます。

Kaspersky Security Center でのアクセス権限の設定

Kaspersky Security Center で、コンピューターグループまたは個別のコンピューターに対して、製品および Kaspersky Security サービスを管理するためのアクセス権限を設定できます。

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **製品および Kaspersky Security サービスを管理するためのアクセス権限を設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 ページのセクション「**ポリシーの設定**」を参照)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**詳細設定**]セクションを開き、次の操作を行います:

- ユーザーまたはユーザーグループに対して Kaspersky Security 10.1 for Windows Server を管理するためのアクセス権を設定するには、[**アプリケーション管理用のユーザーアクセス権限**]セクションで[設定]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して Kaspersky Security サービスを管理するためのアクセス権を設定するには、[**Security サービス管理用のユーザーアクセス権限**]セクションで[**設定**]をクリックします。

4. 表示されたウィンドウで、必要に応じてアクセス権限を設定します(152 ページのセクション「Kaspersky Security 10.1 for Windows Server の各種機能に対するアクセス権限」を参照)。

指定された設定が保存されます。

Kaspersky Security Center での隔離およびバックアップ設定

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **Kaspersky Security Center でバックアップの全般的な設定を行うには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 ページのセクション「ポリシーの設定」を参照)。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

  > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**詳細設定**]セクションで、[**保管領域**]ブロックの[**設定**]をクリックします。
4. 必要に応じて、[**保管領域**]の設定ウィンドウの[**バックアップ**]タブを使用して、次の[**バックアップ**]設定を行います:
   - **バックアップフォルダー**を指定するには、[**バックアップフォルダー**]を使用して保護対象のサーバーのローカルドライブ上の必要なフォルダーを選択するか、フォルダーの絶対パスを入力します。
   - **バックアップ**の最大サイズを設定するには、[**バックアップの最大サイズ(MB)**]をオンにして、入力フィールドに該当する値(メガバイト単位)を指定します。
   - バックアップの空き容量のしきい値を設定するには、[**バックアップの最大サイズ(MB)**]設定の値を定義し、[**空き容量のしきい値(MB)**]をオンにして、**バックアップ**フォルダーの空き容量の最小値(メガバイト単位)を指定します。
   - 復元したオブジェクト用のフォルダーを指定するには、[復元設定]セクションで保護されたサーバーのローカルドライブ上の該当するフォルダーを選択するか、[**オブジェクトの復元先フォルダー**]でフォルダーの名前と完全パスを入力します。
5. [**保管領域**]の設定ウィンドウの[**隔離**]タブで、次の**隔離**設定を行います:
   - **隔離**フォルダーを変更するには、[**隔離フォルダー**]で保護されたサーバーのローカルドライブ上のフォルダーへの完全パスを指定します。
   - **隔離**の最大サイズを設定するには、[**隔離の最大サイズ(MB)**]をオンにして、入力フィールドにこの

パラメータの値（メガバイト単位）を指定します。

- **隔離**の保管領域の最小空き容量を設定するには、[**隔離の最大サイズ（MB）**]と[**空き容量のしきい値（MB）**]をオンにして、入力フィールドにこのパラメータの値（メガバイト単位）を指定します。
- 隔離されたオブジェクトの復元先フォルダーを変更するには、[**オブジェクトの復元先フォルダー**]で保護対象サーバーのローカルドライブ上のフォルダーへの絶対パスを指定します。

6. [**OK**]をクリックします。

隔離およびバックアップの設定内容が保存されます。

信頼しないコンピューターのブロック：ブロック対象コンピューター

このセクションでは、信頼しないコンピューターをブロックする方法と、ブロック対象コンピューターのストレージを設定する方法について説明します。

このセクションの内容

信頼しないコンピューターのブロックについて

次のコンポーネントのいずれかがインストールされている場合、次のブロック対象コンピューターのストレージが既定でインストールされます：リアルタイム保護、NetApp のアンチクリプター、アンチクリプター。コンポーネントは信頼しないコンピューターのリストに従って、保護対象サーバーまたはネットワーク接続ストレージ共有ネットワークフォルダーへのリモートコンピューターによるアクセス試行を監視します。全保護対象サーバーのブロック対象コンピューターに関する情報は、Kaspersky Security Center に送信されます。Kaspersky Security 10.1

for Windows Server は、ブロック対象コンピューターのリストにあるすべてのリモートコンピューターによる、サーバーのネットワーク共有フォルダーまたはネットワーク接続ストレージのフォルダーへのアクセスをブロックします。

ブロック対象コンピューターのストレージは、次のタスクのうち最低 1 つがアクティブモードで起動し、なおかつ指定の条件が満たされている場合に追加されます:

- ファイルのリアルタイム保護タスクの実行時に、ネットワークファイルリソースにアクセスするコンピューターによる悪意のある動作が検知され、ファイルのリアルタイム保護タスク設定で[**悪意のある動作を示すコンピューターを信頼しないリストに追加する**]がオンにされている。
- アンチクリプタータスクの実行時に、ネットワークファイルリソースにアクセスするコンピューターによる悪意のある暗号化が検知された。
- NetApp のアンチクリプタータスクの実行時に、ネットワーク接続ストレージにランサムウェア攻撃が検知された。

悪意のある動作または暗号化の試行が検知されると、タスクは攻撃元のコンピューターに関する情報をブロック対象コンピューターの保管領域に送信し、ブロックしているコンピューターに関する緊急イベントが作成されます。このコンピューターから実行される保護対象のネットワーク共有フォルダーへのアクセス試行は、すべてブロックされます。

Kaspersky Security 10.1 for Windows Server は既定で、信頼しないコンピューターがリストに追加されてから 30 分すると、そのコンピューターをリストから削除します。信頼しないコンピューターのリストから削除されると、ネットワークファイルリソースへのコンピューターのアクセスは自動的に復元されます。ブロック対象コンピューターが自動的にブロック解除されるまでの期間を設定できます。

信頼しないコンピューターのブロックの有効化

悪意ある動作または暗号化動作を示すコンピューターを[**ブロック対象コンピューター**]の保管領域に追加し、これらのコンピューターのネットワークファイルリソースへのアクセスをブロックするには、次のタスクのうち最低 1 つを使用中モードで実行する必要があります:

- ファイルのリアルタイム保護
- アンチクリプター
- NetApp のアンチクリプター

► **ファイルのリアルタイム保護タスクの設定**:

1. Kaspersky Security Center 管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。
2. [**ポリシー**]タブを選択して、アプリケーションを設定する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、[**プロパティ:<ポリシー名>**]ウィンドウを開きます。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開きます。
4. [**サーバーのリアルタイム保護**]セクションで、[**ファイルのリアルタイム保護**]セクションの[**設定**]をクリックします。

   [**サーバーのリアルタイム保護**]ウィンドウが開きます。
5. [**他のコンポーネントとの統合**]セクションで、ファイルのリアルタイム保護タスクの実行中に悪意のある動作が検知されたコンピューターに対してネットワークファイルリソースへのアクセスをブロックするには、[**悪意のある動作を示すコンピューターを信頼しないリストに追加する**]をオンにします。
6. タスクが開始されていない場合、[**タスク管理**]タブを開きます:
   a. [**スケジュールに従って実行する**]をオンにします。
   b. ドロップダウンリストから[**アプリケーションの起動時**]の頻度を選択します。
7. [**サーバーのリアルタイム保護**]ウィンドウで[**OK**]をクリックします。

新しい設定が保存されます。

► **アンチクリプタータスクの設定:**

1. Kaspersky Security Center 管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。
2. [**ポリシー**]タブを選択して、アプリケーションを設定する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、[**プロパティ:<ポリシー名>**]ウィンドウを開きます。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開きます。
4. [**ネットワークアクティビティの管理**]セクションで、[**アンチクリプター**]セクションの[**設定**]をクリックします。[**アンチクリプター**]ウィンドウが開きます。
5. タスクが開始されていない場合、[**タスク管理**]タブを開きます:
   a. [**スケジュールに従って実行する**]をオンにします。
   b. ドロップダウンリストから[**アプリケーションの起動時**]の頻度を選択します。
6. [**アンチクリプター**]ウィンドウで[**OK**]をクリックします。

新しい設定が保存されます。

► **NetApp のアンチクリプターの設定:**

1. Kaspersky Security Center 管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。
2. [**ポリシー**]タブを選択して、アプリケーションを設定する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、[**プロパティ:<ポリシー名>**]ウィンドウを開きます。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開きます。

4. [ネットワーク接続ストレージの保護]セクションで、[NetApp のアンチクリプター]セクションの[設定]をクリックします。

5. [**NetApp のアンチクリプター**]ウィンドウが表示されます。

6. タスクが開始されていない場合、[**タスク管理**]タブを開きます:

   a. [**スケジュールに従って実行する**]をオンにします。

   b. ドロップダウンリストから[**アプリケーションの起動時**]の頻度を選択します。

7. [**NetApp のアンチクリプター**]ウィンドウで[**OK**]をクリックします。

Kaspersky Security 10.1 for Windows Server は、悪意ある動作または暗号化動作を示すコンピューターのネットワークファイルリソースへのアクセスをブロックします。

ブロック対象コンピューターの設定

► **ブロック対象コンピューターのストレージを設定するには:**

1. Kaspersky Security Center の管理コンソールで、[アプリケーションのプロパティ]ウィンドウを開きます(「Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定」(190 ページ)を参照)。

2. [**詳細設定**]セクションで、[**保管領域**]ブロックの[**設定**]をクリックします。

   [**保管領域の設定**]ウィンドウが表示されます。

ポリシー設定を使用して、管理対象サーバーのグループにコンピューターのブロック期間を設定できます。コンピューターのブロック期間を設定するには、[**プロパティ: <ポリシー名>**]ウインドウの[**詳細設定**]セクションの[**保管領域**]セクションにある[設定]をクリックします。[**ブロック対象コンピューター**]タブで、コンピューターのブロック期間を調整します。ブロック対象コンピューターのリストは、ポリシー設定では使用できません。

3. [**ブロック対象コンピューター**]タブを開きます。
4. [**コンピューターのブロック期間**]セクションで、ブロック対象コンピューターが、ブロックされてからネットワークファイルリソースに再びアクセスできるようになるまでの日数および時間(時間、分)を指定します。
5. アプリケーションのプロパティウィンドウで[**ブロック対象コンピューターのリスト**]をクリックします。
6. 次のいずれかの処理を実行します:
   - 表示された[**ブロック対象コンピューターのリスト**]ウィンドウで、アクセスを復元するコンピューターを選択し、[**リストから削除**]をクリックします。
   - 信頼しないコンピューターのリストからコンピューターを削除し、ブロックされたすべてのコンピューターに対するアクセスを復元するには、[**リスト全体を消去**]をクリックします。
7. [**OK**]をクリックします。

   選択したコンピューターのブロックが解除され、ブロック対象コンピューターのリストから削除されます。
8. [**保管領域の設定**]ウィンドウで[**OK**]をクリックします。

新たに設定したブロック対象コンピューターの設定が保存されます。

ログと通知の設定

Kaspersky Security Center の管理コンソールを使用して、Kaspersky Security 10.1 for Windows Server や、保護対象サーバーのアンチウイルスによる保護のステータスに関する次のイベントについて、管理者やユーザー向けの通知を設定できます:

- 管理者は、選択したイベント種別の情報を受信できます。
- 保護対象のサーバーにアクセスする LAN ユーザーとターミナルサーバーのユーザーは、**検知したオブジェクト**種別のイベントに関する情報を受信できます。

Kaspersky Security 10.1 for Windows Server イベントに関する通知は、選択したコンピューターのコンピューターのプロパティウィンドウを使用して選択したコンピューター 1 台に対して設定するか、選択した管理グループのポリシーのプロパティウィンドウ内でコンピューターのグループに対して設定することができます。

[**イベント通知**]セクション、または[**通知の設定**]ウィンドウで、次の種類の通知を設定できます:

- 選択した種別のイベントに関する管理者通知は、[**イベント通知**]セクション(Kaspersky Security Center 製品の標準タブ)を使用して設定できます。通知方法の詳細については、『**Kaspersky Security Center ヘルプ**』を参照してください。
- 管理者通知とユーザー通知は、両方とも[**通知の設定**]ウィンドウで設定できます。

> Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

一部の種別のイベントの通知は、[**通知の設定**]ウィンドウまたは[**イベント通知**]セクションでしか設定できません。その他の種別のイベントの通知は、[**通知の設定**]ウィンドウと[**イベント通知**]セクションの両方で設定できます。

同じ種別のイベントに関する通知を、同じモードで、[**イベント通知**]セクションと[**通知の設定**]ウィンドウで設定すると、システム管理者はこれらのイベントの通知を同じモードで 2 回受信します。

このセクションの内容

ログの設定

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **Kaspersky Security 10.1 for Windows Server ログを設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーの**

プロパティウィンドウを開きます（170 **ページのセクション「ポリシーの設定」を参照**）。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください（190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照）。

> デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ログと通知の設定**]セクションで、[**実行ログ**]ブロックの[**設定**]をクリックします。
4. [**ログの設定**]ウィンドウで、要件に従って Kaspersky Security 10.1 for Windows Server の次の設定を定義します:
   - ログのイベント詳細レベルの設定を設定します。それには、次の操作を実行します:
     a. [**コンポーネント**]リストで、詳細レベルを設定する Kaspersky Security 10.1 for Windows Server のコンポーネントを選択します。
     b. 選択したコンポーネントのタスク実行ログとシステム監査ログの詳細レベルを定義するには、[**重要度**]から必要なレベルを選択します。
   - ログの既定の場所を変更するには、フォルダーの完全パスを指定するか、[**指定**]をクリックして選択します。
   - タスク実行ログの保存日数を指定します。
   - [**システム監査ログ**]フォルダーに表示される情報の保存日数を指定します。
5. [**OK**]をクリックします。

ログの設定が保存されます。

セキュリティイベントログ

Kaspersky Security 10.1 for Windows Server では、保護対象サーバーでのセキュリティ侵害や試行されたセキュリティ侵害に関連するイベントのログが保持されています。このログには次のイベントが記録されます:

- 脆弱性攻撃ブロックイベント
- 重要な Windows イベントログ監視イベント
- 試行されたセキュリティ侵害を示す重要なイベント(リアルタイム保護タスク、オンデマンドスキャンタスク、ファイル変更監視タスク、アプリケーション起動コントロールタスク、およびデバイスコントロールタスク用)

[セキュリティログ]と[システム監査ログ]はオフにできます。さらに Kaspersky Security 10.1 for Windows Server では、[セキュリティログ]のオフに関するシステム監査イベントが記録されます。

SIEM 統合設定

低パフォーマンスデバイスの負荷を低下させ、アプリケーションログ容量の肥大化によるシステム劣化のリスクを低減するために、Syslog プロトコルによる **syslog サーバー**への監査イベントおよびタスクパフォーマンスイベントの公開を設定できます。

syslog サーバーは、イベント(SIEM)を集計するための外部サーバーです。受信したイベントを収集、分析し、その他のログ管理処理も実行します。

次の 2 つのモードで SIEM 統合を使用できます:

- **syslog プロトコルでリモート syslog サーバーにイベントを送信する**:このモードでは、ログの設定で公開が設定されたタスクパフォーマンスイベントとすべてのシステム監査イベントが、SIEM への送信後もローカルコンピューターに引き続き格納されます。

  このモードは、保護対象サーバー上の負荷を最大限に低下させるために使用することをお勧めします。

- **リモート syslog サーバーに送信されたイベントの場合、ローカルコピーを削除する**:このモードでは、

アプリケーションの操作中に登録され、SIEM に公開されたすべてのイベントが、ローカルコンピューターから削除されます。

セキュリティログのローカルバージョンは決して削除されません。

Kaspersky Security 10.1 for Windows Server はアプリケーションログのイベントを syslog サーバーでサポートされる形式に変換して、イベントを送信し SIEM が正常に認識できるようにできます。
STRUCTURED-DATA 形式や JSON 形式への変換がサポートされています。

SIEM へのイベント送信失敗のリスクを低下させるために、ミラー syslog サーバーに接続する設定を定義できます。

ミラー syslog サーバーは追加の syslog サーバーで、メインの syslog サーバーに接続できないか、メインのサーバーが使用できない場合に、自動的に切り替えられます。

既定では、SIEM 統合は使用されません。SIEM 統合は、有効化や無効化、機能の設定ができます(次の表を参照)。

表 30. SIEM 統合設定

設定	既定値	説明
syslog プロトコルでリモート syslog サーバーにイベントを送信する	オフ	それぞれ、チェックボックスをオンまたはオフにすることによって、SIEM 統合を有効または無効にできます。
リモート syslog サーバーに送信されたイベントの場合、ローカルコピーを削除する	オフ	チェックボックスをオンまたはオフにすることによって SIEM に送信されたログのローカルコピーの保存設定を行うことができます。

設定	既定値	説明
イベント形式	STRUCTURED-DATA	これらのイベントを syslog サーバーに送信して SIEM で良好に認識するために、イベントの変換形式には 2 つのいずれかを選択できます。
接続プロトコル	TCP	ドロップダウンリストを使用して、メイン syslog サーバーへの接続プロトコルに UDP または TCP を設定できます。ミラー syslog サーバーへの接続プロトコルには TCP を設定できます。
メイン syslog サーバー接続設定	IP アドレス:127.0.0.1 ポート:514	適切なフィールドを使用して、メインの syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。 IP アドレスは IPv4 形式でのみ指定できます。
メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する	オフ	チェックボックスを使用してミラー syslog サーバーの使用を有効または無効にできます。
ミラー syslog サーバー接続設定	IP アドレス:127.0.0.1 ポート:514	適切なフィールドを使用して、ミラーの syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。 IP アドレスは IPv4 形式でのみ指定できます。

► **SIEM 統合設定を設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ログと通知の設定**]セクションで、[**実行ログ**]ブロックの[**設定**]をクリックします。

   [**ログと通知の設定**]ウィンドウが開きます。

4. [**SIEM 統合**]タブを選択します。

5. [**統合設定**]セクションで、[**syslog プロトコルでリモート syslog サーバーにイベントを送信する**]をオンにします。

   このチェックボックスを使用して、公開されたイベントを外部 syslog サーバーに送信する機能を有効または無効にできます。

   チェックボックスがオンの場合、公開されたイベントは SIEM 統合設定を使用して SIEM に送信されます。

   チェックボックスがオフの場合、SIEM 統合は実行されません。チェックボックスがオフの場合、SIEM 統合を設定できません。

   既定では、このチェックボックスはオフです。

6. 必要に応じて、[**統合設定**]セクションの[**リモート syslog サーバーに送信されたイベントの場合、ローカルコピーを削除する**]をオンにします。

   このチェックボックスを使用して、SIEM に送信したログのローカルコピーの削除を有効

または無効にします。

チェックボックスがオンの場合、SIEM に正常に公開されると、イベントのローカルコピーが削除されます。低パフォーマンスのコンピューターにはこのモードをお勧めします。

チェックボックスがオフの場合、ただ SIEM にイベントが送信されます。ログのコピーは、引き続きローカルに保存されます。

既定では、このチェックボックスはオフです。

[**リモート syslog サーバーに送信されたイベントの場合、ローカルコピーを削除する**]の状態は、セキュリティログのイベントを保存する設定に影響を及ぼしません。セキュリティログイベントが自動的に削除されることはありません。

7. [**イベント形式**]セクションで、アプリケーション操作イベントを SIEM に送信できるように変換する形式を指定します。

   既定では、 STRUCTURED-DATA 形式に変換されます。

8. [**接続設定**]セクション:

   - SIEM 接続プロトコルを指定します。
   - メインの syslog サーバーに接続する設定を指定します。

     IP アドレスは IPv4 形式でのみ指定できます。

   - メインの syslog サーバーにイベントを送信できない場合にその他の接続設定を使用するようにするには、必要に応じて、[**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**]をオンにします。

     - ミラー syslog サーバーに接続する設定を指定します:[**IP アドレス**]および[**ポート**]

       [**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**]がオフの場合、ミラー syslog サーバーの[**IP アドレス**]および[**ポート**]は編集できません。

IP アドレスは IPv4 形式でのみ指定できます。

9. [**OK**]をクリックします。

設定済みの SIEM 統合設定が適用されます。

通知の設定

► **Kaspersky Security 10.1 for Windows Server 通知を設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ログと通知の設定**]セクションで、[**イベント通知**]ブロックの[**設定**]をクリックします。

4. [**通知の設定**]ウィンドウで、要件に従って Kaspersky Security 10.1 for Windows Server の次の設定を定義します:

   - [**通知設定**]リストより、設定を編集する通知の種別を選択します。

- [**ユーザーへの通知**]セクションで、ユーザーへの通知方法を設定します。必要に応じて、通知メッセージのテキストを入力します。
- [**管理者への通知**]セクションで、管理者への通知方法を設定します。必要に応じて、通知メッセージのテキストを入力します。必要に応じて[**設定**]をクリックし、通知の詳細設定を行います。
- [**イベント生成しきい値**]セクションでは、Kaspersky Security 10.1 for Windows Server が[**定義データベースがアップデートされていません**]、[**定義データベースが長期間アップデートされていません**]、および[**重要領域のスキャンが長期間実行されていません**]の各イベントを記録する時間間隔を指定できます。
  - **定義データベースがアップデートされていません(日)**

    前回定義データベースのアップデートが実行されてから経過した日数。

    既定では 7 日です。
  - **定義データベースが長期間アップデートされていません(日)**

    前回定義データベースのアップデートが実行されてから経過した日数。

    既定では 14 日です。
  - **重要領域のスキャンが長期間実行されていません(日)**

    重要領域のスキャンが前回正常に実行されてから経過した日数。

    既定では 30 日です。

5. [**OK**]をクリックします。

通知の設定内容が保存されます。

管理サーバーとの対話設定

► **Kaspersky Security 10.1 for Windows Server が Kaspersky Security Center 管理サーバーに情報を送信するオブジェクトの種別を選択して、次の操作を行います:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ログと通知の設定**]セクションで、[**管理サーバーとのインタラクション**]ブロックの[**設定**]をクリックします。

   [**管理サーバーのネットワークリスト**]ウィンドウが開きます。

4. 表示されたウィンドウで、Kaspersky Security 10.1 for Windows Server が Kaspersky Security Center 管理サーバーに情報を送信するオブジェクトの種別を選択します:

   - 隔離オブジェクトに関する情報。

   - バックアップオブジェクトに関する情報。

   - ブロック対象コンピューターに関する情報。

5. [**OK**]をクリックします。

選択した種別のオブジェクトに関する情報が管理サーバーに送信されます。

サーバーのリアルタイム保護

このセクションでは、リアルタイム保護タスク:リアルタイムファイル保護、スクリプト監視、KSN の使用、脆弱性攻撃からの保護に関する情報について説明します。また、リアルタイム保護タスクを設定する手順、および保護対象のサーバーのセキュリティ設定を管理する手順についても説明します。

この章の内容

ファイルのリアルタイム保護

このセクションでは、ファイルのリアルタイム保護タスクとその設定方法について説明します。

このセクションの内容

ファイルのリアルタイム保護タスクについて

ファイルのリアルタイム保護タスクが実行されている場合、次の保護対象のサーバーのオブジェクトにアクセスされたときに、Kaspersky Security 10.1 for Windows Server によってそのオブジェクトがスキャンされます:

- ファイル
- 代替のファイルシステムスレッド(NTFS スレッド)
- ローカルハードディスクおよび外部デバイスのマスターブートレコードとブートセクター
- Windows Server 2016 のコンテナーファイル

何らかのアプリケーションがサーバーに対してファイルの書き込みを行った場合、またはサーバーからファイルの読み取りを行った場合に、Kaspersky Security 10.1 for Windows Server によってそのファイルがインターセプトされ、脅威がスキャンされます。脅威が検知された場合は、ファイルの駆除を試行する処理、[隔離]に移動する処理、または削除する処理のうち、既定の処理または指定した処理が実行されます。感染していない場合、または正常に駆除された場合、Kaspersky Security 10.1 for Windows Server からアプリケーションにファイルが返されます。

Kaspersky Security 10.1 for Windows Server は、Windows Server 2016 コンテナーで実行されるファイル

操作をインターセプトします。

コンテナーとは、オペレーティングシステムには影響しないでアプリケーションを実行できる、またはアプリケーションによって影響されない独立した環境です。コンテナーがタスクの保護範囲内にある場合、Kaspersky Security 10.1 for Windows Server は、アクセスされているコンテナーファイルをスキャンしてコンピューター内の脅威をチェックします。脅威が検知された場合、コンテナーの駆除を試行します。正常に駆除された場合、コンテナーは継続して機能します。駆除できない場合は、コンテナーを停止します。

Kaspersky Security 10.1 for Windows Server は、Windows Subsystem for Linux® で実行するプロセスでも悪意のあるソフトウェアを検知します。そのようなプロセスに対して、ファイルのリアルタイム保護タスクは現在の設定で定義されている処理を適用します。

ファイルのリアルタイム保護タスクの設定

既定では、ファイルのリアルタイム保護のシステムタスクでは、次の表の設定が使用されます。これらの設定の値を変更できます。

表 31. ファイルのリアルタイム保護タスクの既定の設定

設定	既定値	説明
保護範囲	仮想ドライブを除くコンピューター全体	保護範囲を制限することができます。
セキュリティレベル	保護範囲全体の共通の設定で、[**推奨**]セキュリティレベルに対応します。	コンピューターのファイルリソースツリーで選択したフォルダーに対して、次の操作を実行できます: • あらかじめ定義された別のセキュリティレベルを適用する • セキュリティレベルを手動で編集する • 後で異なるフォルダーに適用するためのテンプレートとして、選択したフォルダーのセキュリティ設定を保存する
オブジェクトの保護モード	アクセス時と変更時	保護モードを選択できます。つまり、Kaspersky Security 10.1 for Windows Server がオブジェクトをスキャンするアクセスの種別を定義できます。
ヒューリスティックアナライザー	[**中**]セキュリティレベルが適用されます。	ヒューリスティックアナライザーを有効または無効にできます。また、分析レベルを設定できます。
信頼ゾーンの適用	適用されます。	選択したタスクで使用できる一般的な信頼するオブジェクト。
KSN の使用サービス	使用	Kaspersky Security Network のクラウドサービスのインフラストラクチャを使用して、コンピューターの保護を改善することができます。

設定	既定値	説明
悪意のある動作を示すコンピューターを信頼しないリストに追加する	オフ	信頼しないコンピューターのリストに、悪意のある動作を示すコンピューターを追加できます。
タスク開始スケジュール	アプリケーション開始時	スケジュールによるタスクの開始について設定できます。

►

► **ファイルのリアルタイム保護タスクを設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**ファイルのリアルタイム保護**]ブロックで、[**設定**]をクリックします。

   [**サーバーのリアルタイム保護**]ウィンドウが開きます。

4. 次のタスクの設定を指定します:

- [**全般**]タブ:
  - 保護モード(275 ページのセクション「保護モードの選択」を参照)
  - ヒューリスティックアナライザーの使用(274 ページを参照)
  - その他の Kaspersky Security 10.1 for Windows Server コンポーネントとの統合の設定。
- [**タスク管理**]タブで:
  - タスク開始スケジュール設定(221 ページの「タスク開始スケジュールの設定」を参照)。

5. [**保護範囲**]タブを選択し、次の操作を行います:
   - [**追加**]または[**編集**]をクリックして保護範囲を編集する(277 ページのセクション「ファイルのリアルタイム保護タスクでの保護範囲」を参照)
     - 表示されたウィンドウで、タスクの保護範囲に含めるものを選択します:
       - **定義済みの範囲**
       - **ディスク、フォルダー、またはネットワークの場所**
       - **ファイル**
     - 定義済みのセキュリティレベルの 1 つを選択するか(278 ページの「定義済みのセキュリティレベルの選択」を参照)、または保護設定を手動で行います(282 ページの「手動でのセキュリティの設定」を参照)。

> タスクに新しい保護範囲設定を適用するには、ファイルのリアルタイム保護タスクを再起動する必要があります。

6. [**サーバーのリアルタイム保護**]ウィンドウで[**OK**]をクリックします。

新しい設定は実行中のタスクにただちに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、実行ログに保存されます。

ヒューリスティックアナライザーの使用

ヒューリスティックアナライザーを使用して Kaspersky Security 10.1 for Windows Server タスクの分析レベルを設定できます。

► **ヒューリスティックアナライザーを設定するには:**

1. ヒューリスティックアナライザーを設定するアプリケーション設定(225 ページのセクション「Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server の管理方法について」を参照)、またはポリシー設定(170 ページのセクション「ポリシーの設定」を参照)を開きます。

2. [**ヒューリスティックアナライザーを使用する**]をオフまたはオンにします。

   このチェックボックスでは、オブジェクトのスキャン中のヒューリスティックアナライザーを有効または無効にできます。

   このチェックボックスをオンにすると、ヒューリスティックアナライザーが有効になります。

   このチェックボックスをオフにすると、ヒューリスティックアナライザーが無効になります。

   既定では、このチェックボックスはオンです。

3. 必要に応じて、スライダーを使用して分析のレベルを調整します。

   スライダーを使用すれば、ヒューリスティック分析のレベルを調整できます。このスキャンの強さのレベルによって、脅威の徹底的な検知、オペレーティングシステムのリソースにかかる負荷、スキャンの所要時間の間のバランスを調整します。

   次のレベルを設定できます:

   - **低**:実行ファイル内部で見つかったスクリプトを少数しか実行しません。脅威が検知される可能性はやや低くなります。スキャンの速度は速く、システムリソースの消費は軽度です。
   - **中**:Kaspersky Lab の推奨に基づき、実行ファイル内部で見つかったスクリプトを多数実行します。

     既定では、このレベルが選択されています。
   - **高**:実行ファイル内部で見つかったスクリプトをさらに多数実行します。脅威が検知

される可能性は非常に高くなります。スキャンには、より多くのシステムリソースを消費し、より多くの時間がかかります。また、非常に多くの誤検知を引き起こす可能性があります。

スライダーは、[**ヒューリスティックアナライザーを使用する**]をオンにすると使用可能になります。

4. [**OK**]をクリックします。

構成されたタスクの設定は、実行中のタスクにただちに適用されます。タスクが実行中でない場合、変更された設定は次回の開始時に適用されます。

保護モードの選択

ファイルのリアルタイム保護タスクでは、保護モードを選択できます。[**オブジェクトの保護モード**]セクションでは、Kaspersky Security 10.1 for Windows Server がスキャンする必要があるオブジェクトへのアクセスの種別を指定できます。

[**オブジェクトの保護モード**]の設定は、タスクで指定される保護範囲全体に共通する値が含まれています。保護範囲内の個別のフォルダーの設定に対して、別の値を指定することはできません。

► **保護モードを選択するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**ファイルのリアルタイム保護**]ブロックで、[**設定**]をクリックします。

   [**サーバーのリアルタイム保護**]ウィンドウが開きます。

4. 表示されたウィンドウの[**全般**]タブで、設定する保護モードを選択します:

   - **スマートモード**

     スキャンするオブジェクトが自動的に選択されます。開いているオブジェクトがスキャンされ、オブジェクトが変更された場合は保存された後にもう一度スキャンされます。プロセスの実行中に、オブジェクトに対して複数の呼び出しが行われて変更が加えられた場合、プロセスによってオブジェクトが最後に保存された後でのみオブジェクトが再スキャンされます。

   - **アクセス時と変更時**

     オブジェクトが開いているときにスキャンされ、オブジェクトが変更された場合、そのオブジェクトが保存された後で再スキャンします。

     既定では、このオプションはオンです。

   - **アクセス時**

     読み取り、実行、または変更のために開いているすべてのオブジェクトがスキャンされます。

   - **実行時**

     Kaspersky Security 10.1 for Windows Server により、ファイルが実行のためにアクセスされたときにのみ、そのファイルがスキャンされます。

5. [**OK**]をクリックします。

選択された保護モードが有効になります。

ファイルのリアルタイム保護タスクでの保護範囲

このセクションでは、ファイルのリアルタイム保護タスクの保護範囲の作成と管理について説明します。

このセクションの内容

定義済みの保護範囲

保護対象サーバーのファイルリソースが、[**サーバーのリアルタイム保護**]タブの[**保護設定**]タブに表示されます。

ファイルリソースのツリーまたはリストには、Microsoft Windows のセキュリティの設定に従って読み取りアクセス権のあるフォルダーが表示されます。

Kaspersky Security 10.1 for Windows Server は次の定義済み保護範囲をカバーします:

- **ローカルハードディスク**:Kaspersky Security 10.1 for Windows Server はサーバーハードディスク上のファイルを保護します。
- **リムーバブルドライブ**:CD や USB ドライブなどの外部デバイスのファイルが保護されます。すべてのリムーバブルディスク、個々のディスク、フォルダー、ファイルを保護範囲に含めたり保護範囲から除外したりすることができます。

- **ネットワーク**：サーバー上で実行されているアプリケーションによってネットワークフォルダーに書き込まれたファイルとネットワークフォルダーから読み取られたファイルが保護されます。他のコンピューターのアプリケーションによってそのようなファイルにアクセスされた場合には、ファイルは保護されません。
- **仮想ドライブ**：共有のクラスタードライブなどの、一時的にサーバーに接続されるダイナミックフォルダー、ファイル、およびドライブを保護範囲に含めることができます。

既定では、ネットワークファイルリソースツリーで、あらかじめ定義された保護範囲を設定、表示できます。保護範囲設定時に、あらかじめ定義された範囲をネットワークファイルリソースリストに追加することもできます。

既定では、仮想ドライブを除くすべての定義済みの領域が保護範囲に含まれます。

SUBST コマンドを使用して作成した仮想ドライブは、Kaspersky Security 10.1 コンソールのサーバーファイルリソースのツリーには表示されません。仮想ドライブ上のオブジェクトを保護範囲に含めるには、仮想ドライブが関連付けられているサーバーのフォルダーを保護範囲に含めます。

接続されているネットワークドライブも、サーバーファイルリソースのツリーには表示されません。ネットワークドライブ上のオブジェクトを保護範囲に含めるには、そのネットワークドライブに対応するフォルダーへのパスを UNC フォーマットで指定します。

あらかじめ定義されたセキュリティレベルの選択

コンピューターのファイルリソースリストで選択したフォルダーに対して、次のいずれかの定義済みセキュリティレベルを適用できます：[**最大のパフォーマンス**]、[**推奨**]、[**最大の保護**]。これらのレベルにはそれぞれ、独自の定義済みセキュリティ設定が含まれます（以下の表を参照）。

最大のパフォーマンス

ネットワーク内部にその他のサーバーセキュリティ対策が適用されている場合（ファイアウォールや既存のセキュリティポリシーなど）、サーバーおよびワークステーションで Kaspersky Security 10.1 for Windows Server を使用する場合を除き、[**最大のパフォーマンス**]セキュリティレベルを使用してください。

推奨

[**推奨**]セキュリティレベルでは、保護と保護対象のサーバーのパフォーマンスへの影響が組み合わせて最適化されます。このレベルは、Kaspersky Lab のエキスパートが、ほとんどの企業ネットワークのサーバーの保護に十分なものとして推奨しています。既定では、[**推奨**]セキュリティレベルが選択されています。

最大の保護

組織のネットワークがコンピューターセキュリティ要件を引きあげている場合、[**最大の保護**]セキュリティレベルを推奨します。

表 32. 設定済みセキュリティレベルと対応する設定値

オプション	セキュリティレベル		
	最大のパフォーマンス	推奨	最大の保護
オブジェクトの保護	拡張子に基づく	形式に基づく	形式に基づく
作成または変更されたファイルのみを保護	有効	有効	無効
感染したオブジェクトと他のオブジェクトの処理	アクセスをブロックして駆除、駆除できない場合は削除	アクセスをブロックして推奨処理を実行	アクセスをブロックして駆除、駆除できない場合は削除
感染の可能性があるオブジェクトの処理	アクセスをブロックして隔離	アクセスをブロックして推奨処理を実行	アクセスをブロックして隔離
除外するファイル	なし	なし	なし
検知しないオブジェクト	なし	なし	なし

オプション	セキュリティレベル		
スキャン時間が次より長い場合は停止する(秒)	60 秒	60 秒	60 秒
スキャンする複合オブジェクトの最大サイズ(MB)	8 MB	8 MB	オフ
NTFS 代替データストリームをスキャン	あり	あり	あり
ディスクのブートセクターと MBR をスキャンする	あり	あり	あり
複合オブジェクトの保護	• 圧縮されたオブジェクト* *新規および変更されたオブジェクトのみ	• SFX アーカイブ* • 圧縮されたオブジェクト* • OLE 埋め込みオブジェクト* *新規および変更されたオブジェクトのみ	• SFX アーカイブ* • 圧縮されたオブジェクト* • OLE 埋め込みオブジェクト* * すべてのオブジェクト

[**オブジェクトの保護**]、[**iChecker テクノロジーを使用する**]、[**iSwift テクノロジーを使用する**]、および[**ヒューリスティックアナライザーを使用する**]の設定は、定義済みのセキュリティレベルの設定に含まれていません。事前に設定されたセキュリティレベルのいずれかを選択した後で、[**オブジェクトの保護**]、[**iChecker テクノロジーを使用する**]、[**iSwift テクノロジーを使用する**]、または[**ヒューリスティックアナライザーを使用する**]のセキュリティ設定を編集しても、選択したセキュリティレベルは変更されません。

► **事前に定義されたセキュリティレベルのいずれかを選択するには、次の手順を実行します**:

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**ファイルのリアルタイム保護**]ブロックで、[**設定**]をクリックします。

   [**サーバーのリアルタイム保護**]ウィンドウが開きます。

4. [**保護範囲**]タブでセキュリティ設定を行うフォルダーを選択し、[**設定**]をクリックします。

   [**ファイルのリアルタイム保護の設定**]ウィンドウが開きます。

5. ドロップダウンリストより希望のセキュリティレベルを選択します。

   - **最大の保護**
   - **推奨**
   - **最高のパフォーマンス**

6. [**OK**]をクリックします。

これで新しい設定が保存されました。

新しい設定は実行中のタスクにただちに適用されます。設定の変更日時に関する情報と変更前と変更後の

タスク設定の値は、実行ログに保存されます。

手動でのセキュリティの設定

ファイルのリアルタイム保護タスクでは、既定で保護範囲全体の共通のセキュリティ設定が使用されます。これらの設定は、あらかじめ定義されたセキュリティレベル[推奨]に対応します(278 ページのセクション「あらかじめ定義されたセキュリティレベルの選択」を参照)。

セキュリティ設定の既定値は、保護範囲全体の共通の設定として設定する方法、またはサーバーのファイルリソースのリストまたはツリーのフォルダーごとに異なる設定として設定する方法で、変更することができます。

サーバーファイルリソースツリーで作業する場合、選択した親フォルダーに対してネットワークファイルリソースツリーで作業したときに行ったセキュリティ設定が、すべてのサブフォルダーに自動的に適用されます。親フォルダーのセキュリティ設定は、個別に設定されたサブフォルダーに適用されません。

► **選択したフォルダーのセキュリティを手動で設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます(170 ページのセクション「ポリシーの設定」を参照)**。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**ファイルのリアルタイム保護**]ブロックで、[**設定**]をクリックします。

[**サーバーのリアルタイム保護**]ウィンドウが開きます。

4. [**保護範囲**]タブでセキュリティ設定を行うフォルダーを選択し、[**設定**]をクリックします。

5. [**設定**]をクリックすると、選択したフォルダーのセキュリティ設定を、必要に合わせて編集できます。それには、次の操作を実行します:

   - [**全般**]タブで、必要に応じて次の設定を行います:

     [**オブジェクトの保護**]セクションで、保護範囲に含めるオブジェクトを指定します:

     - **すべてのオブジェクト**

       Kaspersky Security 10.1 for Windows Server はすべてのオブジェクトをスキャンします。

     - **ファイル形式によってオブジェクトをスキャン**

       ファイル形式に基づいて感染の可能性があるオブジェクトのみがスキャンされます。

       形式のリストがコンパイルされます。Kaspersky Security 10.1 for Windows Server データベース内に含まれています。

     - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**

       ファイル拡張子に基づいて感染の可能性があるオブジェクトのみがスキャンされます。

       拡張子のリストがコンパイルされます。Kaspersky Security 10.1 for Windows Server データベース内に含まれています。

     - **指定の拡張子リストによってオブジェクトをスキャンする**

       ファイル拡張子に基づいてファイルをスキャンします。拡張子のリストは、[**変更**]をクリックすると表示される[**拡張子のリスト**]ウィンドウで手動でカスタマイズできます。

     - **ディスクのブートセクターと MBR をスキャンする**

       ブートセクターとマスターブートレコードの保護を有効にします。

       このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、サーバーのハードディスクおよびリムーバブルドライブのブートセクターとマス

ターブートレコードがスキャンされます。

既定では、このチェックボックスはオンです。

- **NTFS 代替データストリームをスキャン**

  NTFS ファイルシステムドライブの代替のファイルおよびフォルダースレッドをスキャンします。

  このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、追加のファイルおよびフォルダースレッドがスキャンされます。

  既定では、このチェックボックスはオンです。

[**パフォーマンス**]セクションで、チェックボックスをオンまたはオフにします:

- **作成または変更されたファイルのみを保護**

  このチェックボックスでは、Kaspersky Security 10.1 for Windows Server により、前回のスキャン以降に新規作成されたファイルまたは変更されたファイルとして認識されたファイルのスキャンおよび保護を有効または無効にします。

  このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、前回のスキャン以降に新規作成されたファイルまたは変更されたファイルとして認識されたファイルのみがスキャンおよび保護されます。

  このチェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、すべてのファイルがスキャンおよび保護されます。

  既定では、セキュリティレベルが[**最高のパフォーマンス**]の場合、このチェックボックスはオンになっています。[**最大の保護**]セキュリティレベルが設定されている場合、このチェックボックスはオフになっています。

[**複合オブジェクトの保護**]で、保護範囲に含める複合オブジェクトを指定します:

- **すべてまたは新しいアーカイブのみ**

  ZIP、CAB、RAR、ARJ やその他のアーカイブ形式のスキャン。

  このチェックボックスをオンにすると、アーカイブがスキャンされます。

  このチェックボックスをオフにすると、スキャン中にアーカイブがスキップされます。

既定値は、選択したセキュリティレベルによって異なります。

- **すべてまたは新しい SFX アーカイブのみ**

  自己抽出アーカイブのスキャン。

  このチェックボックスをオンにすると、SFX アーカイブがスキャンされます。

  このチェックボックスをオフにすると、スキャン中に SFX アーカイブがスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

  [**アーカイブ**]をオフにすると、このオプションがアクティブになります。

- **すべてまたは新しいメールデータベースのみ**

  Microsoft Outlook と Microsoft Outlook Express メールデータベースファイルのスキャン。

  このチェックボックスをオンにすると、メールデータベースファイルがスキャンされます。

  このチェックボックスをオフにすると、スキャン中にメールデータベースファイルがスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

- **すべてまたは新しく圧縮された実行ファイルのみ**

  UPX や ASPack などのバイナリコードパッカーで圧縮された実行可能ファイルのスキャン。

  このチェックボックスをオンにすると、パッカーで圧縮された実行可能ファイルがスキャンされます。

  このチェックボックスをオフにすると、パッカーで圧縮された実行可能ファイルが、スキャン中にスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

- **すべてまたは新しい通常のメールのみ**

  Microsoft Outlook メッセージや Microsoft Outlook Express メッセージなどのメール

形式のファイルのスキャン。

このチェックボックスをオンにすると、メール形式のファイルがスキャンされます。

このチェックボックスをオフにすると、スキャン中にメール形式のファイルがスキップされます。

既定値は、選択したセキュリティレベルによって異なります。

- **すべての OLE 埋め込みオブジェクト / 新しい OLE 埋め込みオブジェクトのみ**

  ファイルに埋め込まれたオブジェクト（Microsoft Word マクロ、メールメッセージの添付ファイルなど）のスキャン。

  このチェックボックスをオンにすると、ファイルに埋め込まれたオブジェクトがスキャンされます。

  このチェックボックスをオフにすると、ファイルに埋め込まれたオブジェクトが、スキャン中にスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

> [**作成または変更されたファイルのみを保護**]をオンにすると、すべての複合オブジェクトを保護するか、新しい複合オブジェクトのみを保護するかを選択できます。[**作成または変更されたファイルのみを保護**]をオフにすると、指定された複合オブジェクトをすべて保護します。

- [**処理**]タブで、必要に応じて次の設定を行います：

  - 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します。
  - 感染の可能性があるオブジェクトの処理を選択します。
  - 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します。
  - 修復できない複合オブジェクトに対して実行する処理を選択します：[**感染などの問題がある埋め込みオブジェクトが検知され、修復できない場合、オブジェクトを完全に削除する**]をオンまたはオフにします。

    このチェックボックスは、悪意のある子オブジェクトまたはその他のオブジェクトが検知された場合に、その親オブジェクトの強制削除を有効または無効にします。

    チェックボックスをオンにすると、感染したかその可能性が高いオブジェクトで実行する

よう選択した処理が[**アクセスをブロックして削除**]である場合、検知された悪意のある子オブジェクトまたはその他のオブジェクトの親の複合オブジェクト全体が強制的に削除されます。検知された子オブジェクトだけを削除できない場合(たとえば、親オブジェクトが変更不可能である場合)、親オブジェクトをすべての内容ごと強制的に削除します。

このチェックボックスがオフで、感染したかその可能性の高いオブジェクトで実行するよう選択した処理が[**アクセスをブロックして削除**]である場合、悪意のある子またはその他のオブジェクトが検知されても、親オブジェクトが変更不可能なら、親オブジェクトに対して選択した処理は実行されません。

既定では、セキュリティレベルが[**最大の保護**]の場合、このチェックボックスはオンになっています。セキュリティレベルが[**最高のパフォーマンス**]の場合、このオプションは既定でオフになります。

- [**パフォーマンス**]タブで、必要に応じて次の設定を行います:

  [**除外リスト**]セクション:

  - **除外するファイル**

    ファイル名やファイル名マスクによって、ファイルをスキャン対象から除外します。

    このチェックボックスをオンにすると、スキャン中、指定されたオブジェクトがスキップされます。

    このチェックボックスをオフにすると、すべてのオブジェクトがスキャンされます。

    既定では、このチェックボックスはオフです。

  - **検知しないオブジェクト**

    検知可能なオブジェクトの名前または名前マスクによって、オブジェクトがスキャン対象から除外されます。検知可能なオブジェクト名のリストについては、ウイルス百科事典の Web サイト(http://www.securelist.com)を参照してください。

    このチェックボックスをオンにすると、スキャン時に指定した検知可能なオブジェクトがスキップされます。

このチェックボックスをオフにすると、指定されたオブジェクトが既定ですべて検知されます。

既定では、このチェックボックスはオフです。

［**詳細設定**］セクション：

- **スキャン時間が次より長い場合は停止する（秒）**

  オブジェクトスキャンの制限時間。既定値は 60 秒です。

  このチェックボックスをオンにすると、スキャン時間が指定した値に制限されます。

  このチェックボックスをオフにすると、スキャン時間は無制限になります。

  既定では、このチェックボックスはオンです。

- **スキャンする複合オブジェクトの最大サイズ（MB）**

  指定したサイズより大きいオブジェクトが、スキャンの対象から除外されます。

  このチェックボックスをオンにすると、指定したサイズ制限を超える複合オブジェクトが、スキャン中にスキップされます。

  このチェックボックスをオフにすると、複合オブジェクトがサイズに関係なくスキャンされます。

  セキュリティレベルが［**推奨**］や［**最高のパフォーマンス**］の場合、このオプションは既定でオンになります。

- **iChecker テクノロジーを使用する**

  前回のスキャン以降に新規作成されたファイルと変更されたファイルのみをスキャンします。

  このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、前回のスキャン以降に新規作成されたファイルまたは変更されたファイルのみがスキャンされます。

  このチェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、ファイルの作成日または変更日が考慮されることなく、ファイルがスキャンされます。

既定では、このチェックボックスはオンです。

- **iSwift テクノロジーを使用する**

  前回の NTFS システムのオブジェクトのスキャン以降に新規作成されたファイルと変更されたファイルのみをスキャンします。

  このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、前回の NTFS システムのオブジェクトのスキャン以降に新規作成されたファイルまたは変更されたファイルのみがスキャンされます。

  このチェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、ファイルの作成日または変更日が考慮されることなく、NTFS システムファイルがスキャンされます。

  既定では、このチェックボックスはオンです。

6. [**OK**]をクリックします。

これで新しい設定が保存されました。

KSN の使用

このセクションでは、KSN の使用タスクとその設定方法について説明します。

このセクションの内容

KSN の使用タスクについて

Kaspersky Security Network（KSN）は、カスペルスキーが運用する、ファイル評価、Web リソース、およびプログラムに関するナレッジベースにアクセスできるオンラインサービスのインフラストラクチャです。Kaspersky Security Network により、Kaspersky Security 10.1 for Windows Server が新しい脅威に迅速に対応でき、いくつかの保護コンポーネントのパフォーマンスを改善し、誤検知の可能性を低下させます。

KSN の使用タスクを開始するには、Kaspersky Security Network 声明に同意する必要があります。

Kaspersky Security 10.1 for Windows Server が Kaspersky Security Network から受信するのは、プログラムの評価に関する情報のみです。

KSN に参加することで、カスペルスキーが新しい脅威の種別と発生源に関する情報をリアルタイムで受信して、無効化する方法を開発し、コンポーネントでの誤検知の数を減少させます。

製品が使用する情報の転送、処理、保管、破棄に関する詳細情報は、KSN の使用タスクのデータ処理ウィンドウと、カスペルスキーの Web サイトのプライバシーポリシーで確認できます。

Kaspersky Security Network への参加は任意です。Kaspersky Security Network への参加に関する決定は、Kaspersky Security 10.1 for Windows Server のインストール後に行います。Kaspersky Security Network への参加についての決定は、いつでも変更できます。

Kaspersky Security Network は、次の Kaspersky Security 10.1 for Windows Server タスクで使用できます:

- ファイルのリアルタイム保護
- オンデマンドスキャン
- アプリケーション起動コントロール
- トラフィックセキュリティ

- RPC ネットワークストレージの保護
- ICAP ネットワークストレージの保護

KSN の使用タスクの設定

KSN の使用タスクは、KSN 声明に同意しない場合は開始できません。

KSN の使用タスクの既定の設定を変更できます(次の表を参照)。

表 33. KSN の使用タスクの既定の設定

設定	既定値	説明
KSN での信頼しないオブジェクトに対する処理	**削除**	KSN によって感染していると認識されたオブジェクトに対して Kaspersky Security 10.1 for Windows Server が実行する処理を指定できます。
データ転送	サイズが 2 MB を超えないファイルのチェックサム(MD5 のハッシュ)が計算されます。	KSN に提供するために MD5 アルゴリズムを使用してチェックサムが計算されるファイルの最大サイズを指定できます。チェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server はすべてのサイズのファイルに対して MD5 のハッシュを計算します。
Kaspersky Security Network 声明の条件に同意する	同意しない	インストール後に KSN へ参加するかどうかを決定します。この決定は、いつでも変更できます。

設定	既定値	説明
Kaspersky Security Network の統計情報の一部としてデータを処理することに同意する	同意しない	KSN 声明に同意すると、このチェックボックスをオフにしない限り、KSN 統計情報が自動的に送信されます。
Kaspersky Managed Protection に関する声明の条件に同意する	同意しない	KMP サービスを有効または無効にできます。このサービスは、製品の購入過程で、個別の同意書にサインした場合にのみ使用できます。
タスク開始	最初の実行がスケジュール設定されていません。	タスクは手動で開始するか、開始スケジュールを設定することもできます。

KSN の使用タスクを設定するには、次の手順を実行します:

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションで、[**KSN の使用**]ブロックの[**設定**]をクリックします。

   [**KSN の使用**]ウィンドウが表示されます。

4. [**全般**]タブで、次のタスク設定を行います:

   - [**KSN での信頼しないオブジェクトに対する処理**]セクションで、KSN によって信頼しないと判定されたオブジェクトを検知した場合に Kaspersky Security 10.1 for Windows Server が実行する処理を指定します:

     - **削除**

       Kaspersky Security 10.1 for Windows Server は、KSN の感染ステータスが設定されているオブジェクトを削除し、バックアップにコピーを配置します。

       既定では、このオプションはオンです。

     - **情報を記録**

       Kaspersky Security 10.1 for Windows Server は、実行ログで KSN の感染ステータスが設定されているオブジェクトに関する情報を記録します。感染オブジェクトは削除しません。

   - [**データ転送**]セクションで、チェックサムが計算されるファイルのサイズを制限します:

     - [**ファイルサイズが次の値を超えたら KSN に送信する前にチェックサムを計算しない(MB):**]をオフまたはオンにします。

       このチェックボックスにより、KSN サービスにこの情報を送信するための、指定されたサイズのファイルのチェックサムの計算を有効または無効にします。

       チェックサムの計算にかかる時間は、ファイルサイズによって異なります。

このチェックボックスをオンにすると、指定された値（MB）を超えるサイズのファイルに対してチェックサムを計算しません。

チェックボックスをオフにすると、すべてのサイズのファイルに対してチェックサムを計算します。

既定では、このチェックボックスはオンです。

c. 必要に応じて、右側のフィールドで、Kaspersky Security 10.1 for Windows Server がチェックサムを計算するファイルの最大サイズを指定します。

d. [**Kaspersky Security Center を KSN プロキシとして使用する**]をオンにします。

このチェックボックスを使用して、保護対象サーバーから KSN へのデータ転送を管理できます。

チェックボックスがオフの場合、管理サーバーおよび保護対象サーバーからのデータは KSN に送信されません。ただし、設定によっては、サーバーは直接（Kaspersky Security Center を介さず）KSN にデータを送信できます。アクティブなポリシーにより、直接 KSN に送信できるデータの種別が決まります。

チェックボックスがオンの場合、すべてのデータは Kaspersky Security Center を経由して KSN に送信されます。

既定では、このチェックボックスはオンです。

> KSN プロキシを有効にするには、KSN 声明に同意し、Kaspersky Security Center を適切に設定する必要があります。詳細については、『**Kaspersky Security Center ヘルプ**』を参照してください。

5. 必要に応じて、[**タスク管理**]タブのタスク開始スケジュールを設定します。たとえば、サーバーが再起動したときにタスクを自動的に実行する場合は、スケジュールによるタスク開始を有効にし、頻度として[**アプリケーションの起動時**]を指定します。

   KSN の使用タスクがスケジュールによって自動的に開始されます。

6. タスクを開始する前にデータ処理を設定してください（295 ページのセクション「データ処理の設定を参照）。

7. [**OK**]をクリックします。

変更された設定が適用されます。設定を変更した日時、および変更前と変更後のタスクの設定に関する情報が、タスク実行ログに保存されます。

データ処理の設定

► **KSN サービスによって処理されるデータを設定して KSN 声明に同意するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 ページのセクション「**ポリシーの設定**」を参照)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションで、[**KSN の使用**]ブロックの[**データの処理**]をクリックします。

   [**データの処理**]ウィンドウが開きます。

4. [**サービス**]タブで、声明の内容を確認し、[**Kaspersky Security Network に関する声明の条件に同**

意する]をオンにします。

5. 保護レベルを上げるため、次のチェックボックスが自動的にオンになります:

   - **スキャンしたファイルに関するデータを送信**

     このチェックボックスをオンにすると、スキャンしたファイルのチェックサムが Kaspersky Lab に送信されます。各ファイルのセキュリティに関する判定は、KSN から取得した評価に基づいています。

     チェックボックスをオフにすると、ファイルのチェックサムは KSN に送信されません。

     既定では、このチェックボックスはオンです。

   - **要求した URL に関するデータを送信**

     このチェックボックスをオンにすると、要求された Web リソースに関するデータ(Web アドレスを含む)が Kaspersky Lab に送信されます。 要求された Web リソースのセキュリティに関する判定は、KSN から取得した評価に基づいています。

     チェックボックスをオフにすると、KSN 内で URL 評価はチェックされません。

     既定では、このチェックボックスはオンです。

     チェックボックスはトラフィックセキュリティタスク設定に影響します。

   いつでもこれらのチェックボックスをオフにして、追加データの送信を停止できます。

6. [**統計情報**]タブを開きます。[**Kaspersky Security Network の統計情報の一部としてデータを処理することに同意する**]は既定でオンになっています。追加の統計情報を Kaspersky Lab に送信しないようにする場合は、いつでもこのチェックボックスをオフにできます。

   このチェックボックスをオンにすると、定義されている目的のために個人情報を含む統計情報が送信されます。Kaspersky Lab が受信したデータは、製品の品質改善と脅威の検知レベルの向上のために使用されます。

   チェックボックスをオフにすると、追加の統計情報は送信されません。

   既定では、このチェックボックスはオンです。

7. [**Kaspersky Managed Protection**]タブで、声明の内容を確認し、[**Kaspersky Managed Protection に関する声明の条件に同意する**]をオンにします。

   このチェックボックスをオンにすると、保護対象のサーバーの動作に関する統計情報を Kaspersky Lab に送信することに同意したことになります。受信したデータは、セキュリティの脅威となるインシデントを防止するために必要な情報で、24 時間体制での分析と報告のために使用されます。

   既定では、このチェックボックスはオフです。

   [**Kaspersky Managed Protection に関する声明の条件に同意する**]の状態を変更しても、データの処理がただちには開始または停止するわけではありません。変更を適用するには、Kaspersky Security 10.1 for Windows Server を再起動する必要があります。

   KMP サービスを使用するには、サービス契約にサインし、保護対象サーバーで設定ファイルを実行する必要があります。

   KMP サービスを使用するは、[サービスと統計情報]タブで KSN 声明のデータ処理に関する条項に同意する必要があります。

8. [**OK**]をクリックします。

データ処理の設定が保存されます。

脆弱性攻撃ブロック

このセクションでは、プロセスメモリ保護を設定する方法について説明します。

この章の内容

脆弱性攻撃ブロックタスクについて

Kaspersky Security 10.1 for Windows Server には、プロセスメモリを脆弱性攻撃から保護する機能があります。この機能は、脆弱性攻撃ブロックで実装されます。コンポーネントのアクティビティステータスを変更し、プロセスメモリ保護を設定できます。

コンポーネントは、プロセスメモリを外部のプロセス保護エージェント(「エージェント」)の保護対象プロセスに挿入することによって脆弱性攻撃から保護します。

プロセス保護エージェントは動的にロードされて保護対象プロセスに挿入される Kaspersky Security 10.1 for Windows Server モジュールで、整合性を監視し、脆弱性を攻撃されるリスクを低下させます。

保護対象プロセス内のエージェントの操作には、プロセスの開始と停止が必要です。保護対象プロセスリストに追加されたプロセスへのエージェントの初期ロードは、プロセスが再起動された場合のみ可能です。また、プロセスが保護対象プロセスリストから削除された後にエージェントをアンロードできるのは、プロセスの再起動後のみです。

エージェントを保護対象プロセスからアンロードするには、停止する必要があります。脆弱性攻撃ブロックをアンインストールすると、環境がフリーズさせられ、エージェントが保護対象プロセスから強制的にアンロードされます。コンポーネントのアンインストール中に保護対象プロセスのいずれかにエージェントが挿入された場合、影響を受けるプロセスを終了する必要があります。サーバーの再起動が必要になることがあります（システムプロセスが保護されている場合など）。

保護対象プロセスに脆弱性攻撃の証拠が検知されると、Kaspersky Security 10.1 for Windows Server は次の処理のいずれかを実行します：

- 脆弱性攻撃が試行された場合、プロセスを終了します。
- プロセスが危険にさらされている事実を報告します。

次の方法のいずれかを使用してプロセス保護を停止できます：

- コンポーネントのアンインストール。
- 保護対象プロセスのリストからプロセスを削除して、プロセスを再起動。

Kaspersky Security ブローカーコンピューターサービス

脆弱性攻撃ブロックの効果を最も高めるためには、保護対象サーバーに Kaspersky Security ブローカーコンピューターサービスが必要です。このサービスおよび 脆弱性攻撃ブロックは、推奨インストールの一部です。kavfswh プロセスは保護対象サーバーのサービスのインストール時に作成、開始されます。これは、コンポーネントからセキュリティエージェントに、保護対象プロセスに関する情報を送信します。

Kaspersky Security ブローカーコンピューターサービスが停止した後、Kaspersky Security 10.1 for Windows Server は、保護対象プロセスリストに追加されたプロセスを引き続き保護し、新しく追加されたプロセスにもロードされ、利用できるすべての脆弱性攻撃による被害の軽減技術を適用してプロセスメモリを保護します。

Kaspersky Security ブローカーコンピューターサービスが停止した場合、アプリケーションは保護対象プロセスに発生したイベントに関する情報を受信しません（脆弱性攻撃およびプロセスの終了に関する情報を含む）。さらに、エージェントは新しい保護設定および保護対象プロセスリストへの新しいプロセスの追加に関する情報を受

信できません。

脆弱性攻撃ブロックモード

次のモードのいずれかを選択して、保護対象プロセスの脆弱性が攻撃されるリスクを軽減する処理を設定できます:

- **脆弱性攻撃時に終了する**:このモードを適用すると、脆弱性攻撃が行われた場合にプロセスを終了します。

  保護されている重要なオペレーティングシステムプロセスの脆弱性に対する攻撃試行を検知した場合、脆弱性攻撃ブロック設定に示されたモードに関係なく、Kaspersky Security 10.1 for Windows Server はプロセスを終了しません。

- **脆弱性攻撃を受けたプロセスについてのみ通知する**:このモードを適用すると、Filtered Security Audit のイベントを使用して保護対象プロセスにおける脆弱性攻撃インスタンスに関する情報を受信します。

  このモードを選択すると、Kaspersky Security 10.1 for Windows Server はイベントを作成することで脆弱性を攻撃するすべての試行を記録します。

プロセスメモリ保護の設定

► **保護対象プロセスのリストに追加されたプロセスのメモリを保護するように設定するには、次の処理を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

  > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションで、[**脆弱性攻撃ブロック**]ブロックの[**設定**]をクリックします。

   [**脆弱性攻撃ブロック**]ウィンドウが表示されます。

4. [**脆弱性攻撃ブロックモード**]セクションで、次の設定を行います:

   - **脆弱なプロセスに対する攻撃から防御する**

     このチェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server は、保護対象プロセスのリストにあるプロセスの脆弱性が攻撃されるリスクを低下させます。

     このチェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server はサーバープロセスを脆弱性攻撃から保護しません。

     既定では、このチェックボックスはオフです。

   - **脆弱性攻撃時に終了する**

     このモードを選択すると、アクティブな脆弱性攻撃による被害の軽減技術がプロセスに適用されている場合、Kaspersky Security 10.1 for Windows Server は脆弱性攻撃試行を検知すると保護対象プロセスを終了します。

   - **脆弱性攻撃を受けたプロセスについてのみ通知する**

     このモードを選択すると、Kaspersky Security 10.1 for Windows Server は脆弱性攻撃をターミナルウィンドウに表示してレポートします。危険にさらされたプロセスは実行され続けます。

Kaspersky Security 10.1 for Windows Server が［**脆弱性攻撃時に終了する**］モードで実行中に重要なプロセスで脆弱性攻撃を検知した場合、コンポーネントが強制的に［**脆弱性攻撃を受けたプロセスについてのみ通知する**］モードに切り替えます。

5. ［**防御処理**］セクションで、次の設定を行います：

- **脆弱性攻撃を受けたプロセスについてターミナルサービスから通知する**

  このチェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server はターミナルウィンドウに保護がアクティベートされた理由の説明と、脆弱性攻撃試行が検知されたプロセスの兆候を表示します。

  チェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server はターミナルウィンドウに、危険にさらされたプロセスの脆弱性攻撃試行または終了が検知された時刻を表示します。ターミナルウィンドウは、Kaspersky Security ブローカーコンピューターサービスのステータスに関係なく表示されます。既定では、このチェックボックスはオンです。

- **Kaspersky Security サービスが無効の場合にも脆弱なプロセスに対する攻撃を防御する**

  このチェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server サービスが実行中かどうかに関係なく、すでに開始されたプロセス内の脆弱性が攻撃されるリスクを低下させます。Kaspersky Security 10.1 for Windows Server サービスが停止すると、追加されたプロセスは保護されません。サービスが開始されると、すべてのプロセスについて脆弱性攻撃の影響軽減が停止されます。

  このチェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server サービスが停止すると、プロセスは脆弱性攻撃から保護されません。

  既定では、このチェックボックスはオンです。

  このチェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server は、保護対象プロセスのリストにあるプロセスの脆弱性が攻撃されるリスクを低下させます。

  このチェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server はサーバープロセスを脆弱性攻撃から保護しません。

既定では、このチェックボックスはオフです。

6. [**OK**]をクリックします。

Kaspersky Security 10.1 for Windows Server では、設定したプロセスメモリ保護が保存されて適用されます。

保護するプロセスの追加

脆弱性攻撃ブロックは、既定で複数のプロセスを保護します。保護しないプロセスは、保護対象プロセスのリストでチェックをオフにします。

► **保護されているプロセスのリストにプロセスを追加するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションで、[**脆弱性攻撃ブロック**]における[**設定**]をクリックします。

   [**脆弱性攻撃ブロック**]ウィンドウが表示されます。

4. [**保護されたプロセス**]タブで、[**参照**]をクリックします。

   Microsoft Windows 標準の[**ファイルを開く**]ウィンドウが表示されます。

5. リストに追加するプロセスを選択します。

6. [**開く**]をクリックします。

7. [**追加**]をクリックします。

   プロセスが保護対象プロセスのリストに追加されます。

8. 追加されたプロセスを選択して、[**脆弱性攻撃ブロック技術の設定**]をクリックします。

   [**脆弱性攻撃ブロックの手法**]ウィンドウが開きます。

9. 次のいずれかのオプションを選択して、脆弱性攻撃による被害の軽減技術を適用します:

   - **利用できるすべての脆弱性攻撃ブロック技術を適用する**

     このオプションを選択すると、リストは編集できません。既定で、すべての技術が適用されます。

   - **選択した脆弱性攻撃ブロック技術を適用**:

     このオプションを選択すると、適用されている脆弱性攻撃による被害の軽減技術のリストを編集できます:

     a. 選択したプロセスを保護するには、適用する技術の隣にあるチェックボックスをオンにします。

     b. [**Attack Surface Reduction 手法を適用する**]をオンまたはオフにします。

10. 脆弱性攻撃による被害の軽減技術 Attack Surface Reduction を設定します:

    - [**次のモジュールを許可しない**]に、起動後に保護対象プロセスからブロックされるモジュールの名前を入力します。

    - [**インターネットゾーンで起動した場合、モジュールを禁止しない**:]で、モジュールの起動を許可するオプションの隣にあるチェックボックスをオンにします:

- インターネット
- ローカルイントラネット
- 信頼するサイト
- 制限されたサイト
- コンピューター

これらの設定は、Internet Explorer®にのみ適用できます。

11. [**OK**]をクリックします。

プロセスがタスクの保護範囲に追加されます。

脆弱性攻撃による被害の軽減技術

表 34. 脆弱性攻撃による被害の軽減技術

脆弱性攻撃による被害の軽減技術	説明
Data Execution Prevention（DEP）	Data Execution Prevention は、保護されたメモリ領域での任意のコードの実行をブロックします。
Address Space Layout Randomization（ASLR）	プロセスのアドレス空間におけるデータ構造の配置に対する変更。
Structured Exception Handler Overwrite Protection（SEHOP）	例外レコードの置換または例外ハンドラの置換。
Null Page Allocation	NULL ポインタのリダイレクト防止。
LoadLibrary Network Call Check（Anti ROP）	ネットワークパスからの DLL ロードに対する保護。

脆弱性攻撃による被害の軽減技術	説明
Executable Stack（ROP 対策）	スタックの領域の無許可実行のブロック。
アンチ RET チェック（ROP 対策）	CALL インストラクションが安全に起動するかどうか確認します。
アンチ Stack Pivoting（ROP 対策）	実行可能アドレスへの ESP スタックポインタの再配置に対する保護。
Export Address Table Access 監視（EAT Access 監視とデバッグレジスタによる EAT Access 監視）	kernel32.dll、kernelbase.dll および ntdll.dll でのエクスポートアドレステーブルに対する読み込みアクセスの保護
ヒープスプレーの割り当て	悪意のあるコードを実行するためのメモリ割り当てに対する保護。
実行フローシミュレーション（Return Oriented Programming 対策）	Windows API コンポーネントにおける疑わしいインストラクション連鎖（ROP ガジェットの可能性あり）の検知。
IntervalProfile コールの監視（Ancillary Function Driver Protection（AFDP））	AFD ドライバーの脆弱性を使用した権限の昇格に対する保護（QueryIntervalProfile のコールによる Ring 0 における任意のコードの実行。
Attack Surface Reduction	保護対象プロセスを介した脆弱なアドインの起動のブロック。

スクリプト監視

このセクションでは、スクリプト監視タスクとその設定方法について説明します。

このセクションの内容

スクリプト監視タスクについて

スクリプト監視タスクが実行されている場合、Kaspersky Security 10.1 for Windows Server により、Microsoft Windows のスクリプトテクノロジー(アクティブスクリプティング)を使用して作成されたスクリプト(VBScript や JScript® など)の実行が制御されます。スクリプトが安全であると判断された場合にのみ、このスクリプトの実行が許可されます。危険であると判断されたスクリプトの実行はブロックされます。Kaspersky Security 10.1 for Windows Server によりスクリプトに潜在的な危険性があると判断された場合、ユーザーの選択した処理に従って、スクリプトの実行がブロックまたは許可されます。

既定では、スクリプト監視タスクは、Kaspersky Security 10.1 for Windows Server の起動時に自動で開始します。

既定では、スクリプト監視は製品の一部としてサーバーにインストールされません。

保護対象サーバーにインストールされているサードパーティ製のアプリケーションの中には、このコンポーネントと競合することがあります。その場合、サードパーティ製スクリプトを監視すると、スクリプトの操作エラーが発生する可能性があります。こうしたサードパーティ製アプリケーションは使用しないでください。また、スクリプト監視タスクを無効にしないでください。タスクを無効にすると、スクリプト実行時のセキュリティに関するリスクが高まります。

スクリプトの監視を使用するには、Kaspersky Security 10.1 for Windows Server のインストール時に、インストール済みコンポーネントのリストで手動で選択する必要があります。

インストール時のアプリケーションコンポーネントの選択に関する詳細な情報については、『Kaspersky Security

10.1 for Windows Server **管理者用ガイド』のインストールに関するセクション**を参照してください。

スクリプト監視タスクを設定できます。

スクリプト監視タスクの設定

スクリプト監視システムタスクでは、次の表の既定の設定が使用されます。これらの設定の値を変更できます。

表 35. スクリプト監視タスクの既定の設定

設定	既定値	説明
危険なスクリプトの実行	ブロック	常時、Kaspersky Security 10.1 for Windows Server によって、危険と認識されたスクリプトの実行がブロックされます。
危険な可能性があるスクリプトの処理	ブロック	危険な可能性があるスクリプトの検知を実行する動作に対して、実行をブロックするか、許可するかを指定できます。
ヒューリスティックアナライザー	[**中**]セキュリティレベルが適用されます。	ヒューリスティックアナライザーを有効または無効にできます。また、分析レベルを設定できます。
信頼リスト	使用	選択したタスクで使用できる一般的な信頼するオブジェクト。

► **スクリプト監視タスクを設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

- サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

> デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

[**プロパティ**:Kaspersky Security 10.1 for Windows Server]ウィンドウが開きます。

3. [**サーバーのリアルタイム保護**]セクションで[**スクリプト監視**]セクションの[**設定**]をクリックし、[**危険な可能性があるスクリプトの処理**]セクションで、次のいずれかの操作を行います:
   - 危険な可能性があるスクリプトの実行を許可する場合は、[**許可**]をオンにします。

     危険な可能性のあるスクリプトの実行が許可されます。
   - 危険な可能性があるスクリプトの実行をブロックする場合は、[**ブロック**]をオンにします。

     危険な可能性のあるスクリプトの実行がブロックされます。

     既定では、このオプションはオンです。
4. [**ヒューリスティックアナライザー**]セクションでは、次のいずれかの操作を行います:
   - [**ヒューリスティックアナライザーを使用する**]をオフまたはオンにします。

     このチェックボックスでは、オブジェクトのスキャン中のヒューリスティックアナライザーを有効または無効にできます。

     このチェックボックスをオンにすると、ヒューリスティックアナライザーが有効になります。

     このチェックボックスをオフにすると、ヒューリスティックアナライザーが無効になります。

既定では、このチェックボックスはオンです。

- 必要に応じて、スライダーを使用して分析のレベルを調整します。

  スライダーを使用すれば、ヒューリスティック分析のレベルを調整できます。このスキャンの強さのレベルによって、脅威の徹底的な検知、オペレーティングシステムのリソースにかかる負荷、スキャンの所要時間の間のバランスを調整します。

  次のレベルを設定できます:

  - **低**:実行ファイル内部で見つかったスクリプトを少数しか実行しません。脅威が検知される可能性はやや低くなります。スキャンの速度は速く、システムリソースの消費は軽度です。
  - **中**:Kaspersky Lab の推奨に基づき、実行ファイル内部で見つかったスクリプトを多数実行します。

    既定では、このレベルが選択されています。
  - **高**:実行ファイル内部で見つかったスクリプトをさらに多数実行します。脅威が検知される可能性は非常に高くなります。スキャンには、より多くのシステムリソースを消費し、より多くの時間がかかります。また、非常に多くの誤検知を引き起こす可能性があります。

    スライダーは、[**ヒューリスティックアナライザーを使用する**]をオンにすると使用可能になります。

5. [**信頼ゾーン**]セクションで、[**信頼ゾーンを適用**]をオンまたはオフにします。

   このチェックボックスにより、タスクに対する信頼ゾーンの使用を有効または無効にします。

   このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、信頼されたプロセスのファイル操作が、タスクの設定で指定されたスキャンの除外対象に追加されます。

   チェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、ファイルのリアルタイム保護タスクの保護範囲を作成するときに信頼されたプロセスのファイル操作を無視します。

既定では、このチェックボックスはオンです。

6. ［**OK**］をクリックします。

新しい設定が適用されます。

トラフィックセキュリティ

このセクションでは、トラフィックセキュリティタスクとトラフィックセキュリティタスクの設定方法について説明します。

このセクションの内容

トラフィックセキュリティタスクについて

トラフィックセキュリティは Web トラフィックを処理し（メールサービス経由で受信するトライフィックを含む）、既

知のコンピューターと保護対象サーバーのその他の脅威を検知するため、Web トラフィックを介して転送されるオブジェクトをインターセプトおよびスキャンします。ICAP サービスは脅威を検知するため着信トラフィックをスキャンし、スキャン結果とスキャン設定に応じてトラフィックをブロックまたは許可します。

Kaspersky Security 10.1 for Windows Server は、Windows Subsystem for Linux でも実行するプロセスが要求したトラフィックを検知しインターセプトします。そのようなプロセスに対して、トラフィックのセキュリティタスクは現在の設定で定義されている処理を適用します。

トラフィックセキュリティは既定でインストールされています。インストールが完了すると、次のサービスが登録および開始されます:

- Kaspersky Security ブローカーコンピューター（KAVFSWH）
- Kaspersky Traffic Security（KAVFSPROXY）

コンポーネントが次の保護を提供します:

- メールの脅威に対する保護:
  - フィッシング対策
  - メールで送信されるマルウェアに対する保護
- Web の脅威に対する保護:
  - フィッシング対策
  - 悪意ある URL スキャン
  - Web ベースのマルウェアに対する保護
  - ウェブコントロール:
    - URL コントロール
    - 証明書コントロール
    - カテゴリベースの Web コントロール

トラフィックセキュリティタスクを開始して脅威検知を強化する場合、KSN サービスを使用することを強く推奨します。KSN クラウドデータベースには、Web 脅威に関する実際のデータがローカルの定義データベースよりも多く含まれています。多数のウェブコントロールのカテゴリの分析は、KSN サービスから取得する判定に基づいて行われます。

トラフィックセキュリティモード

トラフィックセキュリティは次のモードで動作します:

- **ドライバーインターセプター**:アプリケーションがネットワークドライバーでトラフィックをインターセプトします。ネットワークカーネルドライブを使用して、指定したポートの着信トラフィックをすべてインターセプトおよび分析します。
- **リダイレクター**:アプリケーションがブラウザーの設定によりトラフィックをリダイレクトします。ブラウザーから、開かれたターミナルセッションの内部プロキシへ、着信トラフィックがリダイレクトされます。Kaspersky Security 10.1 for Windows Server は内部プロキシとして指定されます。
- **外部プロキシ**:アプリケーションが外部プロキシサーバーからのトラフィックを処理します。トラフィックは外部プロキシサーバーから Kaspersky Security 10.1 for Windows Server へ転送されます。アプリケーションがトラフィックを分析し、外部プロキシに対する動作を推奨します。Kaspersky Security 10.1 for Windows Server は、ICAP プロトコルを使用してトラフィックを転送するプロキシのみと互換性があります。

トラフィックセキュリティルールについて

Kaspersky Security 10.1 for Windows Server では証明書および Web サイトのアドレスに対する許可または拒否ルールの追加と設定、および望ましくないコンテンツをブロックするためカテゴリに対して事前設定された

ルールの使用が可能です。証明書に対するルールは、タスクを[**ドライバーインターセプター**]または[**リダイレクター**]モードで実行中に適用できます。

ウェブコントロール

この種別のコントロールは、Web サイトのアドレスおよび証明書に許可および拒否ルールを適用することによって実施されます。許可ルールは KSN とシグネチャ解析から得られる判定よりも優先度が高くなります。

URL または証明書は、優先順が付いた判定に基づいて(高い順から低い順へ)許可またはブロックされます。

1. 許可または拒否ルール。
2. フィッシング対策および定義データベース。
3. KSN。
4. カテゴリ。

カテゴリベースの Web コントロール

Kaspersky Security 10.1 for Windows Server では、カテゴリに基づいて Web サイトのアドレスがブロックされます。カテゴリ分類に使用するヒューリスティック分析のレベルが設定可能です。カテゴリベースのウェブコントロールは、設定済みのカテゴリリストを分析に使用します。リスト自体は変更できませんが、許可またはブロックする Web リソースのカテゴリを選択すること、あるいはカテゴリベースのコントロールをオフにすることができます。その他のカテゴリには、リスト内の他のカテゴリに該当しないすべての Web リソースが含まれます。このチェックボックスをオンにすると、カテゴリ分類されていないすべての Web リソースが許可されます。チェックボックスをオフにすると、すべての Web リソースがブロックされます。

> カテゴリ分類は優先順位が最低です。

Kaspersky Security 10.1 for Windows Server が既定で適用するルールは TOR 証明書ルールの拒否の 1 つだけです。ルール設定でこのルールをオフにして、TOR 接続を許可することができます。 ルールが適用されると、送受信するすべての TOR 接続がブロックされます。

トラフィックセキュリティでは `not-a-virus`(非ウイルス)マスク(これ自体はウイルスではないが保護対象サーバーに害をもたらす目的で使用される可能性のあるリソースまたはオブジェクト)に対する判定も考慮され

ます。Kaspersky Security 10.1 for Windows Server は既定で、カテゴリに not-a-virus（非ウイルス）マスクを適用しません（343 ページのセクション「カテゴリベースの Web コントロールの設定」を参照）。

メールの脅威に対する保護

トラフィックセキュリティは、Microsoft Outlook（2010、2013、2016 32 ビット版および 64 ビット版）のメールをスキャンします。メールの脅威に対する保護は、Kaspersky Security 10.1 for Windows Server コンポーネントとは別にインストールされる Kaspersky Security 10.1 Microsoft Outlook アドインを介して行われます。

> Kaspersky Security 10.1 Microsoft Outlook アドインは、Kaspersky Security 10.1 for Windows Server および Microsoft Outlook メールクライアントがインストールされている場合にのみ、保護対象サーバーにインストールできます。

► **アドインをインストールするには、¥email_plugin フォルダーから ksmail_x86(x64).msi パッケージを実行します。**

メールの脅威に対する保護は次を含みます：

- 受信メールのスキャン。
- ウイルス対策のためのメールスキャン。
- ウイルス対策のための添付ファイル（圧縮されたオブジェクトを含む）のスキャン。
- フィッシング対策のためのメールスキャン。
- フィッシング対策のための添付ファイル（圧縮されたオブジェクトを含む）のスキャン。

脅威が検知された場合、Kaspersky Security 10.1 for Windows Server は次を実行します：

- 添付ファイルの削除。
- 感染したメール本体の修正。

- 「**メールの脅威が検知されました**」イベントの記録。

Kaspersky Security 10.1 for Windows Server はサーバーによるメール受信時ではなく、メール開封時にメールをスキャンします。スキャンは初回の開封時に 1 回のみ実行されます。スキャンされたメールと添付ファイルは、Outlook が再起動されるまでキャッシュに保存されます。再起動後、再開封時にすべてのメールがスキャンされます。

► **アドインは、起動時に Microsoft Outlook メールクライアントに読み込まれます。Outlook の実行中に Kaspersky Security 10.1 Microsoft Outlook アドインをインストールする場合:**

1. **[ファイル] - [オプション] - [アドイン]**の順に選択します。
2. Kaspersky Security 10.1 Microsoft Outlook アドインが、リストの 1 つに追加されていることを確認してください(使用中または使用停止中)。
3. Microsoft Outlook を再起動します。
4. Kaspersky Security 10.1 Microsoft Outlook アドインのステータスが、**使用中**になっていることを確認します。

トラフィックセキュリティタスクの設定

トラフィックセキュリティタスクの既定の設定を変更できます(次の表を参照)。

表 36. 既定のトラフィックセキュリティタスクの設定

表 37.

設定	既定値	説明
タスクモード	**外部プロキシ**	ICAP サービスは外部プロキシサーバーからのトラフィックを処理します。

設定	既定値	説明
ネットワークポート番号	1345	ICAP サービスの既定のポート番号です。
サービス ID	webscan	インストールされたウイルス対策サーバーのアドレスに対する ICAP サービス識別子です。
悪意のある URL データベースを使用して Web リンクをスキャンする	適用されます。	各 URL のシグネチャ解析を有効または無効にします。
アンチフィッシングデータベースを使用して Web ページをスキャンする	適用されます。	ヒューリスティック分析に基づいて、URL フィッシング対策スキャンを有効または無効にします。
保護に KSN を使用する	適用されます。	タスク実行中、保護のため KSN アプリケーション評価データを使用できます。
信頼ゾーンを使用する	適用されます。	必要に応じて信頼ゾーンを適用できます。
セキュリティレベル	推奨	ウイルス対策のためセキュリティレベルを選択および設定します。
タスク開始スケジュール	最初の実行がスケジュール設定されていません。	トラフィックセキュリティタスクは、自動的には開始されません。タスクは手動で開始するか、開始スケジュールを設定することもできます。

► **トラフィックセキュリティタスクを設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

- サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

> デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**タスクモード**]タブでタスクの処理モードを選択および設定します(319 ページのセクション「タスクの処理モードの選択」を参照)。

5. [**URL と Web アドレスの処理**]タブで URL のフィッシング対策およびウイルス対策スキャンを設定します(334 ページのセクション「URL と Web アドレスの処理の設定」を参照)。

6. [**マルウェア保護**]タブで、ヒューリスティックアナライザーとセキュリティレベルを設定します(327 ページのセクション「Web ベースのマルウェアに対する保護の設定」を参照)。

7. [**タスク管理**]タブで、スケジュールに基づいてタスクを開始します(220 ページのセクション「タスクスケジュールの管理」を参照)。

8. [**OK**]をクリックします。

タスクの設定が保存されます。

タスクの処理モードの選択

► **タスクの処理モードを設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**全般**]タブで、[**タスクモード**]ドロップダウンリストから使用可能なモードのいずれかを選択します:

   - **ドライバーインターセプター**(320 ページのセクション「**ドライバーインターセプターモードの設定**」を参照)

   - **リダイレクター**(323 ページのセクション「**リダイレクターモードの設定**」を参照)

   - **外部プロキシ**

5. ICAP サービス接続設定を指定(3 つのモードすべてで必要):

   - **ネットワークポート番号**

     Kaspersky Security 10.1 for Windows Server の ICAP サービスのポート番号。

   - **サービス ID**

     ICAP の RESPMOD URI パラメータ の一部を構成する ID(ドキュメント RFC 3507 参照)。RESPMOD URI は、ネットワークストレージ領域にインストールされている アンチウイルス ICAP サーバーのアドレスを指定します。

     たとえば、保護対象サーバーの IP アドレスが 192.168.10.10、ポート番号が 1345、ICAP サービス ID が webscan の場合、対応する RESPMOD URI アドレスは icap://192.168.10.10/webscan:1345 です。

6. 選択したタスクのモードを設定します。

   [**外部プロキシ**]モードの場合、追加の設定は不要です。設定は外部プロキシサーバーで実行されます。

7. [**OK**]をクリックします。

設定が保存されます。

ドライバーインターセプターモードの設定

► **[トラフィックセキュリティ]ウィンドウで:**

1. [**全般**]タブを選択します。
2. [**ドライバーインターセプター**]タスクモードを選択します。
3. [**タスクモード設定**]ブロックで次の設定を行います:

   - **HTTPS トラフィックをスキャンする**

チェックボックスをオンにすると、インターセプトされた暗号化 HTTPS トラフィックが解凍され、脅威の有無がスキャンされます。

チェックボックスをオフにすると、暗号化 HTTPS トラフィックは解凍されません。

既定では、このチェックボックスはオンです。

スキャンは HTTPS ポートが開いているときのみ使用できます。

- 使用する暗号化プロトコルのバージョンを選択します:
  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

    [**TLS 1.0**]は既定でオンにされており、変更はできません。
- **証明書が無効の Web サーバーを信頼しない**

  [**HTTPS トラフィックをスキャンする**]がオンのとき、このチェックボックスをオンにできます。

  このチェックボックスがオンの場合、証明書が無効の Web ページはブロックされます(証明書が有効期限切れ、シグネチャ検証エラー、証明書が取り下げられたなど)
- **セキュリティポート**

  Web ベースの脅威を検知するために Kaspersky Security 10.1 for Windows Server により作成された内部ポートに、ブラウザーまたはネットワークドライバーからのトラフィックをリダイレクトする際に使用するポート番号を指定します。既定のポートの変更は推奨されません。ポート番号は ICAP サービスのために開くほかのポートと一致しないようにします。[**リダイレクター**]タスクモードを使用する場合、すでに使用されているポートが[**HTTPS トラフィックをスキャンする**]にリストアップされています。

4. ポートを遮断領域に追加する、またはそこから除外するには、[**遮断領域の設定**]をクリックします。

   [**遮断領域**]ウィンドウが開きます。

5. [**ポートの遮断**]タブで次のオプションのいずれかを選択します:

   - **すべて遮断する**
   - **指定したポートを遮断する**:

     a. テキストフォールドにポート番号を入力します。ポート番号間をセミコロンで区切って、複数のポートを追加できます。

     b. [**追加**]をクリックします。

     ポートが遮断領域に追加されます。

   > 既定では、Kaspersky Security 10.1 for Windows Server は、ポート:80、8080、3128、443から転送されるトラフィックをインターセプトします。

6. 遮断領域から除外するポートを[**ポートの除外**]タブで指定するには:

   a. テキストフォールドにポート番号を入力します。ポート番号間をセミコロンで区切って、複数のポートを追加できます。

   b. [**追加**]をクリックします。

   ポートがエリアから除外されます。

   > 既定では、Kaspersky Security 10.1 for Windows Server は他のアプリケーションによって使用されるポートを除外するため、暗号化された接続(3389、1723、13291)から転送されたデータを読み込もうとするときに問題が発生することがあります。

7. [**IP アドレスの除外**]タブで遮断領域から IP アドレスを除外するには:

   a. IPv4 フォーマットまたはマスクを使用して IP アドレスを入力します。

   b. [**追加**]をクリックします。

c. [**OK**]をクリックして、変更内容を保存します。

8. [**プロセスの除外**]タブで、トラフィック交換が必要なプロセスまたは実行ファイルを除外するには:

a. [**プロセスの除外を適用**]をオンにします。

b. ファイルを除外するには:

1. [**実行ファイル**]をクリックします。

標準の[**ファイルを開く**]ウィンドウが表示されます。

2. 除外する実行ファイルを選択して、[**ファイルを開く**]をクリックします。

a. ローカルコンピューターで実行されているプロセスを除外するには:

3. [**実行中のプロセス**]をクリックします。

[**実行中のプロセス**]ウィンドウが表示されます。

4. 現在実行中のプロセスを選択して、[**OK**]をクリックします。

> Kaspersky Security Center でプロセスを選択することはできません。

9. [**トラフィックのセキュリティ**]ウィンドウで[**OK**]をクリックします。

タスクモードの設定が保存されます。

リダイレクターモードの設定

► **[トラフィックのセキュリティ]ウィンドウで:**

1. [**全般**]タブを選択します。

2. [**リダイレクター**]タスクモードを選択します。

3. [**タスクモード設定**]ブロックで次の設定を行います:

- **HTTPS トラフィックをスキャンする**

  チェックボックスをオンにすると、インターセプトされた暗号化 HTTPS トラフィックが解凍され、脅威の有無がスキャンされます。

  チェックボックスをオフにすると、暗号化 HTTPS トラフィックは解凍されません。

  既定では、このチェックボックスはオンです。

  > スキャンは HTTPS ポートが開いているときのみ使用できます。

- 使用する暗号化プロトコルのバージョンを選択します:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

    > [**TLS 1.0**]は既定でオンにされており、変更はできません。

- **確認後に外部プロキシにトラフィックをリダイレクトする**

  チェックボックスをオンにすると、スキャン済みのトラフィックが外部プロキシ(企業ネットワーク範囲内で使用される企業プロキシサーバーなど)へリダイレクトされます。

  チェックボックスをオフにすると、トラフィックが内部プロキシへ直接送られます。

  - **プロキシサーバーのアドレス**

    リダイレクションに使用する内部ターミナルプロキシサーバーのアドレス。IPv4 フォーマットでアドレスを入力します。

  - **ポート**

    内部プロキシのポート番号。

- **セキュリティポート**

  Web ベースの脅威を検知するために Kaspersky Security 10.1 for Windows Server により作成された内部ポートに、ブラウザーまたはネットワークドライバーからのトラ

フィックをリダイレクトする際に使用するポート番号を指定します。既定のポートの変更は推奨されません。ポート番号は ICAP サービスのために開くほかのポートと一致しないようにします。[**リダイレクター**]タスクモードを使用する場合、すでに使用されているポートが[**HTTPS トラフィックをスキャンする**]にリストアップされています。

> [**リダイレクター**]モードの場合、オペレーティングシステムは Kaspersky Security 10.1 for Windows Server によって指定されたポート経由で暗号化トラフィックを転送するよう設定する必要があります。

4. [**OK**]をクリックします。

タスクモードの設定が保存されます。

定義済みセキュリティレベルの設定

サーバーのファイルリソースツリーで選択したフォルダーに対して、3 つの定義済みセキュリティレベルのいずれかを適用できます:[最高のパフォーマンス]、[推奨]、[最大の保護]。 これらのレベルにはそれぞれ、独自の定義済みセキュリティ設定が含まれます(以下の表を参照)。

最大のパフォーマンス

ネットワーク内部にその他のサーバーセキュリティ対策が適用されている場合(ファイアウォールや既存のセキュリティポリシーなど)、サーバーおよびワークステーションで Kaspersky Security 10.1 for Windows Server を使用する場合を除き、[**最大のパフォーマンス**]セキュリティレベルを使用してください。

推奨

[**推奨**]セキュリティレベルでは、保護と保護対象のサーバーのパフォーマンスへの影響が組み合わせて最適化されます。このレベルは、Kaspersky Lab のエキスパートが、ほとんどの企業ネットワークのサーバーの保護に十分なものとして推奨しています。既定では、[**推奨**]セキュリティレベルが選択されています。

最大の保護

組織のネットワークがコンピューターセキュリティ要件を引きあげている場合、[**最大の保護**]セキュリティレベルを推奨します。

表 38.　定義済みセキュリティレベルと対応するセキュリティ設定

オプション	セキュリティレベル		
	最大のパフォーマンス	推奨	最大の保護
オブジェクトのスキャン	データベース内の拡張子リストに従う	形式に基づく	すべてのオブジェクト
感染したオブジェクトと他のオブジェクトの処理	ブロック	ブロック	ブロック

オプション	セキュリティレベル		
	最大のパフォーマンス	推奨	最大の保護
検知しないオブジェクト	なし	なし	なし
スキャン時間が次より長い場合は停止する(秒)	60 秒	60 秒	60 秒
次のサイズより大きいオブジェクトはスキャンしない(MB)	20 MB	20 MB	なし
複合オブジェクトのスキャン	• 圧縮されたオブジェクト* * 新規および変更されたオブジェクトのみ	• アーカイブ* • SFX アーカイブ* • 圧縮されたオブジェクト* • OLE 埋め込みオブジェクト* * 新規および変更されたオブジェクトのみ	• アーカイブ* • SFX アーカイブ* • 圧縮されたオブジェクト* • OLE 埋め込みオブジェクト* * すべてのオブジェクト

Web ベースのマルウェアに対する保護の設定

次の保護設定も受信メールのトラフィックに影響を与えます。ただし、感染したオブジェクトおよびその他の検知されたオブジェクトに対して選択された処理は、メールの添付ファイルに対してのみ実行されます。

► **ウイルスおよび Web トラフィック経由で転送されるその他のコンピューターセキュリティの脅威を検知するため、ヒューリスティック分析を設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**マルウェア保護**]タブで:

   - [**ヒューリスティックアナライザーを使用する**]をオンにします。

   - マルウェアのスキャンに要求されるヒューリスティック分析のレベルを設定します。

   - セキュリティレベル(325 ページのセクション「定義済みセキュリティレベルの設定」を参照)をドロップダウンリストから選択します:

     - **推奨**
     - **最大の保護**
     - **最大のパフォーマンス**

- **カスタム**

5. 下部の[**説明**]タブで、選択したセキュリティレベルの設定を確認できます。

6. [**全般**]タブを開き、[**オブジェクトの保護**]セクションでスキャンの範囲に含めるオブジェクトを指定します:

- **すべてのオブジェクト**

  Kaspersky Security 10.1 for Windows Server はすべてのオブジェクトをスキャンします。

- **ファイル形式でスキャンするオブジェクト**

  ファイル形式に基づいて感染の可能性があるオブジェクトのみがスキャンされます。

  形式のリストがコンパイルされます。Kaspersky Security 10.1 for Windows Server データベース内に含まれています。

- **定義データベース指定の拡張子リストによってオブジェクトをスキャン**

  ファイル拡張子に基づいて感染の可能性があるオブジェクトのみがスキャンされます。

  拡張子のリストがコンパイルされます。Kaspersky Security 10.1 for Windows Server データベース内に含まれています。

- **指定の拡張子リストによってスキャンされたオブジェクト**

  ファイル拡張子に基づいてファイルをスキャンします。拡張子のリストは、[**変更**]をクリックすると表示される[**拡張子のリスト**]ウィンドウで手動でカスタマイズできます。

  a. 拡張子のリストを編集するには、[**変更**]をクリックします。

  b. 開いたウィンドウで拡張子を指定します。

  c. [**追加**]をクリックします。

［**既定値**］をクリックして、設定済みの除外拡張子リストをリストに追加します。

7. ［**複合オブジェクトの保護**］で、スキャン範囲に含める複合オブジェクトを指定します：

- **アーカイブ**

  ZIP、CAB、RAR、ARJ やその他のアーカイブ形式のスキャン。

  このチェックボックスをオンにすると、アーカイブがスキャンされます。

  このチェックボックスをオフにすると、スキャン中にアーカイブがスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

- **SFX アーカイブ**

  自己抽出アーカイブのスキャン。

  このチェックボックスをオンにすると、SFX アーカイブがスキャンされます。

  このチェックボックスをオフにすると、スキャン中に SFX アーカイブがスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

  ［**アーカイブ**］をオフにすると、このオプションがアクティブになります。

- **圧縮されたオブジェクト**

  UPX や ASPack などのバイナリコードパッカーで圧縮された実行可能ファイルのスキャン。

  このチェックボックスをオンにすると、パッカーで圧縮された実行可能ファイルがスキャンされます。

  このチェックボックスをオフにすると、パッカーで圧縮された実行可能ファイルが、スキャン中にスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

- **OLE 埋め込みオブジェクト**

  ファイルに埋め込まれたオブジェクト(Microsoft Word マクロ、メールメッセージの添付ファイルなど)のスキャン。

  このチェックボックスをオンにすると、ファイルに埋め込まれたオブジェクトがスキャンされます。

  このチェックボックスをオフにすると、ファイルに埋め込まれたオブジェクトが、スキャン中にスキップされます。

  既定値は、選択したセキュリティレベルによって異なります。

8. [**処理**]タブで、感染したオブジェクトおよび検知したその他のオブジェクトの処理を選択します。

   - **ブロック**

     悪意あるコンテンツが検出された際に、Web ページのローディングがブロックされます。Web ページのかわりに、要求された Web ページがブロックされた理由が表示されます。

   - **許可**

     要求された Web ページはブロックされませんが、悪意あるコンテンツ検知についてのイベントがログに記録されます。

9. [**パフォーマンス**]タブで次の設定を行います:

   - [**除外**]セクションで、[**検知しない:**]をオンまたはオフにします:除外するオブジェクトのリストを設定するには:

     検知可能なオブジェクトの名前または名前マスクによって、オブジェクトがスキャン対象から除外されます。検知可能なオブジェクト名のリストについては、ウイルス百科事典の Web サイト(http://www.securelist.com)を参照してください。

     このチェックボックスをオンにすると、スキャン時に指定した検知可能なオブジェクトがスキップされます。

このチェックボックスをオフにすると、指定されたオブジェクトが既定ですべて検知されます。

既定では、このチェックボックスはオフです。

a. ［**変更**］をクリックします。

b. 開いたウィンドウ内で、オブジェクト名またはマスクを指定します。

c. ［**追加**］をクリックします。

- ［**詳細設定**］セクションで、スキャン時間間隔とオブジェクトのサイズを制限します：
  - **スキャン時間が次より長い場合は停止する（秒）**

    オブジェクトスキャンの制限時間。既定値は 60 秒です。

    このチェックボックスをオンにすると、スキャン時間が指定した値に制限されます。

    このチェックボックスをオフにすると、スキャン時間は無制限になります。

    既定では、このチェックボックスはオンです。
  - **次のサイズより大きいオブジェクトはスキャンしない（MB）**

    指定したサイズより大きいオブジェクトが、スキャンの対象から除外されます。

    このチェックボックスをオンにすると、指定したサイズ制限を超えるオブジェクトはスキャン中にスキップされます。

    このチェックボックスをオフにすると、オブジェクトはサイズに関係なくスキャンされます。

    セキュリティレベルが［**推奨**］や［**最大のパフォーマンス**］の場合、このオプションは既定でオンになります。

10. ［**マルウェア保護設定**］ウィンドウで［**OK**］をクリックします。

セキュリティレベルの設定が保存されます。

メールの脅威に対する保護の設定

メールの脅威に対する保護を使用するには、Kaspersky Security 10.1 Microsoft Outlook アドイン がインストールされ、保護対象サーバーが正しく設定されている必要があります(315 ページのセクション「脅威からのメールの保護」を参照)。

► **メールの脅威に対する保護を有効にするには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます(170 ページのセクション「ポリシーの設定」を参照)**。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**メール脅威対策**]タブで、[**メール脅威対策を有効にする**]をオンにします。

   このチェックボックスをオンにすると、Kaspersky Security 10.1 Microsoft Outlook アドインを使用するすべての受信メールでウイルス対策スキャンとフィッシング対策スキャ

ンが実行されます。

このチェックボックスをオフにすると、メールはスキャンされません。

既定では、このチェックボックスはオンです。

5. [**OK**]をクリックします。

変更内容が保存されます。

URL と Web アドレスの処理の設定

► **定義データベースと KSN からの URL 評価に従って、Web リソースにフィッシング脅威があるかどうかのチェックおよび悪意があると判定された Web サイトのアドレスの特定を行うためには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**タスクモード**]タブでタスクの処理モードを選択および設定します(319 ページのセクション「タスクの処理モードの選択」を参照)。

5. [**URL と Web アドレスの処理**]タブで:

   - [**悪意のある URL データベースを使用して Web リンクをスキャンする**]をオンまたはオフにします。

     チェックボックスをオンにすると、各 URL にシグネチャ解析が実行されます。

     チェックボックスをオフにすると、URL スキャンに定義データベースが使用されません。

     既定では、このチェックボックスはオンです。

   - [**アンチフィッシングデータベースを使用して Web ページをスキャンする**]をオフまたはオンにします。

     チェックボックスをオンにすると、フィッシング対策データベースを使用して各 URL がチェックされます。 フィッシング対策スキャンはヒューリスティック分析に基づいて行われます。

     チェックボックスをオフにすると、フィッシング攻撃の検知は行われません。

     既定では、このチェックボックスはオンです。

     URL のフィッシング対策スキャンを設定するときは、フィッシング対策がメールに自動適用されますのでご注意ください。

   - [**信頼ゾーンを使用する**]をオフまたはオンにします。

     このチェックボックスにより、タスクに対する信頼ゾーンの使用を有効または無効にします。

     このチェックボックスをオンにすると、Kaspersky Security 10.1 for Windows Server により、信頼されたプロセスのファイル操作が、タスクの設定で指定されたスキャンの除外対象に追加されます。

チェックボックスをオフにすると、Kaspersky Security 10.1 for Windows Server により、ファイルのリアルタイム保護タスクの保護範囲を作成するときに信頼されたプロセスのファイル操作を無視します。

既定では、このチェックボックスはオンです。

- [**保護に KSN を使用する**]をオンまたはオフにします。

  このチェックボックスで KSN サービスの使用を有効または無効にします。

  このチェックボックスをオンにすると、Kaspersky Security Network データを使用して、新しい脅威に対する応答時間を迅速化し、誤検知の可能性を減少させます。

  このチェックボックスをオフにすると、タスクは KSN サービスを使用しません。

  既定では、このチェックボックスはオンです。

  URL の KSN 評価は次の条件が満たされた場合のみ使用可能です:

  a. トラフィックセキュリティ設定で[**保護に KSN を使用する**]がオンになっている。

  b. KSN 声明に同意している。

  c. [**要求した URL に関するデータを送信**](291 ページのセクション「**KSN の使用タスクの設定**」を参照)がオンになっている。

  d. KSN の使用タスクが開始されている。

6. [**OK**]をクリックします。

URL と Web アドレスの処理の設定が保存されている。

URL ベースのルールの追加

特定の URL を拒否または許可するため、URL ベースのルールを追加できます。これらのルールは他のすべての判定よりも優先順位が高くなります。

► **新しい URL ベースのルールを作成するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**トラフィックセキュリティ**]ブロックで、[**ルール**]をクリックします。

   [**Web コントロールルール**]ウィンドウが開きます。

4. [**ウェブコントロール**]タブで[**URL ベースのルールを適用する**]をオンにしてルールを適用します。

   チェックボックスをオンにすると、カスタムの証明書拒否ルールの適用により HTTPS 証明書がブロックされます。

   チェックボックスをオフにすると、ルールは適用されません。

   既定では、このチェックボックスはオフです。

   このチェックボックスは、[**HTTPS トラフィックをスキャンする**]をオンにした場合にのみ使用可能になります。

5. [**追加**]をクリックして新しいルールを追加します。

6. コンテキストメニューの［**追加**］で、［**URL ベースのルール**］を選択します。

7. ［**URL ベースのルール**］ウィンドウが開いたら：

    a. ルール名を入力します。

    b. ［**ルール種別：**］で、［**拒否**］または［**許可**］を選択します。

    c. ［**ルールを適用する**］をオンにします。

    d. 下のフィールドで［**URL**］を指定します。

    e. ［**OK**］をクリックします。

8. ルールを編集するには、リスト内のルールのいずれかを選択して、［**変更**］をクリックします。

9. ［**ウェブコントロールルール**］ウィンドウで［**OK**］をクリックします。

新しいルールが適用されます。

ウェブコントロールの設定

ルールの適用を設定して、証明書スキャンとカテゴリベースのウェブコントロールの設定を管理します。

このセクションの内容

証明書スキャンの設定

Kaspersky Security 10.1 for Windows Server では、無効および期限切れの証明書を使用している Web リソースをスキャンしたり、ブロックできます。証明書のスキャンを設定するには、次の手順を実行する必要があります:

a. [**ドライバーインターセプター**]または[**リダイレクター**]モードを選択します。

b. トラフィックセキュリティタスクを設定します(339 ページのセクション「タスクモードの選択と設定」を参照)。

c. ウェブコントロールルールを適用します。

d. 証明書のルールを追加および適用します(341 ページのセクション「証明書ルールの追加」を参照)。

証明書のルールは[**ドライバーインターセプター**]または[**リダイレクター**]モードのみで使用できます。Kaspersky Security 10.1 for Windows Server は証明書の拒否ルールのみを既定で作成します。

タスクモードの選択と設定

► **証明書で実行するモードを選択および設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます(170 ページのセクション「ポリシーの設定」を参照)**。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**サーバーのリアルタイム保護**]セクションの[**トラフィックのセキュリティ**]ブロックで、[**設定**]をクリックします。

   [**トラフィックのセキュリティ**]ウィンドウが開きます。

4. [**全般**]タブの[**タスクモード**]ドロップダウンリストから、証明書スキャンをサポートするモードを選択します:

   - [**ドライバーインターセプター**](320 ページのセクション「**ドライバーインターセプターモードの設定**」を参照)
   - [**リダイレクター**](323 ページのセクション「リダイレクターモードの設定」を参照)

5. [**タスクモード設定**]ブロックで次の設定を行います:

   - **HTTPS トラフィックをスキャンする**

     チェックボックスをオンにすると、インターセプトされた暗号化 HTTPS トラフィックが解凍され、脅威の有無がスキャンされます。

     チェックボックスをオフにすると、暗号化 HTTPS トラフィックは解凍されません。

     既定では、このチェックボックスはオンです。

     スキャンは HTTPS ポートが開いているときのみ使用できます。

   - 使用する暗号化プロトコルのバージョンを選択します:
     - **TLS 1.0**
     - **TLS 1.1**
     - **TLS 1.2**

［**TLS 1.0**］は既定でオンにされており、変更はできません。

6. ［**OK**］をクリックします。

タスクの設定が保存されます。

証明書ルールの追加

証明書のルールは［**ドライバーインターセプター**］または［**リダイレクター**］モードのみで使用できます。Kaspersky Security 10.1 for Windows Server は証明書の拒否ルールのみを既定で作成します。

► **証明書ルールを追加または設定するには：**

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します：

   - サーバーグループに対してアプリケーションを設定するには、［**ポリシー**］タブを選択して、**ポリシーのプロパティウィンドウを開きます**（170 **ページのセクション「ポリシーの設定」を参照**）。

   - 単一のサーバーに対してアプリケーションを設定する場合、［**デバイス**］タブを選択して、［**アプリケーションのプロパティ**］ウィンドウを開いてください（190 ページのセクション「**Kaspersky Security Center の［アプリケーションのプロパティ］ウィンドウでのローカルタスクの設定**」を参照）。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、［**アプリケーションのプロパティ**］ウィンドウでこれらの設定を編集することはできません。

3. ［**トラフィックセキュリティ**］ブロックで、［**ルール**］をクリックします。

   ［**Web コントロールルール**］ウィンドウが開きます。

4. [**ウェブコントロールルール**]タブで、[**証明書ベースのルールを適用する**]をオンにしてルールを適用します。

   チェックボックスをオンにすると、カスタムの証明書拒否ルールの適用により HTTPS 証明書がブロックされます。

   チェックボックスをオフにすると、証明書のスキャンは行われません。

   既定では、このチェックボックスはオフです。

   このチェックボックスは、[**HTTPS トラフィックをスキャンする**]をオンにした場合にのみ使用可能になります。

5. [**追加**]をクリックして新しいルールを追加します。

6. コンテキストメニューの[**追加**]で、[**証明書ベースのルール**]を選択します。

7. [**証明書ベースのルール**]ウィンドウが開いたら:

   a. ルール名を入力します。

   b. [**ルールを適用する**]をオンにします。

   c. [**演算子の種別**]:[**マスク**]または[**正規表現**]を選択します。

   d. マスクまたは表現を[**演算子**]で指定します。

   e. [**OK**]をクリックします。

8. ルールを編集するには、リスト内のルールのいずれかを選択して、[**変更**]をクリックします。

9. [**ウェブコントロールルール**]ウィンドウで[**OK**]をクリックします。

新しいルールが適用されます。

カテゴリベースのウェブコントロールの設定

► **トラフィックセキュリティのカテゴリベースのルールを追加または変更するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**トラフィックセキュリティ**]ブロックで、[**ルール**]をクリックします。

   [**Web コントロールルール**]ウィンドウが開きます。

4. [**カテゴリ**]タブを開きます。

5. [**Web トラフィックカテゴリコントロールにルールを適用する**]をオンにします。

   チェックボックスをオンにすると、選択したカテゴリに該当する Web リソースのカテゴリ分類とブロックが行われます。

   チェックボックスをオフにすると、カテゴリ分類は行われません。

   既定では、このチェックボックスはオフです。

カテゴリコントロール設定が使用可能になります。

6. 以下のチェックボックスをオンまたはオフにします。

   - **Web ページをカテゴリに分類できない場合はアクセスを許可する**
   - **サーバーに損害を与えるために使用される可能性がある、正当な Web リソースへのアクセスを許可する**
   - **正当な広告へのアクセスを許可する**

7. 使用可能なカテゴリ分類リスト内(345 ページのセクション「カテゴリのリスト」を参照):

   - カテゴリを許可するため、該当するチェックボックスをオンにします。

     [**種別**]列が[**許可**]に変わります。

   - 該当するチェックボックスをオフにして、カテゴリをブロックします。

     [**種別**]列が[**拒否**]に変わります。

   > カテゴリリストは定義済みのため変更できません(カテゴリの追加または削除ができません)。

8. [**OK**]をクリックします。

ルールの設定が保存されます。

not-a-virus(非ウイルス)マスクの使用

► カテゴリ分析に `not-a-virus`(非ウイルス)マスクを使用するには:

1. Kaspersky Security Center 管理コンソールで、[KSN の使用タスクの設定]を開きます(291 ページのセクション「KSN の使用タスクの設定」を参照)。
2. [**要求した URL に関するデータを送信**]をオンにします。
3. KSN の使用タスクを開始します。

4. トラフィックセキュリティの設定ウィンドウ（316 ページのセクション「トラフィックセキュリティタスクの設定」を参照）で、[**保護に KSN を使用する**]をオンにします。

5. [**ウェブコントロールルール**]ウィンドウの[**カテゴリ**]タブで、[**Web トラフィックカテゴリコントロールにルールを適用する**]をオンにします。

6. カテゴリリスト内で、not-a-virus（非ウイルス）マスクを適用するカテゴリを選択します。

   マスクに対応する、選択したカテゴリのオブジェクトは、トラフィックセキュリティタスクによって検知されません。

not-a-virus（非ウイルス）マスクの使用は、**信頼ゾーン** 設定で定義されます（242 ページのセクション「非ウイルスマスクの適用」を参照）。

カテゴリのリスト

Web リソースがタグに応じて分析およびカテゴリ分類されます。タグは、複数のカテゴリに適用できます（以下の表を参照）。

表 39. Web リソースカテゴリのタグ

タグ	説明	カテゴリのリスト
18+ (adult)	成人（18 歳以上）向けコンテンツ（例：暴力描写やポルノ、卑語など）を含む可能性のある Web リソースを含む可能性があります。	堕胎、成人向けデート、拒食、憎悪、差別、猥褻、違法薬物、違法ソフトウェア、LGBT、ランジェリー、非成人向けデート、ヌード、政策決定、ポルノ、世界的な法規制による制限、RF 法による制限、ロシア連邦通信局による制限（RF）、性教育、ポルノショップ、ソーシャルネットワーク、自殺、卑語、暴力、武器。

タグ	説明	カテゴリのリスト
children	子供向けのコンテンツを含む可能性のある Web リソースを含む可能性があります。例：教育 Web サイト、子供向けエンターテインメント Web サイト、育児フォーラムおよびブログ。	子供向け、連邦法 436（RF）による制限、学校および大学のページ。
drug	麻薬およびその他の合法 / 非合法物質に関する情報を含む可能性のある Web リソースを含む可能性があります。例：禁止薬物またはアルコールの流通に関する情報、または登録された医薬品企業の Web サイト。	堕胎、アルコール、拒食、薬物、健康と美容、違法薬物、医薬品、調剤薬、煙草。
education	教育素材または指導に関わる素材を含む可能性のある Web リソースを含む可能性があります。 例：オンライン百科事典、ナレッジベース、ウィキ、教育機関の Web ページまたは性教育に関する Web ページ。	書籍および著作物、教育、子供向け、情報技術、オンライン百科事典、学校および大学のページ、検索エンジン、性教育。

タグ	説明	カテゴリのリスト
hobby&entertainment	エンターテインメント、趣味、リエクレーション活動に関わる可能性のある Web リソースを含む可能性があります。 例：ギャンブルやソーシャルネットワークを含む各種オンラインゲーム、書籍またはハンティングに関する Web ページ、健康や美容、ニュースフィードに関わるページ。	成人向けデート、趣味とエンターテインメント、すべての通信メディア、占星術と秘教、音楽、映像とソフトウェア、賭博、ブログ、カジノ、カードゲーム、カジュアルゲーム、チャットとフォーラム、コンピューターゲーム、文化と社会、猥褻、ファッション、ファイル共有、釣りとハンティング、子供向け、ギャンブル、健康と美容、趣味とエンターテインメント、ホーム＆ファミリー、ユーモア、LGBT、ランジェリー、富くじ、メディアホスティングとストリーミング、医薬、音楽、ニュース、非成人向けデート、ヌード、オンラインショッピング、オンラインショッピング（自己負担）、ペットと動物、ポルノ、レストラン、カフェと食品、ポルノショップ、ソーシャルネットワーク、スポーツ、急流くだり、旅行、テレビとラジオ、戦争ゲーム。
gaming	各種ゲームに関わる可能性のある Web リソースを含む可能性があります。例：賭博ゲーム、富くじ、オンラインまたはカジュアルゲーム、ゲームに関する Web サイトとフォーラム。	カジュアルゲーム、コンピューターゲーム、スポーツ、戦争ゲーム。

タグ	説明	カテゴリのリスト
hazard	このカテゴリは、以下を含む Web ページを参照します: • 「プレイのための支払い」がある賭博ゲーム • プール賭博 • 券や番号の購入を伴う宝くじ	賭博、カジノ、カードゲーム、ギャンブル、ギャンブル（広義の意）、宝くじ。
health&medicine	健康的なライフスタイルに関する Web ページ。フィットネス、健康的な食事、代替療法、治療方法を専門に扱うサイトや、医薬品、薬局、製薬会社、薬物療法、サプリメントに関する Web ページが含まれます。	中絶、拒食症、ドラッグ（合法および違法）、健康と美容、薬剤、薬局、スポーツ。
illegal	違法である可能性のある Web リソースを含む可能性があります。例: 違法なメディアファイルまたはインストールパッケージの共有、または各国の法律で禁止された Web サイト。	アルコール、音楽、映像およびソフトウェア、薬物、ファイル共有、違法薬物、違法ソフトウェア、富くじ、世界的な法規制による制限、RF 法による制限、ロシア連邦通信局による制限（RF）、煙草。
IT	大まかに言えば、ユーザーがアカウントを持っていてもいなくても、他のユーザーに個人的なメッセージを送信できる Web ページです（メールサービス、ソーシャルネットワーク、ブログなどを含む）。	匿名プロキシサーバー、ホスティングとドメインサービス、違法ソフトウェア、情報技術、検索エンジン、Web メール。

タグ	説明	カテゴリのリスト
forbidden by law	連邦法によって統制されている可能性、または政府や政策に関わる可能性のある Web リソースを含む可能性があります。	法律および政策、連邦過激主義者リスト(RF)における言及、連邦法 436(RF)による制限、世界的な法規制による制限、RF 法による制限、ロシア連邦通信局による制限(RF)。
legal	合法である可能性の Web リソースを含む可能性があります。	アルコール、音楽、映像およびソフトウェア、薬物、ファイル共有、合法広告、富くじ、軍事、調剤薬、宗教、性教育、ティーザー広告サービス、煙草、戦争ゲーム。
media sharing	ファイル共有を可能にする可能性のある Web リソースを含む可能性があります。 例:トレント、ファイル共有 Web サイト、音楽と映像ホスティング、合法および非合法。	音楽、映像およびソフトウェア、書籍と著作物、ファイル共有、子供向け、インターネットワービス、メディアホスティングおよびストリーミング、音楽、検索エンジン、トレント、テレビとラジオ。
money&paying	ファイナンスおよび金融取引に関わる可能性のある Web リソースを含む可能性があります。 例:銀行の公式 Web サイト、オンライン銀行、オンラインストア、および送金を実行する Web ページ。	銀行、書籍および著作物、カジュアルゲーム、電子商取引、オンラインショッピング(自己負担)、クレジットカードによる支払い、支払いシステム、レストラン、カフェおよび食品、旅行。

タグ	説明	カテゴリのリスト
online collaboration	オンライン通信に関わる可能性のある Web リソースを含む可能性があります。 例：専門分野のブログおよびフォーラム、プライベートなチャットルーム、ソーシャルネットワークおよびデートサイト。	成人向け出会い系、ブログ、チャットとフォーラム、子供向け、健康と美容、求職サイト、薬剤、未成年向け出会い系、ソーシャルネットワーク、旅行。
psychotropic&drug	これらのカテゴリには、あらゆる種類の薬物、向精神薬、タバコに関連する Web リソースが含まれます。	ドラッグ（合法および違法）、健康と美容、違法薬物、薬剤、薬局、タバコ。
sex&adult	性的または猥褻な素材を含む可能性のある Web リソースを含む可能性があります。 例：ポルノのホスティング、性教育に関わる Web ページ、性的少数者に関する Web サイト。	成人向けデート、猥褻、LGBT、ランジェリー、ヌード、ポルノ、性教育、ポルノショップ。
society&law	このカテゴリには、社会および人生の多くの側面が含まれます。宗教と宗教団体、政府と政治と法律、家庭と家族、マスコミ、軍隊と武器を含みます。	文化と社会、法律と政治、軍隊、宗教、武器。

タグ	説明	カテゴリのリスト
shopping	オンラインショッピングに関わる可能性のある Web リソースを含む可能性があります。	書籍と著作物、ランジェリー、オンラインショッピング、オンラインショッピング（自己負担）、クレジットカードによる支払い、レストラン、カフェと食品、ポルノショップ、旅行。
violence	明示的な攻撃的表現、残酷な描写、過激主義者のプロパガンダ、自殺に関する描写を含む可能性のある Web リソースを含む可能性があります。	憎悪、差別、過激思想と人種主義、釣りとハンティング、ヘイトおよび差別、連邦過激主義者リスト（RF）における言及、軍事、政策決定（JP）、世界的な法規制による制限、RF 法による制限、ロシア連邦通信局による制限（RF）、自殺、暴力、戦争ゲーム、武器。
web services	各種 Web サービスを提供する可能性のある Web リソースを含む可能性があります。例：匿名化、Web ホスティング、またはメールサービス。	匿名のプロキシサーバー、ホスティングおよびドメインサービス、インターネットサービス、検索エンジン、ティーザー広告サービス、Web メール。

ローカルアクティビティの管理

このセクションでは、USB 経由で外部デバイスによってアプリケーションの開始と接続をコントロールする Kaspersky Security 10.1 for Windows Server 機能に関する情報について説明します。

この章の内容

Kaspersky Security Center を使用したアプリケーションの起動管理

サーバーのグループに対して Kaspersky Security Center 側でアプリケーション起動コントロールルールの共通リストを作成して、企業ネットワーク内にあるすべてのサーバーでのアプリケーションの起動を許可または拒否できます。

このセクションの内容

アプリケーション起動コントロールタスクの設定

既定のアプリケーション起動コントロールタスク設定を変更できます（次の表を参照）。

表 40. アプリケーション起動コントロールタスクの既定の設定

設定	既定値	説明
タスクモード	**統計のみ**：設定されたルールに基づき、アプリケーションのブロックイベントおよび起動イベントを記録します。アプリケーション起動は実際には拒否されません。	最終的なルールのリストが生成された後で、サーバーの保護に対して[**使用中**]モードを選択できます。

実行するコマンドのないコマンドインタープリターの起動を拒否する	適用されません。	実行するコマンドのないコマンドインタープリターの起動を拒否できます。
ルールの管理	**ポリシールールでローカルルールを上書きする**	ポリシーで指定したルールがローカルコンピューター上のルールと組み合わせて適用されるモードを選択できます。
ルールの適用範囲	タスクでは、実行ファイル、スクリプト、および MSI パッケージの起動を制御します。	ルールによって起動が制御されるファイルの種別を指定できます。
KSN の使用	KSN でのアプリケーション評価データは使用されません。	アプリケーション起動コントロールタスクの実行時、KSN アプリケーション評価データを使用できます。
Windows インストーラーによるソフトウェア配布を常に許可する	適用されます。	Windows インストーラーによって実行されるすべてのソフトウェアインストールまたはアップデートを許可することができます。

タスク開始	最初の実行がスケジュール設定されていません。	アプリケーション起動コントロールタスクは、Kaspersky Security 10.1 for Windows Server の起動時に自動的に開始されません。タスクは手動で開始するか、開始スケジュールを設定することもできます。

► **アプリケーション起動コントロールタスクの全般的な設定を行うには、次の手順を実行します**:

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ローカルアクティビティの管理**]セクションで、[**アプリケーション起動コントロール**]セクションの[**設定**]をクリックします。

   [**アプリケーション起動コントロール**]ウィンドウが開きます。

4. [**全般**]タブの[**タスクモード**]セクションで、次の設定を選択します:

   - [**タスクモード**]ドロップダウンリストで、タスクの処理モードを指定します。

     このドロップダウンリストで、アプリケーション起動コントロールのタスクモードを選択で

きます:

- **使用中**:指定されたルールを使用して、実行中のアプリケーションを監視します。
- **統計のみ**:アプリケーションの起動に指定されたルールを使用せず、これらのアプリケーション起動に関する情報を実行ログへ記録することのみを行います。すべてのプログラムの起動が許可されます。このモードを使用して、タスク実行ログに記録される情報に基づき、アプリケーション起動コントロールルールのリストを生成できます。

既定では、アプリケーション起動コントロールタスクは**統計のみ**モードで動作します。

- [**最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す**]をオフまたはオンにします。

  このチェックボックスでは、2 回目以降のアプリケーションの起動試行に対して、キャッシュに保存されたインシデント情報による起動コントロールを有効または無効にします。

  このチェックボックスをオンにすると、アプリケーションの初回起動の際にタスクにより送信された判定を基にしたアプリケーションの再起動を許可または拒否します。たとえば、アプリケーションの初回起動がルールにより許可された場合、この処理に関する情報がキャッシュに保存され、2 回目以降の起動はすべて許可されて、追加の再チェックは行われません。

  このチェックボックスをオフにすると、アプリケーションの起動を試みると、Kaspersky Security 10.1 for Windows Server により毎回アプリケーションが分析されます。

  既定では、このチェックボックスはオンです。

- [**実行するコマンドのないコマンドインタープリターの起動を拒否する**]をオフまたはオンにします。

  チェックボックスをオンにすると、インターセプターの起動が許可された場合でもコマンドラインインターセプターの起動が拒否されます。コマンドのないコマンドラインは、以下の両方の条件が満たされた場合のみ起動されます:

  - コマンドラインインターセプターの起動が許可されている。
  - 実行されたコマンドが許可されている。

  チェックボックスをオフにすると、コマンドライン起動の許可ルールのみが考慮されます。

許可ルールが適用されていない、または実行プロセスに KSN 信頼ステータスがない場合、起動は拒否されます。許可ルールが適用されているか、プロセスに KSN 信頼ステータスがある場合、コマンドラインは実行コマンドがある場合でもない場合でも起動できます。

Kaspersky Security 10.1 for Windows Server は次のコマンドラインインターセプターを認識します:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

5. [**ルールの管理**]セクションで、ルールの適用を設定します:

   a. タスク起動管理の許可ルールを追加するには、[**ルールリスト**]をクリックします。

> Kaspersky Security 10.1 for Windows Server は、スラッシュ「/」を含むパスを認識しません。パスを正しく入力するには、円記号「¥」を使用してください。

   b. ルール適用のモードを選択します:

- **ローカルルールをポリシールールで上書きする**。

  コンピューターのグループに対して、集中アプリケーション起動コントロールのポリシーで指定したルールリストを適用します。ローカルルールリストは作成、編集、適用できません。

- **ローカルルールにポリシールールを追加する**。

  ポリシーで指定したルールリストをローカルルールリストとともに適用します。アプリケーション起動コントロールルールの自動作成タスクを使用してローカルルールリストを編集できます。

既定で、Kaspersky Security 10.1 for Windows Server は、証明書に基づいてスクリプトのリスト、MSI パッケージおよびスタートアップファイルを許可する 2 つのプリセットルールを適用します。

6. ［**ルールの適用範囲**］セクションで、次の設定を行います：

- **実行ファイルにルールを適用する**

  プログラムの実行ファイルの開始に対するコントロールを有効または無効にします。

  このチェックボックスをオンにすると、実行ファイルを範囲として設定する、指定されたルールを使用してプログラムの実行ファイルの開始を許可またはブロックします。

  このチェックボックスをオフにすると、指定されたルールによるプログラムの実行ファイルの開始は制御されません。プログラムの実行ファイルの開始が許可されます。

  既定では、このチェックボックスはオンです。

- **DLL モジュールの読み込みを監視する**

  このチェックボックスでは、DLL モジュールの読み込みの監視を有効または無効にします。

  このチェックボックスをオンにすると、実行ファイルを範囲として設定する、指定されたルールを使用して DLL モジュールのダウンロードを許可またはブロックします。

  このチェックボックスをオフにすると、指定されたルールを使用して DLL モジュールのダウンロードを監視しません。DLL モジュールのダウンロードが許可されます。

  このチェックボックスは、［実行ファイルにルールを適用する］をオンにすると使用可能になります。

  既定では、このチェックボックスはオフです。

DLL モジュールのダウンロードを監視すると、オペレーティングシステムのパフォーマンスに影響を与えることがあります。

-

- **スクリプトと MSI パッケージにルールを適用する**

  このチェックボックスでは、スクリプトと MSI パッケージの起動を有効または無効にします。

  このチェックボックスをオンにすると、スクリプトと MSI パッケージを範囲として設定する、指定されたルールを使用して、スクリプトおよび MSI パッケージの実行を許可またはブロックします。

  このチェックボックスをオフにすると、指定されたルールを使用したスクリプトおよび MSI パッケージの起動のコントロールは実行されません。スクリプトおよび MSI パッケージの起動は許可されます。

  既定では、このチェックボックスはオンです。

7. ［**KSN の使用**］セクションで、次のアプリケーション起動を設定します：

- **KSN で信頼されていないアプリケーションを拒否する**

  このチェックボックスでは、KSN でのアプリケーションの評価に基づくアプリケーション起動コントロールを有効または無効にします。

  このチェックボックスをオンにすると、アプリケーションが KSN で信頼しないステータスになっている場合に、そのアプリケーションの実行をブロックします。KSN で信頼しないアプリケーションに適用されるアプリケーション起動コントロールの許可ルールは適用されません。チェックボックスをオンにすると、マルウェアに対する保護も提供されます。

  このチェックボックスをオフにすると、KSN の信頼しないプログラムの評価は考慮されず、そのようなプログラムに適用するルールに従って起動を許可またはブロックします。

  既定では、このチェックボックスはオフです。

- **KSN で信頼されているアプリケーションを許可する**

  このチェックボックスでは、KSN でのアプリケーションの評価に基づくアプリケーション

起動コントロールを有効または無効にします。

チェックボックスをオンにすると、アプリケーションが KSN で信頼するステータスになっている場合に、そのアプリケーションの実行を許可します。KSN の信頼するアプリケーションに適用されるアプリケーション起動コントロールルールの拒否は、高い優先度を持っています:アプリケーションが KSN サービスによって信頼されているとみなされた場合、このアプリケーションの起動は拒否されます。

このチェックボックスをオフにすると、KSN の信頼するプログラムの評価は考慮されず、そのようなプログラムに適用するルールに従って起動を許可またはブロックします。

既定では、このチェックボックスはオフです。

- KSN で信頼されているアプリケーションの起動を許可するユーザーまたはユーザーグループ。

8. [**ソフトウェア配布コントロール**]タブでソフトウェア配信管理を設定します(360 ページのセクション「ソフトウェア配信管理の設定」を参照)。

9. [**タスク管理**]タブで、タスクの開始スケジュールを設定します(221 ページのセクション「タスク開始スケジュールの設定」を参照)。

10. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

新しい設定は実行中のタスクにただちに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、実行ログに保存されます。

ソフトウェア配信管理の設定

ソフトウェア配信管理を使用すると、ソフトウェアのインストールやアップデートが簡単になる場合があります。ソフトウェア配信管理を使用すると、信頼するアプリケーションまたは信頼する配布パッケージが起動する場合のアプリケーションの自動起動を許可できます。信頼する配布パッケージが開始されると、Kaspersky Security 10.1 for Windows Server は自動的にそれぞれの子ファイルのチェックサムを計算し、その後はそうしたファイルに既定の拒否ポリシーを適用しません。Kaspersky Security 10.1 for Windows Server を使用すると、信頼する配布パッケージがデバイスコントロールタスクルールによってブロックされているか、KSN で信頼しないようにリストされていない限り、それらのオブジェクトを解凍してすべての子ファイルを起動することができます。

子ファイルの編集または移動により、ファイルを開始できない場合があります。

► **信頼する配布パッケージを追加するには、次の操作を行います:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 ページのセクション「**ポリシーの設定**」を参照)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ローカルアクティビティの管理**]セクションで、[**アプリケーション起動コントロール**]セクションの[**設定**]をクリックします。

   [**アプリケーション起動コントロール**]ウィンドウが開きます。

4. [ソフトウェア配布コントロール]タブで、[**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**]をオンにします。

   このチェックボックスで、リストで指定した配布パッケージを使用して開始されたすべてのファイルに関する除外の自動作成を有効または無効にできます。

   チェックボックスがオンの場合、信頼する配布パッケージ内のファイルの開始が自動的に許可されます。開始を許可するアプリケーションおよび配布パッケージのリストは編

集できます。

チェックボックスがオフの場合、リストで指定された除外は適用されません。

既定では、このチェックボックスはオフです。

[**アプリケーション起動コントロール**]タスクの設定で[全般]タブの[**実行ファイルにルールを適用する**]がオンになっている場合、[**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**]をオンにできます。

5. 必要に応じて[**Windows インストーラーによるソフトウェア配布を常に許可する**]をオフにします。

   このチェックボックスで、Windows インストーラーによって実行されるすべてのファイルに関する除外の自動作成を有効または無効にできます。

   チェックボックスがオンの場合、Windows インストーラーによってインストールされたファイルの開始は常に許可されます。

   チェックボックスがオフの場合、Windows インストーラーによって開始されたアプリケーションでも、無条件では許可されません。

   既定では、このチェックボックスはオンです。

   [リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する]がオフの場合、このチェックボックスは編集できません。

[**Windows インストーラーによるソフトウェア配布を常に許可する**]をオフにすることは、どうしても必要な場合以外お勧めできません。この機能をオフにすると、オペレーティングシステムファイルのアップデートに問題が発生したり、配布パッケージ子ファイルを開始できなくなったりする場合があります。

6. 必要に応じて、[**バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する**]をオンにします。

   このチェックボックスで、システムセンター設定マネージャーを使用した自動ソフトウェア配信をオンまたはオフにできます。

   チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server はシス

テムセンター設定マネージャーを使用した Microsoft Windows 導入を自動的に許可します。ソフトウェア配信は、バックグラウンドインテリジェント転送サービスによる場合のみ許可されます。

次の拡張子を持つオブジェクトの起動が管理されます:

- exe
- msi

既定では、このチェックボックスはオフです。

パッケージ配信からインストールやアップデートまで、サーバー上のソフトウェア配信サイクルが管理されます。配信段階のいずれかがサーバーへのアプリケーションのインストールの前に実行された場合、プロセスは管理されません。

7. 信頼する配布パッケージのリストを編集するには、[**パッケージリストの変更**]をクリックし、表示されたウィンドウで次の方法のいずれかを選択します:

- **1 つの配布パッケージを追加**

a. [**参照**]をクリックして、アプリケーションスタートアップファイルまたは配布パッケージを選択します。

[**信頼の基準**]セクションには、選択したファイルに関するデータが自動的に読み込まれます。

b. ファイルまたは配布パッケージを信頼するかどうかを決定するのに使用する基準について、2 つのオプションのいずれかを選択します:

- **デジタル証明書を使用する**

このオプションをオンにすると、アプリケーション起動コントロールに対して新しく生成された許可ルールの設定で、デジタル証明書の存在がルールの適用基準として指定されます。デジタル証明書が指定されたファイルを使用して起動されるプログラムの開始が許可されます。オペレーティングシステムで信頼されているすべてのアプリケーションの起動を許可する場合は、このオプションをオンにしてください。

- **SHA256 ハッシュを使用する**

このオプションをオンにすると、ルールの作成に使用されるファイルのチェックサムの値が、アプリケーション起動コントロールに対して新しく作成された許可ルールの設定でルールの適用基準として指定されます。指定されたチェックサムの値を持つファイルを使用して起動されるプログラムの開始が許可されます。

このオプションは生成されたルールが最高のセキュリティレベルを満たすことを要求される場合：SHA256 チェックサムがユニークなファイル ID として適用される可能性がある場合に推奨されます。ルール有効化の条件として SHA256 チェックサムを使用すると、ルール使用範囲を 1 つのファイルに制限します。

既定では、このオプションはオンです。

- **ハッシュで複数のパッケージを追加**

  無制限の数のスタートアップファイルおよび配布パッケージを選択して、すべて同時にリストに追加できます。Kaspersky Security 10.1 for Windows Server はハッシュを検査し、オペレーティングシステムが指定ファイルを開始するのを可能にします。

- **選択したパッケージを変更**

  異なるスタートアップファイルまたは配布パッケージを選択するか、信頼の基準を変更するには、このオプションを使用します。

- **ファイルから配布パッケージリストをインポート**

  信頼する配布パッケージのリストを設定ファイルからインポートできます。Kaspersky Security 10.1 for Windows Server によって認識されるファイルは、次のパラメータを満たす必要があります：

  - ファイルがテキストの拡張子を持っている
  - ファイルに含まれる情報は行のリストとして構造化されており、各行には 1 つの信頼するファイルのデータが含まれる
  - ファイルに含まれるリストは、次の形式のいずれかである：
    - <ファイル名>:<ハッシュ SHA256>

- <ハッシュ SHA256>*<ファイル名>

[**開く**]ウィンドウで、信頼する配布パッケージのリストを含む設定ファイルを指定します。

8. 以前に追加されたアプリケーションまたは信頼するリストの配布パッケージを削除するには、[**配布パッケージの削除**]をクリックします。子ファイルの実行が許可されます。

> 子ファイルの開始を防止するには、保護対象サーバー上でアプリケーションをアンインストールするか、アプリケーション起動コントロールタスクの設定で拒否ルールを作成します。

9. [**OK**]をクリックします。

これで新しい設定が保存されました。

既定の許可モードを有効にする

アプリケーションがルールまたは KSN の信頼しない判定によってブロックされていない場合、既定の許可モードですべてのアプリケーションの起動が許可されます。既定の許可モードは、指定された許可ルールを追加することによって有効にできます。既定の許可は、スクリプトまたはすべての実行可能なファイルに対してのみ有効にできます。

► 既定の許可ルールを追加するには:

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security**

Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定」を参照)。

> デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ローカルアクティビティの管理**]セクションで、[**アプリケーション起動コントロール**]ブロックの[**設定**]をクリックします。
4. [**全般**]タブで、[ルールリスト]をクリックします。

   [**アプリケーション起動コントロールルール**]ウィンドウが開きます。
5. [**追加**]をクリックして、ボタンのコンテキストメニューで[**1 つのルールを追加**]を選択します。

   [**ルール設定**]ウィンドウが開きます。
6. [**名前**]で、ルールの名前を入力します。
7. [**種別**]ドロップダウンリストで、**許可**するルールの種別を選択します。
8. [**範囲**]ドロップダウンリストで、起動がルールによって制御されるファイルの種別を選択します:
   - **実行ファイル**:ルールによってアプリケーションの実行ファイルの起動が制御されます。
   - **スクリプトと MSI パッケージ**:ルールによってスクリプトと MSI パッケージの起動が制御されます。
9. [**ルール有効化の条件**]セクションで、[**ファイルのパス**]を選択します。
10. 次のマスクを入力します:**?:¥**
11. [**ルール設定**]ウィンドウで[**OK**]をクリックします。

既定で許可モードが適用されます。

全コンピューターに対する Kaspersky Security Center でのアプリケーション起動コントロールルールの作成について

Kaspersky Security Center のタスクとポリシーを使用して、アプリケーション起動コントロールルールのリストを企業ネットワーク上の全サーバーおよびサーバーグループに対して一度に作成できます。参照マシンが企業ネットワークになく、その参照マシンにインストールされているアプリケーションに基づいて許可ルールを作成するタスクを使用してルールの共通リストを作成できない場合、このシナリオを使用してください。

Kaspersky Security Center 側でアプリケーション起動コントロールのリストを作成する方法は 2 つあります:

- アプリケーション起動コントロール用のアプリケーション起動コントロールルールの自動作成グループタスクを使用する。

  このシナリオを使用する場合、ネットワーク上の各サーバーに対して、アプリケーション起動コントロールルールの独自のリストがグループタスクにより生成され、指定した共有ネットワークフォルダーの XML ファイルにそれらのリストが保存されます。その後、作成したルールのリストを Kaspersky Security Center のポリシーのアプリケーション起動コントロールタスクに手動でインポートできます。Kaspersky Security Center のポリシーを設定して、アプリケーション起動コントロールルールの自動作成グループタスク完了時に、作成したルールをアプリケーション起動コントロールルールのリストに自動で追加することができます。

  アプリケーション起動コントロールルールを急いで作成する必要がある場合にこのシナリオを使用してください。アプリケーション起動コントロールルールの自動作成タスクのスケジュールによる開始は、許可ルールのアプリケーションの範囲に、安全であることがわかっているファイルが入っているフォルダーが含まれる場合にのみ設定してください。

ネットワークでアプリケーション起動コントロールポリシーを使用する前に、すべての保護対象サーバーがネットワーク共有フォルダーにアクセスできることを確認します。組織のポリシーによりネットワークでネットワーク共有フォルダーを使用できない場合は、ルールの自動生成タスクを開始して、テストコンピューターグループ上、またはテンプレートマシン上にサーバー管理ルールを作成することをお勧めします。

- Kaspersky Security Center で生成される、**統計のみ**モードでのアプリケーション起動コントロールタスクの処理に対するタスクイベントに関するレポートをベースにする。

  このシナリオの使用時に Kaspersky Security 10.1 for Windows Server はアプリケーション起動を拒否しませんが、[**統計のみ**]モードでのアプリケーション起動コントロールの実行中、Kaspersky Security Center の[**イベント**]セクションで、ネットワークサーバー全体で許可および拒否されたすべてのアプリケーション起動が報告されます。Kaspersky Security Center は、実行ログに基づいて、拒否されたアプリケーション起動イベントの統一リストを作成します。

  タスクの実行期間を設定する必要があります。それにより、保護対象サーバーおよびサーバーグループの可能なすべての処理シナリオを実行し、指定された時間間隔のあいだに再起動が 1 回以上実施されます。その後、アプリケーション起動コントロールタスクにルールが追加されると、保存された Kaspersky Security Center のイベントレポートファイル(TXT 形式)からアプリケーション起動のデータをインポートし、このデータに基づいてアプリケーション起動コントロールの許可ルールをそれらのアプリケーションに対して作成できます。

  企業ネットワークに種別の異なるサーバー(異なるソフトウェアのセットがインストールされているサーバー)が多数存在する場合、このシナリオを使用してください(「Kaspersky Security Center のポリシーでアプリケーション起動コントロールタスクを設定するためのプロファイルの使用について」(353 ページ)を参照)。

- Kaspersky Security Center を介して受け取った、拒否されたアプリケーション起動イベントに基づけば、設定ファイルの作成やインポートは不要です。

  この機能を使用するには、ローカルコンピューター上のアプリケーション起動コントロールタスクが、アクティブな Kaspersky Security Center ポリシーの下で実行されている必要があります。この場合、ローカルコンピューター上のすべてのイベントが管理サーバーに送信されます。

ネットワークサーバーにインストールされているアプリケーションのセットが変更した場合、ルールのリストをアップデートしてください（アップデートがインストールされた場合、オペレーティングシステムが再インストールされた場合など）。アップデートされたルールのリストを生成するために、アプリケーション起動コントロールタスクの自動生成、または**統計のみ**モードでのアプリケーション起動コントロールポリシーを使用し、テスト管理グループのサーバー上で実行することをお勧めします。テストの管理グループには、新しいアプリケーションをネットワークサーバーにインストールする前にテスト起動するために必要なサーバーが含まれます。

許可ルールを追加する前に、利用できるルール適用モードのいずれかを選択します（353 ページのセクション「アプリケーション起動コントロールタスクの設定」を参照）。Kaspersky Security Center ポリシールールのリストには、ルール適用モードに関係なく、ポリシーによって指定されたルールのみが表示されます。ローカルルールのリストには、適用されたすべてのルール（ローカルルールと、ポリシーを介して追加されたルールの両方）が表示されます。

このセクションの内容

Kaspersky Security Center イベントからの許可ルールの作成

► **アプリケーション起動コントロールで[Kaspersky Security Center イベントからアプリケーションの許可ルールを作成]オプションを使用して許可ルールを作成するには、次の操作を行います:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。

2. ポリシーを設定する管理グループを展開し、詳細ペインの［**ポリシー**］タブを選択します。

3. 設定するポリシーのコンテキストメニューで、［**プロパティ**］を選択します。

   ポリシーのプロパティウィンドウが開きます。

4. ［**ローカルアクティビティの管理**］セクションで、［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。

5. ［**全般**］タブで、［ルールリスト］をクリックします。

   ［**アプリケーション起動コントロールルール**］ウィンドウが開きます。

6. ［**追加**］をクリックし、コンテキストメニューで［**Kaspersky Security Center イベントからアプリケーションの許可ルールを作成**］を選択します。

7. ルールを以前作成されたアプリケーション起動コントロールルールのリストに追加する方法を選択します。

   - **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
   - **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。
   - **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます。

   ［**アプリケーション起動コントロールルール作成**］ウィンドウが開きます。

8. 次の要求を設定します：

   - **管理サーバーのアドレス**
   - **ポート**
   - **ユーザー**
   - **パスワード**

9. 作成タスクのベースにするイベントの種別を選択します:

   - [**統計のみモード:アプリケーションの起動が拒否されました**]。
   - [**アプリケーションの起動が拒否されました**]。

10. [**期間内に生成された要求イベント**]ドロップダウンリストから、時間間隔を選択します。

11. [**ルールの生成**]をクリックします。

12. [**アプリケーション起動コントロールルール**]ウィンドウで[**保存**]をクリックします。

    アプリケーション起動コントロールポリシーのルールリストには、Kaspersky Security Center 管理コンソールがインストールされたサーバーのシステムデータに基づいて生成される新しいルールが入ります。

    > アプリケーション起動コントロールルールのリストがポリシーですでに指定されている場合、Kaspersky Security 10.1 for Windows Server は選択したルールをブロックイベントからすでに指定したルールに追加します。リスト内のすべてのルールは一意である必要があるため、同じハッシュを持つルールは追加されません。

XML ファイルからのアプリケーション起動コントロールルールのインポート

アプリケーション起動コントロールルールの自動作成グループタスクの終了に続いて生成されるレポートをインポートし、許可ルールのリストとして設定中のポリシーに適用することができます。

アプリケーション起動コントロールルールの自動作成グループタスクが終了すると、作成した許可ルールは、指定された共有のネットワークフォルダーに保存してある XML ファイルにエクスポートされます。ルールのリストの各ファイルは、企業ネットワーク上のそれぞれのサーバーで実行されたファイルと起動されたアプリケーションの分析に基づいて作成されます。リストには、アプリケーション起動コントロールルールの自動作成グループタスクで指定された種別と同じ種別のファイルとアプリケーションに対する許可ルールが含まれます。

Kaspersky Security Center で Kaspersky Security 10.1 for Windows Server の機能コンポーネントを設定するプロセスは、Kaspersky Security 10.1 コンソールを使用して機能コンポーネントをローカルで設定するプロセスと同様です。タスクの設定方法とアプリケーションの機能の設定方法の詳細については、『**Kaspersky Security 10.1 for Windows Server ユーザーガイド**』の関連するセクションに記載されています。

► **自動で生成された許可ルールのリストに従ってサーバーグループに対するアプリケーション起動の許可ルールを指定するには、次の手順を実行します:**

1. 設定中のサーバーグループのコントロール パネルの[**タスク**]タブで、アプリケーション起動コントロールルールの自動作成グループタスクを作成するか、既存のタスクを選択します。

2. 作成したアプリケーション起動コントロールルールの自動作成グループタスクのプロパティまたはタスクのウィザードで、次の設定を行います:

   - [**通知**]セクションで、タスクの実行レポートの保存設定を行います。

     このセクションでの設定方法の詳細については、『**Kaspersky Security Center ヘルプ**』を参照してください。

   - [**設定**]セクションで、作成したルールで起動が許可されるアプリケーションの種別を指定します。タスクの範囲からの既定のフォルダーを除外したり、新しいフォルダーを手動で追加して、許可されたアプリケーションがあるフォルダーの内容を編集できます。

   - [**オプション**]セクションで、タスクの実行中と完了後の処理を指定します。ルールが生成される基準と、それらのルールのエクスポート先のファイル名を指定します。

   - [**スケジュール**]セクションで、タスクの開始スケジュールを設定します。

   - [**アカウント**]セクションで、タスクが実行されるユーザーアカウントを指定します。

   - [**タスク範囲からの除外**]セクションで、タスク範囲から除外するサーバーのグループを指定します。

     除外対象のサーバーで起動されるアプリケーションに対して許可ルールは作成されません。

3. 設定中のサーバーグループのコントロール パネルにある、[**タスク**]タブのグループタスクのリストで、作成したアプリケーション起動コントロールルールの自動作成を選択し、[**開始**]をクリックしてタスクを開始します。

   タスクが完了すると、自動で生成された許可ルールのリストは XML ファイルとして共有のネットワークフォルダーに保存されます。

   > ネットワークでアプリケーション起動コントロールポリシーを使用する前に、すべての保護対象サーバーがネットワーク共有フォルダーにアクセスできることを確認します。組織のポリシーによりネットワークでネットワーク共有フォルダーを使用できない場合は、ルールの自動生成タスクを開始して、テストコンピューターグループ上、またはテンプレートマシン上にサーバー管理ルールを作成することをお勧めします。

4. 生成された許可ルールのリストをアプリケーション起動コントロールタスクに追加します。それには、設定中のポリシーのプロパティのアプリケーション起動コントロールタスクの設定で、次の手順を実行します:

   a. [**全般**]タブで、[ルールリスト]をクリックします。

   [**アプリケーション起動コントロールルール**]ウィンドウが開きます。

   b. [**追加**]をクリックして、表示されるリストで[**XML ファイルからルールをインポート**]を選択します。

   c. 自動で生成された許可ルールを以前作成されたアプリケーション起動コントロールルールのリストに追加する方法を選択します。

   - **既存のルールに追加する**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
   - **既存のルールを置き換える**:既存のルールをインポートされたルールで置き換えます。
   - **既存のルールとマージする**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます。

d. 表示される Microsoft Windows の標準のウィンドウで、アプリケーション起動コントロールルールの自動作成グループタスクの完了後に作成される XML ファイルを選択します。

e. [**アプリケーション起動コントロールルール**]および[**タスクの設定**]ウィンドウで[**OK**]を選択します。

5. 作成したルールを適用してアプリケーションの起動を管理する場合は、アプリケーション起動コントロールタスクのプロパティのポリシーで[**使用中**]タスク実行モードを選択します。

各サーバーで実行されるタスクに基づいて自動で生成される許可ルールは、設定中のポリシーの範囲となっているすべてのネットワークサーバーに適用されます。これらのサーバーでは、許可ルールが作成されたアプリケーションに対してのみ起動が許可されます。

ブロックされたアプリケーションに関する Kaspersky Security Center のファイルからのルールのインポート

[**統計のみ**]モードでアプリケーション起動コントロールタスクを実行後、Kaspersky Security Center で生成されるレポートからブロックされたアプリケーションの起動のデータをインポートできます。そのデータを使用して設定中のポリシーでアプリケーション起動コントロールの許可ルールのリストを生成できます。

アプリケーション起動コントロールタスクの実行中に発生したイベントのレポートの生成時に、起動がブロックされたアプリケーションの記録をつけることができます。

ブロックされたアプリケーションのレポートのデータをポリシー設定にインポートする場合は、使用するリストには起動を許可するアプリケーションのみが含まれていることを確認してください。

► **Kaspersky Security Center からのブロックされたアプリケーションのレポートに従い、サーバーのグループに対してアプリケーションの起動を許可するルールを指定するには、次の手順を実行します:**

1. アプリケーション起動コントロールタスクの設定のポリシーのプロパティで、[**統計のみ**]の処理モードを選択します。

2. ポリシーのプロパティの[**イベント通知**]セクションで、次の内容を確認します。

- [アプリケーションの起動が拒否されました]イベントの[**緊急イベント**]タブに、**統計のみ**モードで予定されたタスクの処理時間を超えるイベントの保管時間が表示されている(既定値は 30 日)。
- [**統計のみ:アプリケーションの起動が拒否されました**]イベントの[**警告**]タブに、**統計のみ**モードで予定されたタスクの処理時間を超えるイベントの保管時間が表示されている(既定値は 30 日)。

[**保管時間**]列で指定されている期間が経過すると、記録されたイベントに関する情報が削除され、レポートファイルに反映されません。**統計のみ**モードでアプリケーション起動コントロールタスクを実行する前に、タスクの実行時間が、指定のイベントに対して設定されている保管時間を超えていないことを確認してください。

3. タスクが完了すると、記録されたイベントを TXT ファイルにエクスポートします。
   a. それには、Kaspersky Security Center 管理コンソールの[**管理サーバー**]フォルダーの詳細ペインで[**イベント**]タブを選択します。
   b. [**抽出の選択**]をクリックし、[**イベント**]セクションで[**ブロック済み**]の基準に従ってイベントの抽出を作成し、アプリケーション起動コントロールタスクによって起動がブロックされるアプリケーションを表示します。
   c. 抽出の詳細ペインで、[**イベントをファイルにエクスポート**]リストをクリックして、ブロックされたアプリケーションの起動のレポートと TXT ファイルに保存します。

生成したレポートとポリシーにインポートして適用する前に、レポートには起動を許可するアプリケーションのデータしか含まれていないことを確認してください。

4. ブロックされたアプリケーション起動のデータをアプリケーション起動コントロールタスクにインポートします。それには、アプリケーション起動コントロールタスク設定のポリシーのプロパティで、次の手順を実行します:
   a. [**全般**]タブで、[**ルールリスト**]をクリックします。

[**アプリケーション起動コントロールルール**]ウィンドウが開きます。

b. [**追加**]をクリックし、コンテキストメニューで[**Kaspersky Security Center のレポートから、ブロックされたアプリケーションのデータをインポート**]を選択します。

c. Kaspersky Security Center のレポートを基に作成されたリストから以前設定されたアプリケーション起動コントロールルールのリストにルールを追加する方法を選択します。

- **既存のルールに追加する**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールを置き換える**:既存のルールをインポートされたルールで置き換えます。
- **既存のルールとマージする**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます。

d. 表示される Microsoft Windows の標準のウィンドウで、ブロックされたアプリケーション起動のレポートからイベントがエクスポートされた TXT ファイルを選択します。

e. [アプリケーション起動コントロールルール]および[**タスクの設定**]ウィンドウで[**OK**]を選択します。

ブロックされたアプリケーションに関する Kaspersky Security Center のレポートに従って作成されたルールが、アプリケーション起動コントロールルールのリストに追加されます。

Kaspersky Security Center 経由でのデバイス接続の管理

ネットワーク上のすべてのサーバーへのフラッシュドライブおよびその他の大容量保管領域の接続を許可または制限するには、サーバーのグループの Kaspersky Security Center を介して統一サーバーコントロールリストを作成します。

このセクションの内容

デバイスコントロールタスクについて

Kaspersky Security 10.1 for Windows Server では大容量記憶デバイスおよび CD / DVD ドライブの登録と使用を制御し、USB 接続フラッシュドライブやその他の種別の外部デバイスとファイルを交換している際に発生する可能性のあるセキュリティ脅威からコンピューターを保護します。大容量記憶デバイスは、サーバーに接続されてファイルのコピーや格納を行う外部デバイスです。

Kaspersky Security 10.1 for Windows Server は、次の USB 外部デバイス接続を制御します:

- USB 接続フラッシュドライブ
- CD ROM ドライブ
- USB 接続フロッピーディスクドライブ
- USB 接続 MTP モバイルデバイス

Kaspersky Security 10.1 for Windows Server は、USB で接続されたすべてのデバイスについて、実行ログおよびイベントログの対応するイベントとともに通知します。イベント詳細には、デバイスの種別と接続パスが含まれます。デバイスコントロールタスクが開始されると、Kaspersky Security 10.1 for Windows Server は USB で接続されたすべてのデバイスをチェックしてリストします。通知は、Kaspersky Security Center の[通知設定]セクションで設定できます。

デバイスコントロールタスクでは保護対象サーバーに USB で接続されている外部デバイスのすべての試行が監視されており、このデバイスの許可ルールが存在しない場合は接続がブロックされます。接続がブロックされると、そのデバイスは使用できなくなります。

アプリケーションでは、接続された大容量記憶デバイスごとに次のいずれかのステータスが規定されています:

- **信頼する**:ファイル交換を許可するデバイス。ルールリストが作成されると、最低 1 つのルールに対してデバイスインスタンスのパス値が適用範囲に含められます。
- **信頼しない**:ファイル交換を制限するデバイス。デバイスインスタンスパスは、許可ルールの適用範囲には含められません。

外部デバイスの許可ルールを作成し、デバイスコントロールルールの自動作成タスクを使用すると、データ交換を許可できます。また、すでに指定したルールの適用範囲を拡張することもできます。許可ルールは手動では作成できません。

Kaspersky Security 10.1 for Windows Server では**デバイスインスタンスパス**値を使用して、システムに登録されている大容量記憶デバイスが識別されます。デバイスインスタンスパスは、外部デバイスごとに一意に指定された既定の機能です。デバイスインスタンスパス値は外部デバイスごとに Windows プロパティで指定され、ルール作成時に Kaspersky Security 10.1 for Windows Server によって自動的に判別されます。

デバイスコントロールタスクは、2 つのモードで実行できます:

- **アクティブ** Kaspersky Security 10.1 for Windows Server ではフラッシュドライブやその他の外部デバイスの接続を制御するためにいくつかのルールが適用され、既定の拒否方法および指定した許可ルールに従って、すべてのデバイスの使用が許可またはブロックされます。信頼する外部デバイスの使用は許可されます。信頼しない外部デバイスの使用は既定でブロックされます。

デバイスコントロールタスクが**使用中**モードで実行されている際に、信頼しないとみなされる外部デバイスが保護対象サーバーに接続されている場合、そのデバイスは製品によってブロックされます。信頼しないデバイスを手動で切断するか、またはサーバーを再起動してください。そうしない場合、このデバイスに既定の拒否方法は適用されません。

- **統計のみ**：Kaspersky Security 10.1 for Windows Server ではフラッシュドライブやその他の外部デバイスの接続は制御されず、保護対象サーバー上での外部デバイスの接続と登録に関する情報、および接続されたデバイスによって適用されるデバイスコントロールの許可ルールに関する情報が記録されるのみです。すべての外部デバイスの使用が許可されます。既定ではこのモードが設定されています。

  このモードは、タスク実行時に記録された情報を基にしてルールを作成する際に適用できます。

全コンピューターに対する Kaspersky Security Center でのデバイスコントロールルールの作成について

Kaspersky Security Center のタスクを使用して、デバイスコントロールルールのリストを企業ネットワーク上の全サーバーおよびサーバーグループに対して一度に作成できます。

Kaspersky Security Center 側でデバイスコントロールのリストを作成する方法は 2 つあります：

- デバイスコントロールルールの自動作成グループタスクの使用

  このシナリオでは、グループタスクは、これまでに保護対象サーバーに接続されたすべての大容量保管領域に関する各コンピューターのシステムデータに基づいてルールリストを作成します。また、タスクでは、タスク実行時に接続されているすべての大容量保管領域デバイスが考慮されます。グループタスク完了時に、Kaspersky Security 10.1 for Windows Server は、ネットワーク内で登録されているすべて大容量記憶デバイスの許可ルールリストを作成し、そのリストを、指定したフォルダーに XML ファイルとして保存します。これで、作成されたルールをデバイスコントロールポリシー設定に手動でインポートできます。ローカルコンピューターのタスクと異なり、ポリシーでは、アプリケーション起動コントロールルールの

自動作成グループタスク完了時に、作成したルールをデバイスコントロールルールのリストに自動で追加する設定はできません。

このシナリオは、最初のデバイスコントロールポリシーをアクティブルールを適用するモードで開始する前に、許可ルールリストを作成する場合に使用してください。

> ネットワークでデバイスコントロールポリシーを使用する前に、すべての保護対象サーバーがネットワーク共有フォルダーにアクセスできることを確認します。組織のポリシーによりネットワークでネットワーク共有フォルダーを使用できない場合は、ルールの自動生成タスクを開始して、テストコンピューターグループ上、またはテンプレートマシン上にサーバー管理ルールを作成することをお勧めします。

- Kaspersky Security Center で生成される、**統計のみ**モードでのデバイスコントロールタスクに対するタスクイベントに関するレポートをベースにする。

  このシナリオでは、Kaspersky Security 10.1 for Windows Server は大容量記憶デバイスの接続を制限せず、**統計のみ**モードでのデバイスコントロールタスクの実行時に、すべてのネットワークコンピューター上のすべてのデバイス接続と大容量記憶デバイスの登録に関する情報を記録します。記録された情報は Kaspersky Security Center の詳細ペインの［**イベント**］タブにある場合があります。Kaspersky Security Center は、実行ログに基づいて、イベントを制限および許可する、大容量保管領域の統一リストを作成します。

  すべての大容量保管領域の接続が設定した期間中に実行されるように、タスク実行期間を設定してください。その後、デバイスコントロールタスクにルールが追加されると、保存された Kaspersky Security Center のイベントレポートファイル（TXT 形式）からデバイス接続のデータをインポートし、このデータに基づいてデバイスコントロールの許可ルールをそれらのデバイスに対して作成できます。インポートされたログが基づくイベントの種別は、作成されるルール種別には影響しません。許可ルールのみが作成されます。

  このシナリオは、多数の新しい大容量保管領域を対象とする許可ルールを追加し、MTP 接続された信頼するモバイルデバイス領域を対象とするルールを作成する場合に、使用してください。

- 接続された大容量保管領域に関するシステムデータに基づいて(デバイスコントロールポリシー設定内の[システムデータに基づいてルールを作成]オプションを使用)。

  このシナリオでは、Kaspersky Security 10.1 for Windows Server は、Kaspersky Security Center がインストールされているコンピューターにこれまでに接続されたか現在接続されている大容量保管領域のための許可ルールを作成します。

  このシナリオは、ネットワーク内のすべてのコンピューターにある、少数の信頼する新しい大容量保管領域を対象とするルールを作成する場合に、使用してください。

- 現在接続しているデバイスに関するデータに基づいて(**接続したデバイスに基づいてルールを作成**を使用)。

  このシナリオでは、Kaspersky Security 10.1 for Windows Server は現在接続しているデバイスのみのための許可ルールを作成します。許可ルールを作成する 1 つ以上のデバイスを選択できます。

  > Kaspersky Security 10.1 for Windows Server は、MTP を介して接続されたモバイルデバイスに関するシステムデータへのアクセス権を取得しません。接続したすべてのデバイスに関するシステムデータに基づいて記入されるルールリストのためのシナリオを使用して、信頼する MTP 接続したモバイルデバイスのための許可ルールを作成することはできません。

ネットワークコンピューターに接続された外部デバイスに関するシステムデータに基づくルール作成

これまでに接続されたか、現在接続されているすべての大容量保管領域に関する Windows データに基づいて、次の 3 つのシナリオでルールを作成できます(379 ページのセクション「全コンピューターに対する Kaspersky Security Center でのデバイスコントロールルールの作成について」を参照):

- デバイスコントロールルールの自動作成:グループタスクの使用すべてのネットワークコンピューター上のシステムによって登録されている、これまでに接続したすべての大容量保管領域を考慮に入れるには、ルール作成プロセス時にこのシナリオを使用します。

- デバイスコントロールポリシー設定で[**システムデータに基づいてルールを作成**]オプションを使用：これまでに接続したことがあり、Kaspersky Security Center 管理コンソールがインストールされたコンピューターのシステムによって登録されている、すべての大容量保管領域を考慮に入れるには、ルール作成プロセス時にこのシナリオを使用します。

- デバイスコントロールポリシー設定およびデバイスコントロールのルールジェネレータタスク設定で[**接続したデバイスに基づいてルールを作成**]を使用：許可ルールの作成時に保護対象サーバーに現在接続されているデバイスに関するデータのみを考慮する場合に、この方法を使用します。

Kaspersky Security 10.1 for Windows Server は、MTP を介して接続されたモバイルデバイスに関するシステムデータへのアクセス権を取得しません。接続したすべてのデバイスに関するシステムデータに基づいて記入されるルールリストのためのシナリオを使用して、信頼する MTP 接続したモバイルデバイスのための許可ルールを作成することはできません。

このセクションの内容

デバイスコントロールルールの自動作成タスクを使用したルールの作成

► **デバイスコントロールルールの自動作成タスクを使用してサーバーのグループのためのデバイスコントロールルールを指定するには、次の手順を実行します。**

1. 設定中のサーバーグループの詳細ペインの[**タスク**]タブで、デバイスコントロールルールの自動作成グループタスクを作成するか、既存のタスクを選択します。

2. 作成したアプリケーション起動コントロールルールの自動作成グループタスクのプロパティで、次の設定を行います:

   - [**通知**]セクションで、タスクの実行レポートの保存設定を行います。
   - [**設定**]セクションで、タスクの完了後の処理を指定します。作成したルールのエクスポート先ファイル名を指定します。
   - [**スケジュール**]セクションで、タスクの起動スケジュールを設定します。

3. 設定中のサーバーグループの詳細ペインにある、[**タスク**]タブのグループタスクのリストで、作成したデバイスコントロールルールの自動作成を選択し、[**開始**]をクリックしてタスクを開始します。

   タスクが完了すると、自動で生成された許可ルールのリストは XML ファイルとして共有のネットワークフォルダーに保存されます。

   > ネットワークでデバイスコントロールポリシーを使用する前に、すべての保護対象サーバーがネットワーク共有フォルダーにアクセスできることを確認します。組織のポリシーによりネットワークでネットワーク共有フォルダーを使用できない場合は、ルールの自動生成タスクを開始して、テストコンピューターグループ上、またはテンプレートマシン上にサーバー管理ルールを作成することをお勧めします。

4. 生成された許可ルールのリストをデバイスコントロールタスクに追加します。それには、設定中のポリシーのプロパティの[ローカルアクティビティの管理]セクションのデバイスコントロールタスクの設定で、次の手順を実行します:

   a. [**全般**]タブで、[**ルールリスト**]をクリックします。

   [**デバイスコントロールルール**]ウィンドウが開きます。

   b. [**追加**]をクリックして、表示されるリストで[**XML ファイルからルールをインポート**]を選択します。

   c. 自動で生成された許可ルールを以前作成されたデバイスコントロールルールのリストに追加す

る方法を選択します。

- **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。
- **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます。

d. 表示される Microsoft Windows の標準のウィンドウで、デバイスコントロールルールの自動作成グループタスクの完了後に作成される XML ファイルを選択します。

e. [デバイスコントロールルール]ウィンドウおよび[ローカルアクティビティの管理]セクションで[**OK**]を選択します。

5. 作成したデバイスコントロールルールを適用する場合[ローカルアクティビティの管理]セクションのデバイスコントロールタスクの設定の[**使用中**]タスクモードを選択します。

各サーバー上のシステムデータに基づいて自動で生成される許可ルールは、設定中のポリシーの範囲となっているすべてのネットワークサーバーに適用されます。これらのサーバーでは、許可ルールが作成されたデバイスに対してのみ接続が許可されます。

Kaspersky Security Center ポリシーでのシステムデータに基づく許可ルールの作成

► **デバイスコントロールポリシーの[システムデータに基づいてルールを作成]オプションを使用して許可ルールを作成するには、次の手順を実行します**：

1. 必要に応じて、信頼する新しい大容量保管領域を、Kaspersky Security Center コンソールがインストールされたコンピューターに接続します。

2. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。

3. ポリシーを設定する管理グループを展開し、詳細ペインの[**ポリシー**]タブを選択します。

4. 設定するポリシーのコンテキストメニューで、[**プロパティ**]を選択します。
5. ポリシーのプロパティウィンドウが開きます。
6. [**ローカルアクティビティの管理**]セクションのデバイスコントロールタスク設定を開き、次の手順を実行します:
    a. [**全般**]タブで、[**ルールリスト**]をクリックします。

    [**デバイスコントロールルール**]ウィンドウが開きます。

    b. 許可ルールを以前作成されたデバイスコントロールルールのリストに追加する方法を選択します。

    c. [**システム情報に基づいてルールを生成する**]ウィンドウのデバイスリストからデバイスを選択し[**選択したデバイスにルールを追加する**]をクリックします。
7. [デバイスコントロールルール]および[ローカルアクティビティの管理]セクションで[OK]を選択します。

デバイスコントロールポリシーのルールリストには、Kaspersky Security Center 管理コンソールがインストールされたコンピューターのシステムデータに基づいて生成される新しいルールが入ります。

接続しているデバイスのためのルール作成

► **デバイスコントロールポリシーの[接続したデバイスに基づいてルールを作成]オプションを使用して許可ルールを作成するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで、[**管理対象デバイス**]フォルダーを展開します。
2. ポリシーを設定する管理グループを展開し、詳細ペインの[**ポリシー**]タブを選択します。
3. 設定するポリシーのコンテキストメニューで、[**プロパティ**]を選択します。
4. ポリシーのプロパティウィンドウが開きます。

5. [**ローカルアクティビティの管理**]セクションで、[**デバイスコントロール**]セクションの[**設定**]をクリックします。
6. [**全般**]タブで、[**ルールリスト**]をクリックします。

   [**デバイスコントロールルール**]ウィンドウが開きます。
7. [**追加**]をクリックし、コンテキストメニューで[**接続したデバイスに基づいてルールを作成**]を選択します。

   [**システム情報に基づいてルールを生成する**]ウィンドウが開きます。
8. 保護対象サーバーに接続されている検知されたデバイスのリストで、許可ルールを作成するデバイスを選択します。
9. [**選択したデバイスにルールを追加する**]をクリックします。
10. [**デバイスコントロール**]ウィンドウの[**保存**]をクリックします。

デバイスコントロールポリシーのルールリストには、Kaspersky Security Center 管理コンソールがインストールされたコンピューターのシステムデータに基づいて生成される新しいルールが入ります。

制限されたデバイスに関する Kaspersky Security Center のレポートファイルからのルールのインポート

統計のみモードでデバイスコントロールタスクを実行後、Kaspersky Security Center で生成されるレポートから制限されたデバイスの接続のデータをインポートできます。そのデータを使用して設定中のポリシーでデバイスコントロールの許可ルールのリストを生成できます。

デバイスコントロールタスクの実行中に発生したイベントのレポートの生成時に、接続が制限されたデバイスの記録をつけることができます。

制限されたデバイスのレポートのデータをポリシー設定にインポートする場合は、使用するリストには接続を許可するデバイスのみが含まれていることを確認してください。

► 制限されたデバイスに関する Kaspersky Security Center レポートに基づいてサーバーのグループのデバイス接続のための許可ルールを指定するには、次の手順を実行します:

1. デバイスコントロールタスクの設定のポリシーのプロパティで、[**統計のみ**]モードを選択します。

2. ポリシーのプロパティの[**イベント通知**]セクションで、次の内容を確認します。

   - [**緊急イベント**]タブの[**信頼しない大容量保管領域が検出および制限されました**]イベントに、**統計のみ**モードで予定されたタスクの処理時間を超えるイベントの保管時間が表示されている(既定値は 30 日)。

   - [**警告**]タブの[**統計のみ:信頼しない大容量保管領域が検出されました**]イベントに、**統計のみ**モードで予定されたタスクの処理時間を超えるイベントの保管時間が表示されている(既定値は 30 日)。

   > [**保管時間**]列で指定されている期間が経過すると、記録されたイベントに関する情報が削除され、レポートファイルに反映されません。**統計のみ**モードでデバイスコントロールタスクを実行する前に、タスクの実行時間が、指定のイベントに対して設定されている保管時間を超えていないことを確認してください。

3. タスクが完了すると、記録されたイベントを TXT ファイルにエクスポートします。それには、Kaspersky Security Center 管理コンソールの[**管理サーバー**]フォルダーの詳細ペインで[**イベント**]タブを選択し、[**抽出の選択**]をクリックします。[**イベント**]セクションでデバイスが制限された基準に従ってイベントの抽出を作成し、デバイスコントロールタスクによって接続が制限されるデバイスを表示します。[**インポート・/エクスポート**]のペインで、[**イベントをファイルにエクスポート**]リストをクリックして、ブロックされたアプリケーションの起動のレポートと TXT ファイルに保存します。

   > 生成したレポートとポリシーにインポートして適用する前に、レポートには接続を許可するデバイスのデータしか含まれていないことを確認してください。

4. 制限されたデバイス接続に関するデータをデバイスコントロールポリシーにインポートします。それには、設定中のポリシーのプロパティの[ローカルアクティビティの管理]セクションの[デバイスコントロール]の

設定で、次の手順を実行します:

a. [**全般**]タブで、[**ルールリスト**]をクリックします。

[**デバイスコントロールルール**]ウィンドウが開きます。

b. [**追加**]をクリックし、コンテキストメニューで[**Kaspersky Security Center のレポートから、ブロック対象デバイスのデータをインポート**]を選択します。

c. Kaspersky Security Center のレポートを基に作成されたリストから以前設定されたデバイスコントロールルールのリストにルールを追加する方法を選択します。

- **既存のルールに追加する**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールを置き換える**:既存のルールをインポートされたルールで置き換えます。
- **既存のルールとマージする**:インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます。

d. 表示される Microsoft Windows の標準のウィンドウで、制限されたデバイスについてのレポートからイベントがエクスポートされた TXT ファイルを選択します。

e. [**デバイスコントロールルール**]および[**ローカルアクティビティの管理**]セクションで[**OK**]を選択します。

制限されたデバイスに関する Kaspersky Security Center のレポートに従って作成されたルールが、デバイスコントロールルールのリストに追加されます。

ネットワークアクティビティの管理

このセクションでは、ファイアウォール管理とアンチクリプタータスクに関する情報について説明します。

この章の内容

ファイアウォール管理

このセクションでは、ファイアウォール管理タスクとその設定方法について説明します。

このセクションの内容

ファイアウォール管理タスクについて

Kaspersky Security 10.1 for Windows Server は、ファイアウォール管理タスクを使用してネットワーク接続を保護するための信頼できるエルゴノミクスソリューションを提供します。

ファイアウォール管理タスクは独立したネットワークトラフィックフィルタリングを実行しませんが、Kaspersky Security 10.1 for Windows Server グラフィックインターフェイスを介して Windows Firewall を管理できます。ファイアウォール管理タスク時に Kaspersky Security 10.1 for Windows Server はオペレーティングシステムのファイアウォールの設定およびポリシーの管理を引き継ぎ、外部ファイアウォール設定のすべての可能性をブロックします。

アプリケーションのインストール時にファイアウォール管理は、Windows Firewall ステータスと指定されたすべてのルールを読み取ってコピーします。その後、Kaspersky Security 10.1 for Windows Server ではルールとルールパラメータのセットのみが変更可能で、ファイアウォールはオンまたはオフにできるだけです。

Windows Firewall が Kaspersky Security 10.1 for Windows Server のインストール時にオフにされた場合、インストールの完了後にファイアウォール管理タスクは実行されません。アプリケーションのインストール時に Windows Firewall をオンにした場合、インストールが完了すると、ファイアウォール管理タスクが実行され、指定したルールによって許可されないすべてのネットワーク接続をブロックします。

ファイアウォール管理は既定でインストールされません。推奨インストールのコンポーネントセットに含まれていないためです。

ファイアウォール管理タスクは、タスクの指定したルールによって許可されないすべての送受信接続を強制的にブロックします。

タスクは定期的に Windows Firewall をポーリングしてステータスを監視します。既定のポーリング間隔は 1 分に設定されており、変更できません。ポーリング時に Kaspersky Security 10.1 for Windows Server が Windows Firewall 設定と ファイアウォール管理タスク設定の不一致を検知すると、オペレーティングシステムファイアウォールにタスク設定が強制的に適用されます。

Windows Firewall を 1 分ごとにポーリングすることで、Kaspersky Security 10.1 for Windows Server は次を監視します:

- Windows Firewall の動作状況
- Kaspersky Security 10.1 for Windows Server のインストール後に他のアプリケーションまたはツールによって追加されたルールのステータス(たとえば、wf.msc を使用したポートやアプリケーションのための新しいアプリケーションルールの追加)。

Windows Firewall に新しいルールを適用すると、Kaspersky Security 10.1 for Windows Server は[**Windows Firewall**]スナップインに設定される Kaspersky Security グループルールを作成します。このルールセットは、ファイアウォール管理タスクを使用して Kaspersky Security 10.1 for Windows Server によって作成されるルールをすべて結合します。Kaspersky Security グループルールは、毎分のポーリング時にはアプリケーションにより監視されず、ファイアウォール管理タスク設定で指定されたルールのリストに自動的には同期しません。

► **手動で Kaspersky Security グループルールをアップデートするには:**

Kaspersky Security 10.1 for Windows Server ファイアウォール管理タスクを再起動します。

Windows Firewall スナップインを手動で使用して Kaspersky Security グループルールを編集することもできます。

> Windows Firewall が Kaspersky Security Center グループポリシーによって管理されている場合、ファイアウォール管理タスクは開始できません。

ファイアウォールのルールについて

ファイアウォール管理タスクは、タスク実行時に Windows Firewall に強制的に適用される許可ルールを使用して送受信ネットワークトラフィックのフィルタリングを管理します。

タスクが初めて開始されたときに、Kaspersky Security 10.1 for Windows Server は Windows Firewall 設定で指定されたすべての着信ネットワークトラフィックルールを読み取ってファイアウォール管理タスク設定にコ

ピーします。続いて、アプリケーションは次のルールに従って動作します:

- Windows Firewall 設定に新しいルールが作成された場合(手動で、または新しいアプリケーションのインストール時に自動的に)、Kaspersky Security 10.1 for Windows Server はそのルールを削除します。
- Windows Firewall 設定から既存のルールが削除された場合、Kaspersky Security 10.1 for Windows Server はそのルールを復元します。
- Windows Firewall 設定で既存のルールのパラメータが変更された場合、Kaspersky Security 10.1 for Windows Server はその変更をロールバックします。
- ファイアウォール管理設定に新しいルールが作成された場合、Kaspersky Security 10.1 for Windows Server は Windows Firewall にルールを強制的に適用します。
- ファイアウォール管理設定から既存のルールが削除された場合、Kaspersky Security 10.1 for Windows Server は Windows Firewall 設定からルールを強制的に削除します。
- ファイアウォール管理設定から既存のルールが削除された場合、Kaspersky Security 10.1 for Windows Server は Windows Firewall 設定からルールを強制的に削除します。

Kaspersky Security 10.1 for Windows Server は、送信ネットワークトラフィックを管理するブロックルールを使用しません。ファイアウォール管理タスクの開始時に、Kaspersky Security 10.1 for Windows Server は Windows Firewall 設定からそのようなルールをすべて削除します。

着信ネットワークトラフィックのフィルタリングルールを設定、削除、編集することはできます。

ファイアウォール管理タスク設定に新しいルールを指定して送信ネットワークトラフィックを管理することはできません。Kaspersky Security 10.1 for Windows Server で指定されているすべてのファイアウォールルールは、着信ネットワークトラフィックのみを管理します。

次の種類のファイアウォールルールを管理できます:

- アプリケーションルール

- ポートルール

アプリケーションルール

この種のルールは、指定したアプリケーションを標的とするネットワーク接続を許可します。これらのルールの有効化の条件は、実行可能ファイルへのパスに基づきます。

アプリケーションルールは管理できます:

- ルールの追加
- 既存のルールの削除
- 指定したルールの有効化と無効化
- 指定したルールのパラメータの編集:ルール名、実行可能ファイルへのパス、およびルール使用範囲の指定

ポートルール

この種のルールは、指定したポートおよびプロトコル(TCP/UDP)によるネットワーク接続を許可します。これらのルールの有効化の条件は、ポート番号およびプロトコルの種別に基づきます。

ポートルールは管理できます:

- ルールの追加
- 既存のルールの削除
- 指定したルールの有効化と無効化
- 指定したルールのパラメータの編集:ルール名、ポート番号、プロトコルの種別、およびルールの適用範囲の設定

ポートルールは、アプリケーションルールより範囲が広くなります。ポートルールに基づく接続を許可すると、保護対象サーバーのセキュリティレベルは低下します。

ファイアウォールのルールの有効化と無効化

► **着信ネットワークトラフィックをフィルタリングする既存のルールを有効または無効にするには、次の処理を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**ファイアウォール管理**]ブロックの[**設定**]をクリックします。

4. 表示されたウィンドウの[**ルールリスト**]をクリックします。

   [**ファイアウォールのルール**]ウィンドウが開きます。

5. ステータスを変更するルールの種別に応じて、[**アプリケーション**]または[**ポート**]を選択します。

6. ルールリストで、ステータスを変更するルールを選択し、次のいずれかの処理を実行します:

- 無効なルールを有効にする場合、ルール名の左側のチェックボックスをオンにします。

  選択したルールが有効になります。

- 有効なルールを無効にする場合、ルール名の左側のチェックボックスをオフにします。

  選択したルールが無効になります。

7. [ファイアウォールのルール]ウィンドウで[**保存**]をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows Firewall に送信されます。

ファイアウォールルールの手動での追加

アプリケーションおよびポートのルールは、追加と編集のみ可能です。新しいグループルールを追加したり既存のグループルールを編集したりすることはできません。

► **着信ネットワークトラフィックをフィルタリングする既存のルールを追加または編集するには、次を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**ファイアウォール管理**]ブロックの[**設定**]をクリックします。
4. 表示されたウィンドウの[**ルールリスト**]をクリックします。

   [**ファイアウォールのルール**]ウィンドウが開きます。
5. 追加するルールの種別に応じて[**アプリケーション**]または[**ポート**]タブを選択し、次の処理のいずれかを実行します:
   - 既存のルールを編集するには、ルールリストで編集するルールを選択し、[**編集**]をクリックします。
   - 新しいルールを追加するには[**追加**]をクリックします。

     設定するルールの種別に応じて、[**ポートルール**]ウィンドウまたは[**アプリケーションルール**]ウィンドウが開きます。
6. 表示されたウィンドウで、次の操作を行います:
   - アプリケーションルールを使用する場合、次を行います:
     a. 編集したルールに**ルール名**を入力します。
     b. このルールを変更して接続を許可するアプリケーションの実行可能ファイルへの**アプリケーションパス**を指定します。

     パスは、手動で、または[**参照**]を使用して設定できます。

     c. [**ルール適用範囲**]で、変更したルールを適用するネットワークアドレスを指定します。

     IPv4 IP アドレスのみ使用できます。
   - ポートルールを使用する場合、次を行います:

a. 編集したルールに**ルール名**を入力します。

b. 接続を許可する**ポート番号**を指定します。

c. 接続を許可する種類のプロトコル(TCP / UDP)を選択します。

d. [**ルール適用範囲**]で、変更したルールを適用するネットワークアドレスを指定します。

> IPv4 IP アドレスのみ使用できます。

7. [**アプリケーションルール**]または[**ポートルール**]ウィンドウで[**OK**]をクリックします。

8. [**ファイアウォールのルール**]ウィンドウで[**保存**]をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows Firewall に送信されます。

ファイアウォールのルールの削除

> 削除できるのはアプリケーションルールおよびポートルールのみです。既存のグループルールを削除することはできません。

► **着信ネットワークトラフィックをフィルタリングする既存のルールを削除するには、次の処理を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security**

Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定」を参照)。

> デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**ファイアウォール管理**]ブロックの[**設定**]をクリックします。
4. 表示されたウィンドウの[**ルールリスト**]をクリックします。

   [**ファイアウォールのルール**]ウィンドウが開きます。
5. ステータスを変更するルールの種別に応じて、[**アプリケーション**]または[**ポート**]タブを選択します。
6. ルールリストで、削除するルールを選択します。
7. [**削除**]をクリックします。

   選択したルールが削除されます。
8. [**ファイアウォールのルール**]ウィンドウで[**保存**]をクリックします。

指定したファイアウォール管理タスクの設定が保存されます。新しいルールパラメータが Windows Firewall に送信されます。

アンチクリプター

このセクションでは、アンチクリプタータスクとその設定方法について説明します。

このセクションの内容

アンチクリプタータスクについて

アンチクリプタータスクは、保護対象サーバーのネットワークファイルリソースの悪意ある暗号化を企業ネットワーク上のリモートコンピューターから検知することを可能にします。

アンチクリプタータスクの実行中、保護対象サーバーのネットワーク共有フォルダー内にあるファイルにアクセスする、リモートコンピューターの呼び出しをスキャンします。リモートコンピューターのネットワークファイルリソース上の処理が悪意ある暗号化と見なされた場合、コンピューターは信頼しないコンピューターのリストに追加され、ネットワーク共有フォルダーへのアクセスを失います。

検知された暗号化処理が、アンチクリプタータスクの範囲から除外されたディレクトリ内で行われる場合、この処理は悪意ある暗号化とは見なされません。

信頼しないコンピューターのネットワークファイルリソースへのアクセスは、既定で 30 分間ブロックされます。

アンチクリプタータスクは、コンピューターの動作を悪意があると認識するまで、ネットワークファイルリソースへのアクセスをブロックしません。暗号化プログラムが悪意のある動作を実行する間、ブロックするまでしばらく時間がかかることがあります。

アンチクリプタータスクが統計のみモードで実行されている場合、リモートコンピューターの悪意のある暗号化の試行のみがログに記録されます。

アンチクリプタータスクの設定

アンチクリプタータスクには、次の既定の設定が使用されます:

- **タスクモード**:アンチクリプタータスクは、[**使用中**]モードまたは[**統計のみ**]モードで開始できます。既定では、[**使用中**]モードが設定されています。
- **保護範囲**:すべての保護対象サーバーのネットワーク共有フォルダーに、アンチクリプタータスクが既定で適用されます。タスクが適用する共有フォルダーを指定することで、保護範囲を変更できます。
- **ヒューリスティックアナライザー**:Kaspersky Security 10.1 for Windows Server は**中レベル**のスキャン詳細を適用します。ヒューリスティックアナライザーを有効または無効にして、スキャンの詳細レベルを調整できます。
- **スケジュール設定**:既定では、初回の開始はスケジュール設定されていません。アンチクリプタータスクは、Kaspersky Security 10.1 for Windows Server 起動時に自動的に起動しません。タスクは手動で開始するか、開始スケジュールを設定することもできます。

► **アンチクリプタータスクを設定するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**アンチクリプター**]ブロックの[**設定**]をクリックします。

   [**アンチクリプター**]ウィンドウが開きます。

4. 表示されたウィンドウで、次の設定を行います:

   - [**全般**]タブでタスクモードとヒューリスティックアナライザーの使用(402 ページのセクション「タスクの全般的な設定」を参照)
   - [**保護範囲**]タブで保護範囲(405 ページのセクション「保護範囲の作成」を参照)
   - [**除外**]タブで除外リスト(406 ページのセクション「除外の追加」を参照)
   - [**タスク管理**]タブでタスク開始スケジュール設定(220 ページのセクション「タスクスケジュールの管理」を参照)

5. [**OK**]をクリックします。

新しい設定は実行中のタスクにただちに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、タスク実行ログに保存されます。

タスクの全般的な設定

► **タスクの全般的な設定を行うには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**アンチクリプター**]ブロックの[**設定**]をクリックします。

   [**アンチクリプター**]ウィンドウが開きます。

4. [**全般**]セクションで、次のいずれかのモードを選択します:

   - **統計のみ**

     このモードを選択すると、悪意のある暗号化のすべての試行が、アンチクリプタータスクのイベントログに記録され、処理は実行されません。既定では、このモードが選択されます。

   - **使用中**

     このモードを選択すると、悪意のある暗号化試行が検知されたとき、Kaspersky Security 10.1 for Windows Server は感染しているコンピューターによる共有フォル

ダーへのアクセスをブロックします。

5. [**ヒューリスティックアナライザーを使用する**]をオフまたはオンにします。

   このチェックボックスでは、オブジェクトのスキャン中のヒューリスティックアナライザーを有効または無効にできます。

   このチェックボックスをオンにすると、ヒューリスティックアナライザーが有効になります。

   このチェックボックスをオフにすると、ヒューリスティックアナライザーが無効になります。

   既定では、このチェックボックスはオンです。

6. 必要に応じて、スライダーを使用して分析のレベルを調整します。

   スライダーを使用すれば、ヒューリスティック分析のレベルを調整できます。このスキャンの強さのレベルによって、脅威の徹底的な検知、オペレーティングシステムのリソースにかかる負荷、スキャンの所要時間の間のバランスを調整します。

   次のレベルを設定できます:

- **低**：実行ファイル内部で見つかったスクリプトを少数しか実行しません。脅威が検知される可能性はやや低くなります。スキャンの速度は速く、システムリソースの消費は軽度です。
- **中**：Kaspersky Lab の推奨に基づき、実行ファイル内部で見つかったスクリプトを多数実行します。

  既定では、このレベルが選択されています。
- **高**：実行ファイル内部で見つかったスクリプトをさらに多数実行します。脅威が検知される可能性は非常に高くなります。スキャンには、より多くのシステムリソースを消費し、より多くの時間がかかります。また、非常に多くの誤検知を引き起こす可能性があります。

  スライダーは、[**ヒューリスティックアナライザーを使用する**]をオンにすると使用可能になります。

7. [**OK**]をクリックして、新しい設定を適用します。

保護範囲の作成

次の種別の保護範囲が、アンチクリプタータスクに適用されます:

- **定義済み**:既定でインストールされ、すべてのネットワーク共有フォルダーをスキャンに含める保護範囲を使用できます。[**サーバー上のすべてのネットワーク共有フォルダー**]がオンの場合に適用されます。
- **ユーザー**:暗号化の保護範囲に含まれる必要があるフォルダーを選択することで、保護範囲を手動で設定できます。[**指定した共有フォルダーのみ**]設定が選択される場合に適用されます。

アンチクリプタータスクの保護範囲の設定には、ローカルパスのみを使用できます。

► **アンチクリプタータスクの保護範囲を設定するには:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。
3. [**ネットワークアクティビティの管理**]セクションで、[**アンチクリプター**]ブロックの[**設定**]をクリックします。

   [**アンチクリプター**]ウィンドウが開きます。

4. [**保護領域**]タブで、アンチクリプタータスクの実行時にスキャンするフォルダーを選択します:

   - **サーバー上のすべてのネットワーク共有フォルダー**

     このオプションをオンにすると、アンチクリプタータスクの実行時に、すべてのサーバーのネットワーク共有フォルダーがスキャンされます。

     既定では、このオプションはオンです。

   - **指定した共有フォルダーのみ**

     このオプションをオンにすると、アンチクリプタータスクの実行中に、手動で指定したサーバーのネットワーク共有フォルダーのみがスキャンされます。

5. 暗号化の保護範囲に含めるサーバーの共有フォルダーを指定するには:

   a. [**指定した共有フォルダーのみ**]をオンにし、[**追加**]をクリックします。

   [**追加するフォルダーの選択**]ウィンドウが開きます。

   b. [**参照**]をクリックしてフォルダーを選択するか、または直接入力します。

   c. [**OK**]をクリックします。

6. [**アンチクリプター**]ウィンドウで[**OK**]をクリックします。

指定された設定が保存されます。

除外の追加

► **暗号化の保護範囲からの除外を追加するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください（190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照）。

  > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ネットワークアクティビティの管理**]セクションで、[**アンチクリプター**]ブロックの[**設定**]をクリックします。

   [**アンチクリプター**]ウィンドウが開きます。

4. [**除外**]タブで、[**除外リストの適用**]をオンにします。

   このチェックボックスをオンにすると、アンチクリプタータスクの実行時に、指定された領域で発生する悪意のある暗号化動作は検知されません。

   このチェックボックスをオフにすると、すべてのネットワーク共有フォルダーで暗号化動作が検知されます。

   既定では、チェックボックスはオフで、除外リストは空です。

5. [**追加**]をクリックします。

   [**追加するフォルダーの選択**]ウィンドウが開きます。

6. フォルダー名を入力するか、[**参照**]をクリックしてフォルダーを選択します。

7. [**OK**]をクリックします。

除外する領域がリストに追加されます。

システム監査

このセクションではファイル変更監視タスクと、オペレーティングシステムログを調査する機能に関する情報が含まれています。

この章の内容

ファイル変更監視

このセクションには、ファイル変更監視タスクの開始と設定に関する情報が含まれています。

このセクションの内容

ファイル変更監視タスクについて

ファイル変更監視タスクは、タスク設定で指定した監視範囲にある指定したファイルおよびフォルダーで実行される処理を追跡します。このタスクを使用して、保護対象サーバーでセキュリティ違反を示した可能性があるファイル変更を検知できます。監視中断期間のファイル変更を追跡するよう設定することもできます。

監視の中断は、監視範囲が一時的にタスク範囲を外れる、たとえばタスクが停止された場合や、保護対象デバイスが保護対象サーバーに物理的に存在しない場合に発生します。大容量記憶デバイスが再接続されるとすぐに、Kaspersky Security 10.1 for Windows Server は監視範囲で検知したファイル操作を報告します。

> ファイル変更監視の再インストールのためにタスクが指定した監視範囲で実行を停止した場合は、監視の中断は発生しません。この場合、ファイル変更監視タスクは実行されません。

環境に関する要件

ファイル変更監視タスクを開始するには、次の条件が満たされている必要があります:

- ReFS および NTFS ファイルシステムをサポートする保管領域デバイスが保護対象サーバーでインストールされている。
- Windows USN ジャーナルが有効である。このコンポーネントはこのジャーナルに対してクエリーを行って、ファイル操作に関する情報を受け取ります。

  > ボリュームに対してルールが作成され、ファイル変更監視タスクが開始された後で USN ジャーナルを有効化した場合、タスクを再起動する必要があります。そうでない場合、ルールは監視時に適用されません。

除外された監視範囲

監視範囲の除外を作成することができます(416 ページのセクション「監視ルールの設定」を参照)。除外は別々のルール各々に対して指定され、指定した監視範囲に対してのみ機能します。各ルールに対して無制限の

数の除外を指定できます。

> 指定したフォルダーまたはファイルが監視範囲内の場合でも、除外は監視範囲より優先度が高いため、タスクによって監視されません。ルールのいずれかの設定が、除外で指定したフォルダーより下位のレベルで監視範囲を指定している場合、タスクの実行時に監視範囲は考慮されません。

除外を指定するために、監視範囲を指定するために使用したのと同じマスクを使用できます。

ファイル変更監視ルールについて

ファイル変更監視は、ファイル変更監視ルールに基づいて実行されます。ルール有効化の条件を使用してタスクを起動させる条件を設定し、実行ログに記録された検知されたファイル操作に対してイベントの重要性レベルを調整することができます。

ファイル変更監視ルールは、各監視範囲に対して指定されます。

次のルール有効化の条件を設定できます:

- 信頼するユーザー
- ファイル操作マーカー

信頼するユーザー

既定では、すべてのユーザーアクションが潜在的なセキュリティ違反とみなされます。信頼するユーザーのリストは空です。ファイル変更監視ルール設定に信頼するユーザーのリストを作成することで、イベントの重要性レベルを設定できます。

信頼しないユーザー - 監視範囲ルール設定の信頼するユーザーリストに示されていないすべてのユーザー。信頼しないユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに緊急イベントを記録します。

信頼するユーザー - 指定した監視範囲でファイル操作を行う許可を与えられているユーザーのユーザーまたはグループ。信頼するユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに情報イベントを記録します。

Kaspersky Security 10.1 for Windows Server は、監視中断期間に操作を開始したユーザーを特定できません。この場合、ユーザーステータスは不明と判断されます。

不明なユーザー - タスク中断、またはデータ同期ドライバーや USN ジャーナルの障害のために Kaspersky Security 10.1 for Windows Server がユーザーに関する情報を受け取ることができない場合、このステータスがユーザーに割り当てられます。不明なユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに**警告**イベントを記録します。

ファイル操作マーカー

ファイル変更監視タスクが実行されているとき、Kaspersky Security 10.1 for Windows Server はファイル操作マーカーを使用して、ファイル上で処理が実行されたと判定します。

ファイル操作マーカーは、ファイル操作を特徴づけることができる一意の記述子です。

各ファイル操作は、単一の処理であることも、ファイルを使用した処理の連鎖であることもあります。この種類の各処理は、ファイル操作マーカーに対応します。ルール有効化の条件として指定するマーカーがファイル操作チェーンで検知された場合、所定のファイル操作が実行されたことを示すイベントが記録されます。

記録されたイベントの重要性レベルは、選択されたファイル操作マーカーまたはイベントの数に依存しません。

既定で、Kaspersky Security 10.1 for Windows Server は利用できるすべてのファイル操作マーカーを考慮します。タスクのルール設定で、手動でファイル操作マーカーを選択できます。

表 41. ファイル操作マーカー

ファイル操作 ID	ファイル操作マーカー	サポートされているファイルシステム
BASIC_INFO_CHANGE	ファイルまたはフォルダーの属性または時間マーカーが変更されました	NTFS、ReFS
COMPRESSION_CHANGE	ファイルまたはフォルダーの圧縮が変更されました	NTFS、ReFS

ファイル操作 ID	ファイル操作マーカー	サポートされているファイルシステム
DATA_EXTEND	ファイルまたはフォルダーのサイズが増加しました	NTFS、ReFS
DATA_OVERWRITE	ファイルまたはフォルダー内のデータが上書きされました	NTFS、ReFS
DATA_TRUNCATION	ファイルまたはフォルダーが切り詰められました	NTFS、ReFS
EA_CHANGE	拡張されたファイルまたはフォルダーの属性が変更されました	NTFS のみ
ENCRYPTION_CHANGE	ファイルまたはフォルダーの暗号化ステータスが変更されました	NTFS、ReFS
FILE_CREATE	ファイルまたはフォルダーが初めて作成されました	NTFS、ReFS
FILE_DELETE	SHIFT+DEL を同時に押して、ファイルまたはフォルダーが完全に削除されました	NTFS、ReFS
HARD_LINK_CHANGE	ファイルまたはフォルダーにハードリンクが作成または削除されました	NTFS のみ
INDEXABLE_CHANGE	ファイルまたはフォルダーの索引ステータスが変更されました	NTFS、ReFS
INTEGRITY_CHANGE	名前付きファイルストリームの整合性属性が変更されました	ReFS のみ

ファイル操作 ID	ファイル操作マーカー	サポートされているファイルシステム
NAMED_DATA_EXTEND	名前付きファイルストリームのサイズが増加しました。	NTFS、ReFS
NAMED_DATA_OVERWRITE	名前付きファイルストリームが上書きされました	NTFS、ReFS
NAMED_DATA_TRUNCATION	名前付きファイルストリームが切り詰められました	NTFS、ReFS
OBJECT_ID_CHANGE	ファイルまたはフォルダー ID が変更されました	NTFS、ReFS
RENAME_NEW_NAME	ファイルまたはフォルダーに新しい名前が割り当てられました	NTFS、ReFS
REPARSE_POINT_CHANGE	新しい再解析ポイントが作成されたか、ファイルまたはフォルダーに対する既存の再解析ポイントが変更されました	NTFS、ReFS
SECURITY_CHANGE	ファイルまたはフォルダーのアクセス権が変更されました	NTFS、ReFS
STREAM_CHANGE	新しい名前付きファイルストリームが作成されたか、既存の名前付きファイルストリームが変更されました	NTFS、ReFS
TRANSACTED_CHANGE	名前付きファイルストリームが TxF トランザクションによって変更されました	ReFS のみ

ファイル変更監視タスクの設定について

ファイル変更監視タスクの既定の設定を変更できます(次の表を参照)。

表 42.　ファイル変更監視タスクの既定の設定

設定	値	設定方法
監視範囲	設定なし	処理が監視されるフォルダーおよびファイルを指定できます。監視イベントは、指定した監視範囲のフォルダーおよびファイルに対して作成されます。
信頼するユーザーリスト	設定なし	指定したディレクトリにおける処理がコンポーネントにより安全なものとみなされるユーザーやユーザーのグループを指定できます。
タスクが実行中でないときにファイル操作を監視します	使用	タスクが実行されていない期間に、指定した監視範囲で実行されたファイル操作の記録を有効または無効にできます。
除外された監視範囲を考慮します	オフ	ファイル操作を監視する必要がないフォルダーに対する除外の使用を確認できます。ファイル変更監視タスクが実行されている場合、Kaspersky Security 10.1 for Windows Server は除外として指定された監視範囲をスキップします。
ファイル操作マーカーを考慮します	利用できるすべてのファイル操作マーカーが考慮されます	ファイル操作マーカーのセットを指定できます。監視範囲で実行されたファイル操作に、指定したマーカーのいずれかが付けられている場合、Kaspersky Security 10.1 for Windows Server は監視イベントを作成します。

設定	値	設定方法
チェックサム計算	オフ	ファイル変更後のファイルチェックサム計算を設定できます。
ファイル操作マーカーを考慮します	利用できるすべてのファイル操作マーカーが考慮されます	ファイル操作マーカーのセットを指定できます。監視範囲で実行されたファイル操作に、1 つ以上の指定したマーカーが付けられている場合、Kaspersky Security 10.1 for Windows Server は監査イベントを作成します。
タスク開始スケジュール	最初の実行がスケジュール設定されていません	スケジュールによるタスクの開始について設定できます。

ファイル変更監視タスクの全般的な設定を行うには、次の手順を実行します:

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:
   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。
   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**システム監査**]セクションの[**ファイル監視**]ブロックで、[**設定**]をクリックします。

   [**ファイル変更監視**]ウィンドウが開きます。

4. 表示されたウィンドウの[**ファイル変更監視設定**]タブで、監視範囲を設定します:

   a. [**監視中断期間におけるファイル操作の情報を記録する**]をオンにします。

      このチェックボックスで、なんらかの理由でタスクが実行されていない場合(ハードディスクの取り外し、ユーザーによるタスク停止、ソフトウェアエラー)における、ファイル変更監視タスク設定で指定したファイル操作の監視を有効または無効にできます。

      チェックボックスがオンの場合、ファイル変更監視タスクが実行されていないとき、Kaspersky Security 10.1 for Windows Server はすべての監視範囲のイベントを記録します。

      チェックボックスがオフの場合、タスクが実行中でないときには、監視範囲のファイル操作を記録しません。

      既定では、このチェックボックスはオンです。

   b. タスクによって監視される監視範囲を追加します(416 ページのセクション「監視ルールの設定」を参照)。

5. [**タスク管理**]タブで、スケジュールに基づいてタスクを開始します(220 ページのセクション「タスクスケジュールの管理」を参照)。

6. [**OK**]をクリックして、変更内容を保存します。

監視ルールの設定

既定では、監視範囲は指定されず、タスクはいかなるディレクトリのファイル操作も監視しません。

► **監視範囲を追加するには、次の手順を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 **ページのセクション「ポリシーの設定」を参照**)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**ファイル変更監視**]ブロックの[**システム監査**]セクションで、[**設定**]をクリックします。

   [**プロパティ:ファイル変更監視**]ウィンドウが開きます。

4. [**監視範囲**]セクションで、[**追加**]をクリックします。

   [**監視範囲**]ウィンドウが開きます。

5. 次のいずれかの方法で、監視範囲を追加します:

   - 標準の Microsoft Windows ダイアログを使用してフォルダーを選択する場合:

     a. [**参照**]をクリックします。

     Microsoft Windows 標準の[フォルダーの参照]ウィンドウが表示されます。

     b. 表示されたウィンドウで操作を監視するフォルダーを選択し、[**OK**]をクリックします。

   - 手動で監視範囲を指定する場合、サポートされているマスクを使用してパスを追加します:

     - <*.ext> - 場所に関係なく、拡張子 <ext> を持つすべてのファイル。
     - <*¥name.ext> - 場所に関係なく、名前 <name> と拡張子 <ext> を持つすべてのファイル。

- <¥dir¥*> - ディレクトリ <¥dir> にあるすべてのファイル。
- <¥dir¥*¥name.ext> - ディレクトリ <¥dir> とそのすべてのサブディレクトリにある、名前 <name> と拡張子 <ext> を持つすべてのファイル。

手動で監視範囲を指定する場合、パスが次の形式であることを確認してください：<volume letter>:¥<mask>。ボリューム文字がない場合、Kaspersky Security 10.1 for Windows Server は指定した監視範囲を追加しません。

6. [**ユーザー**]タブで、[**追加**]をクリックします。

   Microsoft Windows 標準の[**ユーザーとグループの選択**]ウィンドウが開きます。

7. 選択した監視範囲でのファイル操作が許可されたユーザーまたはユーザーのグループを選択し、[**OK**]をクリックします。

   既定では、Kaspersky Security 10.1 for Windows Server においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い（410 ページのセクション「ファイル変更監視ルールについて」を参照）、重要なイベントを作成します。

8. [**ファイル操作マーカー**]タブを選択します。

9. 必要に応じて、次の処理を実行して複数のマーカーを選択します：

   a. [**次のマーカーに基づいてファイル操作を検出する**]オプションを選択します。

   b. 使用可能なファイル操作のリストで（「ファイル変更監視ルールについて」（410 ページ）を参照）、監視する操作の横にあるチェックボックスをオンにします。

   既定では、Kaspersky Security 10.1 for Windows Server によりすべてのファイル操作マーカーが検知され、[**すべての認識できるマーカーに基づいてファイル操作を検出する**]がオンになります。

10. 操作の実行後に Kaspersky Security 10.1 for Windows Server がファイルチェックサムを計算するようにするには、次の手順を実行します：

a. [**チェックサムの計算**]セクションで、[可能な場合、**ファイルのチェックサムを計算する。チェックサムはタスクレポートで表示できます**]をオンにします。

チェックボックスがオンの場合、Kaspersky Security 10.1 for Windows Server は、少なくとも 1 つの選択したマーカーを持つファイル操作が検知された場所で、変更されたファイルのチェックサムを計算します。

複数のマーカーを持つファイル操作が検知された場合、すべての変更後の最終的なファイルのチェックサムのみが計算されます。

チェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server は変更されたファイルのチェックサムを計算しません。

次の場合、チェックサムの計算は実行されません:

- ファイルが利用できなくなった場合(アクセス権限の変更などのため)。
- ファイル操作が、その後、削除されたファイル内で検知された場合。

既定では、このチェックボックスはオフです。

b. [**チェックサム種別**]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します:

- **MD5 ハッシュ**
- **SHA256 ハッシュ**

11. 利用できるファイル操作のリストにあるすべてのファイル操作を監視するのでない場合は、監視する操作の隣にあるチェックボックスをオンにします(410 ページのセクション「ファイル変更監視ルールについて」を参照)。

12. 必要に応じて、次の手順を実行して、除外された監視範囲を追加します:

a. [**除外リスト**]タブを選択します。

b. [次のフォルダーをコントロールから除外する]をオンにします。

このチェックボックスは、ファイル操作を監視する必要がないフォルダーにおける除外

の使用を無効にします。

チェックボックスがオンの場合、ファイル変更監視タスクの実行時に、Kaspersky Security 10.1 for Windows Server は除外リストで指定された監視範囲をスキップします。

チェックボックスがオフの場合、Kaspersky Security 10.1 for Windows Server は指定されたすべての監視範囲のイベントを記録します。

既定では、チェックボックスはオフで、除外リストは空です。

c. [**追加**]をクリックします。

[**追加するフォルダーの選択**]ウィンドウが開きます。

d. 表示されたウィンドウで、監視範囲から除外するフォルダーを指定します。

e. [**OK**]をクリックします。

指定したフォルダーが、除外される範囲のリストに追加されます。

13. [**ファイル操作監視ルール**]ウィンドウで[**OK**]をクリックします。

指定したルール設定は、ファイル変更監視タスクの、選択した監視範囲に適用されます。

Windows イベントログ監視

このセクションでは、Windows イベントログ監視タスクとタスク設定に関する情報について説明します。

このセクションの内容

Windows イベントログ監視タスクについて

Windows イベントログ監視タスクの実行時に、Windows イベントログの監査結果に基づいて保護環境の整合性を監視します。サイバー攻撃の試みを示す可能性のある異常な動作がシステム内で検知されると、管理者に通知されます。

Kaspersky Security 10.1 for Windows Server では、Windows イベントログ監視タスクによって使用される、ユーザー指定のルールまたはヒューリスティックアナライザーの設定で指定されたルールに基づいて、Windows イベントログの検討と侵入工作の特定が行われます。

定義済みのルールとヒューリスティック分析

既存のヒューリスティックに基づき、定義済みのルールを適用することにより、Windows イベントログ監視タスクを使用して保護対象システムの状態を監視できます。ヒューリスティックアナライザーは、攻撃の試みを示す可能性のある異常な活動を保護サーバー上で特定します。異常な動作を特定するテンプレートは、定義済みのルール設定で使用可能なルールに含まれています。

Windows イベントログ監視タスク用のルールリストには、7 つのルールが含まれています。各ルールの使用を有効または無効にできます。既存のルールを削除したり、新しいルールを作成したりすることはできません。

以下の操作に対して、イベントを監視するルールの適用基準を設定できます:

- ブルートフォース攻撃の検知
- ネットワークログイン検知

タスク設定内で除外を設定することもできます。信頼するユーザーまたは信頼する IP アドレスからのログイン実施時は、ヒューリスティックアナライザーは起動しません。

> Kaspersky Security 10.1 for Windows Server では、ヒューリスティックアナライザーがタスクで使用されない場合、Windows ログの監査にヒューリスティックを使用しません。ヒューリスティックアナライザーは既定で有効化されています。

ルールが適用されると、Windows イベントログ監視タスクのログに**緊急イベント**が記録されます。

Windows イベントログ監視タスクのルールのカスタマイズ

タスクルール設定を使用して、指定した Windows ログ内で選択したイベントを検知する際のルール有効化条件を指定および変更できます。Windows イベントログ監視タスクルールのリストには、既定で 4 つのルールが含まれます。これらのルールの使用、ルールの削除、およびルール設定の編集を有効化および無効化できます。

各ルールに対して、次のルール有効化の条件を設定できます:

- Windows イベントログ内の記録識別子のリスト

  ルールに対して指定されたイベント識別子がイベントプロパティに含まれる場合、Windows イベントログ内で新しいレコードが作成された際にルールが有効化されます。各指定ルールに対する識別子の追加と削除もできます。

- イベントソース

  各ルールに対して、Windows イベントログのサブログを定義できます。このサブログ内のみで、指定されたイベント識別子を含む記録が検索されます。標準サブログ（アプリケーション、セキュリティ、システム）のいずれかを選択するか、またはソース選択フィールドに名前を入力してカスタムのサブログを指定できます。

  > 指定されたサブログが実際に Windows イベントログに存在するかは検証されません。

ルールが適用されると、Windows イベントログ監視タスクのログに緊急イベントが記録されます。

ログ検査タスクは既定でカスタムルールを適用しません。

> Windows イベントログ監視タスクを開始する前に、システム監査ポリシーが正しく設定されていることを確認してください。詳細は、Microsoft の記事（https://technet.microsoft.com/ja-jp/library/cc952128.aspx）を参照してください。

定義済みタスクルールの設定

► **Windows イベントログ監視タスクに対して定義済みのルールを設定するには、次の処理を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

   - サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、**ポリシーのプロパティウィンドウを開きます**(170 ページのセクション「**ポリシーの設定**」を参照)。

   - 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

     > デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**システム監査**]セクションで、[**Windows イベントログ監視**]ブロックの[**設定**]をクリックします。

   [**Windows イベントログ監視の設定**]ウィンドウが表示されます。

4. [**定義済みのルール**]タブを選択します。

5. [**Windows イベントログ監視に定義済みのルールを適用する**]をオンまたはオフにします。

   このチェックボックスをオンにすると、保護対象サーバー上の異常な動作を検知するため、ヒューリスティックアナライザーが適用されます。

   このチェックボックスをオフにすると、ヒューリスティックアナライザーは実行されず、異常な動作を検知するため、定義済みまたはカスタムルールが適用されます。

既定では、このチェックボックスはオンです。

> タスクを実行するには、少なくとも 1 つのWindows イベントログ監視のルールを選択する必要があります。

6. 定義済みのルールのリストから、適用するルールを選択します:

   - システムにブルートフォース攻撃の可能性があるパターンがあります
   - Windows イベントログ悪用の可能性があるパターンがあります
   - インストールされた新しいサービスによる異常処理が検出されました
   - 明示的な資格証明を使用する異常ログオンが検出されました
   - システムに Kerberos 偽造 PAC（MS14-068）攻撃の可能性があるパターンがあります
   - 組み込みの特権グループ Administrators に向けた異常なアクションが検出されました
   - ネットワークログオンセッション時に異常なアクティビティが検出されました

7. 選択したルールを設定するには、[**詳細設定**]をクリックします。

   [**Windows イベントログ監視**]ウィンドウが開きます。

8. [**ブルートフォース攻撃の検知**]セクションで、ヒューリスティックアナライザーの有効化と見なされる試行の数と試行の発生時間帯を設定します。

9. [**ネットワークログオンの検知**]セクションで、Kaspersky Security 10.1 for Windows Server がサインインの試行を異常な動作として扱う時間帯の開始と終了を提示します。

10. [**除外**]タブを選択します。

11. 信頼するユーザーを追加するため、次の処理を実行します:

    a. [**参照**]をクリックします。

    b. ユーザーを選択します。

c. [**OK**]をクリックします。

選択したユーザーが、信頼するユーザーのリストに追加されます。

12. 信頼する IP アドレスを追加するため、次の処理を実行します:

a. IP アドレスを入力します。

b. [**追加**]をクリックします。

13. 入力した IP アドレスが、信頼する IP アドレスのリストに追加されます。

14. [**タスク管理**]タブで、タスクの開始スケジュールを設定します(221 ページのセクション「タスク開始スケジュールの設定」を参照)。

15. [**OK**]をクリックします。

Windows イベントログ監視のタスク設定が保存されます。

Windows イベントログ監視ルールの設定

► **新しい Windows イベントログ監視カスタムルールを追加および設定するには、次の処理を実行します:**

1. Kaspersky Security Center の管理コンソールツリーで[**管理対象デバイス**]フォルダーを展開し、アプリケーションを設定する管理グループを選択します。

2. 選択した管理グループの詳細ペインで、次のいずれかを実行します:

- サーバーグループに対してアプリケーションを設定するには、[**ポリシー**]タブを選択して、ポリシーのプロパティウィンドウを開きます(170 ページのセクション「**ポリシーの設定**」を参照)。

- 単一のサーバーに対してアプリケーションを設定する場合、[**デバイス**]タブを選択して、[**アプリケーションのプロパティ**]ウィンドウを開いてください(190 ページのセクション「**Kaspersky Security Center の[アプリケーションのプロパティ]ウィンドウでのローカルタスクの設定**」を参照)。

デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、[**アプリケーションのプロパティ**]ウィンドウでこれらの設定を編集することはできません。

3. [**システム監査**]セクションで、[**Windows イベントログ監視**]ブロックの[**設定**]をクリックします。

   [**Windows イベントログ監視**]ウィンドウが開きます。

4. [**Windows イベントログ監視のルール**]タブで[**Windows イベントログ監視にカスタムルールを適用する**]をオンまたはオフにします。

   チェックボックスをオンにすると、各ルール設定に従ってWindows イベントログ監視にカスタムルールが適用されます。Windows イベントログ監視ルールは追加、削除、設定ができます。

   チェックボックスをオフにすると、カスタムルールを追加または修正できません。Kaspersky Security 10.1 for Windows Server では既定のルール設定が適用されます。

   既定では、このチェックボックスはオンです。ポップアップ検知ルールのみがアクティブです。

事前設定ルールをWindows イベントログ監視に適用するかどうかをコントロールできます。Windows イベントログ監視に適用するルールに該当するチェックボックスをオンにします。

5. 新しいカスタムルールを追加するには[**追加**]をクリックします。

   [**Windows イベントログ監視のルール**]ウィンドウが開きます。

6. [**全般**]セクションで新しいルールに関する次の情報を入力します:

   - **ルール名**
   - **ソース**

     記録したイベントを分析に使用するためソースログを選択します。次の Windows イベ

ントログの種類が利用可能です:

- アプリケーション
- セキュリティ
- システム

[**ソース**]にログ名を入力することによって、新しいカスタムログを追加できます。

7. [**起動されるイベントの ID**]セクションで、検知時にルールを有効化する項目 ID を指定します:

   a. ID の数値を入力します。

   b. [**追加**]をクリックします。

   選択したルール ID がリストに追加されます。各ルールに対して無制限の識別子の除外を追加できます。

   c. [**OK**]をクリックします。

Windows イベントログ監視ルールがルールのリストに追加されます。

コマンドラインからの Kaspersky Security 10.1 for Windows Server の使用

このセクションでは、コマンドラインからの Kaspersky Security 10.1 for Windows Server の使用について説明します。

この章の内容

コマンドラインのコマンド

Kaspersky Security 10.1 for Windows Server のインストール時、インストール対象機能のリストにコマンドラインユーティリティを追加した場合は、Kaspersky Security 10.1 for Windows Server の基本的な管理コマンドを保護対象サーバーのコマンドラインから実行できます。

コマンドラインのコマンドを使用すると、Kaspersky Security 10.1 for Windows Server で自分に割り当てられた権限に基づいてアクセス可能な機能のみを管理できます。

特定の Kaspersky Security 10.1 for Windows Server のコマンドは次のモードで実行されます:

- 周期モード:管理機能がコンソールに返されるのは、コマンド実行の完了後のみです。
- 非同期モード:コマンド実行直後に管理機能がコンソールに返されます。

► **同期モードでのコマンド実行の中断**

キーボードショートカット **Ctrl+C** を押します。

Kaspersky Security 10.1 for Windows Server のコマンド入力時は、次のルールに従います:

- 修飾子とコマンドの入力には、大文字と小文字を使用する。
- 修飾子は空白文字で区切る。
- ファイル名またはフォルダー名について、キー値として指定するパスに空白文字が含まれる場合は、そのファイルまたはフォルダーのパスを引用符で囲んで指定する。例:`"C:¥TEST¥test cpp.exe"`
- 必要に応じて、ファイル名またはパスマスクにプレースホルダーを使用する。例:“`C:¥Temp¥Temp*¥`”, “`C:¥Temp¥Temp???.doc`”, “`C:¥Temp¥Temp*.doc`”

Kaspersky Security 10.1 for Windows Server の管理に必要になる操作全般にコマンドラインを使用できます(次の表を参照)。

表 43. Kaspersky Security 10.1 for Windows Server のコマンド

コマンド	説明
KAVSHELL APPCONTROL(セクション「アプリケーション起動コントロールルールのリストの入力」(450 ページ)を参照)	選択した追加方法による指定したルールリストの更新。
KAVSHELL APPCONTROL /CONFIG(セクション「アプリケーション起動コントロールタスクの管理:KAVSHELL APPCONTROL /CONFIG」(445 ページ)を参照)	アプリケーション起動コントロールタスクの処理モードのコントロール。

コマンド	説明
KAVSHELL APPCONTROL /GENERATE（セクション「アプリケーション起動コントロールルールの自動作成：KAVSHELL APPCONTROL /GENERATE」（446 ページ）を参照）	アプリケーション起動コントロールルールの自動作成タスクの開始。
KAVSHELL VACUUM（セクション「Kaspersky Security 10.1 for Windows Server ログファイルのデフラグ：KAVSHELL VACUUM」（464 ページ）を参照）	Kaspersky Security 10.1 for Windows Server ログファイルのデフラグ。
KAVSHELL PASSWORD	パスワード保護設定の管理。
KAVSHELL HELP（セクション「Kaspersky Security 10.1 for Windows Server コマンドヘルプの表示：KAVSHELL HELP」（433 ページ）を参照）	Kaspersky Security 10.1 for Windows Server コマンドヘルプの表示。
KAVSHELL START（セクション「Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP」（434 ページ）を参照）	Kaspersky Security 10.1 for Windows Server サービスの開始。
KAVSHELL STOP（セクション「Kaspersky Security サービスの開始と停止：KAVSHELL	Kaspersky Security 10.1 for Windows Server サービスの停止。

コマンド	説明
START、KAVSHELL STOP」（434 ページ）を参照）	
KAVSHELL SCAN（セクション「選択した領域のスキャン：KAVSHELL SCAN」（434 ページ）を参照）	一時的なオンデマンドスキャンタスクの作成と起動（スキャン範囲とセキュリティ設定についてはコマンド修飾子により指定）。
KAVSHELL SCANCRITICAL（セクション「重要領域のスキャンタスクの開始：KAVSHELL SCANCRITICAL」（441 ページ）を参照）	重要領域のスキャンのシステムタスクの開始。
KAVSHELL TASK（セクション「指定されたタスクの非同期での管理：KAVSHELL TASK」（442 ページ）を参照）	選択したタスクの非同期による開始、一時停止、再開、停止、および現在のタスクの状態または統計の表示。
KAVSHELL RTP（セクション「リアルタイム保護タスクの開始と停止：KAVSHELL RTP」（444 ページ）を参照）	すべてのリアルタイム保護タスクの開始または停止。
KAVSHELL UPDATE（セクション「Kaspersky Security 10.1 for Windows Server 定義データベースのアップデートタスクの開始：KAVSHELL UPDATE」（454 ページ）を参照）	Kaspersky Security 10.1 for Windows Server の定義データベースアップデートタスクの開始（設定についてはコマンド修飾子により指定）。

コマンド	説明
KAVSHELL ROLLBACK（セクション「Kaspersky Security 10.1 for Windows Server 定義データベースのロールバック：KAVSHELL ROLLBACK」（459 ページ）を参照）	以前のバージョンへの定義データベースのロールバック。
KAVSHELL LICENSE（セクション「製品のアクティベート：KAVSHELL LICENSE」（460 ページ）を参照）	ライセンスおよびアクティベーションコードの管理。
KAVSHELL TRACE（セクション「トレースログの有効化、設定、無効化： KAVSHELL TRACE」（462 ページ）を参照）	トレースログの有効化または無効化、およびトレースログの設定管理。
KAVSHELL DUMP（セクション「ダンプファイル作成の有効化と無効化：KAVSHELL DUMP」（466 ページ）を参照）	プロセスが不正に終了した場合の Kaspersky Security 10.1 for Windows Server プロセスのダンプファイルの有効化または無効化。
KAVSHELL IMPORT（セクション「設定のインポート：KAVSHELL IMPORT」（468 ページ）を参照）	以前に作成した設定ファイルからの一般的な Kaspersky Security 10.1 for Windows Server 設定、機能、およびタスクのインポート。
KAVSHELL EXPORT（セクション「設定のエクスポート：KAVSHELL EXPORT」（469 ページ）を参照）	Kaspersky Security 10.1 for Windows Server のすべての設定および既存タスクの設定ファイルへのエクスポート。

コマンド	説明
KAVSHELL DEVCONTROL（セクション「デバイスコントロールルールのリストの入力：KAVSHELL DEVCONTROL」（452 ページ）を参照）	選択した方法に応じて、作成されたデバイスコントロールルールのリストに追加します。

Kaspersky Security 10.1 for Windows Server コマンドヘルプの表示：KAVSHELL HELP

すべての Kaspersky Security 10.1 for Windows Server コマンドのリストを取得するには、次のコマンドのいずれかを実行します：

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

コマンドの説明とその構文を表示するには、次のコマンドのいずれかを実行します：

```
KAVSHELL HELP <コマンド>

KAVSHELL <コマンド> /?
```

KAVSHELL HELP コマンドの例

KAVSHELL SCAN コマンドの詳細情報を表示するには、次のコマンドを実行します：

```
KAVSHELL HELP SCAN
```

Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP

Kaspersky Security サービスを実行するには、コマンドを実行します

```
KAVSHELL START
```

既定では、Kaspersky Security サービスの起動時に、ファイルのリアルタイム保護、オペレーティングシステムの起動時にスキャンといったタスクに加え、**アプリケーションの起動時**に開始するようにスケジュールされたその他のタスクが開始されます。

Kaspersky Security サービスを停止するには、コマンドを実行します

```
KAVSHELL STOP
```

> コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、`[/pwd:<パスワード>]` キーを使用します。

選択した領域のスキャン：KAVSHELL SCAN

保護対象サーバーの特定領域をスキャンするタスクを開始するには、`KAVSHELL SCAN` コマンドを使用します。このコマンド修飾子では、選択したフォルダーのスキャン範囲とセキュリティ設定を指定します。

`KAVSHELL SCAN` コマンドを使用して起動したオンデマンドスキャンタスクは一時的なタスクです。このタスクは実行中のみ Kaspersky Security 10.1 コンソールに表示されます（タスク設定を Kaspersky Security 10.1 コンソールで確認することはできません）。タスクパフォーマンスログが同時に生成されます。ログは、Kaspersky Security 10.1 コンソールの［**タスク実行ログ**］に表示されます。Kaspersky Security Center のポリシーは、SCAN コマンドを使用して作成および実行されるタスクに適用できます。

スキャンタスク内で特定領域のパスを指定する際には、環境変数を使用できます。ユーザーに対して設定された環境変数を使用する場合は、そのユーザーの権限で `KAVSHELL SCAN` コマンドを実行してください。

`KAVSHELL SCAN` コマンドは、同期モードで実行されます。

既存のオンデマンドスキャンタスクをコマンドラインから開始するには、KAVSHELL TASK コマンドを使用します（セクション「指定されたタスクの非同期での管理 . KAVSHELL TASK」（442 ページ）を参照）。

KAVSHELL SCAN コマンドの構文

```
KAVSHELL SCAN <スキャン範囲>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<スキャン範囲のリストが含まれるファイルのパス>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<”マスク”>] [/ES:<サイズ>] [/ET:<秒数>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<日数>]
[NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<タスク実行ログのファイルのパス>] [/ANSI] [/ALIAS:<タスクのエイリアス>] [/ANSI]
```

KAVSHELL SCAN コマンドには、必須のキーとオプションのキーの両方があります（以下の表を参照）。

KAVSHELL SCAN コマンドの例

```
KAVSHELL SCAN Folder56 D:¥Folder1¥Folder2¥Folder3¥ C:¥Folder1¥ C:¥Folder2¥3.exe “¥¥another server¥Shared¥” F:¥123¥*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:”*.xtx;*.fff;*.ggg;*.bbb;*.info” /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:¥log.log
```

表 44. KAVSHELL SCAN コマンドの修飾子

ライセンス	説明
スキャン範囲：必須の修飾子	
<ファイル>	スキャン範囲（ファイル、フォルダー、ネットワークパス、および定義済み領域のリスト）を指定します。
<フォルダー>	

ライセンス	説明
<ネットワークパス>	ネットワークパスを UNC（ユニバーサルネーミング規約）形式で指定します。 次の例では、Folder4 フォルダーはパスなしで指定されています。このフォルダーは、KAVSHELL コマンドを実行するフォルダー内にあります： KAVSHELL SCAN Folder4 チェックするオブジェクトの名前に空白が含まれている場合は、この名前を引用符で囲む必要があります。 フォルダーが選択されている場合、そのフォルダー内のすべてのサブフォルダーもチェックされます。 * 記号または ？ 記号はファイルのグループをスキャンするために使用できます。
/MEMORY	RAM 内のオブジェクトをスキャンします。
/SHARED	サーバーにある共有フォルダーをスキャンします。
/STARTUP	スタートアップオブジェクトをスキャンします。
/REMDRIVES	リムーバブルドライブをスキャンします。
/FIXDRIVES	ハードディスクをスキャンします。
/MYCOMP	保護対象サーバーのすべての領域をスキャンします。
/L:<スキャン範囲のリストを含むファイルのパス>	スキャン範囲のリストを含むファイル名（ファイルのフルパスを含む）。 ファイル内では、改行を使用してスキャン範囲を区切ります。スキャン範囲リストを含む次のファイル例で、次のように定義済みのスキャン範囲を指定できます： C:¥ D:¥Docs¥*.doc E:¥My Documents /STARTUP /SHARED

ライセンス	説明
スキャン対象オブジェクト(ファイル種別):この修飾子の値を指定しない場合は、形式に基づくオブジェクトのスキャンが実行されます。	
/FA	すべてのオブジェクトをスキャンします。
/FC	オブジェクトを形式に基づいてスキャンします(既定)。感染の可能性があるオブジェクト形式のリストに含まれている形式のオブジェクトのみスキャンします。
/FE	オブジェクトを拡張子に基づいてスキャンします。感染の可能性があるオブジェクト拡張子のリストに含まれている拡張子を持つオブジェクトのみスキャンします。
/NEWONLY	作成または変更されたファイルのみスキャン この修飾子を指定しない場合は、すべてのオブジェクトがスキャンされます。
感染などの問題があるオブジェクトの処理:この修飾子の値を指定しない場合は、**スキップ**処理が実行されます。	
DISINFECT	駆除し、駆除できない場合はスキップします。
DISINFDEL	駆除し、駆除できない場合は削除します。
DELETE	削除 DISINFECT 設定と DELETE 設定は、以前のバージョンとの互換性を確保するために、現在のバージョンの Kaspersky Security 10.1 for Windows Server で維持されています。これらの設定はキーコマンド /AI: および /AS: のかわりに使用できます。この場合、感染の可能性があるオブジェクトは処理されません。
REPORT	レポートを送信します(既定)。
AUTO	推奨処理を実行
感染の可能性があるオブジェクトの処理:この修飾子の値を指定しない場合は、**スキップ**処理が実行されます。	

ライセンス	説明
QUARANTINE	隔離
DELETE	削除
REPORT	レポートを送信します（既定）。
AUTO	推奨処理を実行
除外	
/E:ABMSPO	次の種別の複合オブジェクトを除外します: A - アーカイブ（SFX アーカイブのみスキャン） B - メールデータベース M - 通常のメール S - アーカイブと SFX アーカイブ P - 圧縮されたオブジェクト O - OLE 埋め込みオブジェクト
/EM:<"マスク">	ファイルをマスクに基づいて除外します。 複数のマスクを指定できます。例：EM:”*.txt;*.png; C¥Videos¥*.avi”。
/ET:<秒数>	この <秒数> の値に指定した秒数よりも長くオブジェクトの処理が続いた場合に、オブジェクトの処理を停止します。 既定では、時間制限はありません。
/ES:<サイズ>	<サイズ> の値に指定したサイズ（MB 単位）よりも大きい複合オブジェクトはスキャンしません。 Kaspersky Security 10.1 for Windows Server は既定ですべてのサイズのオブジェクトをスキャンします。

ライセンス	説明
/TZOFF	信頼ゾーンの除外指定を無効にします。
詳細設定（オプション）	
/NOICHECKER	iChecker の使用を無効にします（既定では有効）。
/NOISWIFT	iSwift の使用を無効にします（既定では有効）。
/ANALYZERLEVEL:<分析レベル>	ヒューリスティックアナライザーを有効にし、分析レベルを設定します。 次のヒューリスティック分析レベルを使用できます： 1 - 低 2 - 中 3 - 高 修飾子を省略した場合は、ヒューリスティックアナライザーは使用されません。
/ALIAS:<タスクエイリアス>	オンデマンドスキャンタスクに一時的な名前を割り当てることができます。タスクの実行中に、TASK コマンドを使用して統計を確認する際などに、その名前を使用してタスクにアクセスできます。タスクのエイリアスは、Kaspersky Security 10.1 for Windows Server のすべての機能コンポーネントのタスクエイリアスの間で一意である必要があります。 この修飾子を指定しない場合、scan_<kavshell_pid> が使用されます（例：scan_1234）。Kaspersky Security 10.1 コンソールで、スキャンオブジェクトの名前（<日時>）がタスクに割り当てられます（例：Scan objects 8/16/2007 5:13:14 PM）。
実行ログの設定（レポート設定）	

ライセンス	説明
/W:<タスク実行ログファイルのパス>	このキーを指定すると、Kaspersky Security 10.1 for Windows Server によって、キーの値で定義された名前のタスクログファイルが保存されます。 ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了（停止）時刻、およびこのタスクのイベントに関する情報が含まれます。 このログを使用して、「イベント ビューアー」のタスク実行ログの設定および Kaspersky Security 10.1 for Windows Server イベントログで定義されたイベントが登録されます。 ファイルの絶対パスまたは相対パスを指定できます。ファイル名のみを指定し、そのパスを指定しなかった場合、ログファイルは現在のフォルダーに作成されます。 同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。 タスクの実行中にログファイルを表示できます。 ログは、Kaspersky Security 10.1 コンソールの［実行ログ］に表示されます。 Kaspersky Security 10.1 for Windows Server でログファイルを作成できない場合、コマンドの実行は停止されませんが、エラーメッセージが表示されます。
/ANSI	このオプションでは、イベントを ANSI エンコーディングとしてタスク実行ログに記録できます。 W オプションを定義していない場合、この ANSI オプションは適用されません。 ANSI オプションを指定しない場合、UNICODE エンコーディングを使用してタスクログが生成されます。

重要領域のスキャンの開始：KAVSHELL SCANCRITICAL

Kaspersky Security 10.1 コンソールで定義された設定を使用して、システムのオンデマンドスキャンタスクである重要領域のスキャンを開始するには、KAVSHELL SCANCRITICAL コマンドを使用します。

KAVSHELL SCANCRITICAL コマンドの構文

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>]
```

KAVSHELL SCANCRITICAL コマンドの例

オンデマンドスキャンタスクの重要領域のスキャンを実行し、現在のフォルダーにタスク実行ログの scancritical.log を保存するには、次のコマンドを実行します：

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

/W 修飾子の構文に応じて、タスクログの場所を設定できます（次の表を参照）。

表 45. KAVSHELL SCANCRITICAL コマンドの /W 修飾子の構文

ライセンス	説明
/W:<タスク実行ログファイルのパス>	このキーを指定すると、Kaspersky Security 10.1 for Windows Server によって、キーの値で定義された名前のタスクログファイルが保存されます。 ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了(停止)時刻、およびこのタスクのイベントに関する情報が含まれます。 このログを使用して、イベント ビューアーのタスク実行ログの設定および製品のイベントログで定義されたイベントが登録されます。 ファイルの絶対パスまたは相対パスを指定できます。ファイル名のみを指定し、そのパスを指定しなかった場合、ログファイルは現在のフォルダーに作成されます。 同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。 タスクの実行中にログファイルを表示できます。 ログは、Kaspersky Security コンソールの[**タスク実行ログ**]に表示されます。 Kaspersky Security 10.1 for Windows Server でログファイルを作成できない場合、コマンドの実行は停止されませんが、エラーメッセージが表示されます。

指定されたタスクの非同期での管理:KAVSHELL TASK

KAVSHELL TASK コマンドを使用すると、指定のタスクを管理できます。タスクの実行、一時停止、再開、停止、およびタスクの現在のステータスと統計情報の表示を実行できます。コマンドは非同期モードで実行されます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL TASK コマンドの構文

```
KAVSHELL TASK [<タスク名のエイリアス> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

KAVSHELL TASK コマンドの構文

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

KAVSHELL TASK コマンドは、修飾子を指定せずに実行することも、1 つまたは複数の修飾子を指定して実行することもできます（次の表を参照）。

表 46. KAVSHELL TASK コマンドの修飾子

ライセンス	説明
キーの指定なし	既存のすべての Kaspersky Security 10.1 for Windows Server タスクのリストを返します。リストには、次のフィールドが含まれます：代替タスク名、タスクカテゴリ（システムまたはカスタム）、タスクの現在のステータス。
<タスクのエイリアス>	SCAN TASK コマンドでは、タスク名の代わりに、Kaspersky Security 10.1 for Windows Server によってタスクに割り当てられた追加の短い形式の名前である、タスクのエイリアスが使用されます。Kaspersky Security 10.1 for Windows Server のタスクのエイリアスを表示するには、修飾子を指定せずにコマンド KAVSHELL TASK を入力します。
/START	指定のタスクを非同期モードで開始します。
/STOP	指定のタスクを停止します。

ライセンス	説明
/PAUSE	指定のタスクを一時停止します。
/RESUME	指定のタスクを非同期モードで再開します。
/STATE	タスクの現在のステータス(**実行中**、**完了**、**一時停止済み**、**停止済み**、**失敗**、**開始中**、**復元中**など)を返します。
/STATISTICS	タスクの統計情報(タスクが開始されてから現在までに処理されたオブジェクトの数に関する情報)を取得します。

KAVSHELL TASK コマンドのリターンコード(475 ページのセクション「KAVSHELL TASK コマンドのリターンコード」を参照)。

リアルタイム保護タスクの開始と停止:KAVSHELL RTP

KAVSHELL RTP コマンドを使用すると、すべてのリアルタイム保護タスクを開始または停止できます。

> コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL RTP コマンドの構文

```
KAVSHELL RTP {/START | /STOP}
```

KAVSHELL RTP コマンドの例

すべてのリアルタイム保護タスクを開始するには、次のコマンドを実行します:

```
KAVSHELL RTP /START
```

KAVSHELL RTP コマンドに、2 つの必須の修飾子を含めることができます(次の表を参照)。

表 47. KAVSHELL RTP コマンドの修飾子

ライセンス	説明
/START	すべてのリアルタイム保護タスクを開始します:ファイルのリアルタイム保護、スクリプト監視、KSN の使用。
/STOP	すべてのリアルタイム保護タスクを停止します。

アプリケーション起動コントロールタスクの管理:KAVSHELL APPCONTROL /CONFIG

KAVSHELL APPCONTROL/CONFIG コマンドを使用して、アプリケーション起動コントロールタスクが DLL モジュールの読み込みを実行、監視するモードを設定できます。

KAVSHELL APPCONTROL /CONFIG コマンドの構文

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<XML ファイルの完全パス>
```

KAVSHELL APPCONTROL /CONFIG コマンドの例

► **アプリケーション起動コントロールタスクを、DLL を読み込まずにルールの[使用中]モードで実行し、完了時にタスク設定を保存するには、次のコマンドを実行します:**

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:¥appcontrol¥config.xml
```

コマンドラインパラメータを使用して、アプリケーション起動コントロールタスク設定を設定できます(次の表を参照)。

表 48. KAVSHELL APPCONTROL /GENERATE コマンドスイッチ

ライセンス	説明
/mode:<applyrules|statistics>	アプリケーション起動コントロールタスクの処理モード 次のいずれかのモードを選択できます: • active - アプリケーション起動コントロールルールを適用。 • statistics - 統計のみ。
/dll:<no|yes>	DLL の読み込みの監視を有効または無効にします。
/savetofile: <XML ファイルのパス>	指定したファイルの指定したルールを XML 形式でエクスポートします。
/savetofile: <xml ファイルの完全名>	ルールのリストをファイルに保存します。
/savetofile: <xml ファイルの完全名> /sdc	ソフトウェア配布コントロールルールのリストをファイルに保存します。
/clearsdc	すべてのソフトウェア配布コントロールルールをリストから削除します。

アプリケーション起動コントロールルールの自動作成:KAVSHELL APPCONTROL /GENERATE

KAVSHELL APPCONTROL /GENERATE コマンドを使用して、アプリケーション起動コントロールルールリストを作成できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL APPCONTROL /GENERATE コマンドの構文

KAVSHELL APPCONTROL /GENERATE <フォルダーのパス> | /source:<フォルダーリストを含むファイルのパス> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<ユーザーまたはユーザーのグループ>] [/export:<XML ファイルのパス>] [/import:<a|r|m>] [/prefix:<ルール名の接頭辞>] [/unique]

KAVSHELL APPCONTROL /GENERATE コマンドの例

► **指定したフォルダーからファイルのルールを作成するには、次のコマンドを実行します:**

```
KAVSHELL APPCONTROL /GENERATE /source:c¥folderslist.txt
/export:c:¥rules¥appctrlrules.xml
```

► **指定したフォルダーにある、使用できるすべての拡張子の実行可能ファイルのルールを作成し、タスク完了時に、指定した XML ファイルに作成したルールを保存するには、次のコマンドを実行します:**

```
KAVSHELL APPCONTROL /GENERATE c:¥folder /masks:edms
/export:c¥rules¥appctrlrules.xml
```

キーの構文によっては、アプリケーション起動コントロールタスクに自動ルール作成を設定できます（次の表を参照）。

表 49. KAVSHELL APPCONTROL /GENERATE コマンドキー

ライセンス	説明
ルールの適用範囲	
<フォルダーのパス>	自動作成された許可ルールを必要とする実行可能ファイルがあるフォルダーへのパスを指定します。

/source: <フォルダーリストを含むファイルのパス>	自動作成された許可ルールを必要とする実行可能ファイルがあるフォルダーのリストを含む TXT ファイルへのパスを指定します。
/masks: <edms>	自動作成された許可ルールを必要とする実行可能ファイルの拡張子を指定します。 次の拡張子のルールの適用範囲ファイルに、以下を含めることができます: • e - EXE ファイル • d - DLL ファイル • m - MSI ファイル • s - スクリプト
/runapp	許可ルールを作成する場合は、タスク実行時に保護対象サーバー上で実行されているアプリケーションを考慮に入れてください。
許可ルールを自動的に作成するときの処理	
/rules: <ch|cp|h>	アプリケーション起動コントロールの許可ルールの作成時に実行する処理を指定します: • ch - デジタル証明書を使用する。証明書がない場合は SHA256 ハッシュを使用します。 • cp - デジタル証明書を使用する。証明書がない場合は、実行可能ファイルへのパスを使用します。 • h - SHA256 ハッシュを使用する。

/strong	アプリケーション起動コントロールの許可ルールを自動作成するときに、デジタル証明書サブジェクトとサムプリントを使用します。/rules: <ch|cp> キーが指定されている場合、コマンドが実行されます。
/user: <ユーザーまたはユーザーのグループ>	ルールを適用するユーザー名またはユーザーのグループを指定します。指定されたユーザーまたはユーザーグループによって実行されるアプリケーションを監視します。
アプリケーション起動コントロールルールの自動作成の完了時の処理	
/export <XML ファイルのパス>	作成したルールを XML ファイルに保存します。
/unique	アプリケーション起動コントロールの許可ルール作成の基礎となるアプリケーションがインストールされたサーバーに関する情報を追加します。
/prefix: <ルール名の接頭辞>	アプリケーション起動コントロールの許可ルールを作成するための名前の接頭辞を指定します。

/import: <a|r|m>	選択した追加方法に従って、指定したアプリケーション起動コントロールルールのリストに、作成したルールをインポートします。: • a - **既存のルールに追加する**(同一の設定を持つルールは重複します) • r - **既存のルールを置き換える**(同一のパラメータを持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます) • m - **既存のルールとマージする**(同一のパラメータを持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます)

アプリケーション起動コントロールルールのリストの入力:KAVSHELL APPCONTROL

KAVSHELL APPCONTROL を使用すると、選択した方法に従って XML ファイルからアプリケーション起動コントロールタスクルールリストにルールを追加し、また、リストから設定したルールをすべて削除できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL APPCONTROL コマンドの構文

KAVSHELL APPCONTROL /append <XML ファイルのパス> | /replace <XML ファイルのパス> | /merge <XML ファイルのパス> | /clear

KAVSHELL APPCONTROL コマンドの例

► **既存のルールに追加する方法に従って、XML ファイルからすでに指定したアプリケーション起動コントロールタスクのルールにルールを追加するには、次のコマンドを実行します:**

```
KAVSHELL APPCONTROL /append c:¥rules¥appctrlrules.xml
```

キーの構文によっては、ルールを追加する方法を選択して、指定した XML ファイルをアプリケーション起動コントロールの定義済みルールのリストに追加できます(次の表を参照)。

表 50. KAVSHELL SCAN コマンドキー

ライセンス	説明
/append <XML ファイルのパス>	指定した XML ファイルに基づいてアプリケーション起動コントロールルールのリストを更新します。追加方法 - **既存のルールに追加する**（同一の設定を持つルールは重複します）
/replace <XML ファイルのパス>	指定した XML ファイルに基づいてアプリケーション起動コントロールルールのリストを更新します。追加方法 - **既存のルールを置き換える**（同一のパラメータを持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます）。
/merge <XML ファイルのパス>	指定した XML ファイルに基づいてアプリケーション起動コントロールルールのリストを更新します。追加方法 - **既存のルールとマージする**（新しいルールは、すでに設定されているルールと重複しません）。
/clear	アプリケーション起動コントロールルールのリストのクリア

デバイスコントロールルールのリストの入力：KAVSHELL DEVCONTROL

KAVSHELL DEVCONTROL を使用すると、選択した方法に従って XML ファイルからデバイスコントロールタスクルールリストにルールを追加し、また、リストから設定したルールをすべて削除できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL DEVCONTROL コマンドの構文

```
KAVSHELL DEVCONTROL /append <XML ファイルのパス> | /replace <XML ファイルのパス> | /merge <XML ファイルのパス> | /clear
```

KAVSHELL DEVCONTROL コマンドの例

► **既存のルールに追加する方法に従って、XML ファイルからすでに指定したデバイスコントロールタスクのルールにルールを追加するには、次のコマンドを実行します:**

```
KAVSHELL DEVCONTROL /append :c:¥rules¥devctrlrules.xml
```

キーの構文によっては、ルールを追加する方法を選択して、指定した XML ファイルをデバイスコントロールの定義済みルールのリストに追加できます(次の表を参照)。

表 51. KAVSHELL DEVCONTROL コマンドキー

ライセンス	説明
/append <XML ファイルのパス>	指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。追加方法 - **既存のルールに追加する**(同一の設定を持つルールは重複します)
/replace <XML ファイルのパス>	指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。追加方法 - **既存のルールを置き換える**(同一のパラメータを持つルールは追加されません。少なくとも 1 つのルールパラメータが一意の場合にルールが追加されます)。

/merge <XML ファイルのパス>	指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。追加方法 - **既存のルールとマージする**(新しいルールは、すでに設定されているルールと重複しません)。
/clear	デバイスコントロールルールのリストのクリア

Kaspersky Security 10.1 for Windows Server 定義データベースのアップデートタスクの開始: KAVSHELL UPDATE

KAVSHELL UPDATE コマンドを使用すると、Kaspersky Security 10.1 for Windows Server 定義データベースのアップデートコマンドを同期モードで開始できます。

KAVSHELL UPDATE を使用して実行する Kaspersky Security 10.1 for Windows Server 定義データベースのアップデートタスクは、一時的なタスクです。実行中に Kaspersky Security 10.1 コンソールにのみ表示されます。タスク実行ログが同時に生成されます。ログは、Kaspersky Security 10.1 コンソールの[**タスク実行ログ**]に表示されます。Kaspersky Security Center のポリシーを、KAVSHELL UPDATE コマンドを使用して作成および開始されたアップデートタスクと Kaspersky Security 10.1 コンソールで作成されたアップデートタスクに適用できます。Kaspersky Security Center を使用したコンピューター上の Kaspersky Security 10.1 for Windows Server の管理については、「Kaspersky Security Center を使用した Kaspersky Security 10.1 for Windows Server の管理」を参照してください。

このタスクでアップデート元のパスを指定する際は、環境変数を使用できます。ユーザー環境変数を使用する場合は、そのユーザーの権限で KAVSHELL UPDATE コマンドを実行します。

KAVSHELL UPDATE コマンドの構文

KAVSHELL UPDATE <アップデート元のパス | /AK | /KL> [/NOUSEKL] [/PROXY:<アドレス>:<ポート>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<ユーザー名>] [/PROXYPWD:<パスワード>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/TIMEOUT:<秒>]

[/REG:<iso3166 コード>] [/W:<タスク実行ログファイルのパス>] [/ALIAS:<タスクのエイリアス>]

KAVSHELL UPDATE コマンドには、必須のキーとオプションのキーの両方があります(以下の表を参照)。

KAVSHELL UPDATE コマンドの例

► **カスタムの定義データベースのアップデートタスクを開始するには、次のコマンドを実行します:**

```
KAVSHELL UPDATE
```

► **ネットワークフォルダー ¥¥server¥databases のアップデートファイルを使用して定義データベースのアップデートタスクを実行するには、次のコマンドを実行します:**

```
KAVSHELL UPDATE ¥¥server¥databases
```

► **FTP サーバー ftp://dnl-ru1.kaspersky-labs.com/ からアップデートタスクを開始し、すべてのタスクイベントをファイル c:¥update_report.log に記録するには、次のコマンドを実行します:**

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:¥update_report.log
```

► **Kaspersky Lab のアップデートサーバーから Kaspersky Security 10.1 for Windows Server 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、プロキシサーバー(プロキシサーバーアドレス:proxy.company.com、ポート:8080)を介してアップデート元に接続し、組み込みの Microsoft Windows NTLM 認証(ユーザー名:inetuser、パスワード:123456)を使用してサーバーにアクセスし、次のコマンドを実行します:**

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

表 52. KAVSHELL UPDATE コマンドのキー

ライセンス	説明
アップデート元(必須のキー)。1 つまたは複数のアップデート元を指定します。Kaspersky Security 10.1 for Windows Server は、表示されている順序でアップデート元にアクセスします。アップデート元をスペースで区切ります。	
<UNC フォーマットのパス>	ユーザー定義のアップデート元。UNC フォーマットのネットワークアップデートフォルダーのパス。

ライセンス	説明
<URL>	ユーザー定義のアップデート元。アップデートフォルダーが配置されている HTTP または FTP サーバーのアドレス。
<ローカルフォルダー>	ユーザー定義のアップデート元。保護対象のサーバー上のフォルダー。
/AK	アップデート元としての Kaspersky Security Center 管理サーバー。
/KL	アップデート元としての Kaspersky Lab のアップデートサーバー。
/NOUSEKL	他のアップデート元が使用できない場合、Kaspersky Lab のアップデートサーバーを使用しません（既定で使用）。
プロキシサーバーの設定	
/PROXY:<アドレス>:<ポート>	プロキシサーバーおよびそのポートのネットワーク名または IP アドレス。このキーを指定しない場合、ローカルエリアネットワークで使用されているプロキシサーバーの設定が Kaspersky Security 10.1 for Windows Server によって自動的に検出されます。
/AUTHTYPE:<0-2>	このキーで、プロキシサーバーにアクセスするための認証方法を指定します。次の値が使用されます: **0** - 組み込みの Microsoft Windows NTLM 認証。**ローカルシステム**（**SYSTEM**）アカウントを使用して Kaspersky Security がプロキシコンピューターに接続します。 **1** - 組み込みの Microsoft Windows NTLM 認証。キー /PROXYUSER と /PROXYPWD で指定したログイン名とパスワードを持つアカウントを使用して Kaspersky Security 10.1 for Windows Server がプロキシコンピューターに接続します。 **2** - キー /PROXYUSER と /PROXYPWD で指定したログイン名とパスワードによる認証（基本認証）。 プロキシサーバーへのアクセスに認証が必要ない場合、キーを指定する必要はありません。

ライセンス	説明
/PROXYUSER:<ユーザー名>	プロキシサーバーへのアクセスに使用するユーザー名。キーの値 /AUTHTYPE:0 を指定すると、/PROXYUSER:<ユーザー名> と /PROXYPWD:<パスワード> キーは無視されます。
/PROXYPWD:<パスワード>	プロキシサーバーへのアクセスに使用するユーザーのパスワード。キーの値 /AUTHTYPE:0 を指定すると、/PROXYUSER:<ユーザー名> と /PROXYPWD:<パスワード> キーは無視されます。/PROXYUSER キーを指定して /PROXYPWD を省略すると、パスワードは空白であるとみなされます。
/NOPROXYFORKL	Kaspersky Lab のアップデートサーバーへの接続にプロキシサーバー設定を使用しません(既定で使用)。
/USEPROXYFORCUSTOM	ユーザー定義のアップデート元への接続にプロキシサーバー設定を使用します(既定では使用しない)。
/USEPROXYFORLOCAL	ローカルのアップデート元への接続にプロキシサーバー設定を使用します。指定しない場合、値[**ローカルアドレスへの接続時はプロキシサーバーを使用しない**]が適用されます。
FTP サーバーと HTTP サーバーの全般設定	
/NOFTPPASSIVE	このキーを指定すると、保護対象のサーバーへの接続に Kaspersky Security 10.1 for Windows Server はアクティブな FTP コンピューターモードを使用します。このキーを指定しないと、Kaspersky Security 10.1 for Windows Server はパッシブな FTP コンピューターモードを使用します(可能な場合)。
/TIMEOUT:<秒数>	FTP サーバーまたは HTTP サーバーの接続タイムアウト。このキーを指定しない場合、既定値: 10 秒が使用されます。キーの値は自然数である必要があります。

ライセンス	説明
/REG:<iso3166 コード>	地域の設定。このキーは、Kaspersky Lab のアップデートサーバーからアップデートを受信する場合に使用します。最も近いアップデートサーバーを選択することにより、Kaspersky Security 10.1 for Windows Server によって保護対象サーバーへのアップデートの読み込みが最適化されます。 このキーの値として、ISO 3166-1 に従って、保護対象のサーバーが配置されている国の文字コードを指定します（/REG: gr、/REG:RU など）。キーを省略した場合や存在しない国コードを指定した場合、Kaspersky Security 10.1 コンソールがインストールされているコンピューターの地域の設定に基づいて、保護対象のサーバーの場所が検出されます。
/ALIAS:<タスクエイリアス>	このキーで、実行中にタスクにアクセスするために使用する、一時的な名前をタスクに割り当てできます。たとえば、TASK コマンドを使用してタスクの統計情報を表示できます。タスクのエイリアスは、Kaspersky Security 10.1 for Windows Server のすべての機能コンポーネントのタスクエイリアスの間で一意である必要があります。 このキーを指定しない場合、update_<kavshell_pid> が使用されます（例：update_1234）。Kaspersky Security 10.1 コンソールで、タスクに Update-databases (日時) が自動的に割り当てられます（例：Update-databases 8/16/2007 5:41:02 PM）。
/W:<タスク実行ログファイルのパス>	このキーを指定すると、Kaspersky Security 10.1 for Windows Server によって、キーの値で定義された名前のタスクログファイルが保存されます。 ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了（停止）時刻、およびこのタスクのイベントに関する情報が含まれます。 このログを使用して、「イベント ビューアー」のタスク実行ログの設定および Kaspersky Security 10.1 for Windows Server イベントログで定義されたイベントが登録されます。 ファイルの絶対パスまたは相対パスを指定できます。パスを指定せずにファイル名のみ指定すると、ログファイルは現在のフォルダーに作成されます。

ライセンス	説明
	同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。 タスクの実行中にログファイルを表示できます。 ログは、Kaspersky Security コンソールの[**タスク実行ログ**]に表示されます。 Kaspersky Security 10.1 for Windows Server でログファイルを作成できない場合、コマンドの実行は停止されず、エラーメッセージも表示されません。

KAVSHELL UPDATE コマンドのリターンコード(477 ページを参照)

Kaspersky Security 10.1 for Windows Server 定義データベースのロールバック:KAVSHELL ROLLBACK

KAVSHELL ROLLBACK コマンドを使用すると、Kaspersky Security 10.1 for Windows Server の定義データベースのロールバックシステムタスク(Kaspersky Security 10.1 for Windows Server 定義データベースを、以前にインストールしたバージョンにロールバック)を実行できます。コマンドは同期的に実行されます。

コマンドの構文:

```
KAVSHELL ROLLBACK
```

KAVSHELL ROLLBACK コマンドのリターンコード(478 ページを参照)

Windows イベントログ監視の管理:KAVSHELL TASK LOG-INSPECTOR

KAVSHELL TASK LOG-INSPECTOR コマンドを使用すると、Windows イベントログ分析に基づいて環境の整合性を監視できます。

コマンドの構文

```
KAVSHELL TASK LOG-INSPECTOR
```

コマンドの例

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

表 53. KAVSHELL TASK LOG-INSPECTOR コマンドの修飾子

ライセンス	説明
/START	指定のタスクを非同期モードで開始します。
/STOP	指定のタスクを停止します。
/STATE	タスクの現在のステータス(**実行中**、**完了**、**一時停止済み**、**停止済み**、**失敗**、**開始中**、**復元中**など)を返します。
/STATISTICS	タスクの統計情報(タスクが開始されてから現在までに処理されたオブジェクトの数に関する情報)を取得します。

KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード(474 ページのセクション「KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード」を参照)。

製品のアクティベート:KAVSHELL LICENSE

Kaspersky Security 10.1 for Windows Server のライセンスおよびアクティベーションコードは、KAVSHELL LICENSE コマンドを使用して管理できます。

> コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL FULLSCAN コマンドの構文

KAVSHELL LICENSE [/ADD:<ライセンス情報ファイル | アクティベーションコード> [/R] | /DEL:<ライセンス番号 | アクティベーションコード番号>]

KAVSHELL SCAN コマンドの例

► **製品をアクティベートするには、次のコマンドを実行します:**

```
KAVSHELL.EXE LICENSE / ADD: <キー番号のアクティベーションコード>
```

► **追加したライセンスの情報を表示するには、次のコマンドを実行します:**

```
KAVSHELL LICENSE
```

► **識別 ID 0000-000000-00000001 の追加したライセンスを削除するには、次のコマンドを実行します:**

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

`KAVSHELL LICENSE` コマンドは、ライセンスを指定してもしなくても実行できます(次の表を参照)。

表 54. KAVSHELL LICENSE コマンドのキー

ライセンス	説明
キーの指定なし	コマンドを実行すると、追加したライセンスの次の情報が返されます: • ライセンス番号。 • ライセンスの種別(製品版または試用版)。 • ライセンスの期間。 • ライセンスのステータス:現在または予備。指定の値が * の場合、ライセンスは予備のライセンスとして追加されています。
/ADD:<ライセンス情報ファイル名またはアクティベーションコード>	指定のファイルまたはアクティベーションコードを使用してライセンスを追加します。 ライセンス情報ファイルのパスを指定するときにシステム環境変数を使用できます。ユーザー環境変数は使用できません。
/R	/R のアクティベーションコードまたはライセンスは /ADD のアクティベーションコードまたはライセンスに加えて使用でき、追加されたアクティベーションコードまたはライセンスが予備のアクティベーションコードまたはライセンスであることを示します。

ライセンス	説明
/DEL:<ライセンス番号またはアクティベーションコード>	指定した番号のライセンスまたは選択したアクティベーションコードを削除します。

KAVSHELL LICENSE コマンドのリターンコード（479 ページのセクション「KAVSHELL LICENSE コマンドのリターンコード」を参照）。

トレースログの有効化、設定、無効化：KAVSHELL TRACE

KAVSHELL TRACE コマンドを使用すると、Kaspersky Security 10.1 for Windows Server のすべてのサブシステムのトレースログの有効化と無効化、およびログの詳細レベルの設定を行うことができます。

Kaspersky Security 10.1 for Windows Server では、暗号化されていない形式でトレースファイルとダンプファイルに情報を書き込みます。

KAVSHELL TRACE コマンドの構文

```
KAVSHELL TRACE </ON /F:<path to trace log file folder> [/S:<maximum log size in megabytes>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

トレースログが保持されている場合にその設定を変更するには、/ON キーを使用して KAVSHELL TRACE コマンドを入力し、/S キーと /LVL キーの値を使用してログ設定を指定します（次の表を参照）。

表 55. KAVSHELL TRACE コマンドのキー

ライセンス	説明
/ON	トレースログの有効化。
/F:<トレースログファイルを保存するフォルダー>	このキーで、トレースログファイルを保存するフォルダーの絶対パスを指定します（必須）。 存在しないフォルダーのパスを指定すると、トレースログは作成されません。ネットワークパスを UNC（汎用命名規則）フォーマットで使用できますが、保護対象のサーバーのネットワークドライブ上のフォルダーのパスは指定できません。 キーの値としてパスを指定するフォルダーの名前に空白文字が含まれる場合、このフォルダーのパスを二重引用符で囲みます。例：/F:"C¥Trace Folder"。 トレースログファイルのパスを指定するときにシステム環境変数を使用できます。ユーザー環境変数は使用できません。
/S: <メガバイト単位でのログファイルの最大サイズ>	このキーで、単一のトレースログファイルの最大サイズを設定します。ログファイルが最大レベルに達するとすぐに、Kaspersky Security 10.1 for Windows Server によって情報は新しいファイルに記録され、前のログファイルは保存されます。 このキーの値を指定しない場合、1 つのログファイルの最大サイズは 50 MB です。
/LVL:debug|info|warning|error|critical	このキーで、すべてのイベントがログに記録される最大（**すべてのデバッグ情報**）から緊急イベントのみ記録される最小（**緊急イベント**）まで、ログの詳細レベルを設定します。 このキーを指定しない場合、詳細レベル「**すべてのデバッグ情報**」のイベントがトレースログに記録されます。
/OFF	このキーで、トレースログを無効にします。

KAVSHELL TRACE コマンドの例

► **詳細レベル「すべてのデバッグ情報」を使用してログの最大サイズ 200 MB でトレースログを有効にし、ログファイルをフォルダー C:¥Trace Folder に保存するには、次のコマンドを実行します:**

```
KAVSHELL TRACE /ON /F:"C:¥Trace Folder" /S:200
```

► **詳細レベル「重要イベント」を使用してトレースログを有効にし、ログファイルをフォルダー C:¥Trace Folder に保存するには、次のコマンドを実行します:**

```
KAVSHELL TRACE /ON /F:"C:¥Trace Folder" /LVL:warning
```

► **トレースログを無効にするには、次のコマンドを実行します:**

```
KAVSHELL TRACE /OFF
```

KAVSHELL TRACE コマンドのリターンコード(479 ページのセクション「KAVSHELL TRACE コマンドのリターンコード」を参照)。

Kaspersky Security 10.1 for Windows Server ログファイルのデフラグ:KAVSHELL VACUUM

`KAVSHELL VACUUM` コマンドを使用すると、アプリケーションのログファイルをデフラグできます。堅固なログ保管領域に接続した Kaspersky Security 10.1 for Windows Server の作業時にシステムエラーやエラーを回避できます。

> コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、`[/pwd:<パスワード>]` キーを使用します。

オンデマンドスキャンのスキャンおよびアップデートタスクが頻繁に開始される場合、`KAVSHELL VACUUM` コマンドを適用してログファイル保管領域を最適化することをお勧めします。コマンドの実行時に、Kaspersky Security 10.1 for Windows Server は、保護対象サーバーの指定したパスに保存されるアプリケーションログファイルの論理構造を更新します。

既定で、アプリケーションログファイルは C:¥ProgramData¥Kaspersky Lab¥Kaspersky Security 10.1 for Windows Server¥10.1¥Reports に保存されます。ログ保管領域として別のパスを手動で指定した場合、

KAVSHELL VACUUM コマンドは、Kaspersky Security 10.1 for Windows Server ログ設定で指定したフォルダーにあるファイルのデフラグを実行します。

サイズの大きいファイルをデフラグすると、KAVSHELL VACUUM コマンドの実行期間が延びます。

リアルタイム保護タスクとサーバー管理タスクは、KAVSHELL VACUUM コマンドの実行中は実行できません。進行中のデフラグプロセスは、Kaspersky Security 10.1 for Windows Server ログへのアクセスを制限し、イベントロギングを拒否します。セキュリティレベルの低下を避けるため、あらかじめダウンタイムに KAVSHELL VACUUM コマンドの実行を計画することをお勧めします。

► **Kaspersky Security 10.1 for Windows Server ログファイルをデフラグするには、次のコマンドを実行します:**

```
KAVSHELL VACUUM
```

コマンドは、ローカル管理者アカウント権限で開始した場合に実行可能です。

iSwift ベースのクリーニング:KAVSHELL FBRESET

Kaspersky Security 10.1 for Windows Server では iSwift テクノロジーが使用されており、前回のスキャン以降に変更されていないファイルがスキャンされないようにすることができます(**iSwift テクノロジーを使用する**)。

ディレクトリ %SYSTEMDRIVE%¥System Volume Information にファイル fidbox.dat が作成されます。これらのファイルには、スキャン済みのクリーンなオブジェクトに関する情報が含まれます。ファイル fidbox.dat のサイズは、スキャン済みのファイル数が増えるにつれて大きくなります。ファイルには、システムに存在するファイルに関する現在の情報のみが含まれます。ファイルが削除されると、fidbox.dat からそのファイルに関する情報が消去されます。

ファイルをクリーンアップするには、コマンド KAVSHELL FBRESET を使用します。

KAVSHELL FBRESET コマンドを使用する場合は、次の特性にご注意ください:

- KAVSHELL FBRESET コマンドを使用してファイル fidbox.dat をクリーニングする場合、(fidbox.dat の手動削除の場合とは異なり)保護が一時停止されることはありません。
- fidbox.dat のデータがクリアされると、サーバーの負荷が増える場合があります。この場合は fidbox.dat のクリア後に初めてアクセスされたファイルがすべてスキャンされます。スキャン後に、スキャン済みの各オブジェクトに関する情報が fidbox.dat に再度追加されます。オブジェクトに新しくアクセスしようとすると、iSwift テクノロジーによって、変更のないファイルは再スキャンされません。

> KAVSHELL FBRESET コマンドは、コマンドラインが SYSTEM アカウントで開始された場合のみ実行できます。

ダンプファイル作成の有効化と無効化:KAVSHELL DUMP

KAVSHELL DUMP コマンドを使用すると、異常終了が発生した場合における Kaspersky Security 10.1 for Windows Server プロセスのスナップショット(ダンプファイル)の作成を有効化または無効化できます(以下の表を参照)。また、進行中の Kaspersky Security 10.1 for Windows Server プロセスのメモリスナップショットをいつでも追加で作成できます。

> ダンプファイルが正常に作成されるようにするには、KAVSHELL DUMP コマンドをローカルシステムアカウント(SYSTEM)で実行する必要があります。

KAVSHELL DUMP コマンドの構文

KAVSHELL DUMP </ON /F:<ダンプファイルのフォルダー>|/SNAPSHOT /F:<ダンプファイルのフォルダー> / P:<PID> | /OFF>

KAVSHELL DUMP コマンドの例

► **ダンプファイルの作成を有効にするには、ダンプファイルをフォルダー C:¥Dump Folder に保存して次のコマンドを実行します:**

```
KAVSHELL DUMP /ON /F:" C:¥Dump Folder"
```

► **ID 1234 のプロセスのダンプを C:/Dumps フォルダーに作成するには、次のコマンドを実行します:**

```
KAVSHELL DUMP /SNAPSHOT /F: C:¥Dumps /P:1234
```

► **ダンプファイルの生成を無効にするには、次のコマンドを実行します:**

```
KAVSHELL DUMP /OFF
```

表 56. KAVSHELL DUMP コマンドのキー

ライセンス	説明
/ON	異常終了が発生した場合の、プロセスのメモリダンプファイル作成を有効にします。
/F:<ダンプファイルを保存するフォルダーのパス>	これは必須のキーです。このキーで、ダンプファイルを保存するフォルダーのパスを指定します。存在しないフォルダーのパスを指定すると、ダンプファイルは作成されません。ネットワークパスを UNC(汎用命名規則)フォーマットで使用できますが、保護対象のサーバーのネットワークドライブ上のフォルダーのパスは指定できません。 メモリダンプファイルを保存するフォルダーのパスを指定するときにシステム環境変数を使用できます。ユーザー環境変数は使用できません。
/SNAPSHOT	進行中の指定の Kaspersky Security 10.1 for Windows Server プロセスのメモリスナップショットを作成して、キー /F でパスを指定したフォルダーにダンプファイルを保存します。
/P	PID プロセス識別子が Microsoft Windows タスクマネージャーに表示されます。
/OFF	異常終了が発生した場合の、メモリのダンプファイル作成を無効にします。

KAVSHELL DUMP コマンドのリターンコード(481 ページのセクション「KAVSHELL DUMP コマンドのリター

ンコード」を参照）。

設定のインポート：KAVSHELL IMPORT

KAVSHELL IMPORT コマンドを使用すると、Kaspersky Security 10.1 for Windows Server の設定、機能、およびタスクを設定ファイルから保護対象のサーバーの Kaspersky Security 10.1 for Windows Server のコピーにインポートできます。設定ファイルを作成するには、KAVSHELL EXPORT コマンドを使用します。

> コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] キーを使用します。

KAVSHELL IMPORT コマンドの構文

KAVSHELL IMPORT <設定ファイルの名前とファイルのパス>

KAVSHELL IMPORT コマンドの例

KAVSHELL IMPORT Host1.xml

表 57. KAVSHELL IMPORT コマンドのキー

ライセンス	説明
<設定ファイルの名前とファイルのパス>	設定のインポート元として使用する設定ファイルの名前。 ファイルのパスを指定するときにシステム環境変数を使用できます。ユーザー環境変数は使用できません。

KAVSHELL IMPORT コマンドのリターンコード（481 ページのセクション「KAVSHELL IMPORT コマンドのリターンコード」を参照）。

設定のエクスポート：KAVSHELL EXPORT

KAVSHELL EXPORT コマンドを使用すると、他のサーバーにインストールされた Kaspersky Security 10.1 for Windows Server のコピーに後でインポートするために、Kaspersky Security 10.1 for Windows Server のすべての設定と現在のタスクを設定ファイルにエクスポートできます。

KAVSHELL EXPORT コマンドの構文

KAVSHELL EXPORT <設定ファイルの名前とファイルのパス>

KAVSHELL EXPORT コマンドの例

KAVSHELL EXPORT Host1.xml

表 58. KAVSHELL EXPORT コマンドのキー

ライセンス	説明
<設定ファイルの名前とファイルのパス>	設定が含まれる設定ファイルの名前。 設定ファイルに任意の拡張子を指定できます。 ファイルのパスを指定するときにシステム環境変数を使用できます。ユーザー環境変数は使用できません。

KAVSHELL EXPORT コマンドのリターンコード（483 ページのセクション「KAVSHELL EXPORT コマンドのリターンコード」を参照）。

MS Operations Management Suite との統合：KAVSHELL OMSINFO

KAVSHELL OMSINFO コマンドを使用すると、製品のステータスや、定義データベースおよび KSN サービスによって検知された脅威に関する情報を確認できます。脅威に関するデータは、使用可能なイベントログから取得されます。

KAVSHELL OMSINFO コマンドの構文

```
KAVSHELL OMSINFO <生成されるファイルの完全パスとファイル名>
```

KAVSHELL OMSINFO コマンドの例

```
KAVSHELL OMSINFO C:¥Users¥Admin¥Desktop¥omsinfo.json
```

表 59. KAVSHELL OMSINFO コマンドのキー

ライセンス	説明
<生成されるファイルのパスとファイル名>	製品のステータスと検知された脅威に関する情報が含まれる、生成されるファイルの名前。

コマンドラインのリターンコード

このセクションの内容

KAVSHELL START および KAVSHELL STOP コマンドのリターンコード

表 60. KAVSHELL START および KAVSHELL STOP コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-3	権限エラー
-5	コマンド構文が無効である
-6	操作が無効である（Kaspersky Security サービスがすでに実行されている、すでに停止されているなど）
-7	サービスが登録されていない
-8	サービスの自動スタートアップが無効
-9	別のユーザーアカウントでのコンピューターの起動に失敗した（既定では、Kaspersky Security サービスはローカルシステムユーザーアカウントで実行されます）
-99	不明なエラー

KAVSHELL SCAN および KAVSHELL SCANCRITICAL コマンドのリターンコード

表 61. KAVSHELL SCAN および KAVSHELL SCANCRITICAL コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した(脅威が検知されなかった)
1	操作がキャンセルされた
-2	サービスが実行されていない
-3	権限エラー
-4	オブジェクトが見つからない(スキャン範囲のリストを含むファイルが見つからない)
-5	コマンド構文が無効であるか、スキャン範囲が定義されていない
-80	感染したオブジェクトとその他のオブジェクトが検知された
-81	感染の可能性があるオブジェクトの検知
-82	処理エラーが検知された
-83	チェックされていないオブジェクトが検知された
-84	破損したオブジェクトが検知された
-85	タスク実行ログの作成が失敗した
-99	不明なエラー
-301	ライセンスが無効である

KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード

表 62. KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-6	操作が無効である（Kaspersky Security サービスがすでに実行されている、すでに停止されているなど）
402	タスクがすでに実行されている（修飾子 /STATE の場合）

KAVSHELL TASK コマンドのリターンコード

表 63. KAVSHELL TASK コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー
-4	オブジェクトが見つからない(タスクが見つからない)
-5	コマンド構文が無効である
-6	操作が無効である(タスクが実行されていない、すでに実行されている、一時停止できないなど)
-99	不明なエラー
-301	ライセンスが無効である
401	タスクが実行されていない(修飾子 /STATE の場合)
402	タスクがすでに実行されている(修飾子 /STATE の場合)
403	タスクがすでに一時停止されている(修飾子 /STATE の場合)
-404	操作の実行でエラーが発生した(タスクステータスの変更によりタスクがクラッシュした)

KAVSHELL RTP コマンドのリターンコード

表 64. KAVSHELL RTP コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー
-4	オブジェクトが見つからない(リアルタイム保護タスクの 1 つまたはすべてのリアルタイム保護タスクが見つからない)
-5	コマンド構文が無効である
-6	操作が無効である(タスクがすでに実行されている、すでに停止されているなど)
-99	不明なエラー
-301	ライセンスが無効である

KAVSHELL UPDATE コマンドのリターンコード

表 65. KAVSHELL UPDATE コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
200	すべてのオブジェクトが最新である（定義データベースまたはプログラムのコンポーネントが最新である）
-2	サービスが実行されていない
-3	権限エラー
-5	コマンド構文が無効である
-99	不明なエラー
-206	拡張ファイルが指定されたアップデート元にないか、不明な形式である
-209	アップデート元への接続エラー
-232	プロキシサーバーへの接続時の認証エラー
-234	Kaspersky Security Center への接続エラー
-235	アップデート元への接続時に Kaspersky Security 10.1 for Windows Server が認証されなかった
-236	定義データベースが破損した
-301	ライセンスが無効である

KAVSHELL ROLLBACK コマンドのリターンコード

表 66. KAVSHELL ROLLBACK コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー
-99	不明なエラー
-221	定義データベースのバックアップコピーが見つからないか、破損している
-222	定義データベースのバックアップコピーが破損している

KAVSHELL LICENSE コマンドのリターンコード

表 67. KAVSHELL LICENSE コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	ライセンスを管理する権限が不十分である
-4	指定した番号のライセンスが見つからない
-5	コマンド構文が無効である
-6	操作が無効である(ライセンスがすでに追加されている)
-99	不明なエラー
-301	ライセンスが無効である
-303	別のアプリケーション用のライセンスである

KAVSHELL TRACE コマンドのリターンコード

表 68. KAVSHELL TRACE コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない

リターンコード	説明
-3	権限エラー
-4	オブジェクトが見つからない（追跡ログフォルダーへのパスとして指定されたパスが見つからない）
-5	コマンド構文が無効である
-6	操作が無効である（トレースログの作成がすでに無効化されている場合に KAVSHELL TRACE /OFF コマンドの実行が試みられた）
-99	不明なエラー

KAVSHELL FBRESET コマンドのリターンコード

表 69. KAVSHELL FBRESET コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-99	不明なエラー

KAVSHELL DUMP コマンドのリターンコード

表 70. KAVSHELL DUMP コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー
-4	オブジェクトが見つからない(ダンプファイルフォルダーへのパスとして指定されたパスが見つからない、指定した PID のプロセスが見つからない)
-5	コマンド構文が無効である
-6	操作が無効である(ダンプファイルの作成がすでに無効化されている場合に KAVSHELL DUMP/OFF コマンドの実行が試みられた)
-99	不明なエラー

KAVSHELL IMPORT コマンドのリターンコード

表 71. KAVSHELL IMPORT コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー

リターンコード	説明
-4	オブジェクトが見つからない（インポートできる設定ファイルが見つからない）
-5	構文が無効である
-99	不明なエラー
501	操作は正常に完了したが、コマンド実行時にエラー / コメントが発生した（たとえば、いくつかの機能コンポーネントのパラメータがインポートされなかった）
-502	インポート対象のファイルがないか、認識できない形式である
-503	設定に互換性がない（異なるプログラムまたは互換性のない Kaspersky Security 10.1 for Windows Server 上位バージョンからエクスポートされた設定ファイル）

KAVSHELL EXPORT コマンドのリターンコード

表 72. KAVSHELL EXPORT コマンドのリターンコード

リターンコード	説明
0	操作が正常に完了した
-2	サービスが実行されていない
-3	権限エラー
-5	構文が無効である
-10	設定ファイルを作成できない（たとえば、ファイルパスで指定されたフォルダーにアクセスできない）
-99	不明なエラー
501	操作は正常に完了したが、コマンド実行時にエラー / コメントが発生した（たとえば、いくつかの機能コンポーネントのパラメータがエクスポートされなかった）

監視パフォーマンス Kaspersky Security 10.1 for Windows Server のカウンター

このセクションでは、Kaspersky Security 10.1 for Windows Server のカウンター：システム監視用パフォーマンスカウンター、SNMP カウンターとトラップに関する情報について説明します。

この章の内容

システム監視用パフォーマンスカウンター

このセクションでは、インストールの際に Kaspersky Security 10.1 for Windows Server によって登録される Microsoft Windows システム監視用のパフォーマンスカウンターについて説明します。

このセクションの内容

Kaspersky Security 10.1 for Windows Server の SNMP カウンターについて

既定では、**パフォーマンスカウンター**は、インストールされた Kaspersky Security 10.1 for Windows Server のコンポーネントに含まれます。インストールの際、Kaspersky Security 10.1 for Windows Server 独自の Microsoft Windows システム監視用パフォーマンスカウンターが登録されます。

Kaspersky Security 10.1 for Windows Server のカウンターを使用すれば、リアルタイム保護タスクの実行中に製品のパフォーマンスを監視できます。他のアプリケーションとともに実行している際の問題箇所やリソース不足について解析できます。また、Kaspersky Security 10.1 for Windows Server の推奨されない設定や運用中のクラッシュについて診断できます。

Kaspersky Security 10.1 for Windows Server パフォーマンスカウンターを参照するには、Windows のコント

ロール パネルの[**管理ツール**]にある[**パフォーマンス**]コンソールを開きます。

以下のセクションで、カウンターの定義、推奨読み取り間隔、しきい値、カウンター値がしきい値を超えた場合の Kaspersky Security 10.1 for Windows Server 設定の推奨事項について示します。

拒否された要求の合計数

表 73. 拒否された要求の合計数

名前	拒否された要求の合計数
定義	ファイルインターセプションドライバーからのオブジェクト処理要求のうち、アプリケーションプロセスによって受け入れられなかった要求の合計数。この数は、Kaspersky Security 10.1 for Windows Server が最後に起動された時点からカウントされます。 Kaspersky Security 10.1 for Windows Server のプロセスによって処理の要求が拒否されたオブジェクトをスキップします。
目的	このカウンターの値により、次の状況を検出できます: • Kaspersky Security 10.1 for Windows Server の処理対象プロセスが停止することによるリアルタイム保護の品質低下 • ファイルインターセプションディスパッチャの障害発生によるリアルタイム保護の中断
標準値 / しきい値	0 / 1

推奨読み取り間隔	1 時間
値がしきい値を超えた場合の設定の推奨事項	拒否された処理要求の数は、スキップされたオブジェクトの数に対応します。 カウンターの動作によって、次のいずれかの状況になっている可能性があります: • カウンターに、長時間拒否されているいくつかの要求が表示されます:Kaspersky Security 10.1 for Windows Server のすべてのプロセスが完全に読み込まれるため、Kaspersky Security 10.1 for Windows Server はオブジェクトをスキャンできませんでした。 オブジェクトのスキップを防ぐには、リアルタイム保護タスク用のアプリケーションプロセスの数を増やしてください。[**実行中プロセスの最大数**]、[**リアルタイム保護の対象プロセスの数**]などの Kaspersky Security 10.1 for Windows Server の設定を使用できます。 • 拒否された要求の数が重大レベルのしきい値を上回り、急増している場合は、ファイルインターセプションディスパッチャがクラッシュしている。Kaspersky Security 10.1 for Windows Server はアクセス時にオブジェクトをスキャンしません。 Kaspersky Security 10.1 for Windows Server の再起動

スキップされた要求の合計数

表 74.　スキップされた要求の合計数

名前	スキップされた要求の合計数
定義	Kaspersky Security 10.1 for Windows Server が受け取ったが処理完了のイベントを生成しなかったオブジェクトを処理する、ファイルインターセプションドライバーからの要求の合計数。この数は、アプリケーションが最後に起動された時点からカウントされます。 処理対象プロセスのいずれかが承認したこのようなオブジェクト処理要求によって処理完了のイベントが送信されなかった場合、ドライバーがその要求を別のプロセスに転送し、**スキップされた要求の合計数**カウンターの値が 1 つ加算されます。ドライバーがすべての処理対象プロセスに要求を転送し、どのプロセスも処理要求を受け取らなかったか（ビジー）、どのプロセスも処理完了のイベントを送信しなかった場合、Kaspersky Security 10.1 for Windows Server はこのオブジェクトをスキップし、**スキップされた要求の合計数**カウンターの値が 1 つ加算されます。
目的	このカウンターの値により、ファイルインターセプションディスパッチャのエラーによるパフォーマンスの低下を検出できます。
標準値 / しきい値	0 / 1
推奨読み取り間隔	1 時間
値がしきい値を超えた場合の設定の推奨事項	カウンターの値がゼロ以外の場合は、1 つまたは複数のファイルインターセプションディスパッチャストリームがフリーズしてダウンしていることを意味します。このカウンターの値は、現在ダウンしているストリームの数に対応します。 スキャン速度が十分でない場合は、Kaspersky Security 10.1 for Windows Server を再起動してオフラインストリームを復元してください。

システムリソースの不足が原因で処理されなかった要求の数

表 75. システムリソースの不足が原因で処理されなかった要求の数

名前	リソースの不足が原因で処理されなかった要求の数
定義	システムリソース（RAM など）が不足しているため処理されなかったファイルインターセプションドライバーからの要求の合計数。この数は、Kaspersky Security 10.1 for Windows Server が最後に起動された時点からカウントされます。 Kaspersky Security 10.1 for Windows Server は、ファイルインターセプションドライバーによって処理されていないオブジェクト処理要求をスキップします。
目的	このカウンターは、システムリソースの不足が原因で発生する、リアルタイム保護の品質低下の可能性を検出して除去するために使用できます。
標準値 / しきい値	0 / 1
推奨読み取り間隔	1 時間
値がしきい値を超えた場合の設定の推奨事項	カウンターの値がゼロ以外の場合は、Kaspersky Security 10.1 for Windows Server 処理対象プロセスが要求を処理するために、より多くの RAM を必要としています。 他のアプリケーションの実行中プロセスが利用可能な RAM をすべて使用している可能性があります。

処理のために送信された要求の数

表 76.　処理のために送信された要求の数

名前	処理のために送信された要求の数
定義	処理対象プロセスによる処理を待っているオブジェクトの数。
目的	このカウンターは、Kaspersky Security 10.1 for Windows Server 処理対象プロセスの負荷およびサーバー上のファイル動作の全体的なレベルを追跡するために使用できます。
標準値 / しきい値	このカウンターの値は、サーバー上のファイル動作のレベルによって変化します。
推奨読み取り間隔	1 分
値がしきい値を超えた場合の設定の推奨事項	なし

ファイルインターセプションディスパッチャスレッドの平均数

表 77. ファイルインターセプションディスパッチャスレッドの平均数

名前	ファイルインターセプションディスパッチャストリームの平均数
定義	1 つのプロセス内のファイルインターセプションディスパッチャストリームの数、およびリアルタイム保護タスクに現在関わっているすべてのプロセスの平均値。
目的	このカウンターは、Kaspersky Security 10.1 for Windows Server プロセスでの過負荷が原因で発生する、リアルタイム保護の品質低下の可能性を検出して除去するために使用できます。
標準値 / しきい値	可変 / 40
推奨読み取り間隔	1 分
値がしきい値を超えた場合の設定の推奨事項	各処理対象プロセスで最大 60 のファイルインターセプションディスパッチャストリームを作成できます。このカウンターの値が 60 に近い場合、いずれの処理対象プロセスも、現在のキューにあるファイルインターセプションドライバーからの次の要求を処理できず、Kaspersky Security 10.1 for Windows Server がそのオブジェクトをスキップする危険性があります。 リアルタイム保護タスク用の Kaspersky Security 10.1 for Windows Server プロセスの数を増やしてください。[**実行中プロセスの最大数**]、[**リアルタイム保護の対象プロセスの数**]などの Kaspersky Security 10.1 for Windows Server の設定を使用できます。

ファイルインターセプションディスパッチャスレッドの最大数

表 78. ファイルインターセプションディスパッチャスレッドの最大数

名前	ファイルインターセプションディスパッチャストリームの最大数
定義	1 つのプロセス内のファイルインターセプションディスパッチャストリームの数、およびリアルタイム保護タスクに現在関わっているすべてのプロセスの最大値。
目的	このカウンターの値により、実行中のプロセスでの不均等な負荷分散を原因としたパフォーマンス低下を検出して除去できます。
標準値 / しきい値	可変 / 40
推奨読み取り間隔	1 分
値がしきい値を超えた場合の設定の推奨事項	このカウンターの値が下記の**ファイルインターセプションディスパッチャストリームの平均数**カウンターの値を継続的に大きく上回る場合は、Kaspersky Security 10.1 for Windows Server の実行中プロセスへの負荷分散が不均等になっています。 Kaspersky Security 10.1 for Windows Server の再起動

感染したオブジェクトのキュー内にある項目数

表 79. 感染したオブジェクトのキュー内にある項目数

名前	感染したオブジェクトのキュー内にある項目数。
定義	現在処理(駆除または削除)を待っている感染したオブジェクトの数。
目的	このカウンターの値により、次の状況を検出できます: • ファイルインターセプションディスパッチャの障害発生の可能性によるリアルタイム保護の中断 • 異なる処理対象プロセスと Kaspersky Security 10.1 for Windows Server 間のプロセッサ時間の配分が不均等であるために処理が過負荷状態であること • ウイルスアウトブレイク
標準値 / しきい値	この値は、Kaspersky Security 10.1 for Windows Server が感染したオブジェクトまたは感染の可能性があるオブジェクトを処理している間はゼロ以外の値を返し、その処理が終了した後はゼロを返します。ゼロ以外の値が返される状況が長時間続きます。
推奨読み取り間隔	1 分

値がしきい値を超えた場合の設定の推奨事項	ゼロ以外のカウンターの値が返される状況が長時間続く場合: • Kaspersky Security 10.1 for Windows Server はオブジェクトを処理していない（ファイルインターセプションディスパッチャがクラッシュした可能性がある）。 Kaspersky Security 10.1 for Windows Server の再起動 • オブジェクトを処理するためのプロセッサ時間が不十分である。 Kaspersky Security 10.1 for Windows Server に追加のプロセッサ時間が割り当てられるようにしてください（コンピューター上の他のアプリケーションの負荷を減らすなど）。 • ウイルスアウトブレイクが発生した。 ファイルのリアルタイム保護タスクで多数の感染したオブジェクトまたは感染の可能性があるオブジェクトが発生している場合も、ウイルスアウトブレイクの兆候を示しています。タスク統計または実行ログで検知されたオブジェクト数に関する情報を表示できます。

1 秒あたりの処理オブジェクト数

表 80. 1 秒あたりの処理オブジェクト数

名前	1 秒あたりの処理オブジェクト数。
定義	処理されたオブジェクト数を、オブジェクトの処理にかかった時間で割った数（等しい時間間隔で計算します）。
目的	このカウンターはオブジェクトの処理速度を示します。これを使用して、Kaspersky Security 10.1 for Windows Server プロセスに割り当てられたプロセッサ時間が不十分であるか、Kaspersky Security 10.1 for Windows Server の動作エラーによって発生した、サーバーパフォーマンスが低下したポイントを検出して除去できます。
標準値 / しきい値	不定 / なし
推奨読み取り間隔	1 分
値がしきい値を超えた場合の設定の推奨事項	このカウンターの値は、Kaspersky Security 10.1 for Windows Server の設定の値と、サーバー上の他のアプリケーションプロセスの負荷に応じて異なります。 カウンター数の平均レベルを長期的に監視してください。カウンター値の通常のレベルが低下した場合、次のいずれかの状況が考えられます： • Kaspersky Security 10.1 for Windows Server プロセスに、オブジェクトを処理するための十分なプロセッサ時間が割り当てられていない。 Kaspersky Security 10.1 for Windows Server に追加のプロセッサ時間が割り当てられるようにしてください（サーバー上の他のアプリケーションの負荷を減らすなど）。 • Kaspersky Security 10.1 for Windows Server でエラーが発生している（複数のストリームがアイドル状態である）。 Kaspersky Security 10.1 for Windows Server の再起動

Kaspersky Security 10.1 for Windows Server の SNMP カウンターおよびトラップ

このセクションでは、Kaspersky Security 10.1 for Windows Server のカウンターおよびトラップについて説明します。

このセクションの内容

Kaspersky Security 10.1 for Windows Server の SNMP カウンターおよびトラップについて

アンチウイルスコンポーネントセットの **SNMP カウンターおよび SNMP トラップ**をインストールに追加した場合、Simple Network Management Protocol（SNMP）を使用して Kaspersky Security 10.1 for Windows Server のカウンターおよびトラップを参照できます。

管理者のワークステーションから Kaspersky Security 10.1 for Windows Server のカウンターおよびトラップを参照するには、保護対象サーバーで SNMP サービスを開始し、さらに管理者のワークステーションで SNMP サービスおよび SNMP トラップサービスを開始します。

Kaspersky Security 10.1 for Windows Server の SNMP カウンター

このセクションでは Kaspersky Security 10.1 for Windows Server SNMP カウンターの設定の概要を表で説明します。

このセクションの内容

パフォーマンスカウンター

表 81. パフォーマンスカウンター

カウンター	定義
currentRequestsAmount	処理のために送信された要求の数（490 ページを参照）
currentInfectedQueueLength	感染したオブジェクトのキュー内にある項目数（493 ページの「感染したオブジェクトのキュー内にある項目数」を参照）。
currentObjectProcessingRate	1 秒あたりの処理オブジェクト数（495 ページを参照）

カウンター	定義
currentWorkProcessesNumber	Kaspersky Security 10.1 for Windows Server で現在動作中のプロセスの数

隔離カウンター

表 82. 隔離カウンター

カウンター	定義
totalObjects	現在隔離にあるオブジェクトの数
totalSuspiciousObjects	現在隔離にある感染の可能性があるオブジェクトの数
currentStorageSize	隔離内のデータの合計サイズ（MB）

バックアップカウンター

表 83. バックアップカウンター

カウンター	定義
currentBackupStorageSize	バックアップ内のデータの合計サイズ（MB）

標準カウンター

表 84. 標準カウンター

カウンター	定義
lastCriticalAreasScanAge	サーバーの重要な領域の前回の完全スキャンからの「経過時間」(前回の**重要領域のスキャン**タスクが完了してからの経過時間)
licenseExpirationDate	ライセンスの有効期限。現在のライセンスと予備のライセンスまたはアクティベーションコードが追加されている場合、予備のライセンスまたはアクティベーションコードに関連付けられたライセンスの有効期限日が表示されます。
currentApplicationUptime	前回の開始以降の Kaspersky Security 10.1 for Windows Server の実行時間(100 秒単位)
currentFileMonitorTaskStatus	ファイルのリアルタイム保護タスクのステータス:[**オン**] – 実行中、[**オフ**] – 中止または停止。

更新カウンター

表 85. 更新カウンター

カウンター	定義
avBasesAge	定義データベースが作成されてからの「経過時間」(インストールされている前回アップデートされた定義データベースの作成日以降の経過時間(100 秒単位))。

リアルタイム保護カウンター

表 86. リアルタイム保護カウンター

カウンター	定義
totalObjectsProcessed	前回のファイルのリアルタイム保護タスクの実行以降にスキャンされたオブジェクトの合計数
totalInfectedObjectsFound	前回のファイルのリアルタイム保護タスクの実行以降に検知された、感染したオブジェクトとその他のオブジェクトの合計数
totalSuspiciousObjectsFound	前回のファイルのリアルタイム保護タスクの実行以降に検知された、感染の可能性があるオブジェクトの合計数
totalVirusesFound	前回のファイルのリアルタイム保護タスクの実行以降に検知されたオブジェクトの合計数
totalObjectsQuarantined	感染したオブジェクト、感染の可能性があるオブジェクト、および隔離に入れられたその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsNotQuarantined	感染した、または感染の可能性があり、隔離しようとしたができなかったオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsDisinfected	感染しており、駆除されたオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsNotDisinfected	駆除しようとしたができなかった、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsDeleted	駆除が成功した、感染したオブジェクト、感染の可能性があるオブジェクト、およびその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算

カウンター	定義
totalObjectsNotDeleted	駆除しようとしたができなかった、感染したオブジェクト、感染の可能性があるオブジェクト、およびその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsBackedUp	バックアップに入れられた、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算
totalObjectsNotBackedUp	バックアップに入れようとしたができなかった、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算

SNMP トラップ

Kaspersky Security 10.1 for Windows Server の SNMP トラップ設定について、次の表に概要を示します。

表 87. Kaspersky Security 10.1 for Windows Server の SNMP トラップ

トラップ	説明	オプション
eventThreatDetected	オブジェクトが検知されました。	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

トラップ	説明	オプション
eventBackupStorageSizeExceeds	バックアップの最大サイズを超過しました。バックアップ内のデータの合計サイズが［**バックアップの最大サイズ（MB）**］で指定した値を超過しました。感染したオブジェクトのバックアップを継続します。	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	バックアップの空き容量がしきい値に達しました。［**空き容量のし**	eventDateAndTime eventSeverity eventSource

トラップ	説明	オプション
	きい値（MB）]で割り当てられたバックアップ内の空き容量が指定された値以下になりました。感染したオブジェクトのバックアップを継続します。	

トラップ	説明	オプション
eventQuarantineStorageSizeExceeds	隔離の最大サイズを超過しました。隔離フォルダー内のデータの合計サイズが[**隔離の最大サイズ（MB）**]で指定した値を超過しました。感染の可能性があるオブジェクトの隔離を継続します。	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	隔離の空き容量がしきい値に達しました。[**空き容量のしきい値（MB）**]で	eventDateAndTime eventSeverity eventSource

トラップ	説明	オプション
	割り当てられた隔離内の空き容量が指定された値以下になりました。感染の可能性があるオブジェクトの隔離を継続します。	
eventObjectNotQuarantined	隔離中にエラーが発生しました。	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason

トラップ	説明	オプション
eventObjectNotBackuped	バックアップ保管領域でのオブジェクトコピーの保存中にエラーが発生しました。	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	隔離中にエラーが発生しました。	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	バックアップでエラーが発生しました。	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	定義データベースがアップデートされていません。前回の定義データベースの	eventSeverity eventDateAndTime eventSource days

トラップ	説明	オプション
	アップデートタスク(ローカルタスク、グループタスク、または特定のコンピューターに対するタスク)が実行されてから経過した日数が計算されています。	

トラップ	説明	オプション
eventAVBasesTotallyOutdated	定義データベースが長期間アップデートされていません。前回の定義データベースのアップデートタスク（ローカルタスク、グループタスク、または特定のコンピューターに対するタスク）が実行されてから経過した日数が計算されています。	eventSeverity eventDateAndTime eventSource days

トラップ	説明	オプション
eventApplicationStarted	Kaspersky Security 10.1 for Windows Server が実行中です。	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security 10.1 for Windows Server が停止しました。	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	重要領域が長期間スキャンされていません。前回の**重要**領域のスキャンタスクが実行されてから経過した日数として計算されます。	eventSeverity eventDateAndTime eventSource days

トラップ	説明	オプション
eventLicenseHasExpired	ライセンスの有効期間が終了しました	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	ライセンスの有効期間がまもなく終了します。ライセンスの有効期限までの日数として計算されます。	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	タスクの実行中にエラーが発生しました。	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	アップデートタスクの実行中にエラーが発生しまし	eventSeverity eventDateAndTime taskName updaterErrorEventReason

トラップ	説明	オプション
	た。	

次の表では、トラップの設定と設定可能なパラメータ値について説明します。

表 88. SNMP トラップ：設定の値

設定	説明と設定可能な値
eventDateAndTime	イベントの時刻。
eventSeverity	重要度この設定では、次の値が使用されます： • critical (1) - 重要。 • warning (2) - 警告。 • info (3) - 情報。
userName	ユーザー名（例：感染したファイルにアクセスしようとしたユーザーの名前）。
computerName	サーバー名（例：感染したファイルにアクセスしようとしたユーザーのサーバーの名前）。

設定	説明と設定可能な値
eventSource	イベント送信元：イベントが生成された機能コンポーネント。この設定では、次の値が使用されます： • unknown (0) - 不明な機能コンポーネント。 • quarantine (1) - 隔離。 • backup (2) - バックアップ。 • reporting (3) - 実行ログ。 • updates (4) - アップデート。 • realTimeProtection (5) - ファイルのリアルタイム保護。 • onDemandScanning (6) - オンデマンドスキャン。 • product (7) - 個々のコンポーネントの操作ではなく Kaspersky Security 10.1 for Windows Server 全体の操作に関連するイベント。 • systemAudit (8) - システム監査ログ。
eventReason	イベントトリガー：イベントを引き起こすもの。この設定では、次の値が使用されます： • reasonUnknown(0) - 不明な理由。 • reasonInvalidSettings (1) - バックアップイベントと隔離イベントのみ。隔離またはバックアップが利用できない場合に表示される（アクセス権限が不十分か、ネットワークパスが指定されているなど、隔離設定でのフォルダー指定に誤りがある）。この場合、既定のバックアップフォルダーまたは隔離フォルダーが使用される。

設定	説明と設定可能な値
objectName	オブジェクト名（例：ウイルスが検知されたファイルの名前）。
threatName	ウイルス百科事典の分類に基づいたオブジェクトの名前。この名前は、オブジェクトの検知時に Kaspersky Security 10.1 for Windows Server によって返される、検知されたオブジェクトの名前に含まれます。実行ログで、検知されたオブジェクトのフルネームを表示できます（257 ページの「ログの設定」を参照）。
detectType	検知したオブジェクトの種別。 この設定では、次の値が使用されます： • undefined (0) - 未定義。 • virware - 古典的なウイルスおよびネットワークワーム。 • trojware - トロイの木馬。 • malware - その他の悪意のあるプログラム。 • adware - 広告目的のソフトウェア。 • pornware - アダルトソフトウェア。 • riskware：ユーザーのコンピューターまたはデータを損傷させるために侵入者が使用している可能性がある合法的なアプリケーション。

設定	説明と設定可能な値
detectCertainty	脅威検知の信憑性。この設定では、次の値が使用されます: • Suspicion（感染の可能性あり） - Kaspersky Security 10.1 for Windows Server により、オブジェクトコードのセクションと既知の悪意のあるコードのセクションの部分一致が検知されている。 • Sure（感染） - Kaspersky Security 10.1 for Windows Server により、オブジェクトコードのセクションと既知の悪意のあるコードのセクションの部分一致が検知されている。
days	日数（例:ライセンスの有効期限までの日数）。
errorCode	エラーコード。
knowledgeBaseId	ナレッジベースの記事のアドレス（例:特定のエラーについて説明している記事のアドレス）。
taskName	タスク名:
updaterErrorEventReason	アップデートエラーの理由。この設定では、次の値が使用されます: • reasonUnknown(0) - 不明な理由。 • reasonAccessDenied - アクセスが拒否された。 • reasonUrlsExhausted - アップデート元リストにあるどのアップデート元にも接続できなかった。 • reasonInvalidConfig - 設定ファイルが無効。 • reasonInvalidSignature - 署名が無効。 • reasonCantCreateFolder - フォルダーを作成できない。

設定	説明と設定可能な値
	• reasonFileOperError - ファイルのエラー。 • reasonDataCorrupted - オブジェクトが破損している。 • reasonConnectionReset - 接続がリセットされた。 • reasonTimeOut - 接続がタイムアウトした。 • reasonProxyAuthError - プロキシの認証エラー。 • reasonServerAuthError - サーバーの認証エラー。 • reasonHostNotFound - コンピューターが見つからない。 • reasonServerBusy - サーバーを使用できない。 • reasonConnectionError - 接続エラー。 • reasonModuleNotFound - オブジェクトが見つからない。 • reasonBlstCheckFailed(16) - ライセンス情報のブラックリストを確認中にエラーが発生した。アップデート時点でデータベースのアップデートが公開中であった可能性があります。数分後に再度アップデートを実行してください。

設定	説明と設定可能な値
storageObjectNotAddedEventReason	オブジェクトのバックアップまたは隔離が実行されなかった理由。この設定では、次の値が使用されます: • reasonUnknown(0) - 不明な理由。 • reasonStorageInternalError - データベースのエラー。Kaspersky Security 10.1 for Windows Server を復元してください。 • reasonStorageReadOnly - データベースが読み取り専用になっている。Kaspersky Security 10.1 for Windows Server を復元してください。 • reasonStorageIOError - 入力-出力エラー:a) Kaspersky Security 10.1 for Windows Server が破損している。Kaspersky Security 10.1 for Windows Server を復元してください。b) Kaspersky Security 10.1 for Windows Server ファイルのディスクが破損している。 • reasonStorageCorrupted - ストレージが破損している。Kaspersky Security 10.1 for Windows Server を復元してください。 • reasonStorageFull - データベースの空き容量がない。空きディスク容量を確保してください。 • reasonStorageOpenError - データベースファイルを開けない。Kaspersky Security 10.1 for Windows Server を復元してください。 • reasonStorageOSFeatureError - 一部のオペレーティングシステム機能が Kaspersky Security 10.1 for Windows Server の要件を満たしていない。

設定	説明と設定可能な値
	• reasonObjectNotFound - 隔離に配置しようとしたオブジェクトがディスク上に存在しない。 • reasonObjectAccessError - Backup API を使用する十分な権限がない。操作を行うために使用されているアカウントには、Backup Operator 権限がありません。 • reasonDiskOutOfSpace - ディスクの空き容量が不十分。

テクニカルサポートへのお問い合わせ

このセクションでは、テクニカルサポートを受ける方法と利用条件について説明します。

この章の内容

テクニカルサポートの利用方法

製品のガイドや製品に関する情報源で問題の解決法が見つからない場合は、テクニカルサポートにお問い合わせください。テクニカルサポートの担当者が、製品のインストール方法または使用方法についての質問に答えます。

テクニカルサポートは、製品版ライセンスを購入したお客様のみが利用できます。試用版のお客様は、テクニカルサポートを利用できません。

テクニカルサポートにご連絡いただく前に、「サポートサービス規約」をお読みください。

カスペルスキーカンパニーアカウントからの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（https://companyaccount.kaspersky.com）は、カスペルスキー製品をご利用の企業向けのポータルです。カスペルスキーカンパニーアカウントによって、ユーザーとカスペルスキーの担当者が、オンライン依頼によってスムーズにやり取りできます。カスペルスキーカンパニーアカウントによって、カスペルスキーの担当者によるオンライン依頼の処理の進捗を監視したり、オンライン依頼の履歴を保存したり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の 1 つのユーザーアカウントで、組織のすべての従業員を登録できます。カスペルスキーカンパニーアカウントを使えば、1 つのアカウントで、登録した従業員からカスペルスキーへのオンライン依頼や、これらの従業員の権限を一元的に管理できます。

カスペルスキーカンパニーアカウントは、次の言語で使用できます：

- 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の詳細については、テクニカルサポートサイト

（http://support.kaspersky.co.jp/faq/companyaccount_help）を参照してください。

トレースファイルと AVZ スクリプトの使用

Kaspersky Lab テクニカルサポートの担当者に問題を報告した後に、担当者から Kaspersky Security 10.1 for Windows Server の操作に関する情報が含まれるレポートの生成と送信をお願いする場合があります。また、トレースファイルの作成をお願いする場合もあります。トレースファイルによって、アプリケーションコマンドの実行プロセスを段階的に追跡し、どの操作段階でエラーが発生したかを特定できます。

カスペルスキーのテクニカルサポートの担当者は、送信されたデータを分析し、AVZ スクリプトを作成してユーザーに送信できます。AVZ スクリプトによって、脅威のアクティブなプロセスの分析、コンピューターの脅威のスキャン、感染したファイルの駆除や削除、システムスキャンレポートの作成を行うことができます。

アプリケーションの問題について、効率的なサポートとトラブルシューティングを提供するために、テクニカルサポートが診断中のデバック目的で、アプリケーションの設定を一時的に変更するようお願いすることがあります。このとき、次の操作を求められることがあります：

- 詳細な診断情報を処理し保存する機能を有効化します。
- 各ソフトウェアコンポーネントの設定を調整します。これは、標準のユーザーインターフェイス項目では使用できません。
- 処理された診断情報の保存と送信の設定を変更します。
- インターセプションを設定してネットワークトラフィックを記録します。

AO Kaspersky Lab

Kaspersky Lab は、ウイルス、マルウェア、迷惑メール（スパム）、ネットワーク攻撃、ハッキング攻撃などのデジタル脅威からコンピューターを保護するシステムの開発企業として、世界各国で高く評価されています。

2008 年、Kaspersky Lab は、エンドユーザー向け情報セキュリティソフトウェアのソリューション開発元として、世界第 4 位に選ばれました（2008 年 IDC『Worldwide Endpoint Security Revenue by Vendor』）。Kaspersky Lab は、コンピューター保護システムの開発企業として、ロシアの個人ユーザーから高い支持を受けています（IDC Endpoint Tracker 2014）。

Kaspersky Lab は 1997 年にロシアで設立され、現在では、33 か国に 38 の事業所を構える国際的なグループ企業となっており、3,000 名を超える高度な技術を有するエキスパートが働いています。

製品：カスペルスキー製品は、スマートフォンから家庭用 PC、大規模な企業ネットワークにいたるまで、すべてのシステムを保護します。

個人向けセキュリティ製品は、デスクトップパソコン、ノート型パソコン、タブレット PC、スマートフォンなどのモバイル端末に対応します。

また、ワークステーションやモバイル端末、仮想マシン、ファイルサーバー、Web サーバー、メールゲートウェイ、ファイアウォールなどのソリューションやテクノロジーに対する保護と管理を提供しています。カスペルスキーのポートフォリオには、DDoS 攻撃に対する保護、産業用制御システムの保護、金銭をねらう詐欺の防止に特化した製品も提供しています。一元管理ツールと組み合わせて使用するこれらのソリューションは、コンピューターに対する脅威から、あらゆる規模の企業や組織を効率的に保護する手段となります。カスペルスキー製品は、主要なテスト機関で認定されており、多数のアプリケーション開発元の製品と互換性があります。また、さまざまなハードウェアプラットフォーム向けに最適化されています。

Kaspersky Lab でのウイルス分析は、24 時間体制で活動しており、毎日発生する膨大な数のコンピューターの脅威を見つけ出し、それを検知および駆除するツールを作成し、カスペルスキー製品で使用する定義データベースにそのシグニチャを登録しています。

技術：現在のアンチウイルスツールに不可欠な技術の多くは、Kaspersky Lab が最初に開発したものです。そ

のため、多くの開発企業が自社製品に Kaspersky Anti-Virus エンジンを使用しています。例として、Alcatel-Lucent、Alt-N、Asus、BAE Systems、Blue Coat、Check Point、Cisco Meraki、Clearswift、D-Link、Facebook、General Dynamics、H3C、Juniper Networks、Lenovo、Microsoft、NETGEAR、Openwave Messaging、Parallels、Qualcomm、Samsung、Stormshield、Toshiba、Trustwave、Vertu、ZyXEL などが挙げられます。また、Kaspersky Lab の革新的な技術の多くは特許を受けています。

成果：長年にわたって、Kaspersky Lab はコンピューターに対する脅威に対抗する上で果たした貢献が評価され、数々の賞を受賞しております。2014 年には、定評あるオーストリアの検査機関 AV-Comparatives が実施したテストと調査で、Advanced+ 評価の数で上位 2 社のうちの 1 社となり、最高位となる Top Rated の評価を受けました。しかし、最も大きな成果は、世界各国のユーザーの信頼を獲得したことと言ってよいでしょう。現在、Kaspersky Lab の製品と技術は、4 億人を超えるユーザー、および 27 万社以上のクライアント企業を保護しています。

Kaspersky Lab の Web サイト：	https://www.kaspersky.com
ウイルス百科事典（英語）：	https://securelist.com
ウイルスラボ：	https://virusdesk.kaspersky.com（疑わしいファイルや Web サイトの分析）
カスペルスキーの Web フォーラム：	https://forum.kaspersky.com

サードパーティ製のコードに関する情報

サードパーティ製のコードに関する情報は、アプリケーションのインストールフォルダーにある legal_notices.txt という名前のファイルに入っています。

商標に関する通知

登録商標およびサービスマークは、それぞれの所有者に属しています。

AWS（Amazon Web Services）は、米国およびその他の国における Amazon.com, Inc. またはその関連会社の商標です。

Citrix、XenApp、XenDesktop は、米国およびその他の国における Citrix Systems, Inc. またはその子会社の登録商標です。

Dell および Dell Compellent は Dell, Inc. の商標です。

Celerra、EMC、Isilon、OneFS、VNX は、米国およびその他の国における EMC Corporation の登録商標または商標です。

Hitachi は Hitachi, Ltd. の商標です。

IBM および System Storage は、世界各国における International Business Machines Corporation の登録商標です。

Excel、Hyper-V、JScript、MultiPoint、Microsoft、Outlook、Windows、Windows Server、Windows Vista は、米国およびその他の国における Microsoft Corporation の登録商標です。

NetApp および Data ONTAP は、米国およびその他の国における NetApp, Inc. の商標または登録商標です。

Linux は、米国およびその他の国における Linus Torvalds の登録商標です。

Mozilla および Firefox は、Mozilla Foundation の商標です。

Oracle は Oracle およびその関連会社の登録商標です。

用語解説

英数字

Kaspersky Security Network（KSN）

Kaspersky Lab のデータベースへのアクセスを提供するクラウドサービスのインフラストラクチャ。ファイル、Web リソース、ソフトウェアの評価に関する情報が絶えず更新されています。Kaspersky Security Network により、カスペルスキー製品は新しい脅威に迅速に対応でき、保護コンポーネントのパフォーマンスを改善し、誤検知の可能性を低下させます。

OLE オブジェクト

Object Linking and Embedding（OLE）技術を使用して別のファイルに添付されたオブジェクト、または別のファイルに埋め込まれたオブジェクト。OLE オブジェクトの例として、Microsoft Office Word ドキュメントに埋め込まれた Microsoft Office Excel® スプレッドシートが挙げられます。

SIEM

各種ネットワークデバイスおよびアプリケーションから開始されるセキュリティイベントを分析する技術。

あ

圧縮ファイル

圧縮によって 1 つまたは複数のファイルを単一のファイルにパッケージ化したもの。データの圧縮と展開には、アーカイバーと呼ばれる専用アプリケーションが必要です。

アップデート

Kaspersky Lab 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製品モジュール）を差し替えまたは追加する処理。

い

イベントの重要度

カスペルスキー製品の動作中に発生したイベントのプロパティ。4 つの重要度があります:

- 緊急イベント
- エラー
- 警告
- 情報

イベントの発生状況に応じて、同じ種別のイベントが異なる重要度になることがあります。

う

疑わしいオブジェクト

既知のウイルスの修正されたコードまたはウイルスに類似したコードを含むオブジェクトで、Kaspersky Lab がまだ特定していないもの。疑わしいオブジェクトはヒューリスティックアナライザーを使用して検知されます。

か

隔離

カスペルスキー製品が感染の可能性があるオブジェクトを検知したときに、そのオブジェクトの移動先となるフォルダー。コンピューターへの影響を防ぐために、オブジェクトは隔離に暗号化された形式で保存されます。

感染したオブジェクト

そのコードの一部が既知の悪意のあるソフトウェアのコードの一部と完全に一致するオブジェクト。そのようなオブジェクトにはアクセスしないでください。

感染の可能性があるファイル

その構造や形式のため、悪意のあるコードを保管し拡散するための「容器」として犯罪者に使用される可能性のあるファイル。通常、これらは実行ファイルであり、.com、.exe、.dll のようなファイル拡張子を持ちます。このようなファイルは、悪意のあるコードが侵入するリスクが極めて高くなります。

管理サーバー

Kaspersky Security Center の機能の 1 つで、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します。これらのカスペルスキー製品の管理にも使用できます。

く

駆除

感染したオブジェクトの処理方法のひとつ。データを完全に復元または一部復元します。感染したすべてのオブジェクトを駆除できるわけではありません。

け

現在のライセンス

本製品によって現在使用されているライセンス。

こ

誤検知

感染していないオブジェクトが、カスペルスキー製品によって感染しているとされる状況。オブジェクトのコードがウイルスのコードと似ているために発生します。

す

スタートアップオブジェクト

コンピューターにインストールされているオペレーティングシステムとソフトウェアが正しく起動し、動作するために必要なアプリケーションのセット。これらのオブジェクトは、オペレーティングシステムが起動するたびに実行されます。そのようなオブジェクトに感染することに特化したウイルスが存在し、オペレーティングシステムの起動をブロックしたりすることがあります。

せ

セキュリティレベル

セキュリティレベルは、製品コンポーネント設定を事前に構成したセットとして定義されます。

脆弱性

オペレーティングシステムまたはアプリケーションに侵入し、その整合性を破損させるために悪意のあるプログラムの作成者によって使用される可能性のあるオペレーティングシステムまたはアプリケーションの欠陥。オペレーティングシステムに侵入するウイルスは、オペレーティングシステム自体とインストール済みアプリケーションで障害を発生させるので、オペレーティングシステムに多数の脆弱性が存在すると、オペレーティングシステムが信頼できないものになります。

た

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ています。例：ファイルのリアルタイム保護、コンピューターの完全スキャン、定義データベースのアップデート。

タスクの設定

各タスク種別に対して固有の製品設定。

て

定義データベース

定義データベースの公開日時現在のセキュリティ上の既知の脅威に関する情報が含まれるデータベース。定義データベースのエントリーによって、スキャン対象のオブジェクトに含まれる悪意のあるコードを検知できます。定義データベースは、カスペルスキーのスペシャリストによって作成され、1 時間ごとにアップデートされます。

は

バックアップ

ファイルのバックアップコピーのための特別な保管領域。駆除または削除が試行される前に作成されます。

ひ

ヒューリスティックアナライザー

カスペルスキーの定義データベースにまだ追加されていない情報について脅威を検知する技術。ヒューリスティックアナライザーは、オペレーティングシステムでの動作がセキュリティの脅威と思われるオブジェク

トを検知します。ヒューリスティックアナライザーで検知されたオブジェクトは、感染の可能性があるとみなされます。たとえば、悪意のあるオブジェクトに典型的なコマンドシーケンス（ファイルを開く、ファイルに書き込む）が含まれる場合、そのオブジェクトは感染の可能性があるとみなされます。

ふ

ファイル名マスク

ワイルドカードを使用したファイル名の表示。ファイル名マスクで使用される基本的なワイルドカードは、* と ？ です。* は任意の数の任意の文字を表します。？ は任意の 1 文字を表します。

フィッシング

ユーザーの個人情報へ不正にアクセスすることを目的とした、インターネット詐欺の一種。

ほ

保護ステータス

現在の保護ステータス。コンピューターセキュリティのレベルを定義します。

ポリシー

ポリシーは、アプリケーションの設定を定義し、管理グループ内のコンピューターにインストールされているアプリケーションの設定に対するアクセスを管理します。各アプリケーションごとに個別の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ているアプリケーションに対して数に制限なくポリシーを作成できますが、管理グループ内で各アプリケーションに適用できるポリシーは同時に 1 つのみです。

ら

ライセンスの有効期間

製品機能へのアクセスとその他のサービスを使用する権利を持つ期間。使用できるサービスはライセンスの種別により異なります。

り

リアルタイム保護

悪意のあるコードが含まれていないか、オブジェクトをリアルタイムでスキャンする動作モード。

オブジェクトを開く試行（読み取り、書き込み、実行）をすべてインターセプトし、脅威がないかオブジェクトをスキャンします。感染していないオブジェクトはユーザーに渡され、脅威を含むオブジェクトまたは感染の可能性があるオブジェクトはタスク設定に従って処理されます（駆除、削除、または隔離）。

ろ

ローカルタスク

単一のクライアントコンピューターで定義され、実行されるタスク。