Kaspersky Security for Windows Server

管理者用ガイド

製品バージョン：10.1.2.996

Kaspersky Lab の製品をお使いの皆さまへ

Kaspersky Lab が提供するセキュリティ製品をご利用いただきありがとうございます。製品の使用方法の確認や問題の解決にこのガイドをお役立てください。

ガイド改訂日：2019 年 5 月 17 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 10.1.2（以降「Kaspersky Security 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 for Windows Server をインストールおよび管理する担当者と、Kaspersky Security 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 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 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 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。

Kaspersky Security for Windows Server

このセクションでは、Kaspersky Security 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 for Windows Server のシステム要件のリストを提供します。

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 for Windows Server のインストール方法と削除方法を説明します。

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 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。

管理プラグインの使用

このセクションでは、Kaspersky Security for Windows Server 管理プラグインについての情報を提供するとともに、保護対象のサーバーまたはサーバーのグループにインストールされている Kaspersky Security for Windows Server を管理する方法について説明します。

アプリケーションコンソールの使用

このセクションでは、Kaspersky Security for Windows Server コンソールについての情報を提供するとともに、保護対象のサーバーまたは別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コンソールを使用してアプリケーションを管理する方法について説明します。

Kaspersky Security for Windows Server の開始と停止

このセクションでは、アプリケーションコンソールの起動に関する情報および Kaspersky Security サービスの開始と停止に関する情報について説明します。

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

このセクションでは、Kaspersky Security 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。

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。

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。

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。

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その設定方法について説明します。

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。

アプリケーション起動コントロール

このセクションでは、アプリケーション起動コントロールタスクとその設定方法について説明します。

デバイスコントロール

このセクションでは、デバイスコントロールタスクおよびタスクを設定する手順について説明します。

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。

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。

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。

オンデマンドスキャン

このセクションでは、オンデマンドスキャンタスク、および保護対象サーバー上でのオンデマンドスキャンタスクとセキュリティの設定手順について説明します。

信頼ゾーン

このセクションでは、Kaspersky Security for Windows Server の信頼ゾーンに関する情報、およびタスク実行時に信頼ゾーンにオブジェクトを追加する手順について説明します。

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。

階層型ストレージの管理

このセクションでは、階層型ストレージ領域とバックアップシステムに配置されているファイルのスキャンを実行する方法について説明します。

サードパーティ製システムとの連携

このセクションでは、Kaspersky Security for Windows Server とサードパーティ製の機能およびテクノロジーとの連携について説明しま

す。

コマンドラインからの Kaspersky Security 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 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

サンプルテキスト	文書規約の説明
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、文頭に矢印記号が示されます。
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。変数名の代わりに、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 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 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 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 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 for Windows Server のページ

カスペルスキーの Web サイトの Kaspersky Security for Windows Server のページ(https://www.kaspersky.co.jp/small-to-medium-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。

ナレッジベースの Kaspersky Security 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 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 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 for Windows Server に関する文書

『Kaspersky Security 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。

カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーの Web コミュニティ(https://community.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。

コミュニティでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

Kaspersky Security for Windows Server

このセクションでは、Kaspersky Security 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 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 for Windows Server について

Kaspersky Security for Windows Server 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接続ストレージを、ファイル交換を介してサーバーやネットワーク接続ストレージ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 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 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 for Windows Server は次の役割を割り当てているサーバーにインストールできます:

- Active Directory® 証明書サービス
- Active Directory ドメインサービス
- Active Directory フェデレーションサービス
- Active Directory ライトウェイトディレクトリサービス
- Active Directory Rights Management サービス
- デバイス正常性構成証明
- DHCP サーバー
- DNS サーバー
- Fax サーバー
- ファイルサービスと記憶域サービス
- ホストガーディアンサービス

- Hyper-V®
- ネットワークコントローラー
- ネットワークポリシーとアクセスサービス
- 印刷とドキュメントサービス
- リモートアクセス
- リモートデスクトップサービス
- ボリュームライセンス認証サービス
- Web サーバー（IIS）
- Windows 展開サービス
- Windows Server® Update Services

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

- Kaspersky Security for Windows Server 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アプリケーション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 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 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 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 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：

- **ファイルのリアルタイム保護**：Kaspersky Security 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 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トリーム（NTFS ストリーム）
  - 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
  - Windows Server 2016 と Windows Server 2019 のコンテナーファイル
- **オンデマンドスキャン**：Kaspersky Security 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。保護対象のサーバーで、ファイルやメモリ、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 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監視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、外部からファイアウォール設定が編集される可能性をすべてブロックします。
- **ファイル変更監視**：Kaspersky Security 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、保護対象のサーバ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 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 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**フォルダー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フォルダーに保存されます。
- **バックアップ**：Kaspersky Security 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への通知**：保護対象のサーバーにアクセスする管理者とユーザーに対して Kaspersky Security for Windows Server の動作におけるイベントとサーバ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 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 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 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を設定できます。
- **Kaspersky Security 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 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 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 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 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 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存用の低速なストレージデバイスとの間で、データを再配置できます。
- **信頼ゾーン**：Kaspersky Security 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脆弱性攻撃から、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の保管領域**：悪意のある動作が検知された場合、サーバーの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 for Windows Server の新機能と機能強化は次のとおりです:

- Microsoft Windows のオペレーティングシステムの新しいバージョンをサポートしました。
  - Windows Server 2019(x64)
- アクティベーションコードの全体を製品の GUI からは閲覧できないようにしました。

  追加済みのアクティベーションコードを製品の GUI で表示しようとするとコードの一部が非表示になるため、どのユーザーも完全なアクティベーションコードを閲覧できません。
- アンチクリプタータスクでの誤検知の発生数を減らしました。

  確実に誤検知である検知を防止するために、一部のファイル種別に対する除外が既定で追加されました。

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 for Windows Server インストールウィザードの起動
- Kaspersky Security for Windows Server コンソール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 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
- Kaspersky Security for Windows Server Microsoft Outlook® アドイン(以降「Kaspersky Security Microsoft Outlook アドイン」)の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。
- 『ネットワーク接続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 for Windows Server のページ(https://www.kaspersky.co.jp/small-to-medium-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 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、アプリケーションコンソール(コンポーネントの「Kaspersky Security 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と使用許諾契約書のテキスト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 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 for Windows Server を管理する管理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。

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、Microsoft Outlook アドインのインストールパッケージと使用許諾契約書のテキストファイルが含まれています。

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 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 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_ja.pdf	管理者用ガイド。
ks4ws_netstorage_guide_ja.pdf	ネットワーク接続ストレージ保護導入ガイド。
migration.txt	このファイルには、本製品の前バージョンからの移行について記載されています。
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。アプリケーション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\license.txt	使用許諾契約書のテキスト。
\client\setup.exe	コンポーネントの「管理ツール」のセット（アプリケーションコンソールを含む）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 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 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 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 Center によって Kaspersky Security for Windows Server を管理する管理プラグイン用インストーラー。これを使用して Kaspersky Security 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。
\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。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。

ファイル	目的
\email_plugin\license.txt	使用許諾契約書のテキスト。

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、保護対象サーバーとネットワーク接続ストレージのすべてのシステム要件について説明します。

このセクションの内容

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

Kaspersky Security 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 for Windows Server 10.1.2 をインストールする前に、Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition をアンインストールする必要があります。Kaspersky Security 10 for Windows Server 以降の製品については、アンインストールせずに Kaspersky Security for Windows Server 10.1.2 を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:100 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 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 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 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(Server Core インストールも可)

Kaspersky Security 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 以降
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 以降(Server Core インストールも可)
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 以降
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 以降(Server Core インストールの場合)
- Windows Storage Server 2008 R2
- Windows Storage Server 2008 SP2
- Windows Storage Server 2008 SP2 Workgroup Edition
- 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
- Windows Server 2012 Standard / Datacenter(Server Core インストールの場合)
- Microsoft Windows MultiPoint™ Server 2012 Standard / Premium
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter

- Windows Server 2012 R2　Standard / Datacenter（Server Core インストールの場合）
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2016 Standard / Datacenter（Server Core インストールの場合）
- Microsoft Windows MultiPoint™ Server 2016
- Windows Storage Server 2016
- Windows Hyper-V Server 2016
- Windows Server 2019 Essentials / Standard / Datacenter（Server Core インストールも可）
- Windows Hyper-V Server 2019

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 for Windows Server は、以下のターミナルサーバーが動作している環境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
- Windows Server 2019 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

Kaspersky Security for Windows Server と互換性がある Kaspersky Security Center のバージョンは次のとおりです：

- Kaspersky Security Center 10.4
- Kaspersky Security Center 10.5
- Kaspersky Security Center 11

保護対象のネットワーク接続ストレージの要件

Kaspersky Security 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
  - クラスターモードの Data ONTAP 9.0
  - クラスターモードの Data ONTAP 9.1
  - クラスターモードの Data ONTAP 9.2

  - クラスターモードの Data ONTAP 9.3
  - クラスターモードの Data ONTAP 9.4
- Dell™ EMC™ Celerra™ /VNX™（次のソフトウェアを搭載）:
  - EMC DART 6.0.36 以降
  - Celerra Antivirus Agent (CAVA) 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 HNAS（ICAP、RPC）:
  - 12.0 以降（ICAP による連携の場合）
  - 11.2 以降（RPC による連携の場合）
- IBM System Storage N シリーズ
- Oracle® ZFS Storage Appliance
- Dell Compellent™ FS8600 プラットフォーム上の Dell NAS:
  - FluidFS 6.x
  - FluidFS 5.x
- HPE 3PAR（File Persona 3.3.1）:
  - HPE 3PAR StoreServ ファイルコントローラー
  - HPE 3PAR StoreServ 7000c、8000、9000、20000 ストレージ

アプリケーション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

アプリケーションコンソールは、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。

アプリケーション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。

アプリケーションコンソールは、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®
- Microsoft Windows 7
- Microsoft Windows 8

- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows 10 Redstone 1
- Windows 10 Redstone 2
- Windows 10 Redstone 3
- Windows 10 Redstone 4
- Windows 10 Redstone 5
- Windows 10 Redstone 6

アプリケーションコンソールは、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(Server Core インストールの場合)
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / 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 Standard / Premium
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2012 Standard / Premium
- Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2016
- Windows Storage Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter
- Microsoft Windows XP Professional Edition SP2 以降
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows 10 Redstone 1
- Windows 10 Redstone 2
- Windows 10 Redstone 3
- Windows 10 Redstone 4

- Windows 10 Redstone 5
- Windows 10 Redstone 6

機能要件および制限事項

このセクションでは、Kaspersky Security 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 for Windows Server のインストールフォルダーの新しいパスが 150 文字以上の場合、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 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コンポーネン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 for Windows Server をインストールして機能させるには、Filter Manager コンポーネントがインストールされている必要があります。
- Kaspersky Security 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。なんらかの使用可能な方法で、指定された証明書をインストールしてください。

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 アドレスは使用できません。
- 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コンポーネントを検出するため、トラフィックセキュリティコンポーネントを導入する前に、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 Kaspersky Security Center 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（Microsoft 管理コンソール）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 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、ファイル整合性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コンポーネント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 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、ログ監査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 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:

- アプリケーション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。
- アプリケーション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アプリケーション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。この手順を行わない場合は、コンパクト診断インターフェイスまたは MMC スナップインを開くことを許可されたユーザーとしてログインする必要があります。
- ユーザーアカウント制御が有効な場合、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 との連携:

- 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、ブロック対象コンピューター）。

脆弱性攻撃防止:

- 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、脆弱性攻撃防止は使用できません。
- 脆弱性攻撃防止コンポーネントは、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防止コンポーネントがインストールされている場合、Kaspersky Security 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 IPv4 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。
- HPE 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。
- 「not-a-virus（非ウイルス）」オブジェクトに対する除外ルールが信頼ゾーンで有効な場合、この除外ルールは ICAP ネットワークストレージの保護タスクにも適用されます。

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、ウェブ脅威対策およびメール脅威対策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 for Windows Server のインストール方法と削除方法を説明します。

この章の内容

Windows インストーラーサービスでの Kaspersky Security for Windows Server ソフトウェアコンポーネントの指定時に使用するコンポーネントコード

既定では、\server\ks4ws_x86(x64).msi ファイルを使用すると、一部のコンポーネントを除きすべての Kaspersky Security for Windows Server コンポーネントがインストールされます。既定ではインストールされないコンポーネントも、カスタムインストールでインストール対象として追加できます。

ファイル ¥client¥ks4wstools_x86(x64).msi により、「管理ツール」セットに含まれるすべてのソフトウェアコンポーネントが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の Kaspersky Security for Windows Server ソフトウェアコンポーネントの指定時に使用するコンポーネント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 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指定することができます。

このセクションの内容

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

Kaspersky Security 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 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、指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、保護対象のサーバーの 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監視およびスキャンします。
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提供するコンポーネントです。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

コンポーネント	コード	実行される機能
オンデマンドスキャン	Ods	Kaspersky Security for Windows Server システムファイルをインストールし、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）を実行できるようにします。 コマンドラインから Kaspersky Security 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 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行されます。
アンチクリプター	AntiCryptor	悪意のある動作を示すブロック対象コンピューターのリストを作成し、これらのリモートデバイスの名前を記録します。 このコンポーネントにより、アンチクリプタータスクが実行されます。
スクリプト監視	ScriptChecker	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コードをスキャンします。スクリプト実行が試行された場合にスキャンが実行されます。 このコンポーネントにより、スクリプト監視タスクが実行されます。
Kaspersky Security Network の使用	Ksn	Kaspersky Lab のクラウド技術に基づく保護を提供します。 このコンポーネントにより、KSN の使用タスクが実行されます（Kaspersky Security 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行されます。
脆弱性攻撃ブロック	AntiExploit	このコンポーネントは、保護対象の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。

コンポーネント	コード	実行される機能
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 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行されます。
Kaspersky Security Center ネットワークエージェントとの連携用のモジュール	AKIntegration	Kaspersky Security for Windows Server と Kaspersky Security Center ネットワークエージェント間の接続を提供します。 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。
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 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 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 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 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 がインストールされている保護対象サーバーにのみ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 for Windows Server アイコン	TrayApp	保護対象サーバーのタスクトレイの通知領域に Kaspersky Security for Windows Server アイコンを表示します。Kaspersky Security for Windows Server アイコンは、サーバー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、Microsoft 管理コンソールのアプリケーションコンソール(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。

ソフトウェアコンポーネントの「管理ツール」セット

「管理ツール」セットに含まれる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 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 for Windows Server スナップイン	MmcSnapin	Kaspersky Security for Windows Server コンソールから Microsoft 管理コンソールスナップイン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。
ヘルプ	Help	Kaspersky Security 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、アプリケーションコンソール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	Help	Kaspersky Security for Windows Server をインストールすると、PDF 形式の『ネットワーク接続ストレージ保護導入ガイド』と『管理者用ガイド』にアクセス可能なカスペルスキーの Web サイトへのショートカットが追加されます。ショートカットは[**スタート**]メニューからアクセスできます。

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

Kaspersky Security for Windows Server と「管理ツール」のセット(アプリケーションコンソールを含む)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、次の変更が保護対象サーバーに加えられます:

- 保護対象サーバーおよびアプリケーションコンソールがインストールされているサーバーに Kaspersky Security for Windows

Server フォルダーが作成されます。

- Kaspersky Security for Windows Server サービスが登録されます。
- Kaspersky Security for Windows Server ユーザーグループが作成されます。
- Kaspersky Security for Windows Server のキーがシステムレジストリに登録されます。

以下に、これらの変更点を示します。

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

Kaspersky Security for Windows Server がインストールされる場合、次のフォルダーが保護対象サーバーに作成されます:

- Kaspersky Security for Windows Server の実行ファイルが配置される Kaspersky Security for Windows Server の既定のインストールフォルダーは、オペレーティングシステムのビットセットによって異なります。既定のインストールフォルダーはそれぞれ次のようになります:
  - 32 ビット版の Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\
  - 64 ビット版の Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\
- SNMP プロトコルを使用して Kaspersky Security for Windows Server により公開されるカウンターとフックの説明を含む、管理情報ベース(MIB)ファイル:
  - %Kaspersky Security for Windows Server%\mibs
- 64 ビット版の Kaspersky Security 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 for Windows Server がインストールされるときにのみ作成されます):
  - %Kaspersky Security for Windows Server%\x64
- Kaspersky Security for Windows Server サービスファイル:
  - %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 Lab\Kaspersky Security for Windows Server\10.1\Dskm\
- アップデート元の設定を含むファイル:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\
- 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\Update\Distribution\
- 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\Reports\
- 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\Current\
- 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\Backup\
- 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\Bases\Temp\
- 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\Quarantine\

- バックアップ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）:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\

アプリケーションコンソールのインストール時に作成されるフォルダー

「管理ツール」を含むアプリケーションコンソールの既定のインストールフォルダーは、オペレーティングシステムのビットセットによって異なります。既定のインストールフォルダーはそれぞれ次のようになります:

- 32 ビット版の Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\
- 64 ビット版の Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\

Kaspersky Security for Windows Server サービス

次の Kaspersky Security 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:

- Kaspersky Security サービス（KAVFS） - Kaspersky Security for Windows Server のタスクとワークフローを管理する、重要な Kaspersky Security for Windows Server サービス。
- Kaspersky Security 管理サービス（KAVFSGT） - アプリケーションコンソールを介して Kaspersky Security for Windows Server の管理を行うサービス。
- Kaspersky Security 脆弱性攻撃ブロックサービス（KAVFSSLP） - 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サービス（KAVFSSCS） - スクリプト監視タスクとともに起動し、Microsoft Windows のスクリプト技術を使用して作成されたスクリプトの実行の制御を可能にするサービス。

Kaspersky Security for Windows Server グループ

KAVWSEE Administrators は、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 管理サービスと Kaspersky Security 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

Kaspersky Security for Windows Server がインストールされる場合、次のシステムレジストリキーが作成されます:

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

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump]

- 64 ビット版の Microsoft Windows:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump]

- トレースファイルの設定:
  - 32 ビット版の Microsoft Windows:[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\Trace]
  - 64 ビット版の Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Trace]
- 製品のタスクと機能の設定:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment]

Kaspersky Security for Windows Server プロセス

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

表 5. Kaspersky Security for Windows Server プロセス

ファイル名	目的
kavfswp.exe	Kaspersky Security for Windows Server ワークフロー
kavtray.exe	システムトレイアイコンのプロセス
kavfsmui.exe	コンパクト診断インターフェイス
kavshell.exe	コマンドラインユーティリティのプロセス
kavfsrcn.exe	Kaspersky Security 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 脆弱性攻撃ブロックサービスプロセス
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

このセクションでは、Kaspersky Security 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 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。

Windows インストーラーのインストール設定とコマンドラインオプション

- 使用許諾契約書の条件に同意:Kaspersky Security for Windows Server をインストールするには、条件に同意する必要があります。

  `EULA=<値>` コマンドラインオプションで取り得る値は、次のとおりです:

  - `0` - 使用許諾契約書の条件を拒否する(既定値)。
  - `1` - 使用許諾契約書の条件に同意する。
- プライバシーポリシーの条件に同意:Kaspersky Security for Windows Server をインストールするには、条件に同意する必要があります。

  `PRIVACYPOLICY=<値>` コマンドラインオプションで取り得る値は、次のとおりです:

  - `0` - プライバシーポリシーの条項を拒否する(既定値)。
  - `1` - プライバシーポリシーの条項に同意する。
- 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、Kaspersky Security for Windows Server のインストールを実行するかどうか。

  `PRESCAN=<値>` コマンドラインオプションで取り得る値は、次のとおりです:

  - `0` - インストール中に、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の事前スキャンを実行しない(既定値)。
  - `1` - インストール中に、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の事前スキャンを実行する。
- インストールのときに Kaspersky Security 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。

  `INSTALLDIR=<フォルダーの完全パス>` コマンドラインオプションの既定値は、次のとおりです:

  - `Kaspersky Security for Windows Server`:%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server
  - 管理ツール:%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools
  - Microsoft Windows 64 ビット版:%ProgramFiles(x86)%
- ファイルのリアルタイム保護タスクを、Kaspersky Security for Windows Server の起動後すぐに開始するかどうかの設定。Kaspersky Security 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)。

  `RUNRTP=<値>` コマンドラインオプションで取り得る値は、次のとおりです:

  - `1` - 開始する(既定値)。
  - `0` - 開始しない。
- Microsoft によって推奨される保護の除外。ファイルのリアルタイム保護タスクで、Microsoft 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。サーバーで動作する一部のアプリケーションでは、使用中のファイルがアン

チウイルス製品によって監視または変更されると、動作が不安定になる場合があります。たとえば、Microsoft は、一部のドメインコントローラアプリケーションを、除外を推奨するオブジェクトのリストに含めています。

ADDMSEXCLUSION=<値> コマンドラインオプションで取り得る値は、次のとおりです:

- 1 - 除外する(既定値)。
- 0 - 除外しない。

- Kaspersky Lab の推奨事項に従って保護範囲から除外されるオブジェクト。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。

  ADDKLEXCLUSION=<値> コマンドラインオプションで取り得る値は、次のとおりです:

  - 1 - 除外する(既定値)。
  - 0 - 除外しない。

- アプリケーションコンソールへのリモート接続を許可。既定では、保護対象サーバーにインストールされたアプリケーション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 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。

  ALLOWREMOTECON=<値> コマンドラインオプションで取り得る値は、次のとおりです:

  - 1 - 許可する。
  - 0 - 拒否する(既定値)。

- ライセンス情報ファイルのパス。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、Windows インストーラーによって有効期限が最も先のライセンス情報ファイルが選ばれます。ライセンス情報ファイルはあらかじめ ¥server フォルダーに保存できます。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 for Windows Server がインストールされたあと、アプリケーション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 for Windows Server は機能しません。

  LICENSEKEYPATH=<ライセンス情報ファイル名> の既定値は、配布キットの ¥server フォルダーです。

- 設定ファイルのパス。Kaspersky Security 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。

  CONFIGPATH=<設定ファイル名> の既定値は指定されていません。

- アプリケーションコンソールに対するネットワーク接続の有効化。別のサーバーに Kaspersky Security 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 for Windows Server コンソールがインストールされた別のコンピューターからサーバー保護をリモート管理できます。Microsoft Windows ファイアウォールでポート 135(TCP)が開き、Kaspersky Security 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。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を行えるようにします。また、サーバーが Microsoft Windows Server 2008 で動作している場合、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 for Windows Server 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(63 ページのセクション「アプリケーション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)。

  ADDWFEXCLUSION=<値> コマンドラインオプションで取り得る値は、次のとおりです:

  - 1 - 許可する。
  - 0 - 拒否する(既定値)。

- 非互換ソフトウェアのチェックの無効化。この設定を使用すると、サーバー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 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サーバー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。

SKIPINCOMPATIBLESW=<値> コマンドラインオプションで取り得る値は、次のとおりです:

- 0 - 非互換ソフトウェアのチェックを実行する(既定値)。
- 1 - 非互換ソフトウェアのチェックを実行しない。

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

- 隔離されたオブジェクトの復元。

  RESTOREQTN=<値> コマンドラインオプションで取り得る値は、次のとおりです:

  - 0 - 隔離されたコンテンツを削除する(既定値)。
  - 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の ¥Quarantine サブ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。

  RESTOREBCK=<値> コマンドラインオプションで取り得る値は、次のとおりです:

  - 0 - バックアップのコンテンツを削除する(既定値)。
  - 1 - バックアップコンテンツをパラメータ RESTOREPATH で指定したフォルダーの ¥Backup サブフォルダーに復元する。
- 現在のパスワードの入力による、アンインストールを実行してよいかの確認(パスワードによる保護が有効の場合)。

  UNLOCK_PASSWORD=<指定されたパスワード> の既定値は指定されていません。
- 復元されたオブジェクトのフォルダー。復元したオブジェクトは、指定されたフォルダーに保存されます。

  RESTOREPATH=<フォルダーの完全パス> コマンドラインオプションの既定値は、%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored です。

Kaspersky Security 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 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。ks4ws_10.1.2_install_<uid>.log(<uid> は 8 文字からなる一意のログ識別子)という名前のログファイルが、setup.exe ファイルを起動したアカウントのユーザーの %temp% フォルダーに保存されます。

[**スタート**]メニューからアプリケーションコンソールまたは Kaspersky Security for Windows Server に対して[**Kaspersky Security 10.1.2 for Windows Server 管理ツールの変更または削除**]オプションを実行すると、ks4ws_10.1_maintenance.log というログファイルが自動的に %temp% フォルダーに作成されます。

Kaspersky Security 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のログファイルは作成されません。

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

- `msiexec /i ks4ws_x86.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`

インストールの計画

このセクションでは、Kaspersky Security for Windows Server 管理ツールの説明と、ウィザード（58 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（73 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（79 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 for Windows Server のインストールおよびアンインストール（84 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）での留意点を記載しています。

Kaspersky Security 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 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（45 ページのセクション「Windows インストーラーサービスでの Kaspersky Security for Windows Server ソフトウェアコンポーネントの指定時に使用するコンポーネントコード」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 for Windows Server の設定およびアプリケーションの管理に使用する管理ツールを決定します。Kaspersky Security for Windows Server の管理には、アプリケーションコンソール、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 for Windows Server コンソール

Kaspersky Security for Windows Server 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 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アプリケーションコンソール経由で管理できます。

複数の Kaspersky Security for Windows Server スナップインを、作成者モードで開かれた 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 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。

アプリケーションコンソールは、「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 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 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 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 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連携用のモジュール**：Kaspersky Security 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 for Windows Server とネットワークエージェントとの通信を可能にします。Kaspersky Security Center ネットワークエージェントとの連携用の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 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 10.1.2 管理プラグイン**: 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サーバーに Kaspersky Security 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。これにより、Kaspersky Security Center によるアプリケーションの管理インターフェイスを利用できるようになります。管理プラグインのインストールファイル server¥klcfginst.exe は、Kaspersky Security 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 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(45 ページのセクション「Windows インストーラーサービスでの Kaspersky Security for Windows Server ソフトウェアコンポーネントの指定時に使用するコンポーネントコード」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:

- Kaspersky Security for Windows Server の特別なインストール設定が必要か、それとも推奨のインストール設定を使用するか(53 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)。
- 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 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 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 for Windows Server をある 1 つのサーバーにインストールして設定し、その設定を設定ファイルに保存しておくと、Kaspersky Security 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インストールを実行できます:

- 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 コンポーネントのインストール(46 ページのセクション「Kaspersky Security 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 ホストの配布キットの \client\setup.exe ファイルからの Kaspersky Security for Windows Server コンソールのインストール(61 ページのセクション「Kaspersky Security for Windows Server 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 for Windows Server は既定の設定でインストールされます。Kaspersky Security 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。

アプリケーションコンソールは、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 for Windows Server とアプリケーションコンソールのインストール用のサンプルコマンド(73 ページの「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」セクションを参照)を使用することもできます。

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サーバーの保護を管理している場合、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 for Windows Server をインストールできます。

Kaspersky Security Center を使用して Kaspersky Security for Windows Server をインストールする場合（79 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 for Windows Server をインストールできます。アプリケーションコンソールは、保護対象サーバーおよび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 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 for Windows Server をインストールするサーバーは（84 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。サーバーの起動時、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、セットアップウィザードを使用した Kaspersky Security for Windows Server とアプリケーションコンソールのインストールとアンインストール、および Kaspersky Security for Windows Server の追加の設定と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 for Windows Server、アプリケーションコンソール、Microsoft Outlook アドインのインストールの情報について説明します。

► Kaspersky Security 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 for Windows Server を保護対象サーバーにインストールします。
3. アプリケーションコンソールは、Kaspersky Security for Windows Server を管理するときに操作するコンピューターにインストールしてください。
4. アプリケーション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、アプリケーションコンソールユーザーが Kaspersky Security for Windows Server をリモート管理できるようにするには、追加設定を実行してください。
5. Microsoft Outlook がインストールされているコンピューターに、Microsoft Outlook アドインをインストールします。

6. Kaspersky Security for Windows Server の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 for Windows Server のインストール

Kaspersky Security for Windows Server のインストール前に、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 Anti-Virus 8.0 for Windows Servers Enterprise Edition がインストールされている場合は、これをアンインストールする必要があります。Kaspersky Security 10 for Windows Server 以降の製品については、アンインストールせずに Kaspersky Security for Windows Server 10.1.2 を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属し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 for Windows Server のインストール設定を指定します。Kaspersky Security 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**]をクリックします。

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(53 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)。

► セットアップウィザードを使用して Kaspersky Security for Windows Server をインストールするには:

1. サーバーで setup.exe ファイルを起動します。
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 for Windows Server のインストール**]をクリックします。
3. Kaspersky Security for Windows Server のセットアップウィザードの開始ウィンドウで[**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。

   インストール先のサーバーに、本製品の互換性のあるバージ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、この手順内のステップ 8 に進んでください。

7. 本製品の以前のバージ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により、製品が Kaspersky Security for Windows Server 10.1.2 にアップグレードされ、互換性のある設定が新しいバージョンに保存されます。アップグレードが完了すると、ウィザードの[**インストールの完了**]ウィンドウが表示されます(この手順内のステップ 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. システムメモリとサーバーのローカルドライブの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**]をクリックします。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 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管理を除くすべての Kaspersky Security 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 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 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**]ウィンドウで、次のように操作します:

    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 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**]をクリックします。

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トする場合は、アクティベーションに使用する Kaspersky Security for Windows Server のライセンス情報ファイルを指定します。

- 製品をあとでアクティベートする場合は、[**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 ¥server フォルダー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を使用している場合、アクティベーションコードを使用して本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本製品をアクティベートする場合は、インストール後にコードを入力します。

  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。ライセンスの有効期限日までの日数を計算して表示します。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、ライセンス情報ファイル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 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. [**終了**]をクリックします。

セットアップウィザードが閉じます。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 for Windows Server が使用できるようになります。

Kaspersky Security for Windows Server 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、アプリケーションコンソールのインストール設定を編集します。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、[セットアップウィザード]ウィンドウで[**キャンセル**]をクリックします。

► アプリケーション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の起動に使用するアカウントが、コンピューターの管理グループに属していることを確認します。
2. サーバーで setup.exe ファイルを実行します。

   プログラムの開始ウィンドウが表示されます。
3. [**Kaspersky Security for Windows Server 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。
4. [**次へ**]をクリックします。
5. 表示されるウィンドウで使用許諾契約書の条項を確認し、[**使用許諾契約書の諸条件をすべて読み、理解した上で、同意します**]をオンにして、インストールを続行します。
6. [**次へ**]をクリックします。

   [**インストールの詳細設定**]ウィンドウが表示されます。
7. [**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:

- アプリケーション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 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」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 for Windows Server コンポーネントに関する詳細情報があります(45 ページのセクション「Windows インストーラーサービスでの Kaspersky Security for Windows Server ソフトウェアコンポーネントの指定時に使用するコンポーネントコード」を参照)。

8. [**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。

9. [**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。

10. [**終了**]をクリックします。

セットアップウィザードが閉じます。アプリケーションコンソールが、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(「アプリケーション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」(63 ページ)を参照)。

Kaspersky Security Microsoft Outlook アドインのインストール

セットアップウィザードの指示に従い、Microsoft Outlook アドインのインストール設定を編集します。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、[セットアップウィザード]ウィンドウで[**キャンセル**]をクリックします。

> Microsoft Outlook アドインは、Kaspersky Security 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。

► Microsoft Outlook アドイン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の起動に使用するアカウントが、コンピューターの管理グループに属していることを確認します。
2. サーバーで setup.exe ファイルを実行します。

   プログラムの開始ウィンドウが表示されます。

3. インストール済みの Microsoft Outlook クライアントのビット数に応じて、[**Kaspersky Security Microsoft Outlook アドイン(x86)のインストール**]または[**Kaspersky Security Microsoft Outlook アドイン(x64)**]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。

4. [**次へ**]をクリックします。
5. 表示されるウィンドウで使用許諾契約書の条項を確認し、[**使用許諾契約書の諸条件をすべて読み、理解した上で、同意します**]をオンにして、インストールを続行します。
6. [**次へ**]をクリックします。

   [**インストール先フォルダー**]ウィンドウが表示されます。

7. [**インストール先フォルダー**]ウィンドウで、次のように操作します:
   - インストール先フォルダーを変更する場合は、[**変更**]をクリックします。

     [**インストール先フォルダーの変更**]ウィンドウが表示されます。

     d. 別のインストール先フォルダーを指定します。

     e. [**OK**]をクリックします。

   - インストール先フォルダーを変更しなくてよい場合は、[**次へ**]をクリックします。

   [**Kaspersky Security for Windows Server Microsoft Outlook アドインのインストール準備完了**]ウィンドウが表示されます。

8. [**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。

9. [**終了**]をクリックします。

セットアップウィザードが閉じます。

アドインのインストール中に Microsoft Outlook メールクライアントが動作中だった場合、インストールの完了後に Outlook を再起動する必要があります。

アプリケーション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

アプリケーションコンソールを、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 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 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(236 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)。
- Microsoft Windows が動作しているコンピューターへのアプリケーション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**]をオンにしなかった場合、コンピューターのファイアウォールを経由するアプリケーション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。

リモートコンピューター上のアプリケーションコンソールは、DCOM プロトコルを使用して、Kaspersky Security 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 管理サービスから受信します。アプリケーションコンソールと Kaspersky Security 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アプリケーション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。

アプリケーションコンソールがインストールされているリモートコンピューター上で、次を実行します:

- 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 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。

  アプリケーション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、TCP ポート 135 が使用されます。
- 接続を許可するための Windows ファイアウォールの送信ルールを設定します。

  単一のプロトコルが固定ポートを持つ従来の TCP/IP や UDP/IP とは異なり、DCOM はリモートの COM オブジェクトのポートを動的に割り当てます。ファイアウォールが、アプリケーションコンソールがインストールされているクライアントと DCOM エンドポイント(保護対象サーバー)の間に存在する場合、広範囲のポートを開く必要があります。

その他のソフトウェアまたはハードウェアのファイアウォールを設定するときにも、同じ手順を適用してください。

► 保護対象サーバーとアプリケーションコンソールがインストールされているコンピューター間の接続を設定中にアプリケーションコンソールが開かれた場合:

1. アプリケーションコンソールを閉じます。
2. Kaspersky Security 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ます。
3. アプリケーション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。

このセクションの内容

COM アプリケーションへの匿名リモートアクセスの許可

インストールされている 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。

► 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 for Windows Server コンソールがインストールされたリモートコンピューターで、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**] - [**ファイル名を指定して実行**]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[**制限の編集**]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。

Kaspersky Security for Windows Server リモート管理プロセスに対するネットワーク接続の許可

インストールされている 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。

► Windows ファイアウォールで TCP ポート 135 を開き、Kaspersky Security for Windows Server リモート管理プロセスに対してネットワーク接続を許可するには次の操作を実行します:

1. リモートコンピューターで Kaspersky Security for Windows Server 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:
     a. 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。

     b. [**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。

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

     d. [**TCP**]プロトコルを選択します。

     e. [**OK**]をクリックします。

     f. [**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。

b. [**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。

c. [**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、Microsoft 管理コンソールを使用して Kaspersky Security for Windows Server コンソールをインストールするときに指定したインストール先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。

Windows ファイアウォールの送信ルールの追加

インストールされている 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。

► Windows ファイアウォールに送信ルールを追加するには、次の手順を行います:

1. [**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。
2. [**Windows ファイアウォール**]ウィンドウで、[**詳細設定**]をクリックします。
   [**セキュリティが強化された Windows ファイアウォール**]ウィンドウが開きます。
3. [**送信の規則**]サブフォルダーを選択します。
4. [**操作**]ペインで[**新しい規則**]オプションをクリックします。
5. 表示された[**新規の送信の規則ウィザード**]ウィンドウで、[**ポート**]を選択し、[**次へ**]をクリックします。
6. [**TCP**]プロトコルを選択します。
7. [**特定のリモートポート**]で、送信接続を許可するための次のポートの範囲を指定します:1024-65535。
8. [**操作**]ウィンドウで、[**接続を許可する**]を選択します。
9. 新しいルールを保存して、[**セキュリティが強化された Windows ファイアウォール**]ウィンドウを閉じます。

Windows ファイアウォールで、アプリケーションコンソールと Kaspersky Security 管理サービスの間のネットワーク接続が許可されます。

Kaspersky Security 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トしている場合、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 for Windows Server のインストール中に[**製品インストール後にリアルタイム保護を有効にする**](既定のオプション)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 時に簡易スキャンタスクが実行されます。

Kaspersky Security 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:

- 定義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 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、簡易スキャンをサーバーで実行します。
- Kaspersky Security 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 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。

LAN でプロキシサーバー設定を自動的に検知するための、Web Proxy Auto-Discovery Protocol(WPAD)がネットワークで設定されていないことがあります。その場合、プロキシサーバーにアクセスするときに認証が必要になる場合があります。

► プロキシサーバーにアクセスするためにオプションのプロキシサーバー設定と認証設定を行うには、次の操作を行います:

1. [**Kaspersky Security**]フォルダーの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。

   [**アプリケーションの設定**] ウィンドウが表示されます。

3. [**接続設定**]タブを選択します。

4. [**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**]をオンにします。

5. [**アドレス**]フィールドにプロキシサーバーのアドレスを入力して、[**ポート**]フィールドにプロキシサーバーのポート番号を入力します。

6. [**プロキシサーバーの認証設定**]セクションで、ドロップダウンリストから必要な認証方法を選択します:

   - **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。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を適用する**: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. [**アプリケーションの設定**]ウィンドウで[**OK**] をクリックします。

► 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アプリケーションコンソールを起動します:

   - 保護対象サーバーでアプリケーション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 for Windows Server**] - [**管理ツール**] - [**Kaspersky Security 10.1.2 for Windows Server コンソール**]の順に選択します。
   - 保護対象サーバー以外でアプリケーション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. アプリケーション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。

     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[**別のコンピューター**]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(236 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)。

   アプリケーションコンソールウィンドウが開きます。

2. アプリケーション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. [**プロキシサーバー設定を使用して Kaspersky Lab のアップデートサーバーに接続する**]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. アプリケーション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。

簡易スキャン

Kaspersky Security 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、簡易スキャンタスクを使用してサーバーをスキャンしてマルウェアの有無を確認します。

► 簡易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. アプリケーション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. [**簡易スキャン**]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、[**実行中**]というタスクステータスが詳細ペインに表示されます。

► タスクの実行ログを確認するには:

[**簡易スキャン**]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 for Windows Server の修復

Kaspersky Security 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、パスワードの入力を求められます。

► Kaspersky Security 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 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 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ます。コンテキストメニューで、次のように選択します:
     - **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ます。コンテキストメニューで、[**コンポーネントを使用しない**]を選択します。

   [**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 for Windows Server のコンポーネントのセットが変更されます。

Kaspersky Security 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 for Windows Server のクラッシュ)、Kaspersky Security for Windows Server の修復を試みることができます。修復は、Kaspersky Security for Windows Server の現在の設定を保存したうえで行えます。または、Kaspersky Security 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 for Windows Server を修復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**]を選択します。
2. [**Kaspersky Security for Windows Server**]を選択します。
3. [**Kaspersky Security for Windows Server の変更または削除**]を選択します。

   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。
4. [**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。
5. アプリケーションの設定をリセットし Kaspersky Security 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。[**次へ**]をクリックします。
6. [**修復準備完了**]ウィンドウで[**インストール**]をクリックし、修復操作を確定します。
7. 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。

指定した設定を使用して、Kaspersky Security for Windows Server が修復されます。

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 / 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 for Windows Server、アプリケーションコンソール、Microsoft Outlook アドインを削除する方法について説明します。

このセクションの内容

Kaspersky Security 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 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 for Windows Server をアンインストールしたあと、再起動が必要になる場合があります。再起動は、あと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、修復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、パスワードの入力を求められます。

► Kaspersky Security 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**]を選択します。
2. [**Kaspersky Security for Windows Server**]を選択します。
3. [**Kaspersky Security for Windows Server の変更または削除**]を選択します。

   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。
4. [**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。

5. 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、次の操作を行います:

   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 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 for Windows Server¥Uninstall

   [**次へ**]をクリックします。

6. [**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。
7. 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 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 for Windows Server 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、サーバーからアプリケーションコンソールをアンインストールできます。

アプリケーション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。

► アプリケーション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**]を選択します。
2. [**Kaspersky Security for Windows Server**]を選択します。
3. [**Kaspersky Security 10.1.2 for Windows Server 管理ツールの変更または削除**]を選択します。

   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。
4. [**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。
5. [**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。
6. [**OK**]をクリックします。

アンインストールが完了し、セットアップウィザードが終了します。

Kaspersky Security Microsoft Outlook アドインのアンインストール

► **Microsoft Outlook アドインをアンインストールするには、次の手順を実行します:**

1. サーバーで setup.exe ファイルを実行します。

   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。

2. [**次へ**]をクリックします。

   [**インストールの修復または削除**]ウィンドウが開きます。

3. [**削除**]をクリックします。

   [**Kaspersky Security Microsoft Outlook アドインの削除準備完了**]ウィンドウが表示されます。

4. [**削除**]をクリックします。

   Microsoft Outlook アドインのアンインストールが開始されます。

5. [**終了**]をクリックします。

アンインストールが完了し、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 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 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 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 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 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アプリケーション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 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 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 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。

setup.exe ファイルからの Kaspersky Security for Windows Server のインストールの例

► ユーザーの操作を求めずに、推奨されているインストール設定で Kaspersky Security 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 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コンポーネントとオンデマンドスキャンコンポーネントのみをインストールする。
- Kaspersky Security for Windows Server の開始時にリアルタイム保護を実行しない。
- Microsoft によってスキャン範囲からの除外が推奨されている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:msi ファイルを実行

- ユーザーの操作を求めずに、推奨されているインストール設定で Kaspersky Security 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 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 for Windows Server をインストールしてアクティベートするには:

```
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 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
```

- Kaspersky Security for Windows Server をインストールフォルダー C:¥WSEE に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 for Windows Server をインストールして、Kaspersky Security for Windows Server msi ファイルが保存されているフォルダーに ks4ws.log という名前のインストールログファイルを保存するには、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 for Windows Server 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
```

- 64 ビット版の Microsoft Outlook メールクライアント用に Microsoft Outlook アドイン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 ksmail_x64.msi /qn EULA=1
```

- 32 ビット版の Microsoft Outlook メールクライアント用に Microsoft Outlook アドインをイン

ストールするには、次のコマンドを実行します:

```
msiexec /i ksmail_x86.msi /qn EULA=1
```

► **Kaspersky Security for Windows Server をインストールしてライセンス情報ファイル 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 の設定に応じて Kaspersky Security 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 for Windows Server がパスワードによって保護されている場合、製品のパッチをインストールするには、次のコマンドを実行します:**

```
msiexec /p "<msp ファイル名とそのパス>" UNLOCK_PASSWORD=<パスワード>
```

Kaspersky Security 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トしている場合、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 for Windows Server のインストール中に[**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、すべてのスクリプトの実行時に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 時に簡易スキャンタスクが実行されます。

Kaspersky Security 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 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 for Windows Server の定義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、定義データベース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 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 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、簡易スキャンをサーバーで実行します。

► **コマンドラインを使用して簡易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 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 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
```

または

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

既にインストールされているコンポーネントをインストール対象のコンポーネントとして指定すると、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
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspector,AKIntegration,P
erfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,RamDisk REMOVE=AppCtrl,Fim" /qn
```

Kaspersky Security 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 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
```

または

- 32 ビットオペレーティングシステムの場合：

```
msiexec /x {6607EF9A-4D10-4D3E-B255-6F280BFB3791} /qn
```

- 64 ビットオペレーティングシステムの場合：

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843} /qn
```

► **Kaspersky Security for Windows Server 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
```

または

- 32 ビットオペレーティングシステムの場合：

```
msiexec /x {54B7D218-5645-46DD-8660-41B336E1BD8A} /qn
```

- 64 ビットオペレーティングシステムの場合：

```
msiexec /x {C10F9B07-7FC9-43C0-A5DC-B6CE8A817D76} /qn
```

► **パスワードによる保護が有効である保護対象サーバーから Kaspersky Security 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 {6607EF9A-4D10-4D3E-B255-6F280BFB3791}
UNLOCK_PASSWORD=*** /qn
```

- 64 ビットオペレーティングシステムの場合:

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843}
UNLOCK_PASSWORD=*** /qn
```

► **Microsoft Outlook アド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:**

- 32 ビットオペレーティングシステムの場合:

```
msiexec /x {6AF88E70-817E-4FFE-8389-04A345E7A3D6} /qn
```

- 64 ビットオペレーティングシステムの場合:

```
msiexec /x {410BC997-5B96-41B3-8B31-AAA074FE728B} /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 6. 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 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 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。

コード	説明
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 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 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 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 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、このグループのサーバーに対して Kaspersky Security for Windows Server をインストール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 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 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 のヘルプ**を参照してください。

Kaspersky Security 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 for Windows Server のインストール先となるサーバーに 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（サーバーのドメインや、サーバ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 for Windows Server と一緒にネットワークエージェントを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 for Windows Server のインストール先となるすべてサーバ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、そのドメイン内のサーバ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$** 共有に対する権限
- **サービスとしてログオンする**権限

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

> 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 のヘルプを参照してください。

今後、Kaspersky Security Center を介して Kaspersky Security 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、管理プラグインもインストールされていること（Kaspersky Security 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 for Windows Server と一緒にネットワークエージェントをインストールできます。

あとで 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 1 つの管理グループにまとめることもできます。

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

1. Kaspersky Security Center 管理コンソールを起動します。
2. Kaspersky Security Center で、[**詳細**]フォルダーを展開します。
3. [**リモートインストール**]サブフォルダーを展開します。
4. [**インストールパッケージ**]サブフォルダーの詳細ペインで、[**インストールパッケージの作成**]をクリックします。
5. インストールパッケージの種別として[**カスペルスキー製品のインストールパッケージを作成する**]を選択します。
6. インストールパッケージ名を入力します。
7. インストールパッケージファイルとして、Kaspersky Security 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。
8. 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、使用許諾契約書とプライバシーポリシーに同意する必要があります。
9. インストールする Kaspersky Security for Windows Server コンポーネントのセット(69 ページのセクション「コンポーネントセットの変更と Kaspersky Security for Windows Server の修復」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(53 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:

   a. 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ます。

   b. [**インストールパッケージ**]サブフォルダーの詳細ペインで、作成した Kaspersky Security 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。

   c. 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**]設定グループで、インストールする Kaspersky Security for Windows Server 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ではないものに指定する場合、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サーバーをスキャンする
      - 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. 前のバージョンの Kaspersky Security 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、対象の設定ファイルを指定します。

d. 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。

10. [**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 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 のヘルプ**を参照してください。

11. Kaspersky Security for Windows Server 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 for Windows Server がインストールされます。

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

Kaspersky Security for Windows Server をインストールしたら、サーバーにある Kaspersky Security 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 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、サーバーの簡易スキャンを実行してください。

Kaspersky Security for Windows Server がインストールされたサーバーが、Kaspersky Security Center で同じ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 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。Kaspersky Security Center の管理サーバーをアップデート元として設定します。
2. 簡易スキャンのステータスを持つオンデマンドスキャンのグループタスクを作成します。簡易スキャンタスクの結果ではなく、このタスクの結果に基づいて、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。ポリシーのプロパティの[**アプリケーションの設定**]セクションで、[**システムタスクの実行**]サブセクションの設定から、オンデマンドスキャンのシステム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 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 を使用したアプリケーション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 のヘルプ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アプリケーションコンソールをインストールするには:

1. Kaspersky Security Center 管理コンソールで、[**詳細**]フォルダーを展開します。
2. [**リモートインストール**]サブフォルダーを展開します。
3. [インストールパッケージ]サブフォルダーの詳細ペインで、[**インストールパッケージの作成**]をクリックします。新しいインストールパッケージの作成ウィザードで、次の操作を行います:

    a. [**新規パッケージウィザード**]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**]をパッケージ

の種別として選択します。

b. 新しいインストールパッケージ名を入力します。

c. Kaspersky Security 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。

d. 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 にあるアプリケーションコンソールのみをインストールする場合は、次のコマンドラインオプションを使用します:

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

4. [**インストールパッケージ**]サブフォルダーで、選択したサーバー(管理グループ)にアプリケーション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 のヘルプを参照してください。

5. 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アプリケーション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 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 for Windows Server 管理がパスワードで保護されている場合、1 つ以上のアプリケーションをアンインストールするタスクを作成する際にはパスワードを入力します。パスワードによる保護が Kaspersky Security Center ポリシーにより集中管理されていない場合、Kaspersky Security for Windows Server は、保護対象サーバーのうち入力したパスワードが設定値に適合したサーバーから正常にアンインストールされます。Kaspersky Security 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 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)、管理サーバーがアンインストールを実行するサーバーにアクセスするために使用するアカウントを指定します。Kaspersky Security 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(53 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 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あとで実行する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 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 for Windows Server をインストールできます。同じ方法でアプリケーションコンソールもインストールできます。

Kaspersky Security for Windows Server またはアプリケーション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 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、同じビット数（32 ビットまたは 64 ビット）である必要があります。

ドメイン管理者権限で実行する必要があります。

Kaspersky Security 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。アプリケーション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 for Windows Server（またはアプリケーションコンソール）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ビット数（32 ビットまたは 64 ビット）に対応する 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上の同じパブリックフォルダーにライセンス情報ファイルを保存します（93 ページのセクション「ライセンス情報ファイルについて」を参照）
3. ドメインコントローラー上の同じパブリックフォルダーに、次の内容の install_props.json ファイルを作成します。これにより、使用許諾契約書の条件とプライバシーポリシーに同意したことになります。

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. 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。
5. **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 for Windows Server(またはアプリケーションコンソール)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。
6. 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。
7. `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、Kaspersky Security for Windows Server がインストールされます。

Kaspersky Security 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 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、簡易スキャンを実行してください。これらの処理(67 ページのセクション「Kaspersky Security for Windows Server インストール後に実行する処理」を参照)は、アプリケーションコンソールから実行できます。

Kaspersky Security 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 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 for Windows Server(またはアプリケーションコンソール)をインストールした場合、このポリシーを使用して Kaspersky Security for Windows Server(またはアプリケーションコンソール)をアンインストールできます。

この方法で本製品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がパスワードによって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 for Windows Server をアンインストールすることはできません。

► **Kaspersky Security for Windows Server（またはアプリケーションコンソール）をアンインストールするには：**

1. Kaspersky Security for Windows Server またはアプリケーションコンソールをアンインストール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 for Windows Server のインストール用に作成したポリシーを選択し、**グループポリシーオブジェクトエディター**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**］ - ［**ソフトウェアの設定**］ - ［**ソフトウェアインストール**］）で Kaspersky Security for Windows Server（またはアプリケーションコンソール）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**］を選択します。
3. アンインストール方法として［**直ちに、ソフトウェアをユーザーとコンピューターからアンインストールする**］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 for Windows Server がサーバーから削除されます。

Kaspersky Security for Windows Server の機能のテスト：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 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テスト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テスト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本物のマルウェアではなく、お使いのコンピューターに損害を与える可能性のある実行コードは含まれていません。ただし、ほとんど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るように作成されています。

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、そのドライブ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 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、アプリケーション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 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 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 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 for Windows Server のファイルのリアルタイム保護タスクと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 7. EICAR ファイルの接頭辞

接頭辞	スキャンおよび Kaspersky Security for Windows Server 処理後のファイルステータス
接頭辞なし	Kaspersky Security 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 for Windows Server によって「**感染の可能性あり**」のステータスがヒューリスティックアナライザーにより検知されたオブジェクトに割り当てられます。さらに、感染の可能性があるオブジェクトは駆除されないため、そのオブジェクトは削除されます。
WARN-	Kaspersky Security for Windows Server によって「**感染の可能性あり**」のステータスがオブジェクト（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）に割り当てられます。さらに、感染の可能性があるオブジェクトは駆除されないため、そのオブジェクトは削除されます。
CURE-	Kaspersky Security 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。

リアルタイム保護機能とオンデマンドスキャン機能のテスト

Kaspersky Security for Windows Server のインストール後、Kaspersky Security 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。これを確認するには、テスト用ウイルス EICAR を使用します(「テスト用ウイルス EICAR について」(86 ページ)を参照)。

► リアルタイム保護機能をテストするには、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 Messenger サービスが有効になっていることを確認してください。
3. アプリケーションコンソールを開きます。
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。
- アプリケーションコンソールで、実行ログに「**緊急**」のステータスが割り当てられている。ファイル eicar.com 内の脅威に関する情報がログの新しい行に記録される(実行ログを確認するには、アプリケーションコンソールツリーで[**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 for Windows Server` によって、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` へのアクセスが <イベント発生時> にブロックされました。理由:脅威の検知。検知した脅威:`EICAR-Test-File`。ユーザー名:<ユーザー名>。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 サービスが実行され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テストするには、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. アプリケーションコンソールを開きます。
3. 次の操作を行います:
    a. アプリケーション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. [**簡易スキャン**]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. 簡易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。
- アプリケーションコンソールで、実行ログに「**緊急**」のステータスが割り当てられている。ファイル eicar.com 内の脅威に関する情報が簡易スキャンタスクのログの新しい行に記録される(実行ログを確認するには、アプリケーションコンソールツリーで[**オンデマンドスキャン**]サブフォルダーを展開し、簡易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

管理プラグインとローカルのアプリケーションコンソールを使用して、Kaspersky Security for Windows Server を管理できます。

ローカルのアプリケーションコンソールインターフェイスでの操作については、セクション「アプリケーションコンソールの使用」で説明しています（143 ページのセクション「Kaspersky Security for Windows Server コンソールの使用」を参照）。

Kaspersky Security Center 管理コンソールインターフェイスは、管理プラグインを使用した操作の実行に使用されます。Kaspersky Security Center インターフェイスの詳細については、**Kaspersky Security Center のヘルプ**を参照してください。

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 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

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(定義データベースをアップデートできないなど)。Kaspersky Security 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。

製品版ライセンスで利用できる製品の機能は、選択した製品に応じて異なります。選択した製品は、[ライセンス証明書]に記載されています(92 ページの「ライセンス証明書について」を参照)。利用可能な製品の情報は、カスペルスキーの Web サイト https://www.kaspersky.co.jp/small-to-medium-business-security に記載されています。

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。

追加する予備のライセンスは、使用中のライセンスよりも有効期限が後に設定されていることを確認してください。

定額制サービスを予備のライセンスとして使用することはできません。

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(該当する場合)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

ライセンス情報について

ライセンス情報は、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。ライセンス情報はカスペルスキーが生成します。

ライセンス情報ファイルを使用して、本製品にライセンスを追加できます。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。製品版のライセンスまたは試用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。

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、カスペルスキーによって提供される .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 for Windows Server の購入時、または Kaspersky Security for Windows Server の試用版の注文時に、メールで提供されます。

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

ライセンス情報ファイルを復元するには、次のいずれかの操作を行います:

- ご購入元の販売代理店へ問い合わせる
- カスペルスキーの Web サイト(https://keyfile.kaspersky.com/ja/)にアクセスし、有効なアクティベーションコードを使用してライセンス情報ファイルを取得します。

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、20 文字の英数字で構成された一意な文字の並びです。Kaspersky Security for Windows Server をアクティベートするライセンスを追加するには、アクティベーションコードを入力する必要があります。アクティベーションコードは、Kaspersky Security for Windows Server の購入時または試用版の提供時に支給されます。

アクティベーションコードを使用して製品をアクティベートするには、Kaspersky Lab のアクティベーションサーバーに接続するためにインターネットアクセスが必要です。

本製品のインストール後にアクティベーションコードを紛失した場合は、復元できます。アクティベーションコードは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。アクティベーションコードを復元するには、カスペルスキーのテクニカルサポートにお問い合わせください。

定額制サービスについて

定額制サービスは、選択されたパラメータ(定額制サービスの有効期限、保護されるデバイスの数)の範囲内で製品を使用する権利を提供します。Kaspersky Security for Windows Server の定額制サービスは、サービスプロバイダー(ご利用の ISP など)で登録できます。定額制サービスは、手動または自動で延長することも、キャンセルすることもできます。定額制サービスを中断して、再開することもできます。定額制サービスは、サービスプロバイダーを通して管理できます。ユーザーが個別で管理することはできません。

定額制サービスの管理オプションは、サービスプロバイダーによって異なります。サービスプロバイダーによっては、定額制サービスの更新に対して**猶予期間**を設定している場合があります。

猶予期間とは、定額制サービスの終了から更新までのあいだ、製品の機能が変わらず残される期間です。

定額制サービスには、**制限ありと無制限**の種別があります。

期限付きの定額制サービスは、有効期間があり、自動で更新されません。

無制限の定額制サービスは、期限より前に支払いが行われた場合、何も行わなくても自動でライセンスが更新されます。また、決められた有効期限はありません。

定額制サービスのステータスは、[**Kaspersky Security**]フォルダーの詳細ペインに表示され、1 時間ごとに自動で更新されます。定額制サービスのステータスは手動で更新できません。

> 定額制サービスによって取得されるアクティベーションコードは、以前のバージョンの製品のアクティベーションに使用することはできません。

データの提供について

Kaspersky Security for Windows Server の使用許諾契約書の「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。使用許諾契約書に同意する前に、その条項ならびに使用許諾契約書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（www.kaspersky.co.jp/Products-and-Services-Privacy-Policy）に従って保護され、処理されます。

使用許諾契約書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仕組みをサポートするための情報 - インストールされている製品とアクティベーションに関する情報：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、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の情報（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。

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：

- 本製品のインストール中、Kaspersky Security for Windows Server インストールウィザードで、使用許諾契約書の全文が表示されます。表示されるのは、使用許諾契約書への同意を要求するステップです。
- TXT 形式のファイル（license.txt）に、使用許諾契約書の全文が記載されており、いつでも参照できます。このファイルは、Kaspersky Security for Windows Server 配布キットに、本製品のインストールファイルとともに同梱されています。

ローカルでのデータ取り扱い方法

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 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。

Kaspersky Security for Windows Server は次のデータをローカルで処理し、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、実行したファイルプロセスのチェックサム（MD5、SHA-256）とタイムスタンプ、デジタル署名属性、実行されたスクリプトの情報など）。

- 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、実行ファイルの起動、ファイルのチェックサムと属性)。
- 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)。
- スキャンされた Web アドレスに関する情報。例:ダウンロードが開始された URL と IP アドレス、ダウンロード元の Web ページ、プロトコルの識別子、接続ポートの番号、アドレスが有害かどうかの属性、ファイルサイズ、チェックサム(MD5、SHA-256)、ファイルをダウンロードしたプロセスのチェックサム(MD5、SHA-256)、デバッグ中の検知であることを示す属性、接続プロトコルの識別子、使用されたポート番号、スキャンされた URL、スキャンされたファイルの名前、Web 証明書のデータ。

Kaspersky Security 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保護されます。

Kaspersky Security 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や、処理されたデータの保管に関する既定の設定の詳細は、本ガイドの該当するセクションを参照してください。

本製品がローカルで処理したデータが、Kaspersky Lab のシステムやその他のサードパーティのシステムに自動的に送信されることはありません。

既定では、本製品が動作中にローカルで処理したすべてのデータは、サーバーから Kaspersky Security for Windows Server をアンインストールすると削除されます。

ただし例外として、診断情報のファイル(トレースファイル、ダンプファイル)と Windows イベントログに記録された本製品のイベントは削除されずに残ります。これらのファイルを手動で削除することを推奨します。

本製品の診断データを含むファイルの取り扱いについて詳しくは、本ガイドの該当するセクションを参照してください。

Kaspersky Security for Windows Server のプログラムイベントを含む Windows イベントログは、オペレーティングシステムの標準の方法で削除できます。

本製品の補助コンポーネントによるローカルでのデータ取り扱い方法

Kaspersky Security for Windows Server のインストールパッケージには、本製品の補助コンポーネントが含まれています。これらの補助コンポーネントは、Kaspersky Security for Windows Server がインストールされていないサーバーまたはワークステーションにもインストールできます。補助コンポーネントとして次のコンポーネントが挙げられます:

- アプリケーションコンソール:Kaspersky Security for Windows Server の管理ツールセットに含まれ、Microsoft 管理コンソールのスナップインとして動作するコンポーネントです。
- Microsoft Outlook メールクライアント用のアドイン:メールのアンチウイルススキャンを提供するコンポーネントです。
- 管理プラグイン:Kaspersky Security Center と本製品との完全な連携を提供するコンポーネントです。

このガイドで説明されている本製品の主要な機能の実行時、本製品の補助コンポーネントはそれぞれがインストールされているサーバーのローカルでデータを処理し、保存します。これは、補助コンポーネントが Kaspersky Security for Windows Server 本体とは別のサーバーにインストールされている場合にも当てはまります。

それぞれの補助コンポーネントは次のデータをローカルで処理し、保存します:

- アプリケーションコンソール:Kaspersky Security for Windows Server がインストールされているサーバーでアプリケーションコンソールが最後にリモート接続したサーバー名(IP アドレスまたはドメイン名)、 Microsoft 管理コンソールで設定されている表示パラメータ、アプリケーションコンソールが最後に選択したオブジェクトが含まれるフォルダーに関するデータ([**参照**]をクリックしてシステムダイアログを開きオブジェクトを選択した場合)。アプリケーションコンソールのトレースファイルには次の情報が含まれます:Kaspersky Security for Windows Server がインストールされているサーバーでリモート接続が確立されたサーバー、リモート接続の確立に使用されたユーザーアカウント名
- Microsoft Outlook メールクライアント用のアドインは、トレースファイルにのみデータを保存します。Microsoft Outlook メールクライアント用のアドインのトレースファイルには次の情報が含まれます:メールメッセージのフィールド(「宛先」「差出人」「件名」)に含まれるデータ、メッセージ本文と添付ファイルのメタデータ(種別、サイズ、添付ファイルの名前)
- 管理プラグインは、Kaspersky Security for Windows Server が処理したデータを処理し、一時的に保存します。該当するデータとして、たとえば、本製品のタスクとコンポーネントで設定したパラメータ、Kaspersky Security Center のポリシーのパラメー

タ、ネットワークリストで送信されたデータなどが含まれます。

補助コンポーネントがローカルで処理したデータが、Kaspersky Lab のシステムやその他のサードパーティのシステムに自動的に送信されることはありません。

既定では、本製品の補助コンポーネントが動作中にローカルで処理したすべてのデータは、該当する補助コンポーネントをアンインストールすると削除されます。

ただし例外として、補助コンポーネントのトレースファイルは削除されずに残ります。これらのファイルを手動で削除することを推奨します。

本製品の補助コンポーネントの診断データを含むファイルの取り扱いについて詳しくは、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

ライセンスを適用して Kaspersky Security for Windows Server をアクティベートできます。

Kaspersky Security 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。以前に追加されたライセンスは削除されます。

Kaspersky Security 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。以前に追加された予備のライセンスは削除されます。

Kaspersky Security 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ります。この場合、予備のライセンスは削除されません。

► Kaspersky Security for Windows Server をアクティベートするには:

1. アプリケーション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。ライセンスを予備のライセンス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、アプリケーションコンソールにある[**Kaspersky Security**]フォルダーの詳細ペインに表示されます。ライセンスには、次のステータスがあります:

- **ライセンスのステータスを確認しています** - Kaspersky Security for Windows Server は、適用されたライセンス情報ファイルまたはアクティベーションコードをチェックして、現在のライセンスのステータスに関する応答を待ちます。

- **ライセンスの有効期限** - Kaspersky Security 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、予備のライセンス情報ファイルが適用されていない。
  - 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** - ライセンス情報ファイルまたは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 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 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 for Windows Server はアクティベートされていません(91 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登録されています** - ライセンス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:

アプリケーション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(次の表を参照)。

表 8. [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。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**]フォルダーの詳細ペインの[**アクティベーション**]には、次のステータスが表示されます: • **適用済み** - アクティベーションコードまたはライセンス情報ファイル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、ステータスは[**適用済み**]に変更されます。 • **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	本製品のアクティベーションに使用されたライセンス。
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。

フィールド	説明
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、またはライセンス情報ファイルのステータス：アクティブまたは追加。

► ライセンスの詳細情報を表示するには：

［**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。

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 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）。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	本製品のアクティベーションに使用されたライセンス。
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**と表示されます。
アプリケーション	そのライセンス情報ファイルまたはアクティベーションコードでアクティベートされたアプリケーションの名前。
機能制限	ライセンスの使用における制限（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識別 ID。
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。
- ファイルのリアルタイム保護、オンデマンドスキャン、およびアプリケーションの整合性チェック以外のすべてのタスクを起動できません。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、期限切れが近づいている旨の通知が表示されます。この時、[**Kaspersky Security**]フォルダーの詳細ペインの、[**ライセンスの有効期限**]のステータスが黄色にハイライト表示されます。

予備のライセンス情報ファイルまたはアクティベーションコードを使用して、有効期限前にライセンスを更新できます。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、サーバ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. アプリケーション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. [**予備のライセンスとして使用する**]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. [**予備のライセンスとして使用する**]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 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. アプリケーション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。

管理プラグインの使用

このセクションでは、Kaspersky Security for Windows Server 管理プラグインについての情報を提供するとともに、保護対象のサーバーまたはサーバーのグループにインストールされている Kaspersky Security for Windows Server を管理する方法について説明します。

この章の内容

Kaspersky Security Center を使用した Kaspersky Security for Windows Server の管理

Kaspersky Security for Windows Server がインストールされ、管理グループに含まれた複数のサーバーを、Kaspersky Security for Windows Server 管理プラグインを使用することで集中管理できます。Kaspersky Security Center では、管理グループに含まれる各サーバーの操作設定を個別に設定することもできます。

管理グループは、Kaspersky Security Center 側で手動で作成され、Kaspersky Security 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 のヘルプ**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 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、個別の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 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、アプリケーション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、およびスケジュールによるシステムタスクの開始設定が行えます。

- **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を使用する**: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個別のサーバーに対して、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 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。

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 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 for Windows Server の管理

Kaspersky Security for Windows Server がインストールされ、管理グループに含まれた複数のサーバーを、Kaspersky Security for Windows Server 管理プラグインを使用することで集中管理できます。Kaspersky Security Center では、管理グループに含まれる各サーバーの操作設定を個別に設定することもできます。

管理グループは、Kaspersky Security Center 側で手動で作成され、Kaspersky Security 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 のヘルプ**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 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、個別の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 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、アプリケーション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、およびスケジュールによるシステムタスクの開始設定が行えます。

- **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を使用する**: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個別のサーバーに対して、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 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。

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

ポリシーでの全般的な製品設定の表示と編集

► ポリシーから Kaspersky Security for Windows Server のアプリケーションの設定を開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**アプリケーションの設定**]セクションを選択します。
6. 設定のサブセクションで、[**設定**]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での全般的な製品設定の表示と編集

► 単一のサーバーで Kaspersky Security for Windows Server のプロパティウィンドウを開くには:

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. タスクを設定する管理グループを選択します。
3. [**デバイス**]タブを選択します。

4. 次のいずれかの方法で、サーバ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。
   - 保護対象サーバーのコンテキストメニューで[**プロパティ**]を選択します。

   サーバーのプロパティウィンドウが表示されます。
5. [**アプリケーション**]セクションで、[**Kaspersky Security for Windows Server**]を選択します。
6. [**プロパティ**]をクリックします。

   Kaspersky Security for Windows Server のアプリケーション設定ウィンドウが開きます。
7. [**アプリケーションの設定**]セクションを選択します。

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 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

► 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:

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. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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。
5. [**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 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**

       使用するプロセス数が自動的に調整されます。

       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 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 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。
   - [**ユーザーインターフェイス**]セクションで、[**タスクバーにシステムトレイアイコンを表示する**]をオンまたはオフにして、通知領域に表示される製品のシステムトレイアイコンの設定を行います。
6. [**階層型ストレージ**]タブで、階層型ストレージにアクセスするためのオプションを選択します(503 ページのセクション「HSM システムの管理プラグインからの設定」を参照)。
7. [**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

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

> Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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。
5. [**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 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 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 for Windows Server によって Kaspersky Security 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 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。
   - [**UPS バックアップ電源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 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、サーバーで 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、サーバーで 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 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、サーバーで UPS 電源に切り替えられたあと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、サーバーで UPS 電源に切り替えられたあとで、Kaspersky Security 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、サーバーで UPS 電源に切り替えられたあとでも、Kaspersky Security 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。
   - [**パスワードによる保護の設定**]セクションで、Kaspersky Security 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。
6. [**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

接続設定は、Kaspersky Security 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 サービスと連携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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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。
5. [**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 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。
     - **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 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 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 for Windows Server がインストールされているコンピューターをホスト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。

6. [**OK**]をクリックします。

接続設定の内容が保存されます。

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以下の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 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: 簡易スキャン、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、アプリケーションの整合性チェック。
- 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 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、目的のグループを展開し、[**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 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**]を選択します。
3. ポリシーの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. 設定するポリシーがアクティブで、選択された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 での隔離およびバックアップ設定

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**詳細設定**]セクションで、[**保管領域**]サブセクションの[**設定**]をクリックします。
5. 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目的の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**]セクションで保護対象の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。

6. [**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**]で保護対象の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。
7. [**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。

ネットワークリソースへのアクセスのブロック：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保管領域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

ブロック対象コンピューターの保管領域について

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保管領域が既定でインストールされます：ファイルのリアルタイム保護、NetApp のアンチクリプター、アンチクリプター。コンポーネントはブロック対象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フォルダー上のオブジェクトをリモートコンピューターから暗号化したり開こうとする、あるいは実行しようとする試行を検出します。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 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保管領域には、次のタスクのうち 1 つ以上のタスクが有効な状態で開始されており、なおかつ指定の条件が満たされている場合に情報が追加されます：

- ファイルのリアルタイム保護タスクの場合：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のネットワーク共有リソースへのア**

クセスをブロックする]がオンにされている。

- アンチクリプタータスクの場合: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場合:ネットワーク接続ストレージへの攻撃が検知された。

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、コンピューターのブロックに関する警告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。

攻撃元のコンピューターの LUID(ローカルで一意な識別子)がブロック対象コンピューターのリストに追加されると、Kaspersky Security for Windows Server はこの攻撃元コンピューターの IP アドレスを特定し、ブロック対象コンピューターのリストに LUID のかわりに IP アドレスを追加します。

Kaspersky Security for Windows Server は既定で、ブロック対象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。ブロック対象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。

任意のユーザーアカウントに対して保管領域の管理操作へのアクセスを制限する場合、ブロック対象コンピューターの保管領域には引き続きアクセスできます。選択したユーザーアカウントが Kaspersky Security for Windows Server を管理するための**編集権限**を持っていない場合に限り、ブロック対象コンピューターの設定を変更することはできません。

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保管領域を設定するには:

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。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**詳細設定**]セクションで、[**保管領域**]サブセクションの[**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。
5. [**ブロック対象コンピューターの保管領域**]タブの[**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。
6. [**OK**]をクリックします。

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 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 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個別のコンピューター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 のヘルプ**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。

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 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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。
5. [**ログの設定**]ウィンドウで、要件に従って Kaspersky Security 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 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、[**参照**]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。
6. [**OK**]をクリックします。

ログの設定が保存されます。

セキュリティログ

Kaspersky Security 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(サーバー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、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では記録内容を削除できます(「システム監査ログからのイベントの削除」(210 ページ)を参照)。さらに Kaspersky Security for Windows Server では、セキュリティログの記録内容の削除に関するシステム監査イベントが記録されます。

SIEM 連携の設定

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の性能低下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実行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 連携を使用できます:

- 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実行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 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指定できます。

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 連携は使用されません。SIEM 連携は、有効化や無効化、機能の設定ができます(次の表を参照)。

表 9. SIEM 連携の設定

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 連携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。
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 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 連携設定を編集するには:

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。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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。

5. [**SIEM 連携**]タブを選択します。

6. [**連携の設定**]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 連携設定を使用して SIEM に送信されます。

   チェックボックスがオフの場合、SIEM 連携は実行されません。チェックボックスがオフの場合、SIEM 連携を設定できません。

   既定では、このチェックボックスはオフです。

7. 必要に応じて、[**連携の設定**]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。

8. [**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。

9. [**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、[**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。

10. [**OK**]をクリックします。

設定済みの SIEM 連携設定が適用されます。

通知の設定

► Kaspersky Security 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます（「ポリシーの設定」（125 ページ）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には、[**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（「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」（129 ページ）参照）。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**ログと通知の設定**]セクションで、[**イベント通知**]サブセクションの[**設定**]をクリックします。
5. [**通知の設定**]ウィンドウで、要件に従って Kaspersky Security 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 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[**簡易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。
     - **簡易スキャンが長期間実行されていません（日）**

簡易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。

6. [**OK**]をクリックします。

通知の設定内容が保存されます。

管理サーバーとのインタラクションの設定

► Kaspersky Security 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。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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。
5. [**管理サーバーのネットワークリスト**]ウィンドウで、Kaspersky Security 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:
   - 隔離されたオブジェクト
   - バックアップされたオブジェクト
   - ブロック対象コンピューター
6. [**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。

ポリシーの作成と編集

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 for Windows Server の管理について説明します。

Kaspersky Security Center のグローバルポリシーは、Kaspersky Security 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 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**」として示されます。

ポリシー適用に関する情報は、Kaspersky Security for Windows Server システム監査ログに記録されます。この情報は、アプリケーションコンソールの[**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 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アプリケーション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、アプリケーションコンソールで編集できます。

また、アクティブポリシーで設定し 🔒 アイコンが付いている設定は、個別のコンピューターに対する Kaspersky Security Center のコンピューターのプロパティウィンドウを使用した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。

ポリシーでサーバーのリアルタイム保護タスクまたは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。

この章の内容

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、サーバーのリアルタイム保護タスク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、サーバーのリアルタイム保護タスクの設定、Kaspersky Security 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 for Windows Server のイベントに関するユーザー通知と管理者へ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 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. 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。

   [**新規ポリシーウィザード**]ウィンドウが開きます。
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**]ウィンドウで、Kaspersky Security for Windows Server を選択して[**次へ**]をクリックします。
4. [**名前**]にグループポリシー名を入力します。

   次の記号をポリシー名に含めることはできません:" * < : > ? ¥ | 。
5. 前の製品のバージョンに使用されたポリシー設定を適用するには:
   a. [**旧バージョンのアプリケーションのポリシー設定を使用する**]をオンにします。
   b. [**選択**]をクリックします。
   c. 適用するポリシーを選択します。
   d. [**次へ**]をクリックします。
6. [**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**]:既定の設定を使用した新しいポリシーを作成します。
   - **以前のバージョンの Kaspersky Security for Windows Server で作成したポリシーをインポート**:該当する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。
7. [**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と KSN の使用タスク、脆弱性攻撃ブロックとスクリプト監視の設定を行います。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、サーバーの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**]サブセクションの[**設定**]をクリックします。表示されるウィンドウで、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**]サブセクションの[**設定**]をクリックします。表示されるウィンドウで、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 の使用タスクを開始するには、[データの取り扱い方法]ウィンドウで KSN に関する声明に同意する必要があります(284 ページのセクション「データの取り扱い方法の管理プラグインからの設定」を参照)。
   - 脆弱性攻撃ブロックコンポーネントの既定の設定を編集するには、[**脆弱性攻撃ブロック**]サブセクションの[**設定**]をクリックします。表示されるウィンドウで、必要に応じて機能の設定を行います。[**OK**]をクリックします。

8. [**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、既存のポリシーは無効となり、新しいポリシーが適用されます。
   - **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、ポリシーはあとで有効にできます。
   - [**ポリシーの作成後すぐにプロパティを開く**]をオンにすると、**新規ポリシーウィザード**が自動的に閉じ、[**次へ**]をクリックしたあとで新しく作成されたポリシーを設定します。
9. [**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 for Windows Server のその他の設定、タスク、機能を設定できます。

Kaspersky Security for Windows Server のポリシーに含まれる設定セクション

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。

イベントの設定

[**イベントの設定**]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**
- **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設定

表 10. [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**]サブセクションで[**設定**]をクリックして、次の設定を行えます: • 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**]サブセクションで[**設定**]をクリックして、次の設定を行えます: • 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による保護の有効化または無効化
接続	[**接続**]サブセクションで[**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**]サブセクションで[**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できます: • 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 11. [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**]サブセクションの[**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**]サブセクションで[**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**]サブセクションで、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 for Windows Server を管理できます。
Kaspersky Security サービス管理用のユーザーアクセス権限	[**Kaspersky Security サービス管理用のユーザーアクセス権限**]サブセクションで、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**]サブセクションで[**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 • 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 12. [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**]サブセクションで[**設定**]をクリックして、次のタスク設定を行えます: • 保護モードの指定 • 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) • タスク開始の設定
KSN の使用	[**KSN の使用**]サブセクションで[**設定**]をクリックして、次のタスク設定を行えます: • KSN で信頼されていないオブジェクトに対する処理の指定 • データ転送と、Kaspersky Security Center の KSN プロキシサーバーとしての使用を設定します。 [**データの取り扱い方法**]をクリックして、KSN 声明と KMP 声明に同意するか同意しないかを選択し、信頼できるデータ交換方法を設定します。
脆弱性攻撃ブロック	[**脆弱性攻撃ブロック**]サブセクションで[**設定**]をクリックして、次のタスク設定を行えます: • 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

ローカルアクティビティの管理

表 13. [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**]サブセクションで[**設定**]を使用して、次のタスク設定を行えます: • タスク処理モードの選択 • 次回以降のアプリケーション起動に対するコントロールの適用設定 • アプリケーション起動コントロールルールの範囲の指定 • KSN の使用設定 • タスク開始の設定

デバイスコントロール	[**デバイスコントロール**]サブセクションで[**設定**]をクリックして、次のタスク設定を行えます: • タスク処理モードの選択 • タスク開始の設定

ネットワークアクティビティの管理

表 14. [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**]サブセクションで[**設定**]をクリックして、次のタスク設定を行えます: • ファイアウォールのルールの設定 • タスク開始の設定

システム監査

表 15. [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**]サブセクションで、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 16. [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
タスク実行ログ	[**実行ログ**]サブセクションで[**設定**]をクリックして、次の設定を行えます: • 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 との連携の指定
イベント通知	[**イベント通知**]サブセクションで[**設定**]をクリックして、次の設定を行えます: • [**オブジェクトが検知されました**]イベント、[**信頼しない大容量ストレージが検出および制限されました**]イベント、[**コンピューターが信頼しないリストに追加されました**]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 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。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を編集することもできます。

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 for Windows Server - ネットワーク接続ストレージ保護導入ガイド**』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。

ポリシーの設定

既存のポリシーのプロパティウィンドウでは、Kaspersky Security 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 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、ポリシーの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**]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** - 選択した管理グループ内のすべてのサーバーで後からポリシーを有効にする場合に選択します。

   モバイルユーザーポリシーは、Kaspersky Security for Windows Server を管理している場合は使用できません。
5. [**イベントの設定**]、[**アプリケーションの設定**]、[**詳細設定**]、[**ログと通知の設定**]、[**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 Center を使用したタスクの作成と編集

このセクションでは、Kaspersky Security 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（109 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 のヘルプ**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 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. 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ます。
     b. タスクを作成する管理グループを選択します。
     c. 詳細ペインで[**タスク**]タブを開き、[**タスクの作成**]を選択します。
   - カスタマイズ可能な条件を指定して、1 台以上のサーバーを対象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の[**デバイスの抽出**]フォルダーで抽出を実行し、抽出結果に対して[**処理を実行**]から[**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. [**タスク種別の選択**]ウィンドウの[**Kaspersky Security for Windows Server**]ヘッダーで、作成するタスクの種別を選択します。
3. 定義データベースのロールバック、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のいずれか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。タスクの種別に応じて、設定が異なります：
   - オンデマンドスキャンタスクを作成します（451 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）。
   - 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指定します：
     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. [**接続設定**]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**]ウィンドウで:

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. 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てインストールするか、インストールはせずに使用可能かどうかのチェックだけを行うかを選択します。

  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。

  c. Kaspersky Security 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へ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には:

  a. [**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。

  b. ライセンスを更新するタスクを作成するには[**予備のライセンスとして使用する**]をオンにします。

- 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作成します(364 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ルールの自動作成タスクの作成」を参照)。
- デバイスコントロールルールの自動作成タスクを作成します(398 ページのセクション「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」を参照)。

4. タスクのスケジュールを設定します(139 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)(定義データベースのロールバックタス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)。
5. [**OK**]をクリックします。
6. 作成したタスクが複数のサーバー用である場合は、タスクを実行するサーバーのグループを選択します。
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 文字以内にする必要があり、**" * < > ? ¥ | :** の記号は使用できません)。

   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。
9. [**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の設定ウィンドウでのローカルタスクの設定

► アプリケーションの設定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の全般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、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 でのグループタスクの設定

► 複数のサーバーに対してグループタスクを設定するには:

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、製品のタスク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[**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 のヘルプ**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、スキャン範囲を設定します。
     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連携を設定します。
   - 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. [**設定**]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、アップデート元の接続を設定します。
   - 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**]セクションで、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て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情報ファイルを追加する場合は、[**予備のライセンスとして使用する**]をオンにします。
   - 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 のヘルプ**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 のヘルプ**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 17. Kaspersky Security for Windows Server グループタスクの設定

Kaspersky Security 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
アプリケーション起動コントロールルールの自動作成	**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: • 実行中のアプリケーションに基づいて許可ルールを作成する • 特定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
	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** • **デジタル証明書の発行先とサムプリントを使用する** • **証明書がない場合に使用** • **SHA256 ハッシュを使用する** • **次の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** Kaspersky Security 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。
デバイスコントロールルールの自動作成	**設定**	• 処理モードを[過去に接続されたすべての大容量ストレージについてシステムデータを考慮する]と[現在接続している大容量ストレージだけを考慮する]から選択します。 • Kaspersky Security for Windows Server がタスク完了時に作成する許可ルールリストで、設定ファイルを設定します。
	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。
製品のアクティベーション(134 ページのセクション「製品のアクティベーションタスク」を参照)	**アクティベーション設定**	製品のアクティベーションやライセンスの更新には、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追加します。
	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。

アップデートのコピー（134 ページのセクション「アップデートタスク」を参照）	**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、Kaspersky 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**］セクションからリンクされた［**接続設定**］ウィンドウでは、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。
	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（134 ページのセクション「アップデートタスク」を参照）	**設定**	［**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、Kaspersky 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** • **最適化に使用するメモリ（MB）**
	［**接続設定**］ウィンドウ	［**アップデート元**］セクションからリンクされた［**接続設定**］ウィンドウでは、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。
	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（「アップデートタスク」（134 ページ）を参照）	**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、Kaspersky 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**]の[**接続設定**]リンクをクリックして開くウィンドウでは、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。
	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の設定（451 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）	**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	[**スキャン範囲**]セクションからリンクされた[**オンデマンドスキャンの設定**]ウィンドウでは、定義済みのセキュリティレベルのいずれかを選択したり、セキュリティレベルを手動でカスタマイズできます。
	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スティックアナライザーの使用を有効または無効にできます。また、スライダーを使用して分析レベルを設定できます。 [**他のコンポーネントとの連携**]セクションで、次の設定を行えます: • 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タスクを実行する(優先度「低」)か、またはタスクを簡易スキャンとします。
	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(136 ページ)	**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 のヘルプ**を参照してください。

このセクションの内容

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 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、製品のタスク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[**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 のヘルプ**を参照してください。
5. [**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指定します。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、[**予備のライセンスとして使用する**]をオンにします。
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 のヘルプ**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 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、製品のタスク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[**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 のヘルプ**を参照してください。

5.

6. 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、Kaspersky 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、メモリ上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メモリのサイズ(MB)。既定のメモリのサイズは 512 MB です。最小のメモリのサイズは 400 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 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 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。

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。

> 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 のヘルプ**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、Kaspersky Security Center の[**通知**]セクションと[**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 のヘルプ**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グループタスクを設定するには:**

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、製品のタスク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[**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 のヘルプ**を参照してください。
5. [**デバイス**]セクションで、アプリケーションの整合性チェックタスクを設定するデバイスを選択します。
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 のヘルプ**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。

   新たに設定したタスクの内容が保存されます。

クラッシュの診断設定

Kaspersky Security for Windows Server の使用中に Kaspersky Security 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 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 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 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 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(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」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設定**]ウィンドウを開きます(129 ページのセクション「**Kaspersky Security Center のアプリケーションの設定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**]タブ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 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 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 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 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 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 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 18. Kaspersky Security 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 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 の連携のためのサブシステム
bl	コントロールプロセス、Kaspersky Security 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 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 for Windows Server スナップインのトレース設定(gui)および Kaspersky Security Center の管理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あとに適用されます。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 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 for Windows Server は、すべての Kaspersky Security for Windows Server コンポーネントのデバッグ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、[**クラッシュ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、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 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

アプリケーションコンソールでは、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。

► グループ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 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. 保護対象サーバーが所属するグループを選択します。
3. 結果ペインで、[**タスク**]タブを選択します。
4. 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:
   - タスクの名前をダブルクリックする。
   - 対象のタスクのコンテキストメニューを開き、[プロパティ]を選択する。
5. [**スケジュール**]セクションを選択します。
6. [**スケジュール設定**]セクションで、[**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。

7. 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、[**間隔:<数字> 時間**]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、[**間隔:<数字> 日**]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、[**間隔:<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 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(109 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)。

8. [**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時間帯を 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。
9. [**OK**]をクリックします。
10. [**適用**]をクリックして、タスクの開始設定を保存します。

Kaspersky Security Center を使用して 1 つのタスクの設定を指定する場合、「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」セクション(129 ページ)で説明されている手順を実行します。

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. 管理コンソールのタスク一覧で、開始スケジュールを設定するタスク名の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。
   [**タスクの設定**]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. [**OK**]をクリックします。

5. [**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。

Kaspersky Security Center のレポート

Kaspersky Security Center のレポートには、管理対象デバイスのステータスに関する情報が含まれます。レポートは管理サーバーに保存される情報に基づきます。

Kaspersky Security Center 11 より、Kaspersky Security for Windows Server で次の種別のレポートが利用できるようになりました:

- アプリケーションコンポーネントのステータスに関するレポート
- ブロック対象アプリケーションのレポート
- テストモードでのブロック対象アプリケーションのレポート

Kaspersky Security Center のレポートやその設定方法の詳細は、**Kaspersky Security Center のオンラインヘルプ**を参照してください。

製品コンポーネントのステータスに関するレポート

すべてのネットワークデバイスの保護ステータスを監視するとともに、各デバイスで設定されているコンポーネントの構造化された概要を取得できます。

レポートには、コンポーネントごとに次のステータスのいずれかが表示されます: **実行中、一時停止済み、停止済み、誤動作、未インストール、開始中**

[**未インストール**]ステータスは、アプリケーション自体ではなくコンポーネントの状態を示します。アプリケーションが Kaspersky Security Center にインストールされていない場合は、N/A(利用不可)のステータスを割り当てます。

コンポーネントを指定したりフィルターを使用して、指定したコンポーネントが指定した状態でインストールされているネットワークデバイスを表示できます。

コンポーネントの指定方法について詳しくは、**Kaspersky Security Center のオンラインヘルプ**を参照してください。

► アプリケーションの設定でコンポーネントステータスを確認するには:

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. [**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(129 ページのセクション「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」を参照)。
3. [**コンポーネント**]セクションを選択します。
4. ステータステーブルを確認します。

► Kaspersky Security Center の標準レポートを確認するには:

1. 管理コンソールツリーで[**管理サーバー <サーバー名>**]フォルダーを選択します。

2. [**レポート**]タブを開きます。
3. [**製品コンポーネントのステータスに関するレポート**]をダブルクリックします。

   レポートが生成されます。
4. 以下のレポートの詳細を確認します:
   - 図表。
   - コンポーネント、各コンポーネントがインストールされているネットワークデバイスの合計数、およびそれらが属するグループの概要のテーブル。
   - コンポーネントステータス、バージョン、デバイス、およびグループを示す詳細なテーブル。

ブロック対象アプリケーションのレポート(処理を実行モードおよび統計情報モード)

アプリケーション起動コントロールタスクの実行結果に基づいて、次の 2 種類のレポートを生成できます:ブロック対象アプリケーションのレポート(処理を実行モードでタスクを

開始した場合)、テストモードでのブロック対象アプリケーションのレポート(統計のみモードでタスクを開始した場合)。これらのレポートは、ネットワークの保護対象サーバー上にあるブロック対象アプリケーションの情報を表示します。すべての管理グループに対して個別のレポートが生成され、保護対象デバイス上にインストールされたすべてのカスペルスキー製品からのデータを蓄積します。

► テストモードでのブロック対象アプリケーションのレポートを表示するには:

1. アプリケーションコントロールタスクを統計のみモードで開始します 349 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)。
2. 管理コンソールツリーで[**管理サーバー <サーバー名>**]フォルダーを選択します。
3. [**レポート**]タブを開きます。
4. [**テストモードでのブロック対象アプリケーションのレポート**]をダブルクリックします。

   レポートが生成されます。
5. 以下のレポートの詳細を確認します:
   - 起動がブロックされた回数が最も多いアプリケーション上位 10 個を表示する図表。
   - ブロックが発生したアプリケーションについて、実行ファイルの名前、理由、ブロックの時刻、発生したデバイスの数を示す概要のテーブル。
   - デバイス、ファイルパス、およびブロックの条件に関するデータを示す詳細なテーブル。

► [処理を実行]モードでブロックされたアプリケーションに関するレポートを表示するには:

1. アプリケーションコントロールタスクを[処理を実行]モードで開始します(349 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)。
2. 管理コンソールツリーで[**管理サーバー <サーバー名>**]フォルダーを選択します。
3. [**レポート**]タブを開きます。
4. [**ブロック対象アプリケーションのレポート**]をダブルクリックします。

   レポートが生成されます。

このレポートは、テストモードでのブロック対象アプリケーションに関するレポートと同じデータブロックで構成されます。

Kaspersky Security for Windows Server コンソールの使用

このセクションでは、Kaspersky Security for Windows Server コンソールについての情報を提供するとともに、保護対象のサーバーまたは別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コンソールを使用してアプリケーションを管理する方法について説明します。

この章の内容

アプリケーションコンソールでの Kaspersky Security for Windows Server の設定

Kaspersky Security for Windows Server の設定の全般設定とトラブルシューティングの設定では、本製品が動作する全般的な条件を設定します。これらの設定では、Kaspersky Security for Windows Server で使用される処理対象プロセスの数を制御したり、異常終了後に Kaspersky Security for Windows Server のタスクを復元できるようにしたり、追跡ログを維持したり、異常終了時に Kaspersky Security for Windows Server プロセスのダンプファイルを作成できるようにしたり、その他の全般的な設定を行ったりすることができます。

Kaspersky Security Center アクティブポリシーによってこれらの設定への変更がブロックされている場合、アプリケーションコンソールではアプリケーションの設定を実行できません。

► Kaspersky Security for Windows Server を設定するには:

1. アプリケーションコンソールツリーで、[**Kaspersky Security**]フォルダーを選択して、次のいずれかを行います:
   - フォルダーの詳細ペインにある[**アプリケーションのプロパティ**]をクリックする。
   - フォルダーのコンテキストメニューで[**プロパティ**]を選択する。

   [**アプリケーションの設定**]ウィンドウが表示されます。
2. 表示されたウィンドウで、必要に応じて Kaspersky Security for Windows Server の全般設定を設定します:
   - [**スケーラビリティとインターフェイス**]タブでは、次の設定を行うことができます:
     - [**スケーラビリティ設定**]セクション:
       - Kaspersky Security for Windows Server で実行可能な処理対象プロセスの最大数。

表 19. 実行中プロセスの最大数

設定	実行中プロセスの最大数
説明	この設定は、Kaspersky Security for Windows Server の[**スケーラビリティ設定**]グループに属します。アプリケーションが同時に実行することのできる実行中プロセスの最大数を設定します。 同時に実行するプロセスの数が増えると、ファイルのスキャン速度が上がり、Kaspersky Security for Windows Server のフェールセーフ機能が向上します。ただし、この値が高すぎると、サーバーの全般的なパフォーマンスが低下してメモリの使用率が上昇する可能性があります。 [**実行中プロセスの最大数**]の設定は、スタンドアロンコンピューターにインストールされている Kaspersky Security for Windows Server に対してのみ、Kaspersky Security Center アプリケーションの管理コンソールで変更することができます([**アプリケーションのプロパティ**]ダイアログボックスを使用)。コンピューターのグループのポリシー設定でこの設定を変更することはできません。
取りうる値	1 ～ 8
既定値	本製品は、コンピューターのプロセッサの数に応じて自動でスケーラビリティを処理します:

プロセッサの数	実行中プロセスの最大数
1	1
1 < プロセッサの数 < 4	2
4 以上	4

- コンピューターのリアルタイム保護の対象プロセスの数

表 20. リアルタイム保護の対象プロセスの数

設定	リアルタイム保護の対象プロセスの数

説明	この設定は、Kaspersky Security for Windows Server の[**スケーラビリティ設定**]グループに属します。 この設定では、リアルタイム保護タスクの実行対象のプロセスの定数を指定できます。 設定値が高ければ、リアルタイム保護タスクのスキャン速度が速くなります。ただし、Kaspersky Security for Windows Server が使用するプロセスが多いほど、保護対象コンピューターの全般的なパフォーマンスに対する影響やメモリのリソース使用への影響が大きくなります。 [**リアルタイム保護の対象プロセスの数**]は、スタンドアロンサーバーにインストールされている Kaspersky Security for Windows Server に対してのみ、Kaspersky Security Center アプリケーションの管理コンソールで変更することができます([**アプリケーションのプロパティ**]ウィンドウを使用)。コンピューターのグループのポリシー設定でこの設定を変更することはできません。
取りうる値	取りうる値:1 ～ N。N は**実行中プロセスの最大数**の設定を使用して設定される値。 [**リアルタイム保護の対象プロセスの数**]の値を実行中プロセスの最大数と同じ値に設定した場合、コンピューター間のファイル交換の速度に対する影響が低減され、リアルタイム保護の実行中のパフォーマンスが向上します。ただし、基本的な優先度が[**中(標準)**]のアップデートタスクおよびオンデマンドスキャンタスクは、すでに実行中の Kaspersky Security for Windows Server のプロセス内で実行されます。オンデマンドスキャンは通常よりも遅い速度で実行されます。タスクの実行が原因でプロセスが異常終了した場合、プロセスの再起動時に通常よりも時間がかかります。 基本的な優先度が[**低**]のオンデマンドスキャンタスクは、常に別のプロセス内で実行されます。
既定値	Kaspersky Security for Windows Server は、コンピューターのプロセッサの数に応じて自動でスケーラビリティを処理します:

プロセッサの数	リアルタイム保護の対象プロセスの数
=1	1
>1	2

- バックグラウンドのオンデマンドスキャンタスクの処理対象プロセスの数

表 21. 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

設定	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

説明	この設定は、Kaspersky Security for Windows Server の[**スケーラビリティ設定**]グループに属します。 バックグラウンドモードでオンデマンドスキャンタスクを実行する際に使用するプロセスの最大数を指定できます。 この設定で指定されるプロセスの数は、[**実行中プロセスの最大数**]の設定で指定される Kaspersky Security for Windows Server のプロセスの合計には含まれません。 例として、各設定項目を以下のように設定したとします: • 実行中プロセスの最大数 - 3 • リアルタイム保護タスクの対象プロセスの数 - 3 • 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 - 1 その後、リアルタイム保護タスクとオンデマンドスキャンタスクをバックグラウンドモードで開始します。Kaspersky Security for Windows Server の kavfswp.exe プロセスの合計は 4 になります。 一部のオンデマンドスキャンタスクは、優先度「低」で 1 つのプロセス内で実行できます。 各タスクに個別のプロセスを割り当てるために複数のタスクをバックグラウンドモードで実行するなどの場合には、プロセスの数を増やすこともできます。タスクごとに個別のプロセスを割り当てることで、タスク実行の信頼性が高くなり、またタスクの実行速度も速くなります。
取りうる値	1 ～ 4
既定値	1

- [**ユーザーインターフェイス**]セクションで、各アプリケーション起動後のタスクバーにシステムトレイアイコンが表示されている場合に選択します(「通知領域のシステムトレイアイコン」(153 ページ)を参照)。

- [**セキュリティと信頼性**]タブでは、次の設定を行うことができます:
  - [**信頼性設定**]セクションで、クラッシュした後に、オンデマンドスキャンタスクの復元を試行する回数を指定します。

表 22. タスクの復元

設定	タスクの復元([**タスク復元を実行する**])
説明	この設定は、Kaspersky Security for Windows Server の[**信頼性設定**]グループに属します。タスクが緊急終了した場合にその復元を可能にし、復元に使用したオンデマンドスキャンタスクの試行回数を定義します。 タスクがクラッシュすると、Kaspersky Security for Windows Server の kavfs.exe プロセスが、クラッシュ発生時にそのタスクが実行されていたプロセスを再起動しようとします。 タスクの復元が無効になっている場合、リアルタイム保護タスクおよびオンデマンドスキャンタスクは復元されません。 タスクの復元が有効になっている場合、正常に起動するまでリアルタイム保護タスクの復元を試行します。また、この設定で指定されている試行回数に応じてオンデマンドスキャンタスクの復元を試みます。
取りうる値	有効または無効 オンデマンドスキャンタスクの復元の試行回数:1 ～ 10
既定値	タスクの復元は有効です。オンデマンドスキャンタスクの復元の試行回数:2

- [**UPS バックアップ電源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 Kaspersky Security

for Windows Server により実行される動作を指定します。

表 23. 無停電電源装置(UPS)の使用

設定	UPS バックアップ電源に切り替える場合の処理。
説明	コンピューターが UPS 電源に切り替わったときに Kaspersky Security for Windows Server が実行する動作を定義します。
取りうる値	スケジュールで開始予定のオンデマンドスキャンタスクを実行する、または実行しない。 実行中のすべてのオンデマンドスキャンタスクを実行する、または停止する。
既定値	コンピューターの電源に UPS が使用される場合の既定の設定は、次のとおりです: • スケジュールで開始予定のオンデマンドスキャンタスクを実行しない。 • 実行中のすべてのオンデマンドスキャンタスクを自動で停止する。

- [**パスワードによる保護設定**]セクションで、アプリケーション機能のパスワードによる保護を設定します(「Kaspersky Security for Windows Server 機能へのパスワードで保護されたアクセス」(238 ページ)を参照)。

- [**接続設定**]タブ:
  - [**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指定します:
  - [**プロキシサーバーの認証設定**]セクションで、プロキシサーバーでの認証に必要な認証種別と詳細を指定します。
  - [**ライセンス**]セクションで、Kaspersky Security Center がアプリケーションのアクティベーション用のプロキシサーバーとして使用されるかどうかを指定します。
- [**トラブルシューティング**]タブ:
  - 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 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 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 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 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 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 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。

アプリケーションでトレースファイルにデバッグ情報を保存する対象の、Kaspersky Security for Windows Server コンポーネントのコードのリスト。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 24. Kaspersky Security 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 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 の連携のためのサブシステム
bl	コントロールプロセス、Kaspersky Security 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 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 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 for Windows Server 管理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あとに適用されます。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 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 for Windows Server は、すべての Kaspersky Security for Windows Server コンポーネントのデバッグ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、[**クラッシュダンプファイルの作成**]をオンにしてください。

Kaspersky Security 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。

- 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。

Kaspersky Security 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 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(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」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。

3. [**OK**]をクリックします。

Kaspersky Security for Windows Server 設定が保存されます。

Kaspersky Security for Windows Server コンソールについて

Kaspersky Security for Windows Server 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。

本製品は、保護対象サーバーや企業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されたアプリケーションコンソールから管理することができます。

アプリケーションコンソールを別のコンピューターにインストールしたあとに、追加の設定が必要です。

アプリケーションコンソールと Kaspersky Security for Windows Server が異なるドメインに割り当てられている別々のコンピューターにインストールされている場合、Kaspersky Security for Windows Server からアプリケーションコンソールへの情報配信が制限される場合があります。たとえば、アプリケーションタスクが開始されても、アプリケーションコンソールではそのステータスが変更されないままの場合があります。

アプリケーションコンソールのインストール中に、インストールウィザードによって、インストールフォルダーにファイル kavfs.msc が作成され、Kaspersky Security for Windows Server スナップインが独立した Microsoft Windows スナップインのリストに追加されます。

アプリケーションコンソールは、[**スタート**]メニューから起動できます。Kaspersky Security for Windows Server スナップインである msc ファイルを実行したり、既存の Microsoft 管理コンソールにツリーの新しい要素として追加したりすることができます。

64 ビット版の Microsoft Windows では、Kaspersky Security for Windows Server スナップインを 32 ビット版の Microsoft 管理コンソールにのみ追加できます。この操作を実行するには、コマンドラインからコマンド mmc.exe /32 を実行して、Microsoft 管理コンソールを開きます。

複数の Kaspersky Security for Windows Server スナップインを、作成者モードで開かれた 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 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 for Windows Server コンソールのインターフェイス

Kaspersky Security for Windows Server コンソールは、Microsoft 管理コンソールツリーに、Kaspersky Security という名前のフォルダーの形式で表示されます。

異なるサーバーにインストールされた Kaspersky Security for Windows Server への接続が確立されると、フォルダーの名前に、アプリケーションがインストールされたサーバーの名前、および接続が確立されたユーザーアカウントの名前が追加されます：**Kaspersky Security <サーバー名> アカウント：<アカウント名>**。アプリケーションコンソールと同じサーバーにインストールされた Kaspersky Security for Windows Server に接続した場合、フォルダー名は **Kaspersky Security** です。

既定で、アプリケーションコンソールウィンドウには、次の要素があります：

- アプリケーションコンソールツリー
- 詳細ペイン
- ツールバー

アプリケーションコンソールツリー

アプリケーションコンソールツリーには、[**Kaspersky Security**]フォルダーと製品の機能コンポーネントのサブフォルダーが表示されます。

[**Kaspersky Security**]フォルダーには、次のサブフォルダーが含まれます：

- **サーバーのリアルタイム保護**：リアルタイム保護タスクと KSN サービスを管理します。[**サーバーのリアルタイム保護**]フォルダーでは、次のタスクを設定できます：
  - **ファイルのリアルタイム保護**
  - **スクリプト監視**
  - **KSN の使用**
  - **トラフィックセキュリティ**
  - **アンチクリプター**
- **サーバーコントロール**：保護対象サーバーにインストールされたアプリケーションの起動や外部デバイスの接続を制御します。[**サーバーコントロール**]フォルダーでは、次のタスクを設定できます：
  - **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**
  - **ファイアウォール管理**
- **ルールの自動生成**：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でのグループおよびシステムルールの自動作成の設定。
  - **アプリケーション起動コントロールルールの自動作成**
  - **デバイスコントロールルールの自動作成**
  - ルール作成グループタスク **<タスク名>**（存在する場合）

    Kaspersky Security Center を使用してグループタスク（155 ページの「Kaspersky Security for Windows Server タスクのカテゴリ」を参照）が作成されます。アプリケーションコンソールを使用してグループタスクを管理することはできません。

- **システム監査**:ファイル動作コントロールと Windows イベントログ監視の設定。
  - **ファイル変更監視**
  - **Windows イベントログ監視**
- **ネットワーク接続ストレージの保護**:ネットワークストレージの保護タスクを設定します。
  - **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**
  - **NetApp のアンチクリプター**
- **オンデマンドスキャン**:オンデマンドスキャンタスクを管理します。各タスクに対して別々のフォルダーがあります:
  - **オペレーティングシステムの起動時にスキャン**
  - **簡易スキャン**
  - **隔離のスキャン**
  - **アプリケーションの整合性チェック**
  - カスタムタスク **<タスク名>**(存在する場合)

  フォルダーには、アプリケーションがインストールされ、カスタムタスク、およびグループオンデマンドタスクが作成され、Kaspersky Security Center を使用してコンピューターに送信されたときに作成されたシステムタスクが表示されます(155 ページのセクション「Kaspersky Security for Windows Server タスクのカテゴリ」を参照してください)。
- **アップデート**:Kaspersky Security for Windows Server データベースおよびモジュールのアップデートを管理し、アップデートをローカルアップデートソースフォルダーにコピーします。このフォルダーには、各アップデートタスクを管理するためのサブフォルダーと、定義データベースのアップデートタスクの最後のロールバックが含まれています:
  - **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**
  - **定義データベースのロールバック**

  フォルダーには、作成され、Kaspersky Security Center を使用してコンピューターに送信されたすべてのカスタムタスクおよびグループアップデートタスクが表示されます(155 ページのセクション「Kaspersky Security for Windows Server タスクのカテゴリ」を参照してください)。
- **保管領域**:隔離、バックアップ、およびブロック対象コンピューターの設定を管理します。
  - **隔離**
  - **バックアップ**
  - **ブロック対象コンピューター**
- **ログと通知の設定**:ローカルタスクログ、セキュリティログ、および Kaspersky Security for Windows Server システム監査ログを管理します。
  - **セキュリティログ**
  - **システム監査ログ**
  - **タスク実行ログ**
- **ライセンス**:Kaspersky Security for Windows Server のライセンス情報ファイルおよびアクティベーションコードを追加または削除し、ライセンスの詳細を表示します。

詳細ペイン

詳細ペインに、選択したフォルダーの情報が表示されます。[**Kaspersky Security**]フォルダーを選択した場合、詳細ペインには現在のサーバーの保護ステータスに関する情報(「保護ステータスと Kaspersky Security for Windows Server の情報の表示」(165 ページ)を参照)、Kaspersky Security for Windows Server に関する情報、およびその機能コンポーネントの保護ステータスと、ライセンスの有効

期限日が表示されます。

[Kaspersky Security]フォルダーのコンテキストメニュー

[**Kaspersky Security**]フォルダーのコンテキストメニューの項目を使用して、次の操作を行えます:

- **別のコンピューターに接続**:別のコンピューターに接続して(154 ページのセクション「別のコンピューターにインストールしたアプリケーションコンソールを使用した Kaspersky Security for Windows Server の管理」を参照)、そこにインストールされた Kaspersky Security for Windows Server を管理します。[**Kaspersky Security**]フォルダーの詳細ペインの右下にあるリンクをクリックして、この操作を実行することもできます。
- **サービスの起動 / サービスの停止**:アプリケーションまたは選択したタスクの開始または停止(「手動でのタスクの開始、一時停止、再開、停止(155 ページ)」を参照)。この操作を実行するために、ツールバーのボタンを使用できます。また、これらの操作をアプリケーションのタスクのコンテキストメニューで実行することもできます。
- **リムーバブルドライブスキャンを設定**:USB ポートを介して保護対象サーバーに接続されたリムーバブルディスクのスキャンを設定します(446 ページのセクション「リムーバブルドライブスキャンについて」を参照)。
- **脆弱性攻撃ブロック:一般設定**:脆弱性攻撃ブロックモードを設定し、防御処理を設定します。
- **脆弱性攻撃ブロック:プロセス保護設定**:保護するプロセスを追加し、脆弱性攻撃ブロック技術を選択します(501 ページのセクション「脆弱性攻撃ブロック技術」を参照)。
- **信頼ゾーンの設定**:信頼ゾーンの設定を表示および設定します(479 ページのセクション「信頼ゾーンについて」を参照)。
- **アプリケーション管理のユーザー権限の変更**:Kaspersky Security for Windows Server の各種機能に対するアクセス権限を表示および設定します(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」を参照)。
- **Kaspersky Security サービス管理のユーザー権限の変更**:Kaspersky Security サービスを管理するユーザー権限を表示および設定します(236 ページのセクション「Kaspersky Security for Windows Server および 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)。
- **階層型ストレージ**:HSM システムのアクセス方法を設定します(505 ページのセクション「アプリケーションコンソールでの信頼ゾーンの設定」を参照)。
- **設定のエクスポート**:設定ファイルのアプリケーション設定を XML 形式で(160 ページのセクション「設定のエクスポート」を参照)保存します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **設定のインポート**:アプリケーション設定を設定ファイルから XML 形式でインポートします(161 ページのセクション「設定のインポート」を参照)。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **アプリケーションと利用できるモジュールアップデートの情報**:Kaspersky Security for Windows Server や、現在使用可能なアプリケーションモジュールのアップデートに関する情報を参照してください。
- **最新の情報に更新**:アプリケーションコンソールウィンドウの内容を更新します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **プロパティ**:Kaspersky Security for Windows Server または選択したタスクを表示および設定します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。

  > また、[**Kaspersky Security**]フォルダーの詳細ペインにある[**アプリケーションのプロパティ**]を使用するか、ツールバーにあるボタンを使用することもできます。

- **ヘルプ**:Kaspersky Security for Windows Server のヘルプ情報を表示します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。

Kaspersky Security for Windows Server タスクのツールバーとコンテキストメニュー

Kaspersky Security for Windows Server タスクを、アプリケーションコンソールツリーにある各タスクのコンテキストメニューの項目を使用して管理できます。

コンテキストメニューの項目を使用して次の操作を実行できます:

- **再開 / 一時停止**:タスク(155 ページのセクション「手動でのタスクの開始、一時停止、再開、停止」を参照)の実行を再開または一時停止します。この操作を実行するために、ツールバーのボタンを使用できます。この操作は、リアルタイム保護タスクおよ

びオンデマンドスキャンタスクで使用できます。

- **タスクの追加**:新規カスタムタスクを作成します(465 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と編集」を参照)。この操作は、オンデマンドスキャンタスクで使用できます。
- **ログを開く**:タスク実行ログ(210 ページのセクション「タスク実行ログについて」を参照)を表示および管理します。この操作は、すべてのタスクで使用できます。
- **タスクを削除**:カスタムタスクを削除します。この操作は、オンデマンドスキャンタスクで使用できます。
- **設定のテンプレート**:テンプレート(162 ページのセクション「セキュリティ設定テンプレートの使用」を参照)を管理します。この操作は、ファイルのリアルタイム保護およびオンデマンドスキャンに対して使用できます。

通知領域のシステムトレイアイコン

コンピューターの再起動後に Kaspersky Security for Windows Server が自動的に起動されるたびに、システムトレイアイコンがツールバーの通知領域に表示されます。このアイコンは、本製品のセットアップ時にシステムトレイアイコンがインストールされた場合に、既定で表示されます。

システムトレイアイコンの外観は、サーバー保護の現在のステータスを反映します。2 つのステータスがあります:

タスクのうち少なくとも 1 つが現在実行中である場合はアクティブ(カラーのアイコン):ファイルのリアルタイム保護、アプリケーション起動コントロール

どのタスクも現在実行中でない場合は非アクティブ(白黒のアイコン):ファイルのリアルタイム保護、アプリケーション起動コントロール

システムトレイアイコンを右クリックすると、コンテキストメニューが開きます。

コンテキストメニューには、製品ウィンドウを表示するために使用できるいくつかのコマンドが表示されます(以下の表を参照)。

表 25. システムトレイアイコンから表示されるコンテキストメニューのコマンド

コマンド	説明
アプリケーションコンソールを開く	Kaspersky Security for Windows Server コンソールを開きます(インストールされている場合)。
コンパクト診断インターフェイスを開く	[コンパクト診断インターフェイス]を開きます。
製品情報	Kaspersky Security for Windows Server に関する情報を含む[製品情報]ウィンドウを開きます。 登録済みの Kaspersky Security for Windows Server ユーザーの場合、[製品情報]ウィンドウには、インストールされている緊急アップデートに関する情報が表示されます。
非表示	ツールバー通知領域のシステムトレイアイコンを非表示にします。

非表示のシステムトレイアイコンは、いつでも表示できます。

► 製品アイコンをもう一度表示するには:

Microsoft Windows の[**スタート**]メニューから、[**すべてのプログラム**] - [**Kaspersky Security for Windows Server**] - [**シス**

テムトレイアイコンを表示]を選択します。

インストールされている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 for Windows Server の全般設定で、サーバー再起動後にアプリケーションが自動起動するたびに、システムトレイアイコンの表示を有効または無効にできます。

別のコンピューターにインストールしたアプリケーションコンソールを使用した Kaspersky Security for Windows Server の管理

リモートコンピューターにインストールされたアプリケーションコンソールから Kaspersky Security for Windows Server を管理できます。

リモートコンピューターで Kaspersky Security for Windows Server コンソールを使用して本製品を管理するには、次の点を確認してください:

- リモートコンピューターのアプリケーションコンソールのユーザーが、保護対象サーバーの[KAVWSEE Administrators]グループに追加されている。
- 保護対象サーバーで Windows ファイアウォールが有効な場合、Kaspersky Security 管理サービスプロセス(kavfsgt.exe)に対してネットワーク接続が許可されている。
- Kaspersky Security for Windows Server のインストール中、インストールウィザードで[**リモートアクセスを許可する**]がオンになっている。

リモートコンピューター上の Kaspersky Security for Windows Server がパスワードで保護されている場合は、パスワードを入力して、アプリケーションコンソールからアプリケーション管理にアクセスします。

Kaspersky Security for Windows Server タスクの管理

このセクションでは、Kaspersky Security 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。

このセクションの内容

Kaspersky Security for Windows Server タスクのカテゴリ

Kaspersky Security for Windows Server では、サーバーのリアルタイム保護、サーバーコントロール、オンデマンドスキャン、およびアップデートの各機能は、タスクとして実装されます。

タスクは、アプリケーションコンソールツリー、ツールバー、およびクイックアクセスバーでタスクのコンテキストメニューを使用して管理できます。詳細ペインで、タスクのステータス情報を表示できます。タスク管理操作は、システム監査ログに記録されます。

Kaspersky Security for Windows Server のタスクには、**ローカルとグループ**の 2 つの種別があります。

ローカルタスク

ローカルタスクは、作成された保護対象サーバーでのみ実行されます。開始方法に応じて、次の種別のローカルタスクがあります:

- **ローカルのシステムタスク**:Kaspersky Security for Windows Server のインストール時に自動的に作成されます。隔離のスキャンおよび定義データベースのロールバック以外のすべてのシステムタスクの設定を編集できます。システムタスクは、名前を変更したり削除したりできません。システムオンデマンドスキャンタスクとカスタムオンデマンドスキャンタスクは同時に実行できます。
- **ローカルのカスタムタスク**:アプリケーションコンソールでは、オンデマンドスキャンタスクを作成できます。Kaspersky Security Center で、オンデマンドスキャンタスク、定義データベースのアップデートタスク、定義データベースのロールバックタスク、およびアップデートのコピータスクを作成できます。このようなタスクはカスタムタスクと呼ばれます。カスタムタスクは、名前の変更や設定変更、削除ができます。いくつかのカスタムタスクを同時に実行することもできます。

グループタスク

Kaspersky Security Center で作成されたグループタスクと特定のコンピューターを対象とするタスクは、アプリケーションコンソールにも表示されます。このようなタスクはグループタスクと呼ばれます。グループタスクは、Kaspersky Security Center から管理および設定できます。アプリケーションコンソールでは、グループタスクのステータスの表示のみができます。

手動でのタスクの開始、一時停止、再開、停止

サーバーのリアルタイム保護タスクとオンデマンドスキャンタスクのみ、一時停止および再開することができます。

► タスクを開始 / 一時停止 / 再開 / 停止するには、次の手順を実行します:

1. アプリケーションコンソールでタスクのコンテキストメニューを開きます。

2. 次のいずれかを選択します：**開始**、**一時停止**、**再開**、または**停止**。

操作が実行され、システム監査ログに登録されます（208 ページを参照）。

オンデマンドスキャンタスクが再開されると、タスクが一時停止したときのオブジェクトのスキャンを続行します。

タスクスケジュールの管理

Kaspersky Security 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

アプリケーションコンソールでは、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。

► タスク開始スケジュールを設定するには：

1. 開始スケジュールを設定するタスクの上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。

   [**タスクの設定**]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、[**スケジュールに従って実行する**]をオンにします。
4. 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**]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、[**間隔：<数字> 時間**]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、[**間隔：<数字> 日**]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、[**間隔：<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 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。

スケジュールに従ったシステムタスクの開始が Kaspersky Security Center ポリシーの設定によって指定された場合、[**次回開始**]に[**ポリシーによりブロック**]と表示されます。

5. [**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時間帯を 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。
6. [**OK**]をクリックします。

設定されたタスクの開始設定が保存されます。

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. アプリケーション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。
   [**タスクの設定**]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. [**OK**]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。

タスクを開始するユーザーアカウントの使用

システムアカウントを使用してタスクを開始することも、別のアカウントを指定することもできます。

このセクションの内容

タスク実行用のアカウントについて

Kaspersky Security for Windows Server の次の機能コンポーネントで、選択したタスクを実行するアカウントを指定できます:

- 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
- オンデマンドスキャンタスク
- アップデートタスク

既定では、これらのタスクはシステムアカウントの権限で実行されます。

次の場合は、適切なアクセス権限を持つ異なるアカウントを指定してください:

- アップデートタスクで、アップデート元としてネットワーク内の別のコンピューター上のパブリックフォルダーを指定した場合
- アップデートタスクで、Windows NTLM 認証が組み込まれたプロキシサーバーを使用してアップデート元にアクセスする場合
- オンデマンドスキャンタスクで、システムアカウントがスキャン対象オブジェクトに対するアクセス権限を所有していない場合(例: サーバーの共有フォルダーのファイルなど)
- 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で、タスクの完成後に、システムアカウントがアクセスできないパスにある設定ファイルに生成されたルールがエクスポートされた場合(例: サーバーの共有フォルダーのパスなど)

システムアカウント権限を使用して、アップデートタスク、オンデマンドスキャンタスク、およびルールの自動作成タスクを実行できます。ネットワーク上の別のコンピューターが保護対象サーバーと同じドメインに登録されている場合、Kaspersky Security for Windows Server は、これらのタスクの実行中にこのコンピューターの共有フォルダーにアクセスします。この場合、システムアカウントには、これらのフォルダーへのアクセス権限が必要です。Kaspersky Security for Windows Server が **<ドメイン名 ¥ コンピューター名>** アカウントの権限を使用してコンピューターにアクセスします。

タスクを実行するユーザーアカウントの指定

► タスクを実行するアカウントを指定するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、アカウントの権限で開始を設定するタスクの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。

   [**タスクの設定**]ウィンドウが表示されます。
3. 表示されるウィンドウの[**実行用アカウント**]タブで、次の操作を行います:
   a. [**ユーザー名**]を選択します。

b. 使用するアカウントのユーザー名とパスワードを入力します。

選択したユーザーは、保護対象サーバーまたはそのサーバーと同じドメイン内に登録されている必要があります。

c. 入力したパスワードを確認します。

4. [**OK**]をクリックします。

ユーザーアカウントの権限でタスクを実行するように変更した設定内容が保存されます。

設定のインポートとエクスポート

このセクションでは、Kaspersky Security for Windows Server の設定または特定の製品コンポーネントの設定を XML 形式で設定ファイルにエクスポートする方法、およびこれらの設定を設定ファイルから製品にインポートする方法について説明します。

このセクションの内容

設定のインポートとエクスポートについて

Kaspersky Security 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 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。

Kaspersky Security for Windows Server のすべての設定をファイルにエクスポートする場合、アプリケーションの全般設定と、次の Kaspersky Security コンポーネントと機能の設定が保存されます:

- ファイルのリアルタイム保護
- KSN の使用
- デバイスコントロール
- 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ルールの自動作成
- アプリケーション起動コントロールルールの自動作成
- オンデマンドスキャンタスク
- トラフィックセキュリティ
- スクリプト監視
- ICAP ネットワークストレージの保護
- RPC ネットワークストレージの保護
- NetApp のアンチクリプター
- ファイル変更監視

- ログ監査
- Kaspersky Security for Windows Server データベースおよびソフトウェアモジュールのアップデート
- 隔離
- バックアップ
- ログ
- 管理者およびユーザーへの通知
- 信頼ゾーン
- 脆弱性攻撃ブロック
- ブロック対象コンピューターの保管領域
- パスワードによる保護

これらに加えて、Kaspersky Security for Windows Server の全般設定とユーザーアカウントの権限をファイルに保存できます。

グループタスクの設定はエクスポートできません。

Kaspersky Security for Windows Server は、タスクを実行したり、プロキシサーバーに接続したりするアカウントのデータなど、アプリケーションが使用するすべてのパスワードをエクスポートします。エクスポートしたパスワードは、暗号化された形式で設定ファイルに保存されます。パスワードは、再インストールまたはアップデートされていない場合に、このサーバーにインストールされた Kaspersky Security for Windows Server を使用してのみインポートできます。

別のコンピューターにインストールされた Kaspersky Security for Windows Server を使用して以前保存されたパスワードはインポートできません。別のコンピューターに設定がインポートされた後で、すべてのパスワードを手動で入力する必要があります。

Kaspersky Security Center のポリシーがエクスポート時にアクティブである場合、そのポリシーによって使用される設定値がエクスポートされます。

Kaspersky Security for Windows Server の個々のコンポーネントのパラメータを含む設定ファイルから(たとえば、インストールされた Kaspersky Security for Windows Server で作成された、コンポーネントの一部を含むファイルから)、設定をインポートできます。設定をインポートすると、設定ファイルに含まれていた Kaspersky Security for Windows Server の設定のみが変更されます。その他の設定は同じです。

ブロックされた Kaspersky Security Center のアクティブポリシーの設定は、設定のインポート時には変更されません。

設定のエクスポート

► 設定ファイルに設定をエクスポートするには、次の手順を実行します:

1. アプリケーションコンソールツリーで、次のいずれかの操作を行います:
   - [**Kaspersky Security**]フォルダーのコンテキストメニューで、[**設定のエクスポート**]を選択してすべての Kaspersky Security for Windows Server 設定をエクスポートする。
   - 設定をエクスポートするタスクでコンテキストメニューを開き、[**設定のエクスポート**]を選択して、本製品の個別の機能コンポーネントの設定をエクスポートする。
   - 信頼ゾーンの設定をエクスポートするには:
     a. アプリケーション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。
     b. [**信頼ゾーンの設定**]を選択します。

[**信頼ゾーン**]ウィンドウが開きます。

c. [**エクスポート**]をクリックします。

設定のエクスポートウィザードの開始ウィンドウが開きます。

2. **ウィザード**の手順に従い、設定を保存する設定ファイルの名前とパスを指定します。

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。

> Kaspersky Security Center のポリシーがエクスポート時にアクティブである場合、そのポリシーによって使用される設定値がエクスポートされます。

3. [**アプリケーション設定のエクスポートが完了しました**]ウィンドウで[**閉じる**]をクリックします。

ウィザードが終了すると、エクスポートした設定が保存されます。

設定のインポート

► 保存された設定ファイルから設定をインポートするには、次の手順を実行します:

1. アプリケーションコンソールツリーで、次のいずれかの操作を行います:
   - [**Kaspersky Security**]フォルダーのコンテキストメニューで、[**設定のインポート**]を選択してすべての Kaspersky Security for Windows Server 設定をインポートする。
   - 設定をインポートするタスクでコンテキストメニューを開き、[**設定のインポート**]を選択して、本製品の個別の機能コンポーネントの設定をインポートする。
   - 信頼ゾーンの設定をインポートするには:

     a. アプリケーション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。

     b. [**信頼ゾーンの設定**]を選択します。

     [**信頼ゾーン**]ウィンドウが開きます。

     c. [**インポート**]をクリックします。

     設定のインポートウィザードの開始ウィンドウが開きます。
2. ウィザードの手順に従い、設定のインポート元となる設定ファイルを指定します。

> Kaspersky Security for Windows Server の全般設定またはサーバー上にあるその機能コンポーネントの全般設定をインポートした後は、以前の設定値に戻すことはできません。

3. [**アプリケーション設定のインポートが完了しました**]ウィンドウにある[**閉じる**]をクリックします。

ウィザードが終了すると、インポートした設定が保存されます。

4. アプリケーションコンソールのツールバーで、[**最新の情報に更新**]をクリックします。

インポートした設定が、アプリケーションコンソールウィンドウに表示されます。

Kaspersky Security for Windows Server が再インストールまたは更新されたのとは別のサーバーまたは同じサーバーで作成されたファイルからパスワード(タスクの実行またはプロキシサーバーへの接続に使用されるアカウントのデータ)がインポートされることはありません。インポート操作が完了したら、パスワードを手動で入力する必要があります。

セキュリティ設定テンプレートの使用

このセクションでは、Kaspersky Security for Windows Server の保護タスクとスキャンタスクでのセキュリティ設定テンプレートの使用について説明します。

このセクションの内容

セキュリティ設定テンプレートについて

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 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を設定できます。

テンプレートを使用して、次の Kaspersky Security for Windows Server タスクのセキュリティ設定を行うことができます:

- ファイルのリアルタイム保護
- RPC ネットワークストレージの保護
- オペレーティングシステムの起動時にスキャン
- 簡易スキャン
- オンデマンドスキャンタスク

コンピューターのファイルリソースツリーでテンプレートから親フォルダーに適用されるセキュリティ設定は、すべてのサブフォルダーに適用されます。次の場合、親フォルダーのテンプレートはサブフォルダーには適用されません:

- サブフォルダーのセキュリティ設定が個別に設定された場合(「セキュリティ設定テンプレートの適用」(163 ページ)を参照)。
- サブフォルダーが仮想の場合。仮想フォルダーごとにテンプレートを個別に適用する必要があります。

セキュリティ設定テンプレートの作成

► フォルダーのセキュリティ設定を手動で保存し、テンプレートに保存するには:

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを適用するタスクを選択します。

2. 選択したタスクの詳細ペインにある[**保護範囲の設定**]または[**スキャン範囲の設定**]をクリックします。
3. サーバーのネットワークファイルリソースのツリーまたはリストで、表示するテンプレートを選択します。
4. [**セキュリティレベル**]タブで、[**テンプレートとして保存**]をクリックします。

   [**テンプレートのプロパティ**]ウィンドウが開きます。
5. [**テンプレート名**]で、テンプレートの名前を入力します。
6. [**説明**]にテンプレートの追加情報を入力します。
7. [**OK**]をクリックします。

一連のセキュリティ設定値を持つテンプレートが保存されます。

テンプレートのセキュリティ設定の表示

► **作成したテンプレートのセキュリティ設定を表示するには、次の手順を実行します:**

1. アプリケーションコンソールツリーで、セキュリティテンプレートを表示するタスクを選択します。
2. 選択したタスクのコンテキストメニューで、[**設定のテンプレート**]を選択します。

   [**テンプレート**]ウィンドウが開きます。
3. 表示されたウィンドウのテンプレートリストで、表示するテンプレートを選択します。
4. [**表示**]をクリックします。

[**<テンプレート名>**]ウィンドウが開きます。[**全般**]タブには、テンプレート名とテンプレートに関する追加情報が表示されます。[**オプション**]タブには、テンプレートに保存されているセキュリティ設定がリスト表示されます。

セキュリティ設定テンプレートの適用

► **選択したフォルダーにテンプレートからセキュリティ設定を適用するには:**

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを適用するタスクを選択します。
2. 選択したタスクの詳細ペインにある[**保護範囲の設定**]または[**スキャン範囲の設定**]をクリックします。
3. サーバーのネットワークファイルリソースのツリーまたはリストで、テンプレートを適用するフォルダーまたは項目のコンテキストメニューを開きます。
4. [**テンプレートの適用**] - [**<テンプレート名>**]の順に選択します。
5. [**保存**]をクリックします。

サーバーのファイルリソースのツリーで選択したフォルダーに、セキュリティ設定のテンプレートが適用されます。選択したフォルダーの[**セキュリティレベル**]タブに[**カスタム**]の値が表示されます。

> サーバーのファイルリソースツリーでテンプレートから親フォルダーに適用されるセキュリティ設定は、すべてのサブフォルダーに適用されます。

サーバーのファイルリソースツリーのサブフォルダーの保護範囲またはスキャン範囲が個別に設定されている場合、テンプレートから親フォルダーに適用されたセキュリティ設定は、そのようなサブフォルダーには自動的に設定されません。

► 選択したすべてのフォルダーにテンプレートからセキュリティ設定を適用するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを適用するタスクを選択します。
2. 選択したタスクの詳細ペインにある[**保護範囲の設定**]または[**スキャン範囲の設定**]をクリックします。
3. 選択したフォルダーおよびそのすべてのサブフォルダーにテンプレートを適用するには、サーバーのネットワークファイルリソースのツリーまたはリストで、親フォルダーを選択します。
4. 右クリックしてコンテキストメニューを開き、[**テンプレートの適用**] - [**<テンプレート名>**]の順に選択します。
5. [**保存**]をクリックします。

セキュリティ設定テンプレートが、サーバーのファイルリソースツリーの親フォルダーとすべてのサブフォルダーに適用されます。選択したフォルダーの[**セキュリティレベル**]タブに[**カスタム**]の値が表示されます。

セキュリティ設定テンプレートの削除

► セキュリティ設定テンプレートを削除するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを設定に使用しないタスクを選択します。
2. 選択したタスクのコンテキストメニューで、[**設定のテンプレート**]を選択します。

   [**オンデマンドスキャン**]親フォルダーの詳細ペインより、オンデマンドスキャンタスクの設定のテンプレートを表示できます。

   [**テンプレート**]ウィンドウが開きます。
3. 表示されたウィンドウのテンプレートリストで、削除するテンプレートを選択します。
4. [**削除**]をクリックします。

   削除を確認するウィンドウが開きます。
5. 表示されたウィンドウで、[**はい**]をクリックします。

選択したテンプレートが削除されます。

セキュリティ設定テンプレートがサーバーファイルリソースのフォルダーの保護またはスキャンに適用された場合、そのフォルダーの設定済みのセキュリティ設定は、テンプレートの削除後に保存されます。

保護ステータスと Kaspersky Security for Windows Server の情報の表示

► Kaspersky Security for Windows Server のサーバー保護ステータスに関する情報を表示するには:

アプリケーションコンソールツリーで、[**Kaspersky Security**]フォルダーを選択します。

既定では、アプリケーションコンソールの詳細ペインの情報は自動的に更新されます:

- ローカル接続の場合は 10 秒ごと
- リモート接続の場合は 15 秒ごと

情報を手動で更新できます。

► [Kaspersky Security]フォルダーの情報を手動で更新するには:

[**Kaspersky Security**]フォルダーのコンテキストメニューで[**最新の情報に更新**]コマンドを選択します。

アプリケーションコンソールの詳細ペインに、以下の製品情報が表示されます:

- Kaspersky Security Network の使用のステータス
- サーバーの保護のステータス
- 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情報
- 実際の診断データ
- サーバーコントロールタスクに関するデータ
- ライセンス情報
- Kaspersky Security Center との連携のステータス。アプリケーションの接続先になっている、Kaspersky Security Center がインストールされているコンピューターの詳細、アクティブポリシーによって制御されるアプリケーションタスクの情報が表示されます。

保護動作ステータスを示すために、異なる色で表示されます:

- **緑色**:タスクは設定に従い実行されています。保護は有効です。
- **黄色**:タスクが開始されなかったか、一時停止または停止されました。セキュリティの脅威が発生する可能性があります。タスクを設定し、開始してください。
- **赤色**:エラーが発生した状態でタスクが終了したか、タスクの実行中に深刻な脅威が検知されました。タスクを開始するか、検知されたセキュリティの脅威を除去するための措置を取ってください。

このブロックの詳細にはリンクになっているものもあり(タスク名、検知された脅威の数など)、クリックすると、関連するタスクのフォルダーに移動したりタスク実行ログが開いたりします。

[**Kaspersky Security Network の使用**]セクションには、**実行中**、**停止済み**、または**一度も実行されていません**など、現在のタスクのステータスが表示されます。インジケーターでは、次の値が使用されます:

- 緑色 - KSN の使用タスクが実行中であり、URL のステータスの要求を KSN に送信中であることを示します。
- 黄色 - 声明の 1 つが同意されたが、タスクが実行中でないか、URL のステータスの要求を KSN に送信中ではないことを

示します。

サーバー保護

[**サーバー保護**]セクション(下の表を参照)には、サーバーの現在の保護ステータスに関する情報が表示されます。

表 26. サーバーの保護ステータスに関する情報

[保護]セクション	情報
サーバー保護ステータスのインジケーター	セクション名が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます: • 緑色 - この色は既定で表示されます。ファイルのリアルタイム保護コンポーネントがインストールされ、タスクが実行中であることを示します。 • 黄色 - ファイルのリアルタイム保護コンポーネントがインストールされておらず、簡易スキャンタスクが長期間実行されていません。 • 赤色 - ファイルのリアルタイム保護タスクが実行されていません。
ファイルのリアルタイム保護	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **検知** - Kaspersky Security for Windows Server が検知したオブジェクトの数。たとえば、Kaspersky Security for Windows Server が 5 つのファイルから 1 つのマルウェアを検知した場合、このフィールドの値が 1 つ加算されます。検知されたマルウェアの数が 0 を超えると、値が赤色で表示されます。
簡易スキャン	**前回のスキャン実行日** - ウイルスおよびその他のコンピューターセキュリティ脅威に対する前回の簡易スキャンの日付。 **一度も実行されていません** - 簡易スキャンタスクが過去 30 日以上実行されていない場合に発生するイベント(既定値)。このイベントが生成されるしきい値は変更可能です。
トラフィックセキュリティ	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **Outlook アドイン** - インストールされているかどうか。
脆弱性攻撃ブロック	**ステータス** - 脆弱性攻撃ブロックの現在のステータス。例:「**適用済み**」または「**未適用**」。 **防御モード** - 使用可能な 2 つのモードのうちの 1 つで、プロセスメモリ保護の設定時に選択します: • 脆弱性攻撃時に終了する • 統計のみ **保護したプロセス** - 保護範囲に追加され、選択したモードに従って処理されたプロセスの合計数。
バックアップされたオブジェクト	**バックアップの空き容量がしきい値より少なくなりました** - このイベントは、バックアップの空き容量が指定のサイズに近付くと発生します。オブジェクトのバックアップ保管領域への移動を継続します。この場合、[**使用済のサイズ**]の値が黄色で表示されます。 **バックアップの最大サイズを超過しました** - このイベントは、バックアップのサイズが指定のサイズに達すると発生します。オブジェクトのバックアップ保管領域への移動を継続します。この場合、[**使用済のサイズ**]の値が赤色で表示されます。 **バックアップされたオブジェクト** - バックアップに現在保存されているオブジェクトの数。 **使用済のサイズ** - バックアップ領域の使用済みのサイズ。

アップデート

[**アップデート**]セクション(下の表を参照)には、最新の定義データベースとアプリケーションモジュールの状態に関する情報が表示され

ます。

表 27. Kaspersky Security for Windows Server の定義データベースとモジュールのステータスに関する情報

[アップデート]セクション	情報
定義データベースとソフトウェアモジュールのステータスインジケーター	セクション名が表示されたパネルの色は、定義データベースとモジュールのステータスを反映します。インジケーターでは、次の値が使用されます: • 緑色 - この色は既定で表示されます。定義データベースが最新で、前回の定義データベースのアップデートが正常に完了したことを示します。 • 黄色 - 定義データベースがアップデートされていないか、前回の定義データベースのアップデートが失敗したことを示します。 • 赤色 - [**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**]または[**定義データベースが破損しています**]のいずれかのイベントが発生したことを示します。
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	**データベースの状態** - 定義データベースのアップデートタスクのステータスの評価。 次の値が使用されます: • **定義データベースは最新です** - 定義データベースが 7 日以内(既定)にアップデートされています。 • **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 7 ～ 14 日前(既定)にアップデートされています。 • **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** - 定義データベースが 14 日以内(既定)にアップデートされています。 **[定義データベースがアップデートされていません]イベントおよび[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]**イベントが生成されるしきい値は変更可能です。 **定義データベースの公開日時** - 最新の定義データベースのアップデートがリリースされた日時。日時は UTC 形式で指定されます。 **前回完了した定義データベースのアップデートタスクのステータス** - 前回の定義データベースのアップデートの日時。日時は、保護対象のサーバーのローカル時刻に基づいて指定されます。このフィールドは、[**失敗**]イベントが発生すると赤色になります。 **利用可能なモジュールのアップデートの数** - ダウンロードしてインストールできる Kaspersky Security for Windows Server モジュールのアップデートの数。 **インストールされたモジュールのアップデートの数** - インストール済みの Kaspersky Security for Windows Server モジュールのアップデートの数。

管理

[**管理**]セクション(下の表を参照)には、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、およびファイアウォール管理タスクに関する情報が表示されます。

表 28. サーバーコントロールステータスに関する情報

管理セクション	情報

管理セクション	情報
サーバーコントロールのステータスのインジケーター	セクション名が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます: • 緑色 - この色は既定で表示されます。アプリケーション起動コントロールコンポーネントがインストールされ、タスクが処理を実行モードで実行中であること、脆弱性攻撃ブロック機能がインストールされ、処理を実行モードで実行中であることを示します。 • 黄色 - アプリケーション起動コントロールが統計のみモードで実行中であることを示します。 • 赤色 - アプリケーション起動コントロールタスクが実行されていないか、失敗したことを示します。
アプリケーション起動コントロール	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **モード** - アプリケーション起動コントロールタスクで使用可能な 2 つのモードのうちの 1 つ: • 処理を実行 • 統計のみ **アプリケーションの起動の拒否** - アプリケーション起動コントロールタスクの実行中に、Kaspersky Security for Windows Server によってブロックされたアプリケーション起動の試行数。ブロックされたアプリケーション起動の数が 0 を超えると、フィールドは赤色になります。 **平均処理時間(ミリ秒)** - Kaspersky Security for Windows Server が保護対象サーバーのアプリケーション起動の試行処理にかかった時間。
デバイスコントロール	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **モード** - デバイスコントロールタスクで使用可能な 2 つのモードのうちの 1 つ: • **処理を実行** • **統計のみ** **ブロック対象デバイス** - デバイスコントロールタスク時に Kaspersky Security for Windows Server によってブロックされた、大容量記憶デバイスへの接続試行の合計数。ブロックされた大容量記憶デバイスの数が 0 を超えると、フィールドは赤色になります。
アンチクリプター	タスクのステータス - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 動作モード - アンチクリプタータスクで使用可能な 2 つのモードのうちの 1 つ: • **処理を実行** • **統計のみ** **ブロックしたコンピューター** - 保護対象コンピューターに接続しようとしたときに悪意がある動作が表示され、ブロックされたコンピューターの数。
ファイアウォール管理	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **接続をブロックしました** - 指定されたファイアウォールのルールによってブロックされた、保護対象サーバーへの接続数。

診断

[**診断**]セクション(下の表を参照)には、ファイル変更監視および Windows イベントログ監視タスクに関する情報が表示されます。

表 29. システム監査ステータスに関する情報

[診断]セクション	情報

診断ステータスのインジケーター	セクション名が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます: • 緑色 - この色は既定で表示されます。システム監査コンポーネントの 1 つまたは両方がインストールされ、タスクが実行中であることを示します。 • 黄色 - 両方のコンポーネントがインストールされていますが、システム監査タスクの 1 つが実行されておらず、[**実行されていません**]イベントが発生したことを示します。 • 赤色 - タスクの 1 つが失敗したことを示します。
ファイル変更監視	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **認可されていないファイル操作** - 監視範囲のファイルへの変更数。この変更数は、保護対象サーバーのセキュリティが侵害されていることを示す場合があります。
Windows イベントログ監視	**タスクのステータス** - 「**実行中**」や「**停止済み**」など、現在のタスクのステータス。 **違反の可能性** - Windows イベントログからのデータに基づく、記録された違反の数。この数は、指定されたタスクルールに基づいて、またはヒューリスティックアナライザーを使用して決定されます。

Kaspersky Security for Windows Server のライセンスに関する情報は、[**Kaspersky Security**]フォルダーの詳細ペインの左下隅にある行に表示されます。

Kaspersky Security for Windows Server のプロパティを設定するには、[アプリケーションのプロパティ]をクリックします(「アプリケーションコンソールでの Kaspersky Security for Windows Server の設定」(143 ページ)を参照)。

別のコンピューターを接続するには、**[別のコンピューターに接続]**をクリックします(154 ページのセクション「別のコンピューターにインストールしたアプリケーションコンソールを使用した Kaspersky Security for Windows Server の管理」を参照)。

[ネットワーク接続ストレージの保護]タブの詳細情報を確認するには、『Kaspersky Security for Windows Server - ネットワーク接続ストレージ保護導入ガイド』を参照してください。

コンパクト診断インターフェイス

このセクションでは、サーバーステータスまたは現在のアプリケーションの動作を確認するためにコンパクト診断インターフェイスを使用する方法や、ダンプファイルおよびトレースファイルの書き込みを設定する方法について説明します。

この章の内容

コンパクト診断インターフェイスについて

コンパクト診断インターフェイス(「CDI」とも表記)は、アプリケーションコンソールが保護対象サーバーにインストールされていない場合、アプリケーションコンソールとは独立して、システムトレイアイコンとともにインストールおよびアンインストールされます。CDI は、システムトレイアイコンから起動します。また、サーバーのアプリケーションフォルダーから kavfsmui.exe を実行することでも起動できます。

CDI ウィンドウからは、以下の操作が可能です:

- 全般的なアプリケーションステータスに関する情報を確認する(170 ページのセクション「コンパクト診断インターフェイスを使用した Kaspersky Security for Windows Server ステータスの確認」を参照)。
- 発生したセキュリティインシデントを確認する(172 ページのセクション「セキュリティイベント統計の確認」を参照)。
- 保護対象サーバーで現在のアプリケーションの動作を確認する(172 ページのセクション「現在のアプリケーション動作の確認」を参照)。
- ダンプファイルおよびトレースファイルの書き込みを開始または停止する(173 ページのセクション「ダンプファイルおよびトレースファイルの書き込みの設定」を参照)。
- アプリケーションコンソールを開きます。
- [**製品情報**]ウィンドウを開くと、インストールされているアップデートおよび使用できるパッチのリストが表示されます。

Kaspersky Security for Windows Server の機能へのアクセスがパスワードで保護されている場合でも、CDI は使用可能です。パスワードは必要ありません。

> CDI は、Kaspersky Security Center を使用して設定できません。

コンパクト診断インターフェイスを使用した Kaspersky Security for Windows Server ステー

タスの確認

► [コンパクトな診断インターフェイス]ウィンドウを開くには、次の処理を実行します:

1. ツールバーの通知領域の Kaspersky Security for Windows Server システムトレイアイコンを右クリックします。
2. [**コンパクト診断インターフェイスを開く**]を選択します。

   [**コンパクト診断インターフェイス**]ウィンドウが表示されます。

[**保護ステータス**]タブで、ライセンスの現在のステータス、サーバーのリアルタイム保護タスク、およびアップデートタスクを確認します。保護ステータスをユーザーに通知するために、異なる色で表示されます(次の表を参照)。

表 30. コンパクト診断インターフェイスの保護ステータス

セクション	ステータス

サーバーのリアルタイム保護	次のいずれかの場合、パネルは**緑色**で表示されます(当てはまる条件の数は問いません):
	• 推奨構成:
	  ◦ ファイルのリアルタイム保護タスクが既定の設定で開始されている。
	  ◦ アプリケーション起動コントロールタスクが、既定の設定で[**処理を実行**]モードで開始されている。
	• 許容できる構成:
	  ◦ ファイルのリアルタイム保護タスクがユーザーにより設定されている。
	  ◦ アプリケーション起動コントロールタスクの設定が変更されている。

	次のいずれかの条件に 1 つでも当てはまる場合、パネルは**黄色**で表示されます: • ファイルのリアルタイム保護タスクが一時停止されている(ユーザーまたはスケジュールにより)。 • アプリケーション起動コントロールタスクが**統計のみ**モードで開始されている。 • 脆弱性攻撃からの保護とアプリケーション起動コントロールが**統計のみ**モードで開始されている。
	次の条件の両方に当てはまる場合、パネルは**赤色**で表示されます: • ファイルのリアルタイム保護がインストールされていないか、タスクが停止または一時停止されている。 • アプリケーション起動コントロールがインストールされていないか、タスクが**統計のみ**モードで開始されている。
ライセンス	現在のライセンスが有効な場合、パネルは**緑色**で表示されます。
	パネルが**黄色**で表示される場合は、次のいずれかのイベントが発生したことを示します: • **ライセンスのステータスの確認**。 • **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**。

	パネルが**赤色**で表示される場合は、次のいずれかのイベントが発生したことを示します: • **製品がアクティベートされていません** • **ライセンスの有効期間が終了しました** • **使用許諾契約書に違反しています** • **ライセンスがブラックリストに掲載されています**
アップデート	定義データベースが最新の場合、パネルは**緑色**で表示されます。
	定義データベースがアップデートされていない場合、パネルは**黄色**で表示されます。
	定義データベースが長期間アップデートされていない場合、パネルは**赤色**で表示されます。

セキュリティイベント統計の確認

[**統計情報**]タブには、すべてのセキュリティイベントが表示されます。保護タスクごとに統計情報がそれぞれのブロックに表示され、インシデント数と最後にインシデントが発生した日時が示されます。インシデントが記録されると、ブロックの色は赤に変わります。

► 統計情報を確認するには:

1. ツールバーの通知領域の Kaspersky Security for Windows Server システムトレイアイコンを右クリックします。
2. [**コンパクト診断インターフェイスを開く**]を選択します。

   [**コンパクト診断インターフェイス**]ウィンドウが表示されます。
3. [**統計情報**]タブを開きます。
4. 保護タスクのセキュリティインシデントを確認します。

現在のアプリケーション動作の確認

このタブでは、現在のタスクおよびアプリケーションプロセスのステータスを確認し、発生する重要なイベントに関する通知をすぐに取得できます。

アプリケーション動作ステータスを示すために、異なる色で表示されます:

- [**タスク**]セクション:
  - **緑色**:黄色や赤色の条件がありません。
  - **黄色**:重要領域の簡易スキャンが長期間実行されていません。
  - **赤色**:次のいずれかの条件を満たしています:
    - タスクが開始されず、開始スケジュールがタスクに対して設定されていない。
    - アプリケーション起動エラーが重要なイベントとして記録されている。
- [**Kaspersky Security Network**]セクション:
  - **緑色**:KSN の使用タスクが開始されている。
  - **黄色**:KSN 声明に同意しているが、タスクが開始されていない。

► サーバー上で現在のアプリケーション動作を確認するには:

1. ツールバーの通知領域の Kaspersky Security for Windows Server システムトレイアイコンを右クリックします。
2. [**コンパクト診断インターフェイスを開く**]を選択します。

   [**コンパクト診断インターフェイス**]ウィンドウが表示されます。
3. [**現在のアプリケーションの動作**]タブを開きます。
4. [**タスク**]セクションで次の情報を確認します:
   - **重要領域の簡易スキャンが長期間実行されていません**

     このフィールドは、簡易スキャンに関する警告が表示された場合にのみ表示されます。
   - **現在実行中**
   - **実行できませんでした**
   - **スケジュールで定義された次の開始**
5. [**Kaspersky Security Network**]セクションで、次の情報を確認します:
   - **KSN は有効です。ファイル評価サービスが使用可能です**または**プロテクションが無効**
   - **アプリケーションの統計情報が KSN に送信されています**

     リアルタイムのファイル保護タスクおよびオンデマンドスキャンタスクの実行時に検知したマルウェア(詐欺ソフトウェアなど)に関する情報や、スキャン時のエラーについてのデバッグ情報を送信します。

     フィールドが表示されるのは、KSN の使用タスクの設定で[**Kaspersky Security Network に統計情報を送信**]がオンになっている場合です。
6. [**Kaspersky Security Center との連携**]セクションで次の情報を確認します:
   - ローカル管理は許可されています
   - ポリシーが適用されます:<Kaspersky Security Center のサーバー名>。

ダンプファイルおよびトレースファイルの書き込みの設定

CDI を使用してダンプファイルおよびトレースファイルの書き込みを設定できます。

アプリケーションコンソールを使用して、トラブルシューティングを設定することもできます(143 ページのセクション「アプリケーションコンソールでの Kaspersky Security for Windows Server の設定」を参照)。

► ダンプファイルおよびトレースファイルの書き込みを開始するには、次の処理を実行します:

1. ツールバーの通知領域の Kaspersky Security for Windows Server システムトレイアイコンを右クリックします。
2. [**コンパクト診断インターフェイスを開く**]を選択します。

   [**コンパクト診断インターフェイス**]ウィンドウが表示されます。

3. [**トラブルシューティング**]タブを開きます。
4. 必要に応じて、次のトレース設定を変更します:
   a. [**デバッグ情報をこのフォルダーのトレースファイルに書き込む**]をオンにします。
   b. [**参照**]ボタンをクリックして、トレースファイルを保存するフォルダーを指定します。

   すべてのコンポーネントで、ログ記録の詳細レベルは[**デバッグ**]レベル、ログの最大サイズは 50 MB の既定値の設定でトレースが有効になります。
5. 必要に応じて、次のダンプファイル設定を変更します:
   a. [**誤動作時のダンプファイルをこのフォルダーに作成する**]をオンにします。
   b. [**参照**]ボタンをクリックして、ダンプファイルを保存するフォルダーを指定します。
6. [**適用**]をクリックします。

   新しい設定が適用されます。

Kaspersky Security for Windows Server の定義データベースとソフトウェアモジュールのアップデート

このセクションでは、Kaspersky Security for Windows Server の定義データベースとソフトウェアモジュールのアップデートタスク、Kaspersky Security for Windows Server のアップデートのコピーと定義データベースのロールバック、および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タスクを設定する手順について説明します。

この章の内容

アップデートタスクについて

Kaspersky Security for Windows Server には、4 つのシステムアップデートタスクが用意されています：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、および定義データベースのロールバック。

既定では、Kaspersky Security for Windows Server は 1 時間ごとにアップデート元（Kaspersky Lab のアップデートコンピューターの 1 つ）に接続します。定義データベースのロールバックタスクを除くすべてのアップデートタスクは、設定が行えます（「アップデートタスクの設定」（181 ページ）を参照）。タスク設定が変更されると、次回のタスク開始時に新しい値が適用されます。

アップデートタスクの一時停止や再開は許可されません。

定義データベースのアップデート

既定では、定義データベースはアップデート元から保護対象サーバーにコピーされ、サーバーのリアルタイム保護タスクの実行ですぐに使用が開始されます。オンデマンドスキャンタスクでは、次回の起動時からアップデートした定義データベースを使用します。

既定では、定義データベースのアップデートタスクは毎時間実行されます。

ソフトウェアモジュールのアップデート

既定では、利用可能なソフトウェアモジュールアップデートがアップデート元にあるかどうかチェックされます。インストールしたソフトウェアモジュールの使用を開始するには、コンピューターや Kaspersky Security for Windows Server の再起動が必要です。

既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます（時刻は、保護対象サーバーの地域設定に準じます）。タスクの実行中、適用可能なソフトウェアモジュールの重要なアップデートおよび定期アップデートの有無をチェックします。アップデートは配信されません。

アップデートのコピー

既定では、タスクの実行中に、定義データベースのアップデートファイルをダウンロードし、指定したネットワークフォルダーやローカルフォルダーに保存します。アップデートファイルは適用されません。

既定では、アップデートのコピータスクは無効になっています。

定義データベースのロールバック

タスクの実行中に、以前にインストールしたアップデートが含まれる定義データベースを使用します。

既定では、定義データベースのロールバックタスクは無効になっています。

Kaspersky Security for Windows Server のソフトウェアモジュールのアップデートについて

カスペルスキーから、Kaspersky Security for Windows Server モジュールのアップデートパッケージが発行される場合があります。アップデートパッケージは、**緊急**(または**重要**)と定期的の場合があります。重要なアップデートパッケージでは、脆弱性やエラーが修正されます。定期的なパッケージでは、新規機能の追加や既存機能の拡張が行われます。

緊急(重要)アップデートパッケージは、Kaspersky Lab のアップデートサーバーにアップロードされます。ソフトウェアモジュールのアップデートタスクを使用して、これらのパッケージの自動インストールを設定できます。既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます(時刻は、保護対象サーバーの地域設定に準じます)。

カスペルスキーは、自動アップデート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、カスペルスキーの 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アップデートタスクを使用して、Kaspersky Security for Windows Server の定期アップデートのリリースに関する情報を受信できます。

重要なアップデートは、インターネットから各保護対象サーバーに対して実行できます。または、1 台のコンピューターを仲介として使用して、このコンピューターにすべてのアップデートをコピーし、ネットワークサーバーに配信することもできます。アップデートをインストールせずにコピーおよび保存するには、アップデートのコピータスクを使用します。

モジュールのアップデートのインストール前に、以前にインストールしたモジュールのバックアップコピーが作成されます。ソフトウェアモジュールのアップデートプロセスが中断されたり、エラーになったりした場合は、以前にインストールしたソフトウェアモジュールが自動的に使用されます。ソフトウェアモジュールは、以前にインストールしたアップデートに手動でロールバックできます。

ダウンロードしたアップデートのインストール中は Kaspersky Security サービスが自動的に停止され、その後再開されます。

Kaspersky Security for Windows Server の定義データベースのアップデートについて

保護対象サーバー上に保存されている Kaspersky Security for Windows Server の定義データベースは、すぐに未アップデートの状態になります。カスペルスキーのウイルスアナリストは、毎日数百個もの新しい脅威を検知し、その識別レコードを作成して、定義データベースのアップデートに追加しています定義データベースのアップデートは、前回のアップデートの作成以降に検知された脅威の識別用レコードが含まれるファイルやファイルセットです。必要なコンピューター保護レベルを維持するには、定義データベースのアップデートを定期的に受信してください。

既定では、インストールされている Kaspersky Security for Windows Server の定義データベースのアップデートが前回作成されてから 1 週間以内に定義データベースがアップデートされない場合、[**定義データベースがアップデートされていません**]イベントが発生します。定義データベースが 2 週間アップデートされていない場合、[**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**]イベントが発生します。データベースの最新のステータスに関する情報(「保護ステータスと Kaspersky Security for Windows Server の情報の表示」(165 ページ)を参照)は、アプリケーションコンソールツリーの[**Kaspersky Security**]フォルダーの詳細ペインに表示されます。Kaspersky Security for Windows Server の全般設定を使用して、これらのイベントが発生するまでの個別の日数を指定できます。また、これらのイベントに関する管理者への通知も設定できます(「管理者およびユーザーへの通知の設定」(221 ページ)を参照)。

Kaspersky Security 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。

アップデートは、インターネットからすべての保護対象サーバーにダウンロードできます。または、1 台のサーバーを仲介として使用して、このサーバーにすべてのアップデートをコピーし、コンピューターに配信することもできます。組織で Kaspersky Security Center を使用してサーバーの保護を一元管理する場合、Kaspersky Security Center 管理サーバーをアップデートのダウンロードの仲介として使用できます。

定義データベースのアップデートタスクは手動またはスケジュールに基づいて開始できます(「タスク開始スケジュールの設定」(156 ページ)を参照)。既定では、定義データベースのアップデートタスクは毎時間実行されます。

アップデートのダウンロードプロセスが中断されたりエラーになったりすると、前回インストールしたアップデートが含まれる定義データベースの使用に自動的に切り替えられます。定義データベースが破損した場合は、以前インストールされたアップデートに手動でロールバックできます(「Kaspersky Security for Windows Server 定義データベースのロールバック」(186 ページ)を参照)。

組織内で使用されるアンチウイルス製品の定義データベースとモジュールのアップデート方式

アップデートタスクでのアップデート元の選択は、組織で使用する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スキームによって異なります。

Kaspersky Security for Windows Server の定義データベースとモジュールは、次のスキームを使用して保護対象サーバーでアップデートできます:

- インターネットから各保護対象サーバーに、アップデートを直接ダウンロードする(スキーム 1)。
- インターネットから仲介コンピューターにアップデートをダウンロードして、このコンピューターからサーバーに配信する。

  以下のソフトウェアがインストールされているコンピューターは、仲介コンピューターとして使用できます:

  - Kaspersky Security for Windows Server(保護対象サーバーの 1 つ)(スキーム 2)
  - Kaspersky Security Center 管理サーバー(スキーム 3)

仲介コンピューターを使用してアップデートすると、インターネットトラフィックを減らせるだけでなく、ネットワークサーバーセキュリティも向上します。

上記のアップデートスキームについて、以下で説明します。

スキーム 1:定義データベースとモジュールをインターネットから直接アップデートする

► インターネットから直接 Kaspersky Security for Windows Server のアップデートを設定するには:

保護対象の各サーバーの定義データベースのアップデートタスクおよびソフトウェアモジュールのアップデートタスクの設定で、Kaspersky Lab のアップデートサーバーをアップデート元として指定します。

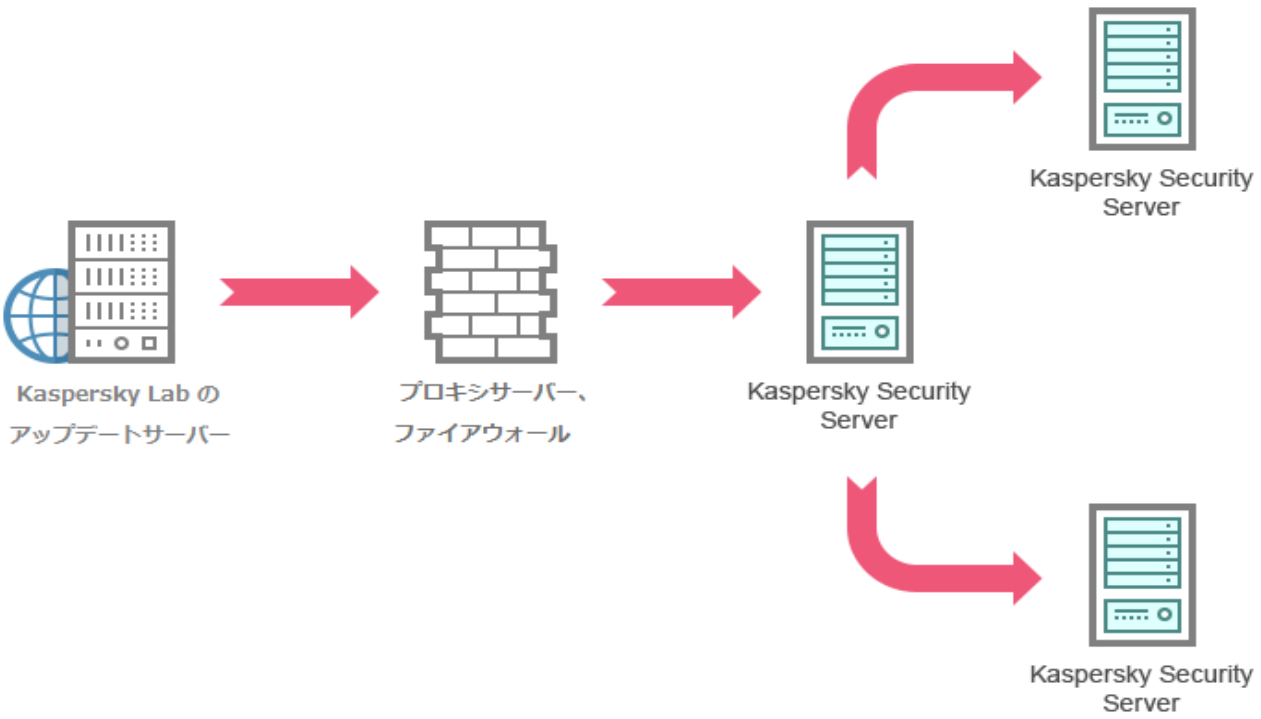
アップデートフォルダーが含まれるその他の HTTP サーバーや FTP サーバーをアップデート元として設定できます。

スキーム 2:定義データベースとモジュールを保護対象サーバーの 1 つを経由してアップデートする

► 保護対象サーバーの 1 つを経由して Kaspersky Security for Windows Server のアップデートを設定するには:

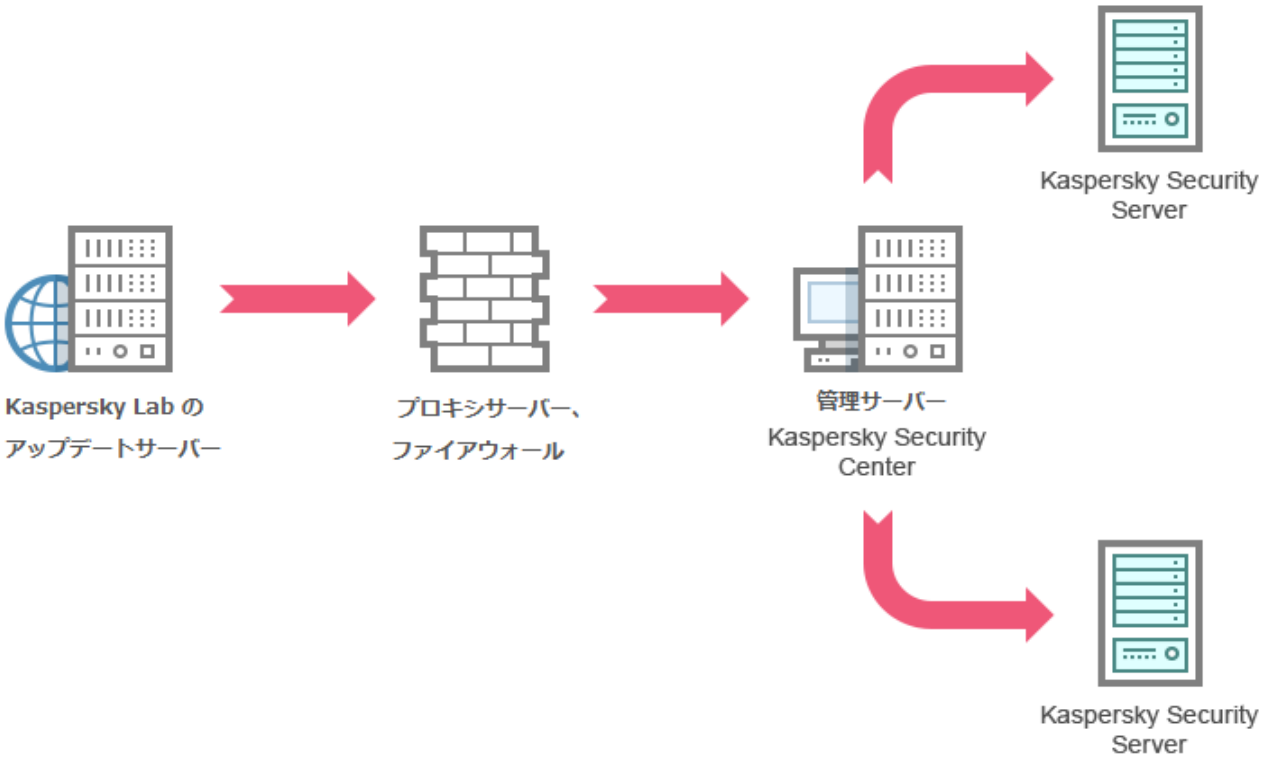
1. 選択した保護対象サーバーにアップデートをコピーします。それには、次の操作を実行します:
   - 選択したサーバーで[アップデートのコピー]タスクを設定します:
     a. アップデート元として、Kaspersky Lab のアップデートサーバーを指定します。
     b. アップデートの保存先として使用する共有フォルダーを指定します。
2. 他の保護対象サーバーにアップデートを配信します。それには、次の操作を実行します:
   - 保護対象の各サーバーで、定義データベースのアップデートタスクとソフトウェアモジュールのアップデートタスクを設定します(次の図を参照)。
     a. アップデート元として、アップデートのダウンロード先の仲介コンピューターのドライブ上のフォルダーを指定します。

保護対象サーバーの 1 つを経由してアップデートが取得されます。



スキーム 3:定義データベースとモジュールを Kaspersky Security Center 管理サーバーを経由してアップデートする

Kaspersky Security Center 製品を使用してアンチウイルスによるサーバーの保護を一元的に管理している場合、ローカルエリアネットワークにインストールされている Kaspersky Security Center 管理サーバー経由でアップデートをダウンロードできます(次の図を参照)。



► Kaspersky Security Center 管理サーバーを経由して Kaspersky Security for Windows Server のアップデートを設定するには:

1. Kaspersky Lab のアップデートサーバーから Kaspersky Security Center 管理サーバーにアップデートをダウンロードします。それには、次の操作を実行します:
   - 指定したコンピューターグループの管理サーバーでアップデートを取得するタスクを設定します。
     a. アップデート元として、Kaspersky Lab のアップデートサーバーを指定します。
2. 保護対象サーバーにアップデートを配信します。それには、次のいずれかの処理を実行します:
   - Kaspersky Security Center で、定義データベース(アプリケーションモジュール)のアップデートグループタスクを設定し、保護対象サーバーにアップデートを配信する:
     a. タスクのスケジュールで、開始の頻度として[**管理サーバーがアップデートを取得した後**]を指定します。

     管理サーバーでは、アップデートを受信するたびにタスクが開始されます(推奨の方法です)。

     [**管理サーバーがアップデートを取得した後**]の開始頻度をアプリケーションコンソールで指定することはできません。
   - 保護対象の各サーバーで、定義データベースのアップデートタスクと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:

a. Kaspersky Security Center の管理サーバーをアップデート元として指定します。

b. 必要に応じて、タスクのスケジュールを設定します。

Kaspersky Security for Windows Server 定義データベースをまれにしかアップデートしない場合（1か月に 1 回から 1 年に 1 回）、脅威を検知する可能性が低くなり、アプリケーションコンポーネントによる誤検知が発生する頻度が高くなります。

Kaspersky Security Center の管理サーバーを経由して、アップデートが取得されます。

Kaspersky Security Center 管理サーバーをアップデート配信に使用する予定の場合は、Kaspersky Security Center の配布キットに含まれるアプリケーションコンポーネントであるネットワークエージェントを保護対象の各サーバーにインストールします。これにより、管理サーバーと Kaspersky Security for Windows Server が保護対象サーバー上でやり取りできます。ネットワークエージェントに関する詳細と Kaspersky Security Center を使用したネットワークエージェントの設定の詳細については、**Kaspersky Security Center のヘルプ**を参照してください。

アップデートタスクの設定

このセクションでは、Kaspersky Security for Windows Server のアップデート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

Kaspersky Security for Windows Server のアップデート元の使用設定

定義データベースのロールバックタスクを除く各アップデートタスクに対して、1 つ以上のアップデート元の指定、ユーザー定義のアップデート元の追加、指定されたソースとの接続設定を行えます。

アップデートタスク設定の変更後、実行中のアップデートタスクに対して新しい設定はすぐには適用されません。設定の内容は、タスクを再起動したときにのみ適用されます。

► アップデート元の種別を指定するには:

1. アプリケーション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. 設定するアップデートタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの詳細ペインで、[**プロパティ**]をクリックします。

[**タスクの設定**]ウィンドウが開き、[**全般**]タブが表示されます。

4. [**アップデート元**]セクションで、Kaspersky Security for Windows Server のアップデート元の種別を選択します:

   - **Kaspersky Security Center 管理サーバー**

     アップデート元として Kaspersky Security Center 管理サーバーが使用されます。

     ネットワーク上のカスペルスキー製品が Kaspersky Security Center リモートアクセスシステムによって管理されている場合と、ネットワークエージェント(サーバーと管理サーバー間の接続を提供する Kaspersky Security Center コンポーネント)が保護対象のサーバーにインストールされている場合のみ、このオプションを選択できます。

   - **Kaspersky Lab のアップデートサーバー**

     アップデート元として、すべてのカスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートをホストするカスペルスキーの Web サイトが使用されます。

     既定では、このオプションはオンです。

   - **カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**

     アップデート元として、管理者が指定した HTTP サーバーか FTP サーバー、またはローカルネットワークフォルダーのフォルダーが使用されます。

     [**カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**]をクリックして、最新のアップデートを受け取るアップデート元のリストを作成できます。

5. 必要に応じて、ユーザー定義のアップデート元の詳細設定を行います:

   a. [**カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**]をクリックします。

      i. 表示される[**アップデートサーバー**]ウィンドウで、ユーザー定義のアップデート元の横にあるチェックボックスをオンまたはオフにし、そのアップデート元の使用を開始または終了します。

      ii. [**OK**]をクリックします。

   b. [**全般**]タブの[**アップデート元**]セクションで、[**指定したサーバーが使用できない場合は Kaspersky Lab のアップデートサーバーを使用する**]をオンまたはオフにします。

      このチェックボックスにより、ユーザー定義のアップデート元を利用できない場合に、 Kaspersky Lab のアップデートサーバーをアップデート元として使用するオプショ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、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ンです。

      [**指定したサーバーが使用できない場合は Kaspersky Lab のアップデートサーバーを使用する**]は、[**カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**]が有効である場合にオンにすることができます。

6. [**タスクの設定**]ウィンドウで[**接続設定**]タブを選択して、アップデート元に接続するための設定を行います。

   - [**プロキシサーバー設定を使用して Kaspersky Lab のアップデートサーバーに接続する**]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、Kaspersky Lab サーバーからアップデートを受信した場合、または[**指定したサーバーが使用できない場合は Kaspersky Lab のアップデートサーバーを使用する**]がオンの場合のプロキシサーバー設定の使用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、プロキシサーバー設定が使用されます。

     このチェックボックスをオフにすると、プロキシサーバー設定が使用されなくなります。

     既定では、このチェックボックスはオンです。

   - [**プロキシサーバー設定を使用して他のサーバーに接続する**]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、アップデート元に[**カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**]が選択されている場合の、プロキシサーバー設定の使用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、プロキシサーバー設定が使用されます。

既定では、このチェックボックスはオフです。

プロキシサーバーにアクセスするためにオプションのプロキシサーバー設定と認証設定を行う方法について詳しくは、「Kaspersky Security 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」を参照してください。

7. [**OK**]をクリックします。

Kaspersky Security for Windows Server のアップデート元の設定内容が保存され、次回のタスクの起動時に適用されます。

Kaspersky Security for Windows Server のユーザー定義のアップデート元のリストを管理できます。

► アプリケーションのユーザー定義のアップデート元のリストを編集するには:

1. アプリケーション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. 設定するアップデートタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが開き、[**全般**]タブが表示されます。
4. [**カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**]をクリックします。

   [**アップデートサーバー**]ウィンドウが開きます。
5. 次の操作を行います:
   - 新しいユーザー定義のアップデート元を追加するには、入力フィールドに UNC(ユニバーサルネーミング規約)フォーマットでローカルフォルダーまたはネットワークフォルダーを指定して、FTP または HTTP サーバー上のアップデートファイルを格納しているフォルダーのアドレスを指定します。**ENTER** キーを押します。

     既定では、追加されたフォルダーはアップデート元として使用されます。
   - ユーザー定義のアップデート元の使用を無効にするには、リストのアップデート元の横にあるチェックボックスをオフにします。
   - ユーザー定義のアップデート元の使用を有効にするには、リストのアップデート元の横にあるチェックボックスをオンにします。
   - Kaspersky Security for Windows Server がユーザー定義のアップデート元にアクセスする順序を変更するには、[**上に移動**]および[**下に移動**]を使用し、選択したアップデート元を他のアップデート元より先に使用するか後に使用するかに応じて、リストの先頭の方向または末尾の方向に移動します。
   - アップデート元へのパスを変更するには、リストからアップデート元を選択し、[**編集**]をクリックして、入力フィールドで必要な変更を行い、**ENTER** キーを押します。
   - ユーザー定義のアップデート元を削除するには、リストからアップデート元を選択し、[**削除**]をクリックします。

     ユーザー定義のアップデート元がリストに 1 つしか残っていない場合、削除することはできません。
6. [**OK**]をクリックします。

ユーザー定義のアップデート元のリストの変更が保存されます。

定義データベースのアップデートタスク実行中のディスク I/O の使用の最適化

定義データベースのアップデートタスクの実行中に、アップデートファイルがサーバーのローカルディスクに保存されます。アップデートタスクの実行中に、メモリ上の仮想ドライブにアップデートファイルを保存することで、サーバーのディスク I/O サブシステムに関する負荷を軽減できます。

この機能は、Microsoft Windows Vista、Microsoft Windows Server 2008 以降のオペレーティングシステムで使用できます。

定義データベースのアップデートタスクの実行中にこの機能を使用すると、余分な論理ドライブがオペレーティングシステムに表示されることがあります。この論理ドライブは、タスクの完了後にオペレーティングシステムから削除されます。

► 定義データベースのアップデートタスク実行中にコンピューターのディスク I/O サブシステムの負荷を低減するには、次の手順を実行します:

1. アプリケーション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**]サブフォルダーを選択します。
3. [**定義データベースのアップデート**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。
4. [**タスクの設定**]ウィンドウが開き、[**全般**]タブが表示されます。
5. [ディスク I/O 使用の最適化]セクションで、次の設定を定義します:
   - [**ディスク I/O の負荷の低減**]をオンまたはオフにします。

     このチェックボックスでは、メモリ上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**]で、メモリのボリューム(MB 単位)を指定します。オペレーティングシステムは、タスクの実行中にアップデートファイルを保存するために、指定されたメモリのボリュームを一時的に割り振ります。既定のメモリのサイズは 512 MB です。最小のメモリのサイズは 400 MB です。
6. [**OK**]をクリックします。

設定の内容が保存され、次回のタスク開始時に適用されます。

アップデートのコピータスクの設定

► アップデートのコピータスクを設定するには:

1. アプリケーション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. [**アップデートのコピー**]サブフォルダーを選択します。

3. [**アップデートのコピー**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。

4. [**全般**]タブおよび[**接続設定**]タブで、アップデート元を使用するための設定を行います(「Kaspersky Security for Windows Server のアップデート元の使用設定」(181 ページ)を参照)。

5. [**全般**]タブの[**アップデートのコピーの設定**]セクション:

   - アップデートのコピーの条件を指定します:
     - **定義データベースのアップデートをコピーする**

       ソフトウェア定義データベースのアップデートのみをダウンロードします。

       既定では、このオプションはオンです。

     - **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する**

       緊急の Kaspersky Security for Windows Server ソフトウェアモジュールのアップデートのみをダウンロードします。

     - **定義データベースと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する**

       ソフトウェア定義データベースのアップデートと、Kaspersky Security for Windows Server の重要なソフトウェアモジュールのアップデートをダウンロードします。
   - ダウンロードしたアップデートが配信されるローカルフォルダーまたはネットワークフォルダーを指定します。

6. [**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの開始スケジュールを設定します(156 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)。

7. [**実行用アカウント**]タブで、アカウント権限を使用して起動するタスクを設定します(「タスクを実行するユーザーアカウントの指定」(158 ページ)を参照)。

8. [**OK**]をクリックします。

設定の内容が保存され、次回のタスク開始時に適用されます。

ソフトウェアモジュールのアップデートタスクの設定

► 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には:

1. アプリケーション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. [**ソフトウェアモジュールのアップデート**]サブフォルダーを選択します。

3. [**ソフトウェアモジュールのアップデート**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。

4. [**全般**]タブおよび[**接続設定**]タブで、アップデート元を使用するための設定を行います(「Kaspersky Security for Windows Server のアップデート元の使用設定」(181 ページ)を参照)。

5. [**全般**]タブの[**アプリケーションのアップデート設定**]セクションで、ソフトウェアモジュールをアップデートするための設定を行います:

   - **適用可能になったソフトウェアの重要なアップデートを確認する**

     アップデートをダウンロードせず、アップデートソースで入手できるソフトウェアモジュールの緊急アップデートについての通知を表示します。この通知は、この種別のイベントに関する通知が有効である場合に表示されます。

     既定では、このオプションはオンです。

- **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**

  ソフトウェアモジュールの重要なアップデートをダウンロードしてインストールします。

- **システムの再起動を許可する**

  再起動を必要とするアップデートがインストールされた後で、オペレーティングシステムが再起動します。

  チェックボックスがオンの場合、再起動を必要とするアップデートをインストールした後に、オペレーティングシステムが再起動されます。

  このチェックボックスは、[**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。

- **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**

  アップデートソースから入手できる、Kaspersky Security for Windows Server ソフトウェアモジュールに対して予定されているすべてのアップデートについての通知が表示されます。この種別のイベントに対して通知が有効である場合に、通知が表示されます。

  チェックボックスがオンの場合、アップデートソースから入手できるソフトウェアモジュールに対して予定されているすべてのアップデートについて、通知が表示されます。

  既定では、このチェックボックスはオンです。

6. [**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの開始スケジュールを設定します(156 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)。既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます(時刻は、保護対象サーバーの地域設定に準じます)。
7. [**実行用アカウント**]タブで、アカウント権限を使用して起動するタスクを設定します(「タスクを実行するユーザーアカウントの指定」(158 ページ)を参照)。
8. [**OK**]をクリックします。

設定の内容が保存され、次回のタスク開始時に適用されます。

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通知を設定できます。このイベントには、定期アップデートのダウンロード元となる Kaspersky Lab の Web サイトの URL が含まれます。

Kaspersky Security for Windows Server 定義データベースのロールバック

定義データベースのアップデートが適用される前に、過去に使用された定義データベースのバックアップコピーが作成されます。アップデートが中断されたり、エラーになったりした場合は、以前にインストールした定義データベースが自動的に使用されます。

定義データベースのアップデート後に問題が発生した場合は、定義データベースのロールバックタスクを開始して、定義データベースを以前にインストールしたアップデートにロールバックできます。

► 定義データベースのロールバックタスクを開始するには:

[**定義データベースのロールバック**]フォルダーの詳細ペインで[**開始**]をクリックします。

アプリケーションモジュールのアップデートのロールバック

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。

ソフトウェアモジュールのアップデートの適用前に、現在使用中のモジュールのバックアップコピーが作成されます。モジュールのアップデートプロセスが中断されたりエラーになったりすると、前回インストールしたアップデートが含まれるモジュールが自動的に使用されるようになります。

ソフトウェアモジュールをロールバックするには、Microsoft Windows コンポーネントの**アプリケーションのインストールと削除**を使用します。

アップデートタスクの統計情報

アップデートタスクの実行中に、タスクの開始から現時点までにダウンロードされたデータ量やその他のタスク実行統計情報に関するリアルタイムな情報を表示できます。

タスクの完了または停止時に、その情報をタスク実行ログで確認できます。

► アップデートタスクの統計情報を表示するには、次の手順を実行します:

1. アプリケーション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. 統計情報を確認するタスクに該当するサブフォルダーを選択します。

選択したフォルダーの詳細ペインにある[**統計情報**]セクションに、タスクの統計情報が表示されます。

定義データベースのアップデートタスクまたはアップデートのコピータスクを表示している場合、[**統計情報**]セクションには現時点で Kaspersky Security for Windows Server によってダウンロードされたデータのボリュームが表示されます(**受信したデータ**)。

ソフトウェアモジュールのアップデートタスクを表示している場合は、次の表の情報が表示されます。

表 31. ソフトウェアモジュールのアップデートタスクに関する情報

フィールド	説明
受信したデータ	ダウンロードしたデータの総量。
適用可能な重要なアップデート	インストール可能な重要なアップデートの数。
適用可能な定期アップデート	インストール可能な定期的なアップデートの数。
アップデートの適用中のエラー	このフィールドの値がゼロ以外の場合、アップデートは適用されませんでした。適用中にエラーが発生したアップデートの名前は、タスク実行ログで確認できます(「タスク実行ログでの Kaspersky Security for Windows Server のタスクに関する統計と情報の表示」(212 ページ)を参照)。

オブジェクトの隔離とバックアップのコピー

このセクションでは、検知された悪意のあるオブジェクトが駆除されたり削除される前にバックアップを取る方法や、感染の可能性のあるオブジェクトの隔離について説明します。

この章の内容

感染の可能性があるオブジェクトの隔離：隔離

このセクションでは、感染の可能性があるオブジェクトを隔離して分離する方法、および隔離の設定を行う方法について説明します。

このセクションの内容

感染の可能性があるオブジェクトの隔離について

Kaspersky Security 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**フォルダー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フォルダーに保存されます。

隔離オブジェクトの表示

隔離されたオブジェクトは、アプリケーションコンソールの［**隔離**］フォルダーで確認できます。

► 隔離されたオブジェクトを表示するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーを選択します。

選択したフォルダーの詳細ペインに、隔離されたオブジェクトの情報が表示されます。

► 隔離されたオブジェクトのリストで必要なオブジェクトを見つけるには、次の手順を実行します:

オブジェクトを並べ替える(「隔離オブジェクトの並べ替え」(189 ページ)を参照)か、オブジェクトをフィルタリングします(「隔離オブジェクトのフィルタリング」(189 ページ)を参照)。

このセクションの内容

隔離オブジェクトの並べ替え

既定では、隔離されたオブジェクトリスト中のオブジェクトは、隔離の日付が新しい順に表示されます。目的のオブジェクトを見つけるため、オブジェクトに関する情報の列でオブジェクトを並べ替えることができます。[**隔離**]フォルダーを閉じて、再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

► オブジェクトを並べ替えるには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーを選択します。
3. [**隔離**]フォルダーの詳細ペインで、リストのオブジェクトの並べ替えに使用する列の見出しを選択します。

選択した設定に基づいて、リストのオブジェクトの表示順が変わります。

隔離オブジェクトのフィルタリング

目的の隔離されたオブジェクトを検索するために、リストでオブジェクトをフィルタリングして、指定したフィルタリング条件(フィルター)を満たすオブジェクトのみ表示することができます。[**隔離**]フォルダーから移動して、再度開いた場合、フィルタリングの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

► 1 つまたは複数のフィルターを指定するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーを選択します。
3. ファイル名の上でコンテキストメニューを開き、[**フィルター**]を選択します。

[**フィルターの設定**]ウィンドウが表示されます。

4. フィルターを追加するには、次の手順を実行します:

a. [**フィールド名**]で、フィルター値と比較する項目を選択します。

b. [**演算子**]リストで、フィルタリング条件を選択します。リストのフィルタリング条件の値は、[**フィールド名**]リストで選択した値に応じて異なる場合があります。

c. [**フィールド値**]にフィルターの値を入力するか、リストから選択します。

d. [**追加**]をクリックします。

追加したフィルターが、[**フィルターの設定**]ウィンドウのフィルターのリストに表示されます。追加するフィルターごとにこれらの手順を繰り返します。フィルターの使用時は、次のガイドラインに従います:

- 論理演算子「AND」を使って複数のフィルターを組み合わせるには、[**すべての条件が満たされた場合**]を選択します。
- 論理演算子「OR」を使って複数のフィルターを組み合わせるには、[**いずれかの条件が満たされた場合**]を選択します。
- フィルターを削除するには、フィルターのリストから削除するフィルターを選択し、[**削除**]をクリックします。
- フィルターを編集するには、[**フィルターの設定**]ウィンドウのリストからフィルターを選択します。次に、[**フィールド名**]、[**演算子**]、または[**フィールド値**]で、対象の値を変更して、[**置換**]をクリックします。

5. すべてのフィルターが追加されたら、[**適用**]をクリックします。

作成したフィルターが保存されます。

► 隔離されたオブジェクトのリストに、すべてのオブジェクトを再表示するには:

[**隔離**]フォルダーのコンテキストメニューで、[**フィルターの削除**]を選択します。

隔離のスキャン

既定では、定義データベースをアップデートするごとに、隔離のスキャンシステムタスクが実行されます。以下の表に、タスクの設定を示します。隔離のスキャンタスクの設定は変更できません。

タスクの起動スケジュールの設定(「タスク開始スケジュールの設定」(156 ページ)を参照)、手動でのタスクの開始、タスクの開始に使用するアカウント権限の変更(「タスクを実行するユーザーアカウントの指定」(158 ページ)を参照)を行えます。

定義データベースのアップデート後に隔離されたオブジェクトがスキャンされると、Kaspersky Security for Windows Server で一部のオブジェクトが感染していないとして再分類されることがあります。それらのオブジェクトのステータスは「**誤検知**」に変更されます。その他のオブジェクトは、感染しているとして再分類されます。この場合、そのようなオブジェクトは隔離のスキャンタスクの設定に従い、駆除または駆除できない場合は削除します。

表 32. 隔離のスキャンタスクの設定

隔離のスキャンタスクの設定	値
スキャン範囲	隔離フォルダー
セキュリティ設定	スキャン範囲全体で共通。これらの値は次の表に示されています。

表 33. 隔離のスキャンタスクのスキャン設定

セキュリティ設定	値
オブジェクトのスキャン	スキャン範囲に含まれているすべてのオブジェクト

セキュリティ設定	値
最適化	無効
感染しているオブジェクトまたはその他の検知したオブジェクトの処理	駆除する。駆除できない場合は削除する
感染したオブジェクトの処理	スキップ
除外するオブジェクト	なし
検知しないオブジェクト	なし
スキャン時間が次より長い場合は停止する（秒）	設定なし
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）	設定なし
NTFS 代替データストリームをスキャン	有効
ドライブのブートセクターと MBR	無効
iChecker テクノロジーを使用する	無効
iSwift テクノロジーを使用する	無効
複合オブジェクトをスキャンします	• 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* * 作成または変更されたファイルのみをスキャンすることはできません。
ファイルの Microsoft の署名をチェックする	実行されていません
ヒューリスティックアナライザーを使用する	有効（分析レベル[**高**]）
信頼ゾーン	オフ

隔離されたオブジェクトの復元

Kaspersky Security for Windows Server では、感染の可能性があるオブジェクトを暗号化して隔離に置き、その悪影響から保護対象サーバーを保護します。

オブジェクトは隔離から復元できます。これは、次の場合に必要となる可能性があります:

- アップデートした定義データベースによる隔離スキャンの後に、オブジェクトのステータスが[**誤検知**]や[**駆除済み**]に変更された場合。
- サーバーにとってオブジェクトが無害であると思われ、使用したい場合。その後のスキャンで、このオブジェクトを隔離したくない場合は、ファイルのリアルタイム保護タスクやオンデマンドスキャンタスクの処理から、このオブジェクトを除外できます。この操作を実行するには、それらのタスクで、このオブジェクトを[**除外するファイル**]または[**検知しないオブジェクト**]セキュリティ設定の値に指定するか、信頼ゾーンに追加します(479 ページ)。

オブジェクトの復元時に、復元したオブジェクトの保管場所を選択できます。選択できるのは、元の場所(既定)、保護対象サーバーの復元したオブジェクト用の特別なフォルダー、アプリケーションコンソールがインストールされているサーバーやネットワーク上のその他のコンピューターのカスタムフォルダーです。

[**フォルダーへの復元**]は、復元したオブジェクトを保護対象サーバーに保存する場合に使用します。このスキャン対象のオブジェクト用に、特別なセキュリティ設定を設定できます。このフォルダーのパスは、[隔離]設定で設定されます。

隔離からオブジェクトを復元すると、サーバーが感染する可能性があります。

オブジェクトを復元して、そのコピーを隔離に保存して後で使用できます。たとえば、定義データベースのアップデート後にオブジェクトを再スキャンする場合です。

隔離されたオブジェクトが(アーカイブなどの)複合オブジェクトに含まれる場合、そのオブジェクトは復元中の複合オブジェクトの中には含まれず、選択したフォルダーに個別に保存されます。

1 つまたは複数のオブジェクトを復元できます。

► 隔離されたオブジェクトを復元するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーを選択します。
3. [**隔離**]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:
   - 1 つのオブジェクトを復元するには、復元するオブジェクトのコンテキストメニューで[**復元**]を選択します。
   - 複数のオブジェクトを復元するには、**Ctrl** キーか **Shift** キーを使用して復元するオブジェクトを選択し、選択したオブジェクトの 1 つを右クリックして、コンテキストメニューから[**復元**]を選択します。

   [**オブジェクトを復元**]ウィンドウが開きます。
4. [**オブジェクトを復元**]ウィンドウで、選択したオブジェクトごとに、復元するオブジェクトの保存先のフォルダーを指定します

   オブジェクトの名前は、ウィンドウ上部の[**オブジェクト**]に表示されます。複数のオブジェクトを選択した場合は、選択したオブジェクトのリストの最初のオブジェクトの名前が表示されます。
5. 次のいずれかの処理を実行します:
   - オブジェクトを元の場所に復元するには、[**元のフォルダーに復元**]を選択します。
   - この設定で復元したオブジェクトの場所として指定したフォルダーにオブジェクトを復元するには、[**既定の復元用フォル**

ダーに復元]を選択します。

- アプリケーションコンソールがインストールされているサーバーの別のフォルダーや共有フォルダーにオブジェクトを保存するには、[**ローカルコンピューターまたはネットワークリソースのフォルダーに復元**]を選択して目的のフォルダーを選択するか、そのフォルダーのパスを指定します。

6. オブジェクトの復元後にこのオブジェクトのコピーを隔離に保存するには、[**復元後にオブジェクトを保管領域から削除する**]をオフにします。
7. 指定した復元条件を残りの選択したオブジェクトに適用するには、[**選択したすべてのオブジェクトに適用する**]をオンにします。

   選択したすべてのオブジェクトが復元されて指定の場所に保存されます。[**元のフォルダーに復元**]を選択した場合、各オブジェクトは前の場所に保存されます。[**既定の復元用フォルダーに復元**]または[**ローカルコンピューターまたはネットワークリソースのフォルダーに復元**]を選択した場合、すべてのオブジェクトは指定したフォルダーに保存されます。
8. [**OK**]をクリックします。

   選択した最初のオブジェクトの復元が開始されます。
9. 指定した場所に同じ名前のオブジェクトがすでに存在する場合は、[**同じ名前のオブジェクトあり**]ウィンドウが開きます。

   a. 次の Kaspersky Security for Windows Server 処理のいずれかを選択します:

   - 既存のオブジェクトの代わりにオブジェクトを復元するには、[**置換**]を選択します。
   - 復元したオブジェクトを別の名前で保存するには、[**名前の変更**]を選択します。入力フィールドに、新しいオブジェクトのファイル名と完全パスを入力します。
   - オブジェクトのファイル名に接尾語を追加して名前を変更するには、[**接尾語を追加して名前を変更**]を選択します。入力フィールドに接尾語を入力します。

   b. 複数のオブジェクトの復元を選択した場合、選択した処理([**置換**]や[**接尾語を追加して名前を変更**]など)を選択した残りのオブジェクトに適用するには、[**選択したすべてのオブジェクトに適用する**]をオンにします。([**名前の変更**]の値を選択した場合、[**選択したすべてのオブジェクトに適用する**]は使用できません)。

   c. [**OK**]をクリックします。

オブジェクトが復元されます。復元操作に関する情報がシステム監査ログに入力されます。

[**オブジェクトを復元**]ウィンドウで[**選択したすべてのオブジェクトに適用する**]を選択しなかった場合は、[**オブジェクトを復元**]ウィンドウがもう一度開きます。このウィンドウを使用して、選択した次のオブジェクトの保存場所を指定できます(この処理の手順 4 を参照してください)。

オブジェクトの隔離への移動

ファイルを手動で隔離できます。

► ファイルを隔離するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**隔離**]フォルダーのコンテキストメニューを開きます。
2. [**追加**]を選択します。
3. [**ファイルを開く**]ウィンドウで、ディスク上の隔離するファイルを選択します。
4. [**OK**]をクリックします。

選択したファイルが隔離されます。

隔離からのオブジェクトの削除

隔離のスキャンタスクの設定に従い、アップデートされた定義データベースで隔離のスキャン中にステータスが**感染**に変更され、駆除できなかった場合には、隔離フォルダーからオブジェクトが自動的に削除されます。他のオブジェクトは隔離から削除されません。

1 つまたは複数のオブジェクトを隔離から削除できます。

► 隔離から 1 つまたは複数のオブジェクトを削除するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーを選択します。
3. 次のいずれかの処理を実行します:
   - 1 つのオブジェクトを削除するには、そのオブジェクトの名前の上でコンテキストメニューを開き[**削除**]を選択します。
   - 複数のオブジェクトを削除するには、**Ctrl** キーまたは **Shift** キーを使用して削除対象のオブジェクトを選択し、選択したいずれかのオブジェクトのコンテキストメニューを開いて、[**削除**]を選択します。
4. 確認ウィンドウで[**はい**]をクリックして操作を確認します。

選択したオブジェクトが隔離から削除されます。

感染の可能性があるオブジェクトを分析するためのカスペルスキーへの送信

ファイルのふるまいから脅威が含まれる可能性があるのに Kaspersky Security for Windows Server で検知されない場合は、定義データベースにまだ特徴が追加されていない未知の脅威である可能性があります。このようなファイルは、カスペルスキーに送信して分析してもらうことができます。カスペルスキーのアンチウイルスアナリストがこのファイルを分析し、新しい脅威が検知された場合は、その識別用レコードを定義データベースに追加します。定義データベースのアップデート後にオブジェクトを再スキャンすると、Kaspersky Security for Windows Server がこのオブジェクトを感染していると検知し、駆除できるようになります。オブジェクトを保持するだけでなく、ウイルスアウトブレイクを防ぐことができます。

分析用に送信できるのは、隔離されたファイルだけです。隔離されたファイルは、暗号化された形式で保管され、送信の際、メールサーバーにインストールされている Kaspersky Security によって削除されません。

ライセンスの有効期間終了後に、隔離されたオブジェクトを分析のためにカスペルスキーに送信することはできません。

► ファイルを分析のためにカスペルスキーに送信するには、次の手順を実行します:

1. ファイルが隔離されていない場合は、まず**隔離**に移動します。
2. [**隔離**]フォルダーで分析用に送信するファイルのコンテキストメニューを開き、コンテキストメニューの[**オブジェクトを解析用に送信**]を選択します。
3. 選択したオブジェクトを分析に送信する場合は、表示される確認ウィンドウで[**はい**]をクリックします。
4. アプリケーションコンソールがインストールされているサーバーでメールクライアントが設定されている場合は、新しいメールメッセージが作成されます。このメッセージを確認して[**送信**]をクリックします。

   [**受信者**]にはカスペルスキーのメールアドレス(newvirus@kaspersky.com)が含まれます。[件名]には「隔離されたオブジェクト」というテキストが含まれます。

メッセージの本文には、次のテキストが含まれます:「オブジェクトが Kaspersky Lab に送信されて解析されます」。メッセージ本文に、ファイルに関する追加情報(感染の可能性や危険性があると思われる理由や、ファイルの動作、システムへ与えた影響など)を含めることができます。

アーカイブ <オブジェクト名>.cab がメッセージに添付されます。このアーカイブには、暗号化されたオブジェクトが含まれるファイル <uuid>.klq、抽出されたオブジェクトに関する情報が含まれるファイル <uuid>.txt、およびサーバーにインストールされている Kaspersky Security for Windows Server とオペレーティングシステムに関する次の情報が含まれるファイル Sysinfo.txt が含まれます:

- オペレーティングシステムの名前とバージョン。
- Kaspersky Security for Windows Server の名前とバージョン。
- インストールされている最新の定義データベースのアップデートの公開日時。
- 現在のライセンス。

この情報は、カスペルスキーのアンチウイルスアナリストがファイルをより早く効率的に分析するのに必要です。ただし、この情報を送信したくない場合は、アーカイブからファイル Sysinfo.txt を削除できます。

アプリケーションコンソールがインストールされているサーバーにメールクライアントがインストールされていない場合、選択した暗号化されているオブジェクトのファイル保存を確認するウィンドウが表示されます。このファイルは、手動でカスペルスキーに送信できます。

► 暗号化されたオブジェクトをファイルに保存するには、次の手順を実行します:

1. オブジェクトの保存について確認するウィンドウが表示されたら、[**OK**]をクリックします。
2. 保護対象サーバーのドライブ上のフォルダーか、オブジェクトが含まれるファイルの保存先のネットワークフォルダーを選択します。

オブジェクトが CAB ファイルに保存されます。

隔離の設定

隔離の設定を行えます。新しい隔離設定は、保存後即座に適用されます。

► 隔離の設定を行うには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**隔離**]サブフォルダーのコンテキストメニューを開きます。
3. [**プロパティ**]を選択します。
4. [**隔離のプロパティ**]ウィンドウで、要件に従って、必要な隔離設定を行います:
   - [**隔離設定**]セクション:
     - **隔離フォルダー**

       UNC(ユニバーサルネーミング規約)フォーマットの[隔離]フォルダーのパス。

       既定のパスは C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\ です。
     - **隔離フォルダーの最大サイズ**

       このチェックボックスにより、[隔離]フォルダーに格納されているオブジェクトの合計サイズを監視する機能を有効または無効に設定できます。指定した値を超過した場合(既定値:200 MB)、Kaspersky Security for Windows Server により、[**隔離の最大サイズを超過しました**]イベントが記録されて、この種別のイベ

ントに関する通知の設定に従って通知が発行されます。

このチェックボックスをオンにすると、Kaspersky Security for Windows Server により、[隔離]に配置されたオブジェクトの合計サイズが監視されます。

このチェックボックスをオフにすると、Kaspersky Security for Windows Server により、[隔離]に配置されたオブジェクトの合計サイズが監視されません。

既定では、このチェックボックスはオフです。

- **空き容量のしきい値**

  このチェックボックスにより、[隔離]の空き容量の下限を監視する機能を有効または無効に設定できます(既定値:50 MB)。空き容量が指定したしきい値を下回った場合、Kaspersky Security for Windows Server により、[**バックアップの空き容量がしきい値より少なくなりました**]イベントが記録されて、この種別のイベントに関する通知の設定に従って通知が発行されます。

  このチェックボックスをオンにすると、Kaspersky Security for Windows Server により、[バックアップ]の空き容量が監視されます。

  [空き容量のしきい値(MB)]は、[隔離の最大サイズ(MB)]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。

> [隔離]に配置されているオブジェクトのサイズが隔離の最大サイズを超過した場合、または空き容量のしきい値を超過した場合、その通知が表示されますが、隔離へのオブジェクトの配置は継続されます。

- [**復元設定**]セクション:
  - **復元先フォルダー**

5. [**OK**]をクリックします。

新しく設定された隔離の内容が保存されます。

隔離の統計情報

隔離されたオブジェクトの数の情報である、隔離の統計情報を確認できます。

► 隔離の統計情報を表示するには:

アプリケーションコンソールツリーで、[**隔離**]フォルダーのコンテキストメニューを開き、[**統計情報**]を選択します。

[**統計情報**]ウィンドウに、隔離に現在保存されているオブジェクトの数の情報が表示されます(次の表を参照)。

フィールド	説明
感染の可能性があるオブジェクト	Kaspersky Security for Windows Server が感染の可能性を検知したオブジェクトの数。
使用済み隔離領域	隔離内のデータの合計サイズ。
誤検知	アップデートされた定義データベースを使用した隔離スキャン時に感染していないと分類されたために、**誤検知**ステータスを受け取ったオブジェクトの数。
駆除されたオブジェクト	隔離のスキャン後に**駆除済み**ステータスを受け取ったオブジェクトの数。

フィールド	説明
オブジェクトの合計数	隔離内のオブジェクトの合計数。

オブジェクトのバックアップコピーの作成：バックアップ

このセクションでは、検知された悪意のあるオブジェクトを駆除または削除する前のバックアップと、バックアップの設定方法に関する情報を提供します。

このセクションの内容

駆除または削除前のオブジェクトのバックアップについて

Kaspersky Security 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。

オブジェクトが複合オブジェクトの一部である場合（アーカイブの一部である場合など）は、複合オブジェクト全体がバックアップに保存されます。たとえば、メールデータベースの 1 つのオブジェクトの感染が検知された場合は、そのメールデータベース全体がバックアップされます。

バックアップにあるオブジェクトのサイズが大きいと、システムの速度が低下したり、ハードディスクのディスク容量が減ったりする場合があります。

ファイルはバックアップから、元のフォルダーや、保護対象サーバーまたはローカルエリアネットワークの他のコンピューターの別のフォルダーに復元できます。たとえば、感染したファイルに重要な情報が含まれていたが、このファイルの駆除中に、整合性を維持できず情報が使用できなくなった場合に、ファイルをバックアップから復元できます。

バックアップからファイルを復元すると、サーバーが感染する可能性があります。

バックアップに保存されたオブジェクトの表示

オブジェクトをバックアップフォルダーに保存する唯一の方法は、[**バックアップ**]フォルダーでアプリケーションコンソールを使用することです。これらのファイルを Microsoft Windows ファイルマネージャーで表示することはできません。

► オブジェクトをバックアップで表示するには:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**バックアップ**]サブフォルダーを選択します。

   選択したフォルダーの詳細ペインに、バックアップ済みのオブジェクトの情報が表示されます。

► バックアップ済みオブジェクトのリストから、重要なオブジェクトを見つけるには:

オブジェクトの並べ替えかオブジェクトのフィルタリングを行います。

このセクションの内容

[バックアップ]内のファイルの並べ替え

既定では、[バックアップ]内のファイルは保存日の新しいものから順に並べ替えられます。目的のファイルを検索するために、詳細ペインの任意の列の内容を基準にファイルを並べ替えることができます。

[**バックアップ**]フォルダーから移動して、再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

► [バックアップ]内のファイルを並べ替えるには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**バックアップ**]サブフォルダーを選択します。
3. [**バックアップ**]内のファイルのリストで、オブジェクトの並べ替えに使用する列見出しを選択します。

   選択した基準に基づいて、[バックアップ]内のファイルの表示順が変わります。

[バックアップ]内のファイルのフィルタリング

[バックアップ]内の目的のファイルを検索するために、ファイルをフィルタリングして、指定したフィルタリング条件(フィルター)を満たすファイルのみを[**バックアップ**]フォルダーに表示することができます。

[**バックアップ**]フォルダーから移動して、再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

► [バックアップ]内のファイルをフィルタリングするには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**バックアップ**]フォルダーのコンテキストメニューを開き、[**フィルター**]を選択します。

[**フィルターの設定**]ウィンドウが表示されます。

2. フィルターを追加するには、次の手順を実行します:

   a. [**フィールド名**]で、フィルタリングでフィルター値と比較する値のフィールドを選択します。

   b. [**演算子**]リストで、フィルタリング条件を選択します。リストのフィルタリング条件の値は、[**フィールド名**]で選択した値に応じて異なる場合があります。

   c. [**フィールド値**]にフィルターの値を入力するか、選択します。

   d. [**追加**]をクリックします。

   追加したフィルターが、[**フィルターの設定**]ウィンドウのフィルターのリストに表示されます。追加するフィルターごとにこれらの手順を繰り返します。フィルターの使用時は、次のガイドラインを使用できます:

   - 論理演算子「AND」を使って複数のフィルターを組み合わせるには、[**すべての条件が満たされた場合**]を選択します。
   - 論理演算子「OR」を使って複数のフィルターを組み合わせるには、[**いずれかの条件が満たされた場合**]を選択します。
   - フィルターを削除するには、フィルターのリストから削除するフィルターを選択し、[**削除**]をクリックします。
   - フィルターを編集するには、[**フィルターの設定**]ウィンドウのフィルターリストからフィルターを選択して、[**フィールド名**]、[**演算子**]、または[**フィールド値**]で、対象の値を変更して、[**置換**]をクリックします。

   すべてのフィルターが追加されたら、[**適用**]をクリックします。指定したフィルターでフィルタリングされたファイルのみがリストに表示されます。

► [バックアップ]に格納されているオブジェクトのリストに含まれるすべてのファイルを表示するには:

[**バックアップ**]フォルダーのコンテキストメニューで、[**フィルターの削除**]を選択します。

バックアップからのファイルの復元

Kaspersky Security for Windows Server では、発生する可能性がある危険から保護対象のサーバーを保護するために、ファイルは暗号化された形式でバックアップフォルダーに保存されます。

すべてのファイルをバックアップから復元できます。

次の場合に、ファイルの復元が必要となる可能性があります。

- 感染したと思われる元のファイルに重要な情報が含まれており、Kaspersky Security for Windows Server で整合性を保持できなかったために、ファイル内の情報が利用できなくなった場合。
- ファイルがサーバーに対して無害であると考えられ、このファイルを使用する必要がある場合。Kaspersky Security for Windows Server でこのファイルが感染しているまたは感染の可能性があるとみなされないようにするときには、以降のスキャン時にこのファイルをファイルのリアルタイム保護タスクおよびオンデマンドスキャンタスクの処理から除外できます。除外するには、対応するタスクでこのファイルを[**除外するファイル**]設定または[**検知しないオブジェクト**]設定として指定します。

  > バックアップからファイルを復元すると、サーバーが感染する可能性があります。

ファイルの復元時に、復元したファイルの保管場所を選択できます。選択できるのは、元の場所(既定)、保護対象サーバーの復元したオブジェクト用の特別なフォルダー、アプリケーションコンソールがインストールされているサーバーやネットワーク上のその他のコンピューターのカスタムフォルダーです。

[**フォルダーへの復元**]は、復元したオブジェクトを保護対象サーバーに保存する場合に使用します。このスキャン対象のオブジェクト用に、特別なセキュリティ設定を設定できます。このフォルダーへのパスは、バックアップ設定で指定します(「バックアップの設定」(201 ページ)を参照)。

既定では、Kaspersky Security for Windows Server でファイルを復元するときに、バックアップにそのファイルのコピーが作成されます。

ファイルの復元後に、ファイルのコピーをバックアップから削除できます。

► バックアップからファイルを復元するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**バックアップ**]サブフォルダーを選択します。
3. [**バックアップ**]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:
   - 1 つのオブジェクトを復元するには、復元するオブジェクトのコンテキストメニューで[**復元**]を選択します。
   - 複数のオブジェクトを復元するには、**Ctrl** キーか **Shift** キーを使用して復元するオブジェクトを選択し、選択したオブジェクトの 1 つを右クリックして、コンテキストメニューから[**復元**]を選択します。

   [**オブジェクトを復元**]ウィンドウが開きます。
4. [**オブジェクトを復元**]ウィンドウで、選択したオブジェクトごとに、復元するオブジェクトの保存先のフォルダーを指定します

   > オブジェクトの名前は、ウィンドウ上部の[**オブジェクト**]に表示されます。複数のオブジェクトを選択した場合は、選択したオブジェクトのリストの最初のオブジェクトの名前が表示されます。
5. 次のいずれかの処理を実行します:
   - オブジェクトを元の場所に復元するには、[**元のフォルダーに復元**]を選択します。
   - この設定で復元したオブジェクトの場所として指定したフォルダーにオブジェクトを復元するには、[**既定の復元用フォルダーに復元**]を選択します。
   - アプリケーションコンソールがインストールされているサーバーの別のフォルダーや共有フォルダーにオブジェクトを保存するには、[**ローカルコンピューターまたはネットワークリソースのフォルダーに復元**]を選択して目的のフォルダーを選択するか、そのフォルダーのパスを指定します。
6. ファイルの復元後にファイルのコピーをバックアップフォルダーに保存するには、[**復元後にオブジェクトを保管領域から削除する**]をオフにします(既定では、このチェックボックスはオフです)。
7. 指定した復元条件を残りの選択したオブジェクトに適用するには、[**選択したすべてのオブジェクトに適用する**]をオンにします。

   選択したすべてのオブジェクトが復元されて指定の場所に保存されます。[**元のフォルダーに復元**]を選択した場合、各オブジェクトは前の場所に保存されます。[**既定の復元用フォルダーに復元**]または[**ローカルコンピューターまたはネットワークリソースのフォルダーに復元**]を選択した場合、すべてのオブジェクトは指定したフォルダーに保存されます。
8. [**OK**]をクリックします。

   選択した最初のオブジェクトの復元が開始されます。
9. 指定した場所に同じ名前のオブジェクトがすでに存在する場合は、[**同じ名前のオブジェクトあり**]ウィンドウが開きます。
   a. 次の Kaspersky Security for Windows Server 処理のいずれかを選択します:
   - 既存のオブジェクトの代わりにオブジェクトを復元するには、[**置換**]を選択します。
   - 復元したオブジェクトを別の名前で保存するには、[**名前の変更**]を選択します。入力フィールドに、新しいオブジェクトのファイル名と完全パスを入力します。
   - オブジェクトのファイル名に接尾語を追加して名前を変更するには、[**接尾語を追加して名前を変更**]を選択します。入力フィールドに接尾語を入力します。

   b. 複数のオブジェクトの復元を選択した場合、選択した処理([**置換**]や[**接尾語を追加して名前を変更**]など)を選択した残りのオブジェクトに適用するには、[**選択したすべてのオブジェクトに適用する**]をオンにします。([**名前の変更**]の値を選択した場合、[**選択したすべてのオブジェクトに適用する**]は使用できません)。

   c. [**OK**]をクリックします。

オブジェクトが復元されます。復元操作に関する情報がシステム監査ログに入力されます。

[**オブジェクトを復元**]ウィンドウで[**選択したすべてのオブジェクトに適用する**]を選択しなかった場合は、[**オブジェクトを復元**]ウィンドウがもう一度開きます。このウィンドウを使用して、選択した次のオブジェクトの保存場所を指定できます(この処理の手順 4 を参照してください)。

バックアップからのファイルの削除

► **バックアップから 1 つまたは複数のファイルを削除するには、次の手順を実行します:**

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**バックアップ**]サブフォルダーを選択します。
3. 次のいずれかの処理を実行します:
   - 1 つのオブジェクトを削除するには、そのオブジェクトの名前の上でコンテキストメニューを開き[**削除**]を選択します。
   - 複数のオブジェクトを削除するには、**Ctrl** キーまたは **Shift** キーを使用して削除対象のオブジェクトを選択し、選択したいずれかのオブジェクトのコンテキストメニューを開いて、[**削除**]を選択します。
4. 確認ウィンドウで[**はい**]をクリックして操作を確認します。

選択したファイルが[バックアップ]から削除されます。

バックアップの設定

► **バックアップの設定を行うには、次の手順を実行します:**

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**バックアップ**]サブフォルダーのコンテキストメニューを開きます。
3. [**プロパティ**]を選択します。
4. [**バックアップのプロパティ**]ウィンドウで、要件に従って、必要なバックアップ設定を行います:

   [**バックアップ設定**]セクション:

   - **バックアップフォルダー**

     UNC(ユニバーサルネーミング規約)フォーマットの[バックアップ]フォルダーのパス。

     既定のパスは C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\ です。

   - **バックアップの最大サイズ(MB)**

     このチェックボックスにより、[バックアップ]フォルダーに格納されているオブジェクトの合計サイズを監視する機能を有効または無効に設定できます。指定した値を超過した場合(既定値:200 MB)、Kaspersky Security for Windows Server により、[*バックアップの最大サイズを超過しました*]イベントが記録されて、この種別のイベントに関する通知の設定に従って通知が発行されます。

     このチェックボックスをオンにすると、Kaspersky Security for Windows Server により、[バックアップ]に配置されたオブジェクトの合計サイズが監視されます。

     このチェックボックスをオフにすると、Kaspersky Security for Windows Server により、[バックアップ]に配置されたオブジェクトの合計サイズが監視されません。

既定では、このチェックボックスはオフです。

- **空き容量のしきい値(MB)**

  このチェックボックスにより、[隔離]の空き容量の下限を監視する機能を有効または無効に設定できます(既定値:50 MB)。空き容量が指定したしきい値を下回った場合、Kaspersky Security for Windows Server により、[**バックアップの空き容量がしきい値より少なくなりました**]イベントが記録されて、この種別のイベントに関する通知の設定に従って通知が発行されます。

  このチェックボックスをオンにすると、Kaspersky Security for Windows Server により、[バックアップ]の空き容量が監視されます。

  [空き容量のしきい値(MB)]は、[隔離の最大サイズ(MB)]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。

> [バックアップ]に配置されているオブジェクトのサイズがバックアップの最大サイズを超過した場合、または空き容量のしきい値を超過した場合、その通知が表示されますが、バックアップへのオブジェクトの配置は継続されます。

[**復元設定**]セクション:

- **復元先フォルダー**

  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。

  既定のパス:C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored

5. [**OK**]をクリックします。

設定したバックアップの内容が保存されます。

バックアップの統計情報

バックアップの現在のステータスに関する情報であるバックアップの統計情報を表示できます。

► バックアップの統計情報を表示するには:

アプリケーションコンソールツリーで、[**バックアップ**]フォルダーのコンテキストメニューを開き、[**統計情報**]を選択します。[**バックアップの統計情報**]ウィンドウが開きます。

[**バックアップの統計情報**]ウィンドウに、バックアップの現在のステータスに関する情報が表示されます(次の表を参照)。

表 34. バックアップの現在のステータスに関する情報

フィールド	説明
現在のバックアップのサイズ	バックアップフォルダーのデータサイズ。ファイルサイズは暗号化された形式で計算されます。
オブジェクトの合計数	バックアップ内のオブジェクトの現在の合計数。

ネットワークリソースへのアクセスのブロック：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保管領域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

ブロック対象コンピューターの保管領域について

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保管領域が既定でインストールされます：ファイルのリアルタイム保護、NetApp のアンチクリプター、アンチクリプター。コンポーネントはブロック対象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フォルダー上のオブジェクトをリモートコンピューターから暗号化したり開こうとする、あるいは実行しようとする試行を検出します。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 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保管領域には、次のタスクのうち 1 つ以上のタスクが有効な状態で開始されており、なおかつ指定の条件が満たされている場合に情報が追加されます：

- ファイルのリアルタイム保護タスクの場合：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のネットワーク共有リソースへのアクセスをブロックする**］がオンにされている。
- アンチクリプタータスクの場合：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場合：ネットワーク接続ストレージへの攻撃が検知された。

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、コンピューターのブロックに関する警告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。

攻撃元のコンピューターの LUID（ローカルで一意な識別子）がブロック対象コンピューターのリストに追加されると、Kaspersky Security for Windows Server はこの攻撃元コンピューターの IP アドレスを特定し、ブロック対象コンピューターのリストに LUID のかわりに IP アドレスを追加します。

Kaspersky Security for Windows Server は既定で、ブロック対象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。ブロック対象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。

任意のユーザーアカウントに対して保管領域の管理操作へのアクセスを制限する場合、ブロック対象コンピューターの保管領域には引き続きアクセスできます。選択したユーザーアカウントが Kaspersky Security for Windows Server を管理するための**編集権限**を持っていない場合に限り、ブロック対象コンピューターの設定を変更することはできません。

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 1 つ以上のタスクを有効な状態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. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**ファイルのリアルタイム保護**]サブフォルダーを選択します。
3. 詳細ペインで[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. [**他のコンポーネントとの連携**]セクションで、[**悪意のある動作を示すコンピューターのネットワーク共有リソースへのアクセスをブロックする**]をオンにすると、リアルタイムのファイル保護タスクの実行中に悪意ある活動が検知されたコンピューターをブロックできます。
5. タスクが開始されていない場合、[**スケジュール**]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. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

新しい設定が保存されます。

► アンチクリプタータスクの設定:

1. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。
3. 詳細ペインで[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. [**全般**]タブで、タスクが[**処理を実行**]モードになっていることを確認します。
5. タスクが開始されていない場合、[**スケジュール**]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. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

新しい設定が保存されます。

► NetApp のアンチクリプターの設定:

1. アプリケーションコンソールツリーで、[**ネットワーク接続ストレージの保護**]フォルダーを展開します。
2. [**NetApp のアンチクリプター**]サブフォルダーを選択します。
3. 詳細ペインで[**プロパティ**]をクリックします。

[**タスクの設定**]ウィンドウが表示されます。

4. [**全般**]タブで、タスクが[**処理を実行**]モードになっていることを確認します。
5. タスクが開始されていない場合、[**スケジュール**]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. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

Kaspersky Security 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保管領域を設定するには:

1. アプリケーションコンソールツリーで、[**保管領域**]フォルダーを展開します。
2. [**ブロック対象コンピューター**]サブフォルダーのコンテキストメニューを開きます。
3. [**プロパティ**]メニューオプションを選択します。

[**ブロック対象コンピューターの保管領域の設定**]ウィンドウが表示されます。

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. [**OK**]をクリックします。
6. すべてのブロック対象コンピューターへのアクセスを復元するには:
   a. [**ブロック対象コンピューター**]サブフォルダーのコンテキストメニューを開きます。
   b. [**すべてブロック解除**]オプションを選択します。

すべてのコンピューターがリストから削除されてブロック解除されます。

7. ブロック対象コンピューターのリストからいくつかのコンピューターを削除するには:
   a. 詳細ペインに表示されるブロック対象コンピューターのリストで、1 つまたは複数のコンピューターを選択します。
   b. [**ブロック対象コンピューター**]サブフォルダーのコンテキストメニューを開きます。

C. ［**選択項目のブロック解除**］オプションを選択します。

選択したコンピューターがブロック解除されます。

イベントの登録：Kaspersky Security for Windows Server のログ

このセクションでは、Kaspersky Security for Windows Server のログ（システム監査ログ、タスク実行ログ、イベントログ）の使用について説明します。

この章の内容

Kaspersky Security for Windows Server のイベントを登録する方法

Kaspersky Security for Windows Server のイベントは、2 つのグループに分けられます：

- Kaspersky Security for Windows Server のタスクでのオブジェクトの処理に関連するイベント
- アプリケーションの起動、タスクの作成や削除、タスク設定の編集などの Kaspersky Security for Windows Server の管理に関連するイベント

Kaspersky Security for Windows Server では、イベントの記録に次の方法を使用します：

- **実行ログ**：タスク実行ログには、タスクの現在のステータスとタスクの実行中に発生したイベントの情報が含まれます。
- **システム監査ログ**：システム監査ログには、Kaspersky Security for Windows Server の管理に関連するイベントの情報が含まれます。
- **イベントログ**：イベントログには、Kaspersky Security for Windows Server の動作エラーの診断に必要なイベントの情報が含まれます。イベントログは、Microsoft Windows イベントビューアーで確認できます。
- **セキュリティログ**：セキュリティログには、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情報が含まれています。

Kaspersky Security for Windows Server の使用中に、Kaspersky Security for Windows Server または個々のタスクが異常終了したり、開始されなかったりする問題が発生した場合、発生した問題を診断するために、トレースファイルと Kaspersky Security for Windows Server プロセスのメモリダンプファイルを作成し、この情報が含まれるファイルを解析用にカスペルスキーのテクニカルサポートに送信できます。

Kaspersky Security 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 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 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(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」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。

システム監査ログ

Kaspersky Security for Windows Server は、Kaspersky Security for Windows Server の管理に関連したイベントのシステム監査を実行します。本製品の起動、Kaspersky Security for Windows Server タスクの開始と停止、タスク設定の変更、オンデマンドスキャンタスクの作成と削除などの情報がログに記録されます。アプリケーションコンソールで[**システム監査ログ**]を選択すると、これらのすべてのイベントの記録が詳細ペインに表示されます。

既定では、記録はシステム監査ログに無期限に保存されます。システム監査ログでの記録の保存期間を指定します。

システム監査ログが含まれたファイルを保存するために Kaspersky Security for Windows Server で使用するフォルダーを既定以外の場所で指定できます。

このセクションの内容

システム監査ログでのイベントの並べ替え

既定では、システム監査ログノードのイベントは、新しいものから順に表示されます。

イベントは、[**イベント**]列以外の列の内容で並べ替えできます。

► システム監査ログでイベントを並べ替えるには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**システム監査ログ**]サブフォルダーを選択します。
3. 詳細ペインで、リストのイベントの並べ替えに使用する列の見出しを選択します。

並べ替えの結果は、システム監査ログの次の表示セッションまで保存されます。

タスク実行ログでのイベントリストの表示

► タスク実行ログでイベントリストを表示するには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]を選択します。

Kaspersky Security for Windows Server のタスク実行ログに保存されているイベントのリストが、詳細ペインに表示されます。イベントは、列で並べ替えたりフィルタリングしたりすることができます。

システム監査ログでのイベントのフィルタリング

指定したフィルタリング条件を満たすイベントのレコードのみが表示されるように、システム監査ログを設定できます。

► システム監査ログのイベントをフィルタリングするには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**システム監査ログ**]サブフォルダーのコンテキストメニューを開き、[**フィルター**]を選択します。

   [**フィルターの設定**]ウィンドウが表示されます。
3. フィルターを追加するには、次の手順を実行します:
   a. [**フィールド名**]リストで、イベントのフィルタリング条件となる列を選択します。
   b. [**演算子**]リストで、フィルタリング条件を選択します。フィルタリング条件は、[**フィールド名**]リストで選択した項目によって変わります。
   c. [**フィールド値**]リストで、フィルターの値を選択します。
   d. [**追加**]をクリックします。

   追加したフィルターが、[**フィルターの設定**]ウィンドウのフィルターのリストに表示されます。
4. 必要に応じて、次のいずれかの処理を実行します:
   - 論理演算子 AND を使って複数のフィルターを組み合わせるには、[**すべての条件が満たされた場合**]を選択します。
   - 論理演算子 OR を使って複数のフィルターを組み合わせるには、[**いずれかの条件が満たされた場合**]を選択します。
5. [**適用**]をクリックして、フィルタリング条件をシステム監査ログに保存します。

   システム監査ログのイベントのリストには、フィルタリング条件を満たすイベントのみが表示されます。フィルタリングの結果は、システム監査ログの次の表示セッションまで保存されます。

► フィルターを無効にするには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**システム監査ログ**]サブフォルダーのコンテキストメニューを開き、[**フィルターの削除**]を選択します。

   システム監査ログのイベントのリストに、すべてのイベントが表示されます。

システム監査ログからのイベントの削除

既定では、記録はシステム監査ログに無期限に保存されます。システム監査ログでの記録の保存期間を指定します。

システム監査ログからすべてのイベントを手動で削除できます。

► システム監査ログからイベントを削除するには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**システム監査ログ**]サブフォルダーのコンテキストメニューを開き、[**クリア**]を選択します。
3. 次のいずれかの処理を実行します:
   - システム監査ログからイベントを削除する前に、ログの内容を CSV 形式や TXT 形式のファイルとして保存するには、削除の確認ウィンドウで[**はい**]をクリックします。ウィンドウが開いたら、ファイルの名前と場所を指定します。
   - ログの内容をファイルとして保存しない場合は、削除の確認ウィンドウで[**いいえ**]をクリックします。

システム監査ログがクリアされます。

タスク実行ログ

このセクションでは、Kaspersky Security for Windows Server のタスク実行ログに関する情報およびタスク実行ログの管理方法について説明します。

このセクションの内容

タスク実行ログについて

アプリケーションコンソールで[**実行ログ**]フォルダーを選択すると、詳細ペインに Kaspersky Security for Windows Server タスクの実行に関する情報が表示されます。

各タスクのログでは、タスク実行の統計、タスクの開始時から現時点までの本製品で処理された各オブジェクトの詳細、およびタスクの設定を表示できます。

既定では、レコードはタスクの完了から 30 日間、タスク実行ログに保存されます。タスク実行ログのレコードの保存期間は変更できます。

Kaspersky Security for Windows Server で使用するフォルダーを指定して、タスク実行ログのファイルを既定以外のフォルダーに保存できます。タスク実行ログに記録されるイベントを選択することもできます。

タスク実行ログでのイベントの並べ替え

既定では、タスク実行ログのイベントは、新しいものから順に表示されます。イベントは、列で並べ替えることができます。

► タスク実行ログのイベントを並べ替えるには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]を選択します。
3. 詳細ペインで、Kaspersky Security for Windows Server のタスク実行ログのイベントの並べ替えに使用する列の見出しを選択します。

並べ替えの結果は、タスク実行ログの次の表示セッションまで保存されます。

タスク実行ログでのイベントのフィルター処理

指定したフィルタリング条件を満たすイベントのレコードのみが表示されるように、タスク実行ログのリストを設定できます。

► タスク実行ログのイベントをフィルタリングするには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]サブフォルダーのコンテキストメニューを開き、[**フィルター**]を選択します。

   [**フィルターの設定**]ウィンドウが表示されます。
3. フィルターを追加するには、次の手順を実行します:
   a. [**フィールド名**]リストで、イベントのフィルタリング条件となる列を選択します。
   b. [**演算子**]リストで、フィルタリング条件を選択します。フィルタリング条件は、[**フィールド名**]リストで選択した項目によって変わります。
   c. [**フィールド値**]リストで、フィルターの値を選択します。
   d. [**追加**]をクリックします。

   追加したフィルターが、[**フィルターの設定**]ウィンドウのフィルターのリストに表示されます。
4. 必要に応じて、次のいずれかの処理を実行します:
   - 論理演算子 AND を使って複数のフィルターを組み合わせるには、[**すべての条件が満たされた場合**]を選択します。
   - 論理演算子 OR を使って複数のフィルターを組み合わせるには、[**いずれかの条件が満たされた場合**]を選択します。
5. [**適用**]をクリックして、フィルタリング条件をタスク実行ログのリストに保存します。

タスク実行ログのイベントのリストには、フィルタリング条件を満たすイベントのみが表示されます。フィルタリングの結果は、タスク実行ログの次の表示セッションまで保存されます。

► フィルターを無効にするには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]サブフォルダーのコンテキストメニューを開き、[**フィルターの削除**]を選択します。

タスク実行ログのイベントリストに、すべてのイベントが表示されます。

タスク実行ログでの Kaspersky Security for Windows Server のタスクに関する統計と情報の表示

タスク実行ログには、タスクの開始から現在までにタスクで発生したすべてのイベントに関する詳細情報、タスク実行の統計、およびタスク設定が表示されます。

► Kaspersky Security for Windows Server のタスクに関する統計と情報を表示するには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]を選択します。
3. 結果ペインで、次のいずれかの方法で[**ログ**]ウィンドウを開きます:
   - ログを表示するタスクで発生したイベントをダブルクリックする
   - ログを表示するタスクで発生したイベントのコンテキストメニューを開き、[**ログを表示**]を選択する
4. ウィンドウが開いて、次の詳細が表示されます:
   - [**統計情報**]タブには、タスクの開始時間と完了時間、およびタスクの統計が表示されます。
   - [**イベント**]タブには、タスクの実行中に記録されたイベントのリストが表示されます。
   - [**オプション**]タブには、タスクの設定が表示されます。
5. 必要に応じて、[**フィルター**]をクリックしてタスク実行ログのイベントをフィルタリングします。
6. 必要に応じて、[**エクスポート**]をクリックして、タスク実行ログのデータを CSV 形式または TXT 形式のファイルでエクスポートします。
7. [**閉じる**]をクリックします。

[**ログ**]ウィンドウが終了します。

タスク実行ログからの情報のエクスポート

タスク実行ログから CSV 形式または TXT 形式のファイルにデータをエクスポートできます。

► タスク実行ログからデータをエクスポートするには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]を選択します。
3. 結果ペインで、次のいずれかの方法で[**ログ**]ウィンドウを開きます:
   - ログを表示するタスクで発生したイベントをダブルクリックする
   - ログを表示するタスクで発生したイベントのコンテキストメニューを開き、[**ログを表示**]を選択する
4. [**ログ**]ウィンドウ下部の[**エクスポート**]をクリックします。

   [**名前を付けて保存**]ウィンドウが開きます。
5. タスク実行ログのデータのエクスポート先となるファイルの名前、場所、種別、エンコーディングを指定します。
6. [**保存**]をクリックします。

指定された設定が保存されます。

タスク実行ログからのイベントの削除

既定では、レコードはタスクの完了から 30 日間、タスク実行ログに保存されます。タスク実行ログのレコードの保存期間は変更できます。

現時点で完了しているタスクのログから、すべてのイベントを手動で削除できます。

現在実行中のタスクと他のユーザーが使用しているタスクのログのイベントは、削除されません。

► タスク実行ログからイベントを削除するには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーを展開します。
2. [**実行ログ**]を選択します。
3. 次のいずれかの処理を実行します:
   - 現時点で完了しているすべてのタスクのログのイベントを削除するには、[**実行ログ**]サブフォルダーのコンテキストメニューを開き、[**クリア**]を選択します。
   - 個々のタスクのログをクリアするには、詳細ペインで、ログをクリアするタスクで発生したイベントのコンテキストメニューを開き、[**削除**]を選択します。
   - 複数のタスク実行ログをクリアするには:
     a. 詳細ペインで、**Ctrl** キーか **Shift** キーを使用して、ログをクリアするタスクで発生したイベントを選択します。
     b. 選択したイベントのコンテキストメニューを開き、[**削除**]を選択します。
4. 削除の確認ウィンドウで[**はい**]をクリックし、ログを削除することを確認します。

選択したタスク実行ログがクリアされます。タスク実行ログからのイベントの削除は、システム監査ログに登録されます。

セキュリティログ

Kaspersky Security 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(サーバー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、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では記録内容を削除できます(「システム監査ログからのイベントの削除」(210 ページ)を参照)。さらに Kaspersky Security for Windows Server では、セキュリティログの記録内容の削除に関するシステム監査イベントが記録されます。

イベントビューアーでの Kaspersky Security for Windows Server のイベントログの表示

Microsoft 管理コンソールで Microsoft Windows の[イベントビューアー]スナップインを使用して Kaspersky Security for Windows Server のイベントログを表示できます。ログには、Kaspersky Security for Windows Server で登録されている、Kaspersky Security の動作エラーの診断に必要なイベントが含まれます。

イベントログに登録されるイベントを次の基準に基づいて選択できます。

- **イベントの種別**
- **詳細レベル**: 詳細レベルは、ログに登録されるイベント(情報イベント、注意が必要なイベント、または緊急イベント)の重要度のレベルに対応しています。最も情報が多いのはすべてのイベントが登録される情報イベントレベルで、最も情報が少ないのは緊急イベントのみ登録される緊急イベントレベルです。既定の詳細レベルはコンポーネントごとに異なります。

► Kaspersky Security for Windows Server のイベントログを表示するには:

1. [**スタート**]をクリックし、検索バーに `mmc` コマンドを入力して、**ENTER** キーを押します。

   Microsoft 管理コンソールのウィンドウが開きます。

2. [**ファイル**] > [**スナップインの追加と削除**]の順に選択します。

   [**スナップインの追加と削除**]ウィンドウが開きます。

3. 使用可能なスナップインのリストで、[**イベントビューアー**]スナップインを選択して[**追加**]をクリックします。

   [**コンピューターの選択**]ウィンドウが開きます。

4. [**コンピューターの選択**]ウィンドウで、Kaspersky Security for Windows Server がインストールされているコンピューターを指定し、[**OK**]をクリックします。

5. [**スナップインの追加と削除**]ウィンドウで、[**OK**]をクリックします。

   Microsoft 管理コンソールツリーに、[**イベントビューアー**]フォルダーが表示されます。

6. [**イベントビューアー**]フォルダーを展開し、[**アプリケーションとサービスログ**] - [**Kaspersky Security**]サブフォルダーを選択します。

Kaspersky Security for Windows Server イベントログが開きます。

Kaspersky Security for Windows Server コンソールでのログ設定

Kaspersky Security for Windows Server のログの次の設定を編集できます:

- タスク実行ログとシステム監査ログのイベントの保管期間
- タスク実行ログとシステム監査ログのファイルの保存先フォルダーの場所
- [**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[**簡易スキャンが長期間実行されていません**]の各イベントの発生のしきい値
- Kaspersky Security for Windows Server によりタスク実行ログおよびシステム監査ログに保存されるイベント、イベントビュー

アー内の Kaspersky Security for Windows Server のイベントログ

- Syslog プロトコルにより syslog サーバーに監査イベントとタスク実行イベントを公開するための設定

► Kaspersky Security for Windows Server ログを設定するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダー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。

   [**ログと通知の設定**]ウィンドウが開きます。

2. [**ログと通知の設定**]ウィンドウで、要件に従ってログを設定します。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、Kaspersky Security for Windows Server によりタスク実行ログおよびシステム監査ログに保存されるイベント、イベントビューアー内の Kaspersky Security for Windows Server のイベントログを選択します。それには、次の操作を実行します:

     - [**コンポーネント**]リストで、詳細レベルを設定する Kaspersky Security for Windows Server のコンポーネントを選択します。

     > ファイルのリアルタイム保護、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、スクリプト監視、オンデマンドスキャン、およびアップデートの各コンポーネントのイベントは、実行ログとイベントログに登録されます。これらのコンポーネントの場合、イベントリストのテーブルには[**実行ログ**]と[**Windows イベントログ**]の列が含まれます。隔離とバックアップのイベントは、システム監査ログおよびイベントログに登録されます。これらのコンポーネントの場合、イベントリストのテーブルには[**監査**]と[**Windows イベントログ**]の列が含まれます。

     - [**重要度**]リストで、選択したコンポーネントのタスク実行ログ、システム監査ログ、イベントログのイベントの詳細レベルを選択します。

       イベントのリストが含まれる次のテーブルでは、タスク実行ログ、システム監査ログ、イベントログと一緒に登録されるイベントの横のチェックボックスが、現在の詳細レベルに従ってオンになります。

     - 選択したコンポーネントの特定のイベントの登録を手動で有効にするには、次の操作を実行します:

       c. [**重要度**]リストで[**カスタム**]を選択します。

       d. イベントのリストが含まれるテーブルで、タスク実行ログ、システム監査ログ、イベントログに登録するイベントの横のチェックボックスをオンにします。

   - [**詳細設定**]タブで、サーバー保護ステータスに対するログの保管領域設定とイベント発生のしきい値を設定します:

     - [**ログの保管領域**]セクション:

       - **ログフォルダー**

       UNC(ユニバーサルネーミング規約)フォーマットのログフォルダーのパス。

       既定のパス:C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\

       既定のパスが変更されると、対応する名前が作成されます。新しいログが新しいフォルダーに保存されます。古いログは保存されます。

       - **実行ログの保管日数**

       このチェックボックスでは、タスク実行ログで公開される完了したタスクとイベントの実行結果が含まれるログを、指定期間(既定値:30 日)後に削除する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、タスク実行ログで公開される完了したタスクとイベントの実行結果が含まれるログが、指定期間後に削除されます。

       既定では、このチェックボックスはオンです。

- **システム監査ログ内のイベントの保管日数**

  このチェックボックスでは、システム監査ログに記録されたイベントを、指定期間(既定値:60 日)後に削除する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、システム監査ログに記録されたイベントが、指定期間後に削除されます。

  既定では、このチェックボックスはオフです。

- [**イベント生成しきい値**]セクション:

  - [**定義データベースがアップデートされていません(日)**]、[**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)**]、[**簡易スキャンが長期間実行されていません(日)**]の各イベントが発生するまでの日数を指定します。

表 35. イベント発生のしきい値

設定	イベント発生のしきい値。
説明	次のイベント種別の発生に対して、しきい値を指定できます: [**定義データベースがアップデートされていません(日)**]および[**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)**]:定義データベースの前回インストールしたアップデートの公開日から、設定で指定されている期間(日数)に定義データベースがアップデートされなかった場合に発生します。このイベントに関する管理者への通知を設定できます。 **簡易スキャンが長期間実行されていません(日)**:このイベントは、指定した日数の間に[**タスクを簡易スキャンとする**]がオンのタスクが実行されない場合に発生します。
取りうる値	1 ～ 365 までの日数。
既定値	定義データベースがアップデートされていません(日) - 7 日 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) - 14 日 簡易スキャンが長期間実行されていません(日) - 30 日

- [**SIEM 連携**]タブで、syslog サーバーに監査イベントとタスク実行イベントを公開するための設定を行います(「SIEM 連携の設定」(217 ページ)を参照)。

3. [**OK**]をクリックして、変更内容を保存します。

このセクションの内容

SIEM 連携について

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の性能低下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実行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 連携を使用できます:

- 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実行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 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。

使用されている SIEM の設定に基づいて、イベントのフォーマットを選択してください。

信頼性設定

SIEM へのイベント送信が失敗するリスクを低下させるには、ミラー syslog サーバーへの接続設定を定義します。

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。

Kaspersky Security for Windows Server では、SIEM への接続試行の失敗およびシステム監査イベントを使用した SIEM へのイベント送信のエラーについても通知します。

SIEM 連携の設定

既定では、SIEM 連携は使用されません。SIEM 連携は、有効化や無効化、機能の設定ができます(次の表を参照)。

表 36. SIEM 連携の設定

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 連携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。
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、メインおよびミラー 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。
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 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 連携設定を編集するには:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダーの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。

   [**ログと通知の設定**]ウィンドウが開きます。
3. [**SIEM 連携**]タブを選択します。
4. [**連携の設定**]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 連携設定を使用して SIEM に送信されます。

   チェックボックスがオフの場合、SIEM 連携は実行されません。チェックボックスがオフの場合、SIEM 連携を設定できません。

   既定では、このチェックボックスはオフです。
5. 必要に応じて、[**連携の設定**]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。
6. [**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。
7. [**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、[**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。

8. [**OK**]をクリックします。

   設定済みの SIEM 連携設定が適用されます。

通知の設定

このセクションでは、Kaspersky Security for Windows Server のユーザーと管理者に対して本製品のイベントとサーバーの保護ステータスを通知する方法、および通知を設定する方法について説明します。

この章の内容

管理者およびユーザーへの通知方法

保護対象のサーバーにアクセスする管理者とユーザーに対して Kaspersky Security for Windows Server の動作におけるイベントとサーバ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。

次のタスクが実行されます:

- 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、ファイルのリアルタイム保護タスクでの[**オブジェクトが検知されました**]のイベント種別の情報を受信できます。

アプリケーションコンソールで、次のさまざまな方法を使用して管理者またはユーザーへの通知を有効にできます:

- ユーザーのへ通知方法:
  a. ターミナルサービスツール

  保護対象のサーバーがターミナルとして使用されている場合、ターミナルサーバーユーザーへの通知にこの方法を適用できます。

  b. メッセージサービスツール

  Microsoft Windows メッセージサービスを使用した通知にこの方法を適用できます。この方法は、保護対象のサーバーが Microsoft Windows Server 2008 以降で動作している場合には適用できません。
- 管理者への通知方法:
  a. メッセージサービスツール

  Microsoft Windows メッセージサービスを使用した通知にこの方法を適用できます。この方法は、保護対象のサーバーが Microsoft Windows Server 2008 以降で動作している場合には適用できません。

  b. 実行ファイルの実行

  この方法では、イベントが発生したときに、保護対象のサーバーのローカルドライブに保存されている実行ファイルを実行します。

  c. メールで送信

  この方法では、メールを使用してメッセージを送信します。

個々のイベント種別用にメッセージのテキストを作成できます。イベントの説明を示す情報フィールドを含めることができます。既定では、定義済みのテキストがユーザーへの通知に使用されます。

管理者およびユーザーへの通知の設定

イベント通知の設定で、メッセージテキストの設定方法と作成方法を選択できます。

► イベント通知の設定を行うには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**ログと通知の設定**]フォルダー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。

   [**ログと通知の設定**]ウィンドウが開きます。

2. [**通知**]タブで、通知モードを選択します:

   a. [**イベント種別**]リストから、通知方法を選択するイベントを選択します。

   b. [**管理者への通知**]または[**ユーザーへの通知**]グループ設定で、設定する通知方法の横にあるチェックボックスをオンにします。

   > [**オブジェクトが検知されました**]イベント、[**信頼しない大容量ストレージが検出および制限されました**]イベント、[**コンピューターが信頼しないリストに追加されました**]イベントのみ、ユーザーへの通知を設定できます。

3. メッセージのテキストを追加するには:

   a. [**メッセージのテキスト**]をクリックします。

   b. 表示されたウィンドウに、対応するイベントメッセージに表示するテキストを入力します。

   > 複数のイベント種別に同じメッセージテキストを作成できます。1 つのイベント種別の通知方法を選択してから、**Ctrl** キーまたは **Shift** キーを使用して、同じメッセージテキストを使用する他のイベント種別を選択し、[**メッセージのテキスト**]をクリックします。

   c. イベントの情報が含まれるフィールドを追加するには、[**マクロ**]をクリックしてドロップダウンリストから該当するフィールドを選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。

   d. イベントメッセージの既定のテキストを復元するには、[**既定値**]をクリックします。

4. 選択したイベントの管理者通知方法を設定するには、[**通知**]タブを選択して[**管理者への通知**]セクションの[**設定**]をクリックし、[**詳細設定**]ウィンドウで通知方法を設定します。それには、次の操作を実行します:

   a. メール通知の場合、[**メール**]タブを開いて、該当するフィールドに受信者のメールアドレス(アドレスをセミコロンで区切ります)、SMTP サーバーの名前またはネットワークアドレス、およびポート番号を指定します。必要に応じて、[**件名**]と[**送信者**]に表示するテキストを指定します。[**件名**]のテキストに、イベントの情報が含まれる変数を含めることもできます(以下の表を参照)。

   SMTP サーバーへの接続時にユーザーアカウント認証を適用するには、[**認証設定**]グループの[**SMTP 認証を使用する**]を選択し、認証対象のユーザーアカウントのユーザー名とパスワードを指定します。

   b. **Windows Messenger サービス**を使用して通知するには、[**Windows Messenger サービス**]タブで通知を受信するコンピューターのリストを作成します。追加するコンピューターごとに、[**追加**]をクリックして入力フィールドにネットワークの名前を入力します。

   > Windows Messenger サービスを使用した通知は、保護対象のサーバーが Microsoft Windows Server 2008 以降のバージョンの Microsoft Windows Server で動作している場合には適用できません。

   c. 実行ファイルを実行するには、イベントによってトリガーされてサーバーで実行される、保護対象のサーバーのローカ

ルドライブ上のファイルを選択するか、[**実行ファイル**]タブに実行ファイルの絶対パスを入力します。ファイルを実行するために使用する、ユーザー名とパスワードを入力します。

実行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。

一定の期間に 1 つのイベント種別のメッセージ数を制限するには、[**詳細設定**]タブで[**同じ通知の最大送信回数**]を選択し、回数と時間単位を指定します。

5. [**OK**]をクリックします。

通知の設定内容が保存されます。

表 37. イベントの情報が含まれるフィールド

変数	説明
%EVENT_TYPE%	イベントの種別。
%EVENT_TIME%	イベントの時刻。
%EVENT_SEVERITY%	重要度
%OBJECT%	オブジェクト名（サーバーのリアルタイム保護タスクとオンデマンドスキャンタスク）。 ソフトウェアモジュールのアップデートタスクには、アップデートの名前、Web ページのアドレス、アップデートに関する情報が含まれます。
%VIRUS_NAME%	ウイルス百科事典の分類（https://encyclopedia.kaspersky.com/knowledge/classification/）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 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。タスク実行ログで検知したオブジェクトの名前を表示できます（「タスク実行ログでの Kaspersky Security for Windows Server のタスクに関する統計と情報の表示」（212 ページ）を参照）。
%VIRUS_TYPE%	「ウイルス」「トロイの木馬」など、カスペルスキーの分類に基づいた、検知されたオブジェクトの種別。この種別は、オブジェクトが感染しているまたは感染の可能性があることが検知されると Kaspersky Security 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。タスク実行ログで、検知されたオブジェクトの名前を表示できます。
%USER_COMPUTER%	ファイルのリアルタイム保護タスクと RPC ネットワークストレージの保護タスクでは、サーバー上のオブジェクトにアクセスしたユーザーのコンピューター名です。
%USER_NAME%	ファイルのリアルタイム保護タスクと RPC ネットワークストレージの保護タスクでは、サーバー上のオブジェクトにアクセスしたユーザー名です。
%FROM_COMPUTER%	通知が発行された保護対象のサーバーの名前。
%EVENT_REASON%	イベントが発生した理由（このフィールドがないイベントもあります）。
%ERROR_CODE%	エラーコード（「内部タスクエラー」イベントでのみ使用）。
%TASK_NAME%	タスク名（タスク実行に関連するイベントのみ）。

Kaspersky Security for Windows Server の開始と停止

このセクションでは、アプリケーションコンソールの起動に関する情報および Kaspersky Security サービスの開始と停止に関する情報について説明します。

この章の内容

Kaspersky Security for Windows Server 管理プラグインの起動

Kaspersky Security Center で Kaspersky Security for Windows Server 管理プラグインを起動するには、追加の操作は必要ありません。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 のヘルプ**を参照してください。

スタートメニューからの Kaspersky Security for Windows Server コンソールの起動

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。

► [スタート]メニューからアプリケーションコンソールを起動するには:

1. [**スタート**]メニューから、[**すべてのプログラム**] - [**Kaspersky Security for Windows Server**] - [**管理ツール**]- [**Kaspersky Security for Windows Server コンソール**]の順に選択します。

アプリケーションコンソールに他のスナップインを追加するには、作成者モードでアプリケーションコンソールを起動します。

► 作成者モードでアプリケーションコンソールを起動するには、次の手順を実行します:

1. [**スタート**]メニューから、[**すべてのプログラム**] - [**Kaspersky Security for Windows Server**] - [**管理ツール**]の順に選択します。
2. アプリケーションコンソールのコンテキストメニューで、[**作成者**]を選択します。

アプリケーションコンソールが作成者モードで起動します。

保護対象のサーバーでアプリケーションコンソールが起動されている場合、アプリケーションコンソールウィンドウが開きます。

保護対象サーバー以外のサーバーでアプリケーションコンソールを起動した場合は、保護対象サーバーに接続します。

► 保護対象サーバーに接続するには:

1. アプリケーション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. [**別のコンピューターに接続**]コマンドを選択します。

   [**コンピューターの選択**]ウィンドウが開きます。
3. 表示されたウィンドウで、[**別のコンピューター**]を選択します。
4. 右側にある入力フィールドで保護対象サーバーのネットワーク名を指定します。
5. [**OK**]をクリックします。

アプリケーションコンソールが、保護対象サーバーに接続されます。

Microsoft Windows のログイン用のユーザーアカウントの権限ではサーバー上の Kaspersky Security 管理サービスにアクセスできない場合は、[**次のユーザーとして接続する**]をオンにして、この権限を持つ別のユーザーアカウントを指定します。

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直後に自動で開始します。Kaspersky Security サービスは、サーバーのリアルタイム保護、サーバーコントロール、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 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)およびオペレーティングシステムの起動時のスキャン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 for Windows Server を開始および停止することができます。

► アプリケーション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. アプリケーション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。

オペレーティングシステムのセーフモードでの Kaspersky Security for Windows Server コンポーネントの起動

このセクションでは、オペレーティングシステムのセーフモードで Kaspersky Security for Windows Server を動作させる方法について説明しています。

この章の内容

オペレーティングシステムのセーフモードでの Kaspersky Security for Windows Server の動作について

オペレーティングシステムをセーフモードで読み込んだ直後に、Kaspersky Security for Windows Server のコンポーネントを起動できます。 Kaspersky Security サービス(kavfs.exe)だけでなく、klam.sys ドライバーも読み込まれます。このドライバーは、オペレーティングシステムの起動中に、Kaspersky Security サービスを保護対象サービスとして登録するために使用されます。詳しくは、「保護対象サービスとしての Kaspersky Security サービスの登録」セクションを参照してください。

Kaspersky Security for Windows Server は、オペレーティングシステムの次の種別のセーフモードで起動できます:

- セーフモード(最小限):オペレーティングシステムのセーフモードの標準のオプションを選択すると起動されます。この場合、Kaspersky Security for Windows Server は次のコンポーネントを起動できます:
  - 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とアプリケーション起動コントロールルールの自動作成
  - Windows イベントログ監視
  - ファイル変更監視
  - アプリケーションの整合性チェック
  - アンチクリプター
  - ブロック対象コンピューターの保管領域
- セーフモードとネットワーク:起動時に、オペレーティングシステムがネットワークドライバーとともに読み込まれるモードです。セーフモード(最小限)で起動されるコンポーネントに加えて、Kaspersky Security for Windows Server は次のコンポーネントを起動できます:
  - 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
- ネットワーク接続ストレージの保護

セーフモードでの Kaspersky Security for Windows Server の起動

既定では、オペレーティングシステムをセーフモードで読み込んだ後に、Kaspersky Security for Windows Server は起動されません。

► オペレーティングシステムのセーフモードで Kaspersky Security for Windows Server を起動するように設定するには、次の操作を実行します:

1. Windows レジストリエディター(C:\Windows\regedit.exe)を起動します。
2. システムレジストリの [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] キーを開きます。
3. 「LoadInSafeMode」パラメータを開きます。
4. 値として「1」を指定します。
5. [**OK**]をクリックします。

► オペレーティングシステムのセーフモードで Kaspersky Security for Windows Server を起動する設定を取り消すには、次の操作を実行します:

1. Windows レジストリエディター(C:\Windows\regedit.exe)を起動します。
2. システムレジストリの [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] キーを開きます。
3. 「LoadInSafeMode」パラメータを開きます。
4. 値として「0」を指定します。
5. [**OK**]をクリックします。

Kaspersky Security for Windows Server のセルフディフェンス機構

このセクションでは、Kaspersky Security for Windows Server のセルフディフェンス機構について説明します。

この章の内容

Kaspersky Security for Windows Server のセルフディフェンス機構について

Kaspersky Security for Windows Server にはセルフディフェンス機構が組み込まれており、本製品のハードディスク上のフォルダーおよび本製品のメモリプロセスとシステムレジストリエントリを改変や削除から保護します。

Kaspersky Security for Windows Server のコンポーネントがインストールされているフォルダーの改変防止

Kaspersky Security for Windows Server では、コンポーネントがインストールされているフォルダーの名前変更と削除は、ユーザーアカウントに対しては許可されません。既定のインストールフォルダーはそれぞれ次のようになります:

- 32 ビット版の Microsoft Windows:%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\
- 64 ビット版の Microsoft Windows:%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\

Kaspersky Security for Windows Server のレジストリキーの改変防止

Kaspersky Security for Windows Server では、本製品のドライバーとサービスの読み込みを行う次のレジストリブランチとレジストリキーへのアクセス権が制限されます。

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump]（64 ビット版の Microsoft Windows 製品の場合）
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Trace]（64 ビット版の Microsoft Windows 製品の場合）

これらのレジストリブランチとレジストリキーの変更権限は、ローカルシステム（SYSTEM）アカウントにのみ付与されます。ユーザーアカウントと管理者アカウントには読み取り権限が付与されます。

保護対象サービスとしての Kaspersky Security サービスの登録

Protected Process Light（または「PPL」とも表記）技術により、オペレーティングシステムが信頼するサービスとプロセスのみを読み込みます。サービスを保護対象サービスとして実行するには、**起動時マルウェア対策**ドライバーを保護対象サーバーにインストールする必要があります。

起動時マルウェア対策（または「ELAM」とも表記）ドライバーは、ネットワーク上のサーバーが起動すると保護を開始し、他のサードパーティ製ドライバーが起動する前の保護を提供します。

Kaspersky Security for Windows Server のインストール中に ELAM ドライバーが自動的にインストールされ、オペレーティングシステムの起動時に Kaspersky Security サービスを PPL として登録するために使用されます。Kaspersky Security Service（KAVFS）がシステムの保護対象プロセスとして起動される場合、システム上のその他の保護されていないプロセスはスレッドの注入、保護対象プロセスの仮想メモリへの書き込み、またはサービスの停止を行うことはできません。

PPL として開始されたプロセスは、ユーザーの持つ権限に関係なく、ユーザーが管理することはできません。ELAM ドライバーを使用した Kaspersky Security Service の PPL としての登録は、Microsoft Windows Server 2016 以降のオペレーティングシステムでサポートされます。Kaspersky Security for Windows Server を、PPL をサポートするオペレーティングシステムのサーバーにインストールする場合、Kaspersky Security サービス（KAVFS）の権限の管理は使用できません。

► **Kaspersky Security を PPL として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_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

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

このセクションでは、Kaspersky Security 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 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 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 グループに、Kaspersky Security 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 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 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 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、アプリケーション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 for Windows Server の全般的な設定、コンポーネントの設定、および Kaspersky Security for Windows Server ユーザーの権限を表示および編集でき、さらに Kaspersky Security 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製品の機能へのアクセス。Kaspersky Security for Windows Server の全般的な設定と、Kaspersky Security for Windows Server コンポーネントの設定を表示および編集できます。
- **読み取り** - Kaspersky Security for Windows Server の全般的な設定、Kaspersky Security for Windows Server コンポーネントの設定、Kaspersky Security for Windows Server の統計情報、Kaspersky Security for Windows Server ユーザーの権限を表示できます。

また、詳細なアクセス権限を設定して、Kaspersky Security for Windows Server の特定の機能へのアクセスを許可したりブロックしたり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[**特殊なアクセス許可**]のアクセス

レベルが設定されます。

表 38. Kaspersky Security 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 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 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 for Windows Server 全般的な設定とタスクの設定の表示。 • Kaspersky Security for Windows Server 設定の設定ファイルへのエクスポート。 • 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 for Windows Server タスクの統計情報を表示できます。
ライセンス	Kaspersky Security for Windows Server のアクティベーションを実行できます。
アプリケーションのアンインストール	Kaspersky Security 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 for Windows Server ユーザーとユーザーごとのアクセス権限のリストを表示できます。
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 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。

登録されたサービスを管理するための権限について

登録された Windows サービスおよび登録されたサービスへのアクセスの設定方法の詳細については、『**Kaspersky Security for Windows Server 管理者用ガイド**』を参照してください。

Kaspersky Security for Windows Server では、インストール時に Kaspersky Security サービス(KAVFS)、Kaspersky Security 管理サービス(KAVFSGT)、および Kaspersky Security 脆弱性攻撃ブロック(KAVFSSLP)が登録されます。

ELAM ドライバーを使用した Kaspersky Security サービスの Protected Process Light(PPL)としての登録は、Microsoft Windows 10 以降のオペレーティングシステムでサポートされます。PPL として開始されたプロセスは、ユーザーの持つ権限に関係なく、ユーザーが管理することはできません。Kaspersky Security for Windows Server を、PPL をサポートするオペレーティングシステムのコンピューターにインストールする場合、Kaspersky Security サービス(KAVFS)の権限の管理は使用できません。

Kaspersky Security サービス

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。

[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(「Kaspersky Security for Windows Server 機能へのパスワードで保護されたアクセス」(238 ページ)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 管理サービス

別のサーバーにインストールされたアプリケーションコンソールから本製品を管理するには、Kaspersky Security 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 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 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 サービスを管理するための権限について

Kaspersky Security 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、ローカルのアプリケーションコンソールや管理プラグインから 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(232 ページのセクション「Kaspersky Security 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 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 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 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[**特殊なアクセス許可**]のアクセスレベルが設定されます。

表 39. Kaspersky Security 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 for Windows Server サービスのリストを確認できます。

Kaspersky Security for Windows Server はインストール時に Kaspersky Security 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アプリケーションコンソールから本製品を管理するには、Kaspersky Security for Windows Server への接続に使用されるアカウントが、保護対象サーバーの Kaspersky Security 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 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 for Windows Server の設定では、Kaspersky Security 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。

ユーザー名とパスワードがローカルアカウントと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 for Windows Server に接続できます。

Kaspersky Security 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 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. アプリケーション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表示して、次のいずれかを行います:
   - Kaspersky Security 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のユーザー権限の変更**]をクリックします。
   - Kaspersky Security サービス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 サービス管理のユーザー権限の変更**]をクリックします。

     [**Kaspersky Security のアクセス許可**]ウィンドウが開きます。
2. 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、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。
3. [**OK**]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 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. アプリケーション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表示して、次のいずれかを行います:
   - Kaspersky Security for Windows Server の機能に対するアクセス権限を設定する場合は、[**アプリケーション管理のユーザー権限の変更**]をクリックします。
   - Kaspersky Security サービスに対するアクセス権限を設定する場合は、[**Kaspersky Security サービス管理のユーザー権限の変更**]をクリックします。

     [**Kaspersky Security のアクセス許可**]ウィンドウが開きます。
2. 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。
3. 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:
   - Kaspersky Security 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のユーザー権限の変更**]サブセクションにある[**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 サービス管理のユーザー権限の変更**]サブセクションにある[**設定**]をクリックします。

     [**Kaspersky Security 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 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 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 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:[**サービス設定の変更**]、[**読み取り権限**]。
- **特殊なアクセス許可**:次の権限で Kaspersky Security サービスを管理します:[**サービスの開始**]、[**サービスの停止**]、[**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を設定するには(**特殊なアクセス許可**)、[**詳細設定**]をクリックします。
   a. 表示された[**Kaspersky Security のセキュリティの詳細設定**]ウィンドウで、目的の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. 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**])。
   d. 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。
   e. [**OK**]をクリックします。
   f. [**Kaspersky Security 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 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 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 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(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」を参照)。Kaspersky Security for Windows Server 設定でパスワードによる保護を設定して、高度な保護を実行することもできます。パスワードによる保護を使用すると、アプリケーションコンソールの管理へのアクセスと、コマンドラインからのコマンドの実行に対する制限を追加できます。パスワードによる保護が適用されると、アプリケーションコンソールの起動時と、コマンドラインからのコマンドの実行時に、Kaspersky Security for Windows Server がすべてのユーザーに対してパスワードの入力を要求するようになります。

► Kaspersky Security for Windows Server 機能へのアクセスを保護するには:

1. アプリケーションコンソールツリーで、[**Kaspersky Security**]フォルダーを選択して、次のいずれかを行います:
   - フォルダーの詳細ペインにある[**アプリケーションのプロパティ**]をクリックする。
   - フォルダーのコンテキストメニューで[**プロパティ**]を選択する。

   [**アプリケーションの設定**]ウィンドウが表示されます。
2. [**セキュリティと信頼性**]タブの[**パスワードによる保護の設定**]で、[**パスワードによる保護を適用する**]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。
3. [**パスワード**]で、Kaspersky Security 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。
4. [**パスワードの確認**]にもう一度パスワードを入力します。
5. [**OK**]をクリックします。

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。

パスワードはいつでもリセットできます。リセットするには[**パスワードによる保護を適用する**]をオフにして、変更内容を保存します。パスワードによる保護が無効になり、古いパスワードのチェックサムが削除されます。新しいパスワードを使用して、パスワード入力プロセスを繰り返します。

Kaspersky Security Center でのアクセス権限の設定

Kaspersky Security Center で、サーバーグループまたは個別のサーバーに対して、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。

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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 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、[**Kaspersky 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。
5. 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(232 ページのセクション「Kaspersky Security for Windows Server の各種機能に対するアクセス権限の管理」を参照)。

指定された設定が保存されます。

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。

この章の内容

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 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トリーム(NTFS ストリーム)
- 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 と Windows Server 2019 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 for Windows Server によってそのファイル操作の情報が取得され、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。駆除または削除の前には、ソースファイルの暗号化されたコピーがバックアップに保存されます。感染していない場合、または正常に駆除された場合、Kaspersky Security for Windows Server から元のフォルダーにファイルが戻されます。

Kaspersky Security for Windows Server は、Windows Server 2016 および Windows Server 2019 のコンテナーで実行されるファイル操作を監視します。

コンテナーは、隔離された環境で、オペレーティングシステムから直接やりとりをすることなくアプリケーションを実行できます。コンテナーがタスクの保護範囲内にある場合、Kaspersky Security 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 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。

タスクの保護範囲とセキュリティ設定について

既定では、ファイルのリアルタイム保護タスクはサーバーのファイルシステムのすべてのオブジェクトを保護します。セキュリティ要件でファイルシステムのオブジェクトすべてを保護することまでは求められていない場合、またはタスク範囲から一部のオブジェクトを除外する場合は、保護範囲を制限できます。

アプリケーションコンソールでは、保護範囲は、Kaspersky Security for Windows Server が操作できるサーバーのファイルリソースのツリーまたはリストとして表示されます。既定では、保護対象サーバーのネットワークファイルリソースがリストビューモードで表示されます。

リストビューは管理プラグインでのみ使用できます。

► ネットワークファイルリソースをアプリケーションコンソールのツリービューモードで表示するには:

[**保護範囲の設定**]ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。

次のように、サーバーファイルリソースのリストビューまたはツリービューモードで項目またはフォルダーが表示されます:

☑ フォルダーが保護範囲に含まれています。

☐ フォルダーが保護範囲から除外されています。

 このフォルダーの 1 つ以上のサブフォルダーが保護範囲から除外されます。または、このサブフォルダーと親フォルダーのセキュリティ設定が異なります(ツリービューモードの場合のみ)。

 アイコンは、親フォルダーを除くすべてのサブフォルダーが選択されている場合に表示されます。この場合、親フォルダーのファイルとフォルダーの構成の変更は、選択したサブフォルダーの保護範囲の作成中は自動的に無視されます。

アプリケーションコンソールを使用して、[仮想ドライブ]を保護範囲に追加することもできます(267 ページのセクション「仮想保護範囲の作成」を参照)。仮想フォルダーの名前は、青色のフォントで表示されます。

セキュリティ設定

タスクのセキュリティ設定は、保護範囲に含まれるすべてのフォルダーや項目の共通の設定として、あるいはサーバーのファイルリソースツリーまたはリストのフォルダーや項目ごとに異なる設定として、設定することができます。

選択した親フォルダーに対するセキュリティ設定は、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。

選択した保護範囲の設定は、次のいずれかの方法で行います:

- 3 つの定義済みセキュリティレベルのいずれかを選択する(242 ページ)。
- ファイルリソースツリーまたはリストで選択したフォルダーや項目に対してセキュリティ設定を手動で行う(セキュリティレベルが[**カスタム**]に変更されます)(254 ページのセクション「手動でのセキュリティの設定」を参照)。

フォルダーや項目の一連の設定をテンプレートに保存して、あとで他のフォルダーや項目に適用することができます。

仮想保護範囲について

Kaspersky Security for Windows Server では、ハードディスクとリムーバブルドライブ上の既存のフォルダーとファイルだけでなく、さまざまなアプリケーションやサービスによってサーバー上に動的に作成された共有のクラスタードライブなどの、サーバーに一時的に接続さ

れているドライブもスキャンすることができます。

保護範囲にすべてのサーバーオブジェクトが含まれている場合、これらのダイナミックフォルダーも自動的に保護範囲に含まれます。ただし、これらのダイナミックフォルダーのセキュリティ設定に特定の値を指定する場合、または保護の対象としてサーバー全体ではなく個別の領域を選択したあとで、ダイナミックドライブ、フォルダー、またはファイルを保護範囲に追加する場合は、最初にそれらをアプリケーションコンソールで作成する(つまり、仮想保護範囲を指定する)必要があります。作成されたドライブ、ファイル、およびフォルダーはアプリケーションコンソールにのみ存在します。保護対象のサーバーのファイル構造内には存在しません。

保護範囲の作成中に、親フォルダーを選択せずにすべてのサブフォルダーまたはファイルを選択した場合は、そこに表示されるすべてのダイナミックフォルダーまたはファイルが自動的に保護範囲に含まれることはありません。これらの「仮想コピー」をアプリケーションコンソールで作成し、保護範囲に追加する必要があります。

定義済みの保護範囲

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 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 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、範囲リストで、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、アプリケーション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リスト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。

定義済みのセキュリティレベル

コンピューターのファイルリソースツリーまたは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)。

最高のパフォーマンス

サーバーおよびワークステーションでの Kaspersky Security for Windows Server の使用に加えて、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（ファイアウォールや既存のセキュリティポリシーなど）を適用している場合、[**最高のパフォーマンス**]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、保護レベルと保護対象のサーバーのパフォーマンスへの影響とのバランスが最適化されます。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で高い水準のコンピューターセキュリティ要件が求められる場合、[**最大の保護**]セキュリティレベルを推奨します。

表 40. 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		
	最高のパフォーマンス	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
感染などの問題がある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
スキャン時間が次を超えたら停止する（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	有効	有効	有効
ディスクのブートセクターと MBR をスキャン	有効	有効	有効
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

オプション	セキュリティレベル		
埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する	無効	無効	有効

[**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。

ファイルのリアルタイム保護タスクで既定でスキャンされるファイルの拡張子

Kaspersky Security for Windows Server で、既定でスキャンされるファイルの拡張子は、次のとおりです:

- **386**
- **acm**
- **ade、adp**
- **asp**
- **asx**
- **ax**
- **bas**
- **bat**
- **bin**
- **chm**
- **cla、clas***
- **cmd**
- **com**
- **cpl**
- **crt**
- **dll**
- **dpl**
- **drv**
- **dvb**
- **dwg**
- **efi**
- **emf**
- **eml**

- exe
- fon
- fpm
- hlp
- hta
- htm、html*
- htt
- ico
- inf
- ini
- ins
- isp
- jpg、jpe
- js、jse
- lnk
- mbx
- msc
- msg
- msi
- msp
- mst
- nws
- ocx
- oft
- otm
- pcd
- pdf
- php
- pht
- phtm*
- pif
- plg
- png
- pot
- prf
- prg
- reg
- rsc
- rtf

- scf
- scr
- sct
- shb
- shs
- sht
- shtm*
- swf
- sys
- the
- them*
- tsp
- url
- vb
- vbe
- vbs
- vxd
- wma
- wmf
- wmv
- wsc
- wsf
- wsh
- do?
- md?
- mp?
- ov?
- pp?
- vs?
- xl?

ファイルのリアルタイム保護タスクの既定の設定

既定では、ファイルのリアルタイム保護タスクでは、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 41. 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。
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 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。
信頼ゾーンを適用する	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。
保護に KSN を使用する	適用されます。	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、サーバーの保護を改善することができます(KSN に関する声明に同意している場合に利用できます)。
タスク開始スケジュール	アプリケーション開始時	タスク開始スケジュールを設定できます。
悪意のある動作を示すコンピューターのネットワーク共有リソースへのアクセスをブロックする	適用されません。	ブロック対象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。

管理プラグインからファイルのリアルタイム保護タスクを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーのタスク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

操作方法

必要なタスクの設定をインターフェイスから操作する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のポリシーの設定ウィンドウ

► Kaspersky Security Center のポリシーからファイルのリアルタイム保護タスクの設定を開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**サーバーのリアルタイム保護**]セクションを選択します。
6. [**ファイルのリアルタイム保護**]サブセクションで[**設定**]をクリックします。

   [**ファイルのリアルタイム保護**]ウィンドウが開きます。

サーバーが 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、アプリケーションコンソールでこれらの設定を編集することはできません。

ファイルのリアルタイム保護タスクのプロパティウィンドウ

► 1 つのネットワークサーバーのファイルのリアルタイム保護タスクの設定ウィンドウを開くには:

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. タスクを設定する管理グループを選択します。
3. [**デバイス**]タブを選択します。
4. 次のいずれかの方法で、サーバ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。
   - 保護対象サーバーのコンテキストメニューで[**プロパティ**]を選択します。

   サーバーのプロパティウィンドウが表示されます。
5. [**タスク**]セクションで、[**ファイルのリアルタイム保護**]タスクを選択します。
6. [**プロパティ**]をクリックします。

   ファイルのリアルタイム保護のプロパティウィンドウが開きます。

ファイルのリアルタイム保護タスクの設定

► ファイルのリアルタイム保護タスクの設定を行うには:

1. [**ファイルのリアルタイム保護**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ」を参照)。
2. 次のタスクの設定を指定します:
   - [**全般**]タブ:
     - **オブジェクトの保護モード**(250 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**
     - **他のコンポーネントとの連携**(251 ページのセクション「**ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携の設定**」を参照)
   - [**タスク管理**]タブ:
     - タスク開始スケジュール設定(139 ページの「タスク開始スケジュールの設定」を参照)。
3. [**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(265 ページのセクション「保護範囲の作成」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**
     - いずれかの定義済みのセキュリティレベルを選択するか(242 ページ)、保護設定を手動で行います(254 ページの「手動でのセキュリティの設定」を参照)。
4. [**ファイル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、システム監査ログに保存されます。

このセクションの内容

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 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:

1. [**ファイルのリアルタイム保護**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ」を参照)。
2. 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**

     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。
3. [**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。

ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携の設定

KSN の使用タスクを開始するには、Kaspersky Security Network に関する声明に同意する必要があります。

► ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携を設定するには:

1. [**ファイルのリアルタイム保護**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ」を参照)。
2. [**全般**]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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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. [**他のコンポーネントとの連携**]セクションで、次の設定を行います:
   - [**信頼ゾーンを適用する**]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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

     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。

[KSN の使用]タスクの設定で、[**スキャンしたファイルに関するデータを送信**]をオンにする必要があります。

- [**悪意のある動作を示すコンピューターのネットワーク共有リソースへのアクセスをブロックする**]をオンまたはオフにします。

5. [**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。

タスク開始スケジュールの設定

アプリケーションコンソールでは、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。

► グループ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 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. 保護対象サーバーが所属するグループを選択します。
3. 結果ペインで、[**タスク**]タブを選択します。
4. 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:
   - タスクの名前をダブルクリックする。
   - 対象のタスクのコンテキストメニューを開き、[プロパティ]を選択する。
5. [**スケジュール**]セクションを選択します。
6. [**スケジュール設定**]セクションで、[**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。

7. 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、[**間隔:<数字> 時間**]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、[**間隔:<数字> 日**]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、[**間隔:<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 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(109 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)。

8. [**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時間帯を 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。
9. [**OK**]をクリックします。
10. [**適用**]をクリックして、タスクの開始設定を保存します。

Kaspersky Security Center を使用して 1 つのタスクの設定を指定する場合、「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」セクション(129 ページ)で説明されている手順を実行します。

タスクの保護範囲の作成と編集

► Kaspersky Security Center からタスクの保護範囲を作成して編集するには:

1. [**ファイルのリアルタイム保護**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ」を参照)。
2. [**保護範囲**]タブを選択します。
3. タスクによってすでに保護されているすべての項目は、[**保護範囲**]テーブルに表示されます。
4. [**追加**]をクリックして、新しい項目をリストに追加します。
   [**保護範囲にオブジェクトを追加**]ウィンドウが開きます。
5. 保護範囲に追加するオブジェクトの種別を選択します:

- **定義済みの範囲**:いずれかの定義済み範囲をサーバーの保護範囲に含めます。ドロップダウンリストで、目的の保護範囲を選択します。
- **ディスク、フォルダー、またはネットワークの場所**:個別のドライブ、フォルダー、またはネットワークオブジェクトを保護範囲に含めます。[**参照**]をクリックして目的の保護範囲を選択します。
- **ファイル**:個別のファイルを保護範囲に含めます。[**参照**]をクリックして目的の保護範囲を選択します。

オブジェクトがすでに保護範囲からの除外対象として追加されている場合、保護範囲には追加できません。

6. 保護範囲から個別の項目を除外するには、これらの項目の名前の横にあるチェックボックスをオフにするか、次の手順を実行します:
   a. 保護範囲を右クリックして、コンテキストメニューを開きます。
   b. コンテキストメニューで、[**除外の追加**]を選択します。
   c. [**除外の追加**]ウィンドウで、保護範囲にオブジェクトを追加する手順と同様に、保護範囲からの除外対象として追加するオブジェクトの種別を選択します。
7. 保護範囲または追加する除外対象を変更するには、該当する保護範囲のコンテキストメニューで[**範囲の編集**]を選択します。
8. ネットワークファイルリソースのリストに以前追加した保護範囲または除外対象を非表示にするには、該当する保護範囲のコンテキストメニューで[**範囲の削除**]を選択します。

保護範囲がネットワークファイルリソースリストから削除されたときに、ファイルのリアルタイム保護タスクの範囲から除外されます。

9. [**保存**]をクリックします。

保護範囲の設定ウィンドウが閉じます。新しい設定が保存されます。

ファイルのリアルタイム保護タスクは、コンピューターのファイルリソースツリーのフォルダーが 1 つ以上保護範囲に含まれている場合に開始できます。

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、定義済みセキュリティレベルの[**推奨**]に対応します(242 ページのセクション「定義済みのセキュリティレベル」を参照)。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはサーバーのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定することができます。

► 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:

1. [**ファイルのリアルタイム保護**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ」を参照)。
2. [**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。
3. [**セキュリティレベル**]タブで、[**設定**]をクリックしてカスタム設定を行えます。
4. 要件に従って、選択したフォルダーのカスタムのセキュリティ設定を行えます:

- 全般設定（255 ページのセクション「タスクの全般的な設定」を参照）
- 処理（257 ページのセクション「処理の設定」を参照）
- パフォーマンス（259 ページのセクション「パフォーマンスの設定」を参照）

5. [**ファイルのリアルタイム保護**]ウィンドウで[**OK**]をクリックします。

新しい保護範囲の設定が保存されます。

このセクションの内容

タスクの全般的な設定

► ファイルのリアルタイム保護タスクのセキュリティの全般設定を行うには：

1. [**ファイルのリアルタイム保護の設定**]ウィンドウを開きます（248 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のポリシーの設定ウィンドウ」を参照）。
2. [**全般**]タブを選択します。
3. [**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の種別を指定します：
   - **すべてのオブジェクト**

     すべてのオブジェクトがスキャンされます。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **指定の拡張子リストによってオブジェクトをスキャン**

     ファイル拡張子に基づいて、ファイルがスキャンされます。拡張子のリストは、[**編集**]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**

     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、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トリームをスキャンします。

このチェックボックスをオンにすると、感染の可能性があるオブジェクトと、そのオブジェクトに関連するすべての NTFS ストリーム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、検知され、感染の可能性があると判断されたオブジェクトのみ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。

4. [**パフォーマンス**]セクションで、[**作成または変更されたファイルのみを保護**]をオンまたはオフにします。

   このチェックボックスでは、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、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、スキャンおよび保護する対象を、新規ファイルまたはすべてのファイル(変更されたかどうかを問わず)のいずれかから選択できます。

   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**]と[**推奨**]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。

> チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の[**すべての / 新しい(～のみ)**]をクリックします。

5. [**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:

   - **すべてのアーカイブ / 新しいアーカイブのみ / 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、アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護レベルによって異なります。

   - **すべての SFX アーカイブ / 新しい SFX アーカイブのみ / 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、SFX アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護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。

   - **すべてのメールデータベース / 新しいメールデータベースのみ / メールデータベース**

     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、メールデータベースファイルがスキャン時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。

   - **すべての圧縮されたオブジェクト / 新しい圧縮されたオブジェクトのみ / 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ファイルが、スキャン時にスキップされま

す。

既定値は、選択した保護レベルによって異なります。

- **すべての通常のメール / 新しい通常のメールのみ / 通常のメール**

  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、メール形式のファイルがスキャン時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 / 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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

6. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

処理の設定

► ファイルのリアルタイム保護タスクで、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の処理を設定するには:

1. [**ファイルのリアルタイム保護の設定**]ウィンドウを開きます(248 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のポリシーの設定ウィンドウ**」を参照)。
2. [**処理**]タブを選択します。
3. 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:

   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。

   - **アクセスをブロック**

     このオプションを選択すると、検知され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へのアクセスがブロックされます。ドロップダウンリストで、ブロックされたオブジェクトに対する追加の処理を選択できます。

   - **その他の処理を実行**

     ドロップダウンリストから処理を選択します:

- **駆除**
- **駆除、駆除できない場合は削除**
- **削除**
- **推奨**

4. 感染の可能性があるオブジェクトの処理を選択します:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **アクセスをブロック**

     このオプションを選択すると、検知され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へのアクセスがブロックされます。ドロップダウンリストで、ブロックされたオブジェクトに対する追加の処理を選択できます。
   - **その他の処理を実行**

     ドロップダウンリストから処理を選択します:
     - **隔離**
     - **削除**
     - **推奨**
5. 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:
   a. [**検知したオブジェクトの種別に応じて処理を実行**]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、チェックボックスの横にある[**設定**]をクリックして、検知したオブジェクトの種別ごとに最初の処理と 2 番目の処理を独立して設定できます。この場合、選択したオプションに関わらず、感染したオブジェクトを開いたり実行することは許可されません。

      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種別ごとに[**感染などの問題があるオブジェクトの処理**]および[**感染の可能性があるオブジェクトの処理**]セクションで選択された処理が実行されます。

      既定では、このチェックボックスはオフです。

   b. [**設定**]をクリックします。

   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理(最初の処理が失敗した場合)を選択します。

   d. [**OK**]をクリックします。
6. 修正できない複合ファイルに対して実行する処理を選択します:[**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**]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、感染の可能性がある子オブジェクト、またはその他の検知された埋め込み子オブジェクトが検知された場合に、その親の複合ファイルの強制削除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していて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、悪意のあるオブジェクト、またはその他の埋め込みオブジェクトが検知されたときに、親の複合オブジェクト全体が強制的に削除されます。親ファイルおよびそこに含まれるすべてのコンテンツの強制削除は、検知された子オブジェクトを単独で削除できない場合に発

生します（たとえば親オブジェクトを修正できない場合）。

このチェックボックスをオフにしていて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、親オブジェクトを修正できないときは選択した処理は実行されません。

7. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

パフォーマンスの設定

► ファイルのリアルタイム保護タスクのパフォーマンスを設定するには：

1. [**ファイルのリアルタイム保護の設定**]ウィンドウを開きます（248 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のポリシーの設定ウィンドウ**」を参照）。
2. [**パフォーマンス**]タブを選択します。
3. [**除外リスト**]セクション：
   - [**除外するファイル**]をオフまたはオンにします。

     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、指定したオブジェクトがスキャン時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、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**]をオフまたはオンにします。

     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（https://encyclopedia.kaspersky.com/knowledge/classification/）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、指定した検知可能なオブジェクトがスキャン時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、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。
   - 除外リストを追加する設定ごとに[**編集**]をクリックします。
4. [**詳細設定**]セクション：
   - **スキャン時間が次を超えたら停止する（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、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。
   - **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、スキャン時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。

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。

- **iSwift テクノロジーを使用する**

  iSwift は、データベースに保管されている NTFS 識別子と、現在の識別子を比較します。スキャンは、識別子が変更されたファイル(新規ファイルと、最後に実行した NTFS システムオブジェクトのスキャン以降に変更されたファイル)に対してのみ実行されます。

  このチェックボックスをオンにすると、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、ネットワークフォルダーのファイル以外では、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 ファイルシステム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ンです。

- **iChecker テクノロジーを使用する**

  iChecker は、スキャンしたファイルのチェックサムを計算し、記憶します。オブジェクトが変更されると、チェックサムも変更されます。スキャンタスク中に、すべてのチェックサムが比較され、最後に実行したファイルスキャン以降に新規作成または更新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ンにすると、新規作成または更新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、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。

アプリケーションコンソールからファイルのリアルタイム保護タスクを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのタスクの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

ファイルのリアルタイム保護の範囲の設定ウィンドウ

► **ファイルのリアルタイム保護タスクの保護範囲の設定ウィンドウを開くには:**

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**ファイルのリアルタイム保護**]サブフォルダーを選択します。
3. 詳細ペインで[**保護範囲の設定**]をクリックします。

   [**保護範囲の設定**]ウィンドウが開きます。

ファイルのリアルタイム保護タスクの設定ウィンドウ

► **タスクの全般的な設定のウィンドウを開くには:**

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**ファイルのリアルタイム保護**]サブフォルダーを選択します。
3. 詳細ペインで[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。

ファイルのリアルタイム保護タスクの設定

► **ファイルのリアルタイム保護タスクの設定を行うには:**

1. [**タスクの設定**]ウィンドウを開きます(261 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の設定ウィンドウ」を参照)。
2. [**全般**]タブで、次のタスク設定を行います:
   - **オブジェクトの保護モード**(262 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**
   - **他のコンポーネントとの連携**(263 ページのセクション「**ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携の設定**」を参照)
3. [**スケジュール**]タブおよび[**詳細設定**]タブで、開始スケジュールを設定します(156 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)。
4. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

   変更された設定が保存されます。
5. [**ファイルのリアルタイム保護**]フォルダーの詳細ペインで、[**保護範囲の設定**]をクリックします。
6. 次の操作を行います:
   - サーバーのファイルリソースのツリーまたはリストで、タスクの保護範囲に含めるフォルダーや項目を選択します。
   - いずれかの定義済みのセキュリティレベルを選択するか、オブジェクトの保護設定を手動で行います(470 ページのセクション「手動でのセキュリティの設定」を参照)。
7. [**保護範囲の設定**]ウィンドウで、[**保存**]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、システム監査ログに保存されます。

このセクションの内容

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 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. [**タスクの設定**]ウィンドウを開きます(261 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の設定ウィンドウ」を参照)。
2. 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**

     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。
3. [**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。

ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携の設定

KSN の使用タスクを開始するには、Kaspersky Security Network に関する声明に同意する必要があります。

► ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携を設定するには:

1. [**タスクの設定**]ウィンドウを開きます(261 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の設定ウィンドウ**」を参照)。
2. [**全般**]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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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. [**他のコンポーネントとの連携**]セクションで、次の設定を行います:
   - [**信頼ゾーンを適用する**]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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

     既定では、このチェックボックスはオンです。

     [**信頼ゾーン**]をクリックして、信頼ゾーンの設定を開きます。
   - [**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。

[KSN の使用]タスクの設定で、[**スキャンしたファイルに関するデータを送信**]をオンにする必要があります。

- [**悪意のある動作を示すコンピューターのネットワーク共有リソースへのアクセスをブロックする**]をオンまたはオフにします。

5. [**OK**]をクリックします。

新しい設定が適用されます。

タスク開始スケジュールの設定

アプリケーションコンソールでは、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。

► タスク開始スケジュールを設定するには:

1. 開始スケジュールを設定するタスクの上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。

   [**タスクの設定**]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、[**スケジュールに従って実行する**]をオンにします。
4. 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**]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、[**間隔:<数字> 時間**]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、[**間隔:<数字> 日**]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、[**間隔:<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 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。

   スケジュールに従ったシステムタスクの開始が Kaspersky Security Center ポリシーの設定によって指定された場合、[**次回開始**]に[**ポリシーによりブロック**]と表示されます。
5. [**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時間帯を 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。

6. [**OK**]をクリックします。

設定されたタスクの開始設定が保存されます。

保護範囲の作成

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

保護範囲の作成

ファイルのリアルタイム保護のタスク範囲を作成する手順は、ネットワークファイルリソースのビューモードに応じて異なります(「タスクの保護範囲とセキュリティ設定について」(241 ページ)を参照)。ネットワークファイルリソースのビューモードは、ツリーまたはリスト(既定の設定)として設定できます。

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。

► ネットワークファイルリソースツリーを使用して保護範囲を作成するには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. ウィンドウの左側のセクションでネットワークファイルリソースツリーを開き、すべてのフォルダーとサブフォルダーを表示します。
3. 次の操作を行います:
   - 保護範囲から個別のフォルダーを除外するには、除外したいフォルダーの名前の横にあるチェックボックスをオフにします。

- 個別のフォルダーを保護範囲に含めるには、[**マイコンピューター**]をオフにして、次の操作を行います:
  - 同じ種別のすべてのドライブを保護範囲に含める場合は、対象のディスク種別の名前の横にあるチェックボックスをオンにします。たとえば、サーバー上のすべてのリムーバブルドライブを追加する場合は、[**リムーバブルドライブ**]をオンにします。
  - 特定の種別の個々のディスクを保護範囲に含める場合は、その種別のドライブのリストを含むフォルダーを展開し、対象のドライブの名前の横にあるチェックボックスをオンにします。たとえば、リムーバブルドライブ F: を選択する場合は、[**リムーバブルドライブ**]フォルダーを展開し、ドライブ **F:** のチェックボックスをオンにします。
  - ドライブ上のフォルダーまたはファイルを 1 つのみ含める場合は、そのフォルダーまたはファイルの名前の横にあるチェックボックスをオンにします。

4. [**保存**]をクリックします。

保護範囲の設定ウィンドウが閉じます。これで新しい設定が保存されました。

► ネットワークファイルリソースリストを使用して保護範囲を作成するには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. 個別のフォルダーを保護範囲に含めるには、[**マイコンピューター**]をオフにして、次の操作を行います:
   a. 保護範囲を右クリックして、コンテキストメニューを開きます。
   b. ボタンのコンテキストメニューで、[**保護範囲の追加**]を選択します。
   c. [**保護範囲の追加**]ウィンドウでオブジェクトの種別を選択し、保護範囲に追加します:
   - **定義済みの範囲**:いずれかの定義済み範囲をサーバーの保護範囲に含めます。ドロップダウンリストで、目的の保護範囲を選択します。
   - **ディスク、フォルダー、またはネットワークの場所**:個別のドライブ、フォルダー、またはネットワークオブジェクトを保護範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。
   - **ファイル**:個別のファイルを保護範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。

   オブジェクトがすでに保護範囲からの除外対象として追加されている場合、保護範囲には追加できません。
3. 保護範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにするか、次の手順を実行します:
   a. 保護範囲を右クリックして、コンテキストメニューを開きます。
   b. コンテキストメニューで、[**除外の追加**]を選択します。
   c. [**除外の追加**]ウィンドウで、保護範囲にオブジェクトを追加する手順と同様に、保護範囲からの除外対象として追加するオブジェクトの種別を選択します。
4. 保護範囲または追加する除外対象を変更するには、該当する保護範囲のコンテキストメニューで[**範囲の編集**]を選択します。
5. ネットワークファイルリソースのリストに以前追加した保護範囲または除外対象を非表示にするには、該当する保護範囲のコンテキストメニューで[**リストから削除**]を選択します。

   保護範囲がネットワークファイルリソースリストから削除されたときに、ファイルのリアルタイム保護タスクの範囲から除外されます。
6. [**保存**]をクリックします。

保護範囲の設定ウィンドウが閉じます。これで新しい設定が保存されました。

ファイルのリアルタイム保護タスクは、コンピューターのファイルリソースツリーのフォルダーが 1 つ以上保護範囲に含まれている場合に開始できます。

複雑な保護範囲が指定されている場合（たとえば、サーバーのファイルリソースツリーで複数のフォルダーが指定され、それらのセキュリティ設定の値が異なる場合）、オブジェクトがアクセスされたときのスキャン速度が低下する場合があります。

仮想保護範囲の作成

ファイルリソースのツリーとして保護範囲またはスキャン範囲が表示されている場合に限り、個別の仮想ドライブ、フォルダー、またはファイルを追加して、保護範囲またはスキャン範囲を拡張することができます（「ネットワークファイルリソースのビューモードの設定」（467 ページ）を参照）。

► 仮想ドライブを保護範囲に追加するには：

1. [**保護範囲の設定**]ウィンドウを開きます（261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照）。
2. ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。
3. [**仮想ドライブ**]のコンテキストメニューを開きます。
4. [**仮想ドライブの追加**]オプションを選択します。
5. 選択可能な名前のリストから、作成中の仮想ドライブの名前を選択します。
6. 追加するドライブの横のチェックボックスをオンにすると、そのドライブが保護範囲に追加されます。
7. [**保護範囲の設定**]ウィンドウで、[**保存**]をクリックします。

これで新しい設定が保存されました。

► 仮想フォルダーまたは仮想ファイルを保護範囲に追加するには：

1. [**保護範囲の設定**]ウィンドウを開きます（261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照）。
2. ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。
3. フォルダーまたはファイルを追加する仮想ドライブのコンテキストメニューを開き、次のいずれかを選択します：
   - **仮想フォルダーの追加**：保護範囲に仮想フォルダーを追加する場合に選択します。
   - **仮想ファイルの追加**：保護範囲に仮想ファイルを追加する場合に選択します。
4. 入力フィールドに、フォルダーまたはファイルの名前を指定します。
5. 作成されたフォルダーまたはファイルの名前と同じチェックボックスをオンにして、このフォルダーまたはファイルを保護範囲に追加します。
6. [**保護範囲の設定**]ウィンドウで、[**保存**]をクリックします。

変更されたタスクの設定が保存されます。

手動でのセキュリティの設定

サーバーのリアルタイム保護タスクでは、既定で保護範囲全体に対して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、定義済みセキュリティレベルの[**推奨**]に対応します(242 ページのセクション「定義済みのセキュリティレベル」を参照)。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはサーバーのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定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。

► 手動でセキュリティを設定するには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. ウィンドウの左側のセクションで、セキュリティ設定を行うフォルダーを選択します。

   セキュリティ設定を含む定義済みのテンプレート(「セキュリティ設定テンプレートについて」(162 ページ)を参照)は、保護範囲内の選択したフォルダーや項目に適用できます。
3. 要件に従って、選択したフォルダーや項目に必要なセキュリティを設定します:
   - **全般設定**(268 ページのセクション「**タスクの全般的な設定**」を参照)
   - **処理**(271 ページのセクション「**処理の設定**」を参照)
   - **パフォーマンス**(272 ページのセクション「**パフォーマンスの設定**」を参照)
4. [**保護範囲の設定**]ウィンドウで、[**保存**]をクリックします。

新しい保護範囲の設定が保存されます。

このセクションの内容

タスクの全般的な設定

► ファイルのリアルタイム保護タスクのセキュリティの全般設定を行うには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. [**全般**]タブを選択します。

3. [**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**

     すべてのオブジェクトがスキャンされます。

   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。

   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。

   - **指定の拡張子リストによってオブジェクトをスキャン**

     ファイル拡張子に基づいて、ファイルがスキャンされます。拡張子のリストは、[**編集**]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**

     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、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トリームをスキャンします。

     このチェックボックスをオンにすると、感染の可能性があるオブジェクトと、そのオブジェクトに関連するすべての NTFS ストリーム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、検知され、感染の可能性があると判断されたオブジェクトのみ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。

4. [**パフォーマンス**]セクションで、[**作成または変更されたファイルのみを保護**]をオンまたはオフにします。

   このチェックボックスでは、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、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、スキャンおよび保護する対象を、新規ファイルまたはすべてのファイル(変更されたかどうかを問わず)のいずれかから選択できます。

   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**]と[**推奨**]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。

   > チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の[**すべての / 新しい(～のみ)**]をクリックします。

5. [**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:

   - **すべてのアーカイブ / 新しいアーカイブのみ / 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、アーカイブがスキャン時にスキップされます。

既定値は、選択した保護レベルによって異なります。

- **すべての SFX アーカイブ / 新しい SFX アーカイブのみ / 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、SFX アーカイブがスキャン時にスキップされます。

  既定値は、選択した保護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。

- **すべてのメールデータベース / 新しいメールデータベースのみ / メールデータベース**

  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、メールデータベースファイルがスキャン時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。

- **すべての圧縮されたオブジェクト / 新しい圧縮されたオブジェクトのみ / 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ファイルが、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

- **すべての通常のメール / 新しい通常のメールのみ / 通常のメール**

  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、メール形式のファイルがスキャン時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 / 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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

6. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

処理の設定

► ファイルのリアルタイム保護タスクで、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の処理を設定するには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. [**処理**]タブを選択します。
3. 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:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **アクセスをブロック**

     このオプションを選択すると、検知され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へのアクセスがブロックされます。ドロップダウンリストで、ブロックされたオブジェクトに対する追加の処理を選択できます。
   - **その他の処理を実行**

     ドロップダウンリストから処理を選択します:
     - **駆除**
     - **駆除、駆除できない場合は削除**
     - **削除**
     - **推奨**
4. 感染の可能性があるオブジェクトの処理を選択します:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **アクセスをブロック**

     このオプションを選択すると、検知され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へのアクセスがブロックされます。ドロップダウンリストで、ブロックされたオブジェクトに対する追加の処理を選択できます。
   - **その他の処理を実行**

     ドロップダウンリストから処理を選択します:

- **隔離**
- **削除**
- **推奨**

5. 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:

   a. [**検知したオブジェクトの種別に応じて処理を実行**]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、チェックボックスの横にある[**設定**]をクリックして、検知したオブジェクトの種別ごとに最初の処理と 2 番目の処理を独立して設定できます。この場合、選択したオプションに関わらず、感染したオブジェクトを開いたり実行することは許可されません。

      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種別ごとに[**感染などの問題があるオブジェクトの処理**]および[**感染の可能性があるオブジェクトの処理**]セクションで選択された処理が実行されます。

      既定では、このチェックボックスはオフです。

   b. [**設定**]をクリックします。

   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理(最初の処理が失敗した場合)を選択します。

   d. [**OK**]をクリックします。

6. 修正できない複合ファイルに対して実行する処理を選択します:[**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**]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、感染の可能性がある子オブジェクト、またはその他の検知された埋め込み子オブジェクトが検知された場合に、その親の複合ファイルの強制削除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していて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、悪意のあるオブジェクト、またはその他の埋め込みオブジェクトが検知されたときに、親の複合オブジェクト全体が強制的に削除されます。親ファイルおよびそこに含まれるすべてのコンテンツの強制削除は、検知された子オブジェクトを単独で削除できない場合に発生します(たとえば親オブジェクトを修正できない場合)。

   このチェックボックスをオフにしていて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、親オブジェクトを修正できないときは選択した処理は実行されません。

7. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

パフォーマンスの設定

► ファイルのリアルタイム保護タスクのパフォーマンスを設定するには:

1. [**保護範囲の設定**]ウィンドウを開きます(261 ページのセクション「ファイルのリアルタイム保護の範囲の設定ウィンドウ」を参照)。
2. [**パフォーマンス**]タブを選択します。
3. [**除外リスト**]セクション:
   - [**除外するファイル**]をオフまたはオンにします。

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、指定したオブジェクトがスキャン時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、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**]をオフまたはオンにします。

  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（https://encyclopedia.kaspersky.com/knowledge/classification/）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、指定した検知可能なオブジェクトがスキャン時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、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。

- 除外リストを追加する設定ごとに[**編集**]をクリックします。

4. [**詳細設定**]セクション：

   - **スキャン時間が次を超えたら停止する（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、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。

   - **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、スキャン時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。

     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。

   - **iSwift テクノロジーを使用する**

     iSwift は、データベースに保管されている NTFS 識別子と、現在の識別子を比較します。スキャンは、識別子が変更されたファイル（新規ファイルと、最後に実行した NTFS システムオブジェクトのスキャン以降に変更されたファイル）に対してのみ実行されます。

     このチェックボックスをオンにすると、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、ネットワークフォルダーのファイル以外では、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 ファイルシステム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ンです。

   - **iChecker テクノロジーを使用する**

     iChecker は、スキャンしたファイルのチェックサムを計算し、記憶します。オブジェクトが変更されると、チェックサムも変更されます。スキャンタスク中に、すべてのチェックサムが比較され、最後に実行したファイルスキャン以降に新規作成または更新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ンにすると、新規作成または更新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、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。

ファイルのリアルタイム保護タスクの統計情報

ファイルのリアルタイム保護タスクの実行中は、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数の詳細をリアルタイムで表示できます。

► ファイルのリアルタイム保護タスクの統計情報を表示するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**ファイルのリアルタイム保護**]サブフォルダーを選択します。

選択したフォルダーの詳細ペインにある[**統計情報**]セクションに、タスクの統計情報が表示されます。

タスクが開始されてから現在までに、Kaspersky Security for Windows Server によって処理されたオブジェクトに関する情報を表示できます(次の表を参照):

表 42. ファイルのリアルタイム保護タスクの統計情報

フィールド	説明
検知	検知されたオブジェクトの数。たとえば、5 つのファイルから 1 つのマルウェアが検知された場合、このフィールドの値が 1 つ加算されます。
感染などの問題があるオブジェクトの検知	検知され、感染として分類されたオブジェクトの数、または侵入者がコンピューターや個人情報に損害を与える目的で使用する可能性がある正規のソフトウェアファイルの検知数。
感染の可能性があるオブジェクトの検知	Kaspersky Security for Windows Server が感染の可能性を検知したオブジェクトの数。
駆除されていないオブジェクト	次の理由により、駆除されなかったオブジェクトの数: • 検知したオブジェクトが、駆除できない種別である。 • 駆除中にエラーが発生した。
隔離されていないオブジェクト	隔離に移動しようとしたが、ディスク容量不足などにより移動できなかったオブジェクトの数。
削除されていないオブジェクト	削除しようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由で削除できなかったオブジェクトの数。
スキャンされていないオブジェクト	スキャンしようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由でスキャンできなかったオブジェクトの数。
バックアップされていないオブジェクト	バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存できなかったオブジェクトの数。
処理エラー	処理がエラーになったオブジェクトの数。

フィールド	説明
駆除されたオブジェクト	駆除されたオブジェクトの数。
隔離済み	隔離されたオブジェクトの数。
バックアップ済み	バックアップに保存されたオブジェクトコピーの数。
削除されたオブジェクト	削除されたオブジェクトの数。
パスワードで保護されているオブジェクト	パスワードで保護されていたため、スキャンできなかったオブジェクト(アーカイブなど)の数。
破損しているオブジェクト	フォーマットが破損していたためスキップされたオブジェクトの数。
処理されたオブジェクト	処理されたオブジェクトの合計数。

ファイルのリアルタイム保護タスクの統計情報をタスク実行ログに表示するには、詳細ペインの[**管理**]セクションにある[**実行ログを開く**]をクリックします。

リアルタイム保護タスク実行ログウィンドウの[**イベント総数**]の値が 0 を超えている場合は、[**イベント**]タブのタスク実行ログに表示されるイベントを手動で処理してください。

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。

この章の内容

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 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。本製品は、PowerShell™ スクリプトや Antimalware Scan Interface(AMSI)をそなえたオペレーティングシステム上の Microsoft Office アプリケーションで実行されるスクリプトも監視対象として処理できます。危険または危険な可能性があるスクリプトの実行を許可したりブロックしたりできます。Kaspersky Security 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。**ブロック**を選択する場合、スクリプトが安全であると判明した場合にのみ、スクリプトの実行が許可されます。

Microsoft Windows Server 2016 オペレーティングシステムから、Kaspersky Security for Windows Server は Antimalware Scan Interface(AMSI)をサポートしています。AMSI を使用すると、アプリケーションとサービスを、コンピューターにインストールされたあらゆるアンチマルウェア製品と連携し、実行されたすべてのスクリプトの情報を解析のために監視してアンチマルウェア製品でスキャンすることが可能になります。

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。スクリプト監視をインストールすると、本製品が AMSI プロバイダーとして登録され、実行されたスクリプトの監視を開始します。

> AMSI 機能をサポートしていない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では、保護対象のサーバー上にインストールされた他のサードパーティ製アプリケーションとこのコンポーネントが競合する場合があります。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 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。このコンポーネントをインストールすると、既定で、Kaspersky Security for Windows Server の起動時にスクリプト監視タスクが自動的に開始されるようになります。

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 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。

AMSI 機能に関する詳細な情報は、Microsoft Windows のサイト

(https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal)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アプリケーションコンソールからの設定」(279 ページ)を参照)。

スクリプト監視タスクの既定の設定

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 43. 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。
信頼ゾーン	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の管理プラグインからの設定

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. ポリシーのプロパティウィンドウの[**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**]の[**設定**]をクリックします。
5. [**全般**]タブの[**危険なスクリプトの処理**]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。

6. [**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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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. [**信頼ゾーン**]セクションで、[**信頼ゾーンを適用する**]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、場所による除外や、信頼ゾーンの除外リストに記載された名前や名前マスクでの除外が考慮されます。

   チェックボックスをオフにすると、スクリプト監視タスクの除外リストが無視されます。

   既定では、このチェックボックスはオンです。

8. [**OK**]をクリックします。

新しい設定が適用されます。

スクリプト監視タスクのアプリケーションコンソールからの設定

► スクリプト監視タスクを設定するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**スクリプト監視**]サブフォルダーを選択します。
3. フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが開き、[**全般**]タブが表示されます。
4. [**危険なスクリプトの処理**]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。
5. [**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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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。
6. [**信頼ゾーン**]セクションで、[**信頼ゾーンを適用する**]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、場所による除外や、信頼ゾーンの除外リストに記載された名前や名

前マスクでの除外が考慮されます。

チェックボックスをオフにすると、スクリプト監視タスクの除外リストが無視されます。

既定では、このチェックボックスはオンです。

7. [**OK**]をクリックします。

新しい設定が適用されます。

スクリプト監視タスクの統計情報

スクリプト監視タスクの実行中は、タスクの開始から現在までに Kaspersky Security for Windows Server によって処理されたスクリプトの数に関する情報を表示できます。

► スクリプト監視タスクの統計情報を表示するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**スクリプト監視**]サブフォルダーを選択します。

現在のタスクの統計情報は、[**管理**]および[**統計情報**]セクションのノード内の詳細ペインに表示されます。

タスクの開始以降、Kaspersky Security for Windows Server によって処理されたオブジェクトに関する情報を表示できます(次の表を参照)。

表 44. スクリプト監視タスクの統計情報

フィールド	説明
ブロックしたスクリプト	Kaspersky Security for Windows Server によって実行がブロックされたスクリプトの数。
危険なスクリプトの検知	検知された危険なスクリプトの数。
危険な可能性のあるスクリプトの検知	検知された危険な可能性があるスクリプトの数。
処理されたスクリプト	処理されたスクリプトの合計数。

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。

この章の内容

KSN の使用タスクについて

Kaspersky Security Network(「KSN」とも表記)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 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 に関する声明に同意する必要があります。

Kaspersky Security for Windows Server が Kaspersky Security Network から受信するのは、プログラムと URL 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の取り扱い方法ウィンドウと、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 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 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 に関する声明の同意の撤回

Kaspersky Security Network の同意はいつでも撤回して、データ交換を停止することができます。次の処理は KSN に関する声明に対する同意の完全または部分的な撤回とみなされます:

- [**スキャンしたファイルに関するデータを送信**]をオフにする:分析のためにスキャンしたファイルのチェックサムを KSN サービスに送信することを停止します。
- [**スキャンした URL に関するデータを送信**]をオフにする:分析用に URL を送信することを停止します。
- [**Kaspersky Security Network に統計情報を送信**]をオフにする:追加の KSN の統計情報のデータ処理を停止します。
- [**Kaspersky Security Network に関する声明の内容に同意する**]をオフにする:すべての KSN 関連のデータ処理および KSN の使用タスクが停止します。
- [**Kaspersky Managed Protection に関する声明の条件に同意する**]をオフにする:KMP サービスが無効になります。
- KSN の使用コンポーネントのアンインストール:すべての KSN 関連のデータ処理が停止します。
- Kaspersky Security for Windows Server のアンインストール:すべての KSN 関連のデータ処理が停止します。

KSN の使用タスクの既定の設定

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 45. KSN の使用タスクの既定の設定

設定	既定値	説明
KSN で信頼されていないオブジェクトに対する処理	削除	KSN によって信頼しないと認識されたオブジェクトに対して Kaspersky Security 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 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。
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。	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。

管理プラグインから KSN の使用を管理する

このセクションでは、KSN の使用タスクとデータの取り扱い方法を、管理プラグインから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

KSN の使用タスクの管理プラグインからの設定

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**サーバーのリアルタイム保護**]セクションで、[**KSN の使用**]サブセクションの[**設定**]をクリックします。

   [**KSN の使用**]ウィンドウが開きます。
5. [**全般**]タブで、次のタスク設定を行います:
   - [**KSN で信頼されてい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 for Windows Server が実行する処理を指定します:
     - **削除**

       Kaspersky Security for Windows Server は、KSN の信頼しない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 for Windows Server は、実行ログで KSN の信頼しない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。信頼しない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。

- 必要に応じて、右側のフィールドで、Kaspersky Security 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変更します。

- [**KSN プロキシ**]セクションで、[**Kaspersky Security Center を KSN プロキシとして使用する**]をオフまたはオンにします。

  このチェックボックスを使用して、保護対象サーバーと KSN の間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が直接 KSN に送信されます(Kaspersky Security Center を経由しません)。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 のヘルプ**を参照してください。

6. 必要に応じて、[**タスク管理**]タブで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。

7. タスクを開始する前にデータの取り扱い方法を設定してください(284 ページのセクション「データの取り扱い方法の管理プラグインからの設定」を参照)。

8. [**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、システム監査ログに保存されます。

データの取り扱い方法の管理プラグインからの設定

データの取り扱い方法の既定の設定を変更できます(次の表を参照)。

表 46. データの取り扱い方法の既定の設定

設定	既定値	説明
Kaspersky Security Network に関する声明の内容に同意する	オフ	オンにすると、インストール後の KSN の使用に同意します。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 に統計情報を送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	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。
スキャンしたファイルに関するデータを送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	KSN に関する声明に同意すると、タスクが開始されてからスキャンおよび分析したファイルに関するデータが送信されます。チェックボックスはいつでもオフにできます。
スキャンした URL に関するデータを送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	KSN 声明に同意すると、アクセスした URL に関する情報が Kaspersky Lab に送信されます。
Kaspersky Managed Protection に関する声明の条件に同意する	オフ	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、追加の同意書にサインした場合にのみ使用できます。

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**サーバーのリアルタイム保護**]セクションで、[**KSN の使用**]サブセクションの[**データの取り扱い**]をクリックします。

   [**データの取り扱い方法**]ウィンドウが開きます。
5. [**統計とサービス**]タブで、声明の内容を確認し、[**Kaspersky Security Network に関する声明の内容に同意する**]をオンにします。
6. 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。

     ファイル評価の要求が制限モードで送信されることがあるので、注意してください。制限は、DDoS 攻撃から Kaspersky Lab の評価サーバーを保護するために使用されます。このシナリオでは、送信中のファイル評価要求のパラメータは、Kaspersky Lab のエキスパートが確立したルールや方法によって定義され、保護対象サーバーでユーザーが設定することはできません。これらのルールと方法のアップデートは、定義データベースのアップデートとともに受信されます。制限が適用されると、[**KSN サーバーを DDoS 攻**

撃から保護するために Kaspersky Lab により有効にされました]ステータスが KSN の使用タスクの統計情報に表示されます。

既定では、このチェックボックスはオンです。

- **スキャンした 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の設定に影響します。

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。

7. [**Kaspersky Security Network に統計情報を送信**]は、既定ではオンです。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、個人情報を含む可能性のある追加の統計情報が送信されます。KSN の統計情報として送信されるすべてのデータのリストは、KSN に関する声明で示されています。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。

8. [**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、データの処理がすぐに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 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、該当する契約にサインし、保護対象サーバーで設定ファイルを実行して、[**統計とサービス**]タブで、[**Kaspersky Security Network に関する声明の内容に同意する**]、[**スキャンしたファイルに関するデータを送信**]、[**要求した URL に関するデータを送信**]、[**Kaspersky Security Network に統計情報を送信**]をオンにする必要があります。

9. [**OK**]をクリックします。

データ処理の設定が保存されます。

アプリケーションコンソールから KSN の使用を管理する

このセクションでは、KSN の使用タスクとデータの取り扱い方法を、アプリケーションコンソールから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

KSN の使用タスクのアプリケーションコンソールからの設定

► 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. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**KSN の使用**]サブフォルダーを選択します。
3. 詳細ペインで[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが開き、[**全般**]タブが表示されます。
4. タスクを設定するには:
   - [**KSN で信頼されてい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 for Windows Server が実行する処理を指定します:
     - **削除**

       Kaspersky Security for Windows Server は、KSN の信頼しない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 for Windows Server は、実行ログで KSN の信頼しない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。信頼しない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。

- 必要に応じて、右側のフィールドで、Kaspersky Security 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変更します。

5. 必要に応じて、[**スケジュール**]タブと[**詳細設定**]タブで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て、[**アプリケーションの起動時**]の開始の頻度を指定します。

   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の取り扱い方法を設定してください(「データの取り扱い方法のアプリケーションコンソールからの設定」(288 ページ)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、システム監査ログに保存されます。

データの取り扱い方法のアプリケーションコンソールからの設定

データの取り扱い方法の既定の設定を変更できます(次の表を参照)。

表 47. データの取り扱い方法の既定の設定

設定	既定値	説明
Kaspersky Security Network に関する声明の内容に同意する	オフ	オンにすると、インストール後の KSN の使用に同意します。この決定は、いつでも変更できます。
Kaspersky Security Network に統計情報を送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	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。
スキャンしたファイルに関するデータを送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	KSN に関する声明に同意すると、タスクが開始されてからスキャンおよび分析したファイルに関するデータが送信されます。チェックボックスはいつでもオフにできます。
スキャンした URL に関するデータを送信	オン(KSN に関する声明に同意した場合にのみ適用されます)	KSN 声明に同意すると、アクセスした URL に関する情報が Kaspersky Lab に送信されます。
Kaspersky Managed Protection に関する声明の条件に同意する	オフ	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、追加の同意書にサインした場合にのみ使用できます。

► 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. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。

2. [**KSN の使用**]サブフォルダーを選択します。
3. 詳細ペインで[**データの取り扱い方法**]をクリックします。

   [**データの取り扱い方法**]ウィンドウが開きます。
4. [**統計とサービス**]タブで、声明の内容を確認し、[**Kaspersky Security Network に関する声明の内容に同意する**]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。

     ファイル評価の要求が制限モードで送信されることがあるので、注意してください。制限は、DDoS 攻撃から Kaspersky Lab の評価サーバーを保護するために使用されます。このシナリオでは、送信中のファイル評価要求のパラメータは、Kaspersky Lab のエキスパートが確立したルールや方法によって定義され、保護対象サーバーでユーザーが設定することはできません。これらのルールと方法のアップデートは、定義データベースのアップデートとともに受信されます。制限が適用されると、[**KSN サーバーを DDoS 攻撃から保護するために Kaspersky Lab により有効にされました**]ステータスが KSN の使用タスクの統計情報に表示されます。

     既定では、このチェックボックスはオンです。

   - **スキャンした 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の設定に影響します。

   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. [**Kaspersky Security Network に統計情報を送信**]は、既定ではオンです。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、個人情報を含む可能性のある追加の統計情報が送信されます。KSN の統計情報として送信されるすべてのデータのリストは、KSN に関する声明で示されています。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、データの処理がすぐに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 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、該当する契約にサインし、保護対象サーバーで設定ファイルを実行して、[**統計とサービス**]タブで、[**Kaspersky Security Network に関する声明の内容に同意する**]、[**スキャンしたファイルに関するデータを送信**]、[**要求した URL に関するデータを送信**]、[**Kaspersky Security Network に統計情報を送信**]をオンに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。

追加のデータ転送の設定

Kaspersky Security for Windows Server では、以下のデータを Kaspersky Lab に送信するよう設定できます:

- スキャンされたファイルのチェックサム([**スキャンしたファイルに関するデータを送信**])。
- 要求された URL と処理された電子メールに関するデータ([**スキャンした URL に関するデータを送信**])。
- 個人情報を含む追加の統計情報([**Kaspersky Security Network に統計情報を送信**])。

Kaspersky Lab に送信されるデータの詳細情報については、このガイドの「ローカルでのデータ取り扱い方法」を参照してください。

[**Kaspersky Security Network に関する声明の内容に同意する**]をオンにした場合のみ、該当するチェックボックスをオンまたはオフにできます(「データの取り扱い方法のアプリケーションコンソールからの設定」(288 ページ)を参照)。

既定では、Kaspersky Security for Windows Server は KSN に関する声明に同意したあとで、ファイルのチェックサムとスキャンした URL に関するデータ、追加の統計情報を送信します。

表 48. 使用可能なチェックボックスの状態と該当する条件

チェックボックスの状態	[スキャンしたファイルに関するデータを送信]の状態	[Kaspersky Security Network に統計情報を送信]の状態	[スキャンした URL に関するデータを送信]の状態	[Kaspersky Managed Protection に関する声明の条件に同意する]の状態	[Kaspersky Security Network に関する声明の内容に同意する]の状態
☑	• 評価の要求が送信される • チェックボックスが編集できる	• 追加の統計情報が送信される • チェックボックスが編集できる	• 追加の統計情報が送信される • チェックボックスが編集できる	• 追加の統計情報が送信される • チェックボックスが編集できる	• 追加の統計情報が送信される • チェックボックスが編集できる

チェックボックスの状態	[スキャンしたファイルに関するデータを送信]の状態	[Kaspersky Security Network に統計情報を送信]の状態	[スキャンしたURL に関するデータを送信]の状態	[Kaspersky Managed Protection に関する声明の条件に同意する]の状態	[Kaspersky Security Network に関する声明の内容に同意する]の状態
☑	• 評価の要求が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない
☐	• 評価の要求が送信されない • チェックボックスが編集できる	• 追加の統計情報が送信されない • チェックボックスが編集できる	• 追加の統計情報が送信されない • チェックボックスが編集できる	• 追加の統計情報が送信されない • チェックボックスが編集できる	• 追加の統計情報が送信されない • チェックボックスが編集できる
☐	• 評価の要求が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない	• 追加の統計情報が送信されない • チェックボックスが編集できない

KSN の使用タスクの統計情報

KSN の使用タスクの実行中は、タスクが開始されてから現在までに Kaspersky Security for Windows Server によって処理されたオブジェクトの数についての詳細情報を、リアルタイムで表示することができます。タスクの実行中に発生したすべてのイベントに関する情報は、タスク実行ログに記録されます(「タスク実行ログについて」(210 ページ)を参照)。

► KSN の使用タスクの統計情報を表示するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**KSN の使用**]サブフォルダーを選択します。

選択したフォルダーの詳細ペインにある[**統計情報**]セクションに、タスクの統計情報が表示されます。

タスクの開始以降、Kaspersky Security for Windows Server によって処理されたオブジェクトに関する情報を表示できます(次の表を参照)。

表 49. KSN の使用タスクの統計情報

フィールド	説明
送信した要求	Kaspersky Security for Windows Server によって KSN に送信されるファイル評価の問い合わせの数。

フィールド	説明
送信された URL リクエスト	Kaspersky Security for Windows Server によって KSN に送信される URL 評価の問い合わせの数。
KSN で信頼されていない URL	KSN によって信頼しないとみなされた URL の数。
KSN で信頼されていないファイル	KSN によって信頼しないとみなされたオブジェクトの数。
要求送信エラー	処理の結果がタスクエラーになった KSN 要求の数。
生成された統計	KSN に送信された生成済み統計パッケージの数。
削除されたオブジェクト	KSN の使用タスクを実行しているときに削除されたオブジェクトの数。
バックアップ済み	バックアップに保存されたオブジェクトコピーの数。
削除されていないオブジェクト	削除しようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由で削除できなかったオブジェクトの数。そのようなオブジェクトの情報は、タスク実行ログに記録されます。
バックアップされていないオブジェクト	バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存できなかったオブジェクトの数。バックアップに移動できないファイルは駆除または削除されません。そのようなオブジェクトの情報は、タスク実行ログに記録されます。
制限モード	このステータスは、制限モードでファイル評価要求を送信するかどうかを示します。

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その設定方法について説明します。

この章の内容

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監視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 for Windows Server は、Windows Subsystem for Linux で実行するプロセスが要求したトラフィックも検知対象として監視します。そのようなプロセスに対して、トラフィック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 脆弱性攻撃ブロック(KAVFSWH)

コンポーネントによる保護の種別は次のとおりです:

- メール脅威対策
  - アンチフィッシング
  - メールで送信されるマルウェアに対する保護
- ウェブ脅威対策
  - アンチフィッシング
  - 悪意ある URL のスキャン
  - Web 感染型マルウェアからの保護
  - 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
- カテゴリベースのウェブコントロール

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のモード

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監視します。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監視および分析します。
- **リダイレクター**:ユーザーの Web ブラウザーから送信された要求を本製品がプロキシサーバーとして処理し、取得したトラフィックを内部の ICAP サーバーにリダイレクトします。このモードでは、Web ブラウザーの追加の設定が必要になり、プロキシサーバー接続のためのアドレスとポートを指定する必要があります。
- **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 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 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 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. アンチフィッシングデータベースおよび定義データベース
3. KSN
4. カテゴリ

カテゴリベースのウェブコントロール

Kaspersky Security 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 for Windows Server が既定で適用するルールは TOR 証明書の拒否ルールの 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 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（312 ページのセクション「カテゴリベースのウェブコントロールの設定」と 326 ページのセクション「カテゴリベースのウェブコントロールの設定」を参照）。

メール脅威対策

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。メール脅威対策は、Kaspersky Security for Windows Server コンポーネントとは別にインストールされる Microsoft Outlook アドインを介して利用できます。

メール脅威対策は次を含みます：

- 受信メールのスキャン
- アンチウイルスのためのメールスキャン
- アンチウイルス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
- アンチフィッシングのためのメールスキャン
- アンチフィッシング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、以下が実行されます：

- 感染した添付ファイルを完全に削除します。
- 感染したメール本体を修正します。この場合、感染したメールの本文のテキストは、脅威に関する情報とともに HTML ページとして添付されます。フィッシングサイトへのリンクが検知された場合、感染したメールの本文のテキストは、脅威に関する情報とともに TXT 形式のファイルとして添付されます。
- 「**メールの脅威が検知されました**」イベントの記録

Kaspersky Security 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 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. 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. 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。

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 50. 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、わいせつな語彙など）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。	中絶、成人向け出会い系、拒食症、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、未成年向け出会い系、ヌード、政策決定、ポルノ、世界的な法規制による制限、ロシア連邦法による制限、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、わいせつな語彙、暴力、武器。
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。	中絶、アルコール、拒食症、薬物、健康と美容、違法薬物、医薬品、薬局、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。
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。	成人向け出会い系、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、宝くじ、メディアホスティングとストリーミング、医薬品、音楽、ニュース、未成年向け出会い系、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、Torrent、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、宝くじ、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、医薬品、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、宝くじ、世界的な法規制による制限、ロシア連邦法による制限、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。
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、ロシア連邦法による制限、ロシア連邦通信局による制限(RF)。
legal	法的な規制の対象となりうる内容に関連した 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、宝くじ、軍事、薬局、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:Torrent、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、インターネットサービス、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、Torrent、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、医薬品、未成年向け出会い系、ソーシャルネットワーク、旅行。
psychotropic&drug	このカテゴリには、あらゆる種類のドラッグ、向精神薬、タバコ製品に関連する 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、医薬品、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。	成人向け出会い系、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。
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、ロシア連邦法による制限、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。

定義済みの保護レベルの設定

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 つの定義済みの保護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）。

最高のパフォーマンス

サーバーおよびワークステーションでの Kaspersky Security for Windows Server の使用に加えて、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（ファイアウォールや既存のセキュリティポリシーなど）を適用している場合、[**最高のパフォーマンス**]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、保護レベルと保護対象のサーバーのパフォーマンスへの影響とのバランスが最適化されます。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で高い水準のコンピューターセキュリティ要件が求められる場合、[**最大の保護**]セキュリティレベルを推奨します。

表 51. 定義済みの保護レベルと対応するセキュリティ設定

オプション	保護レベル		
	最高のパフォーマンス	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	すべてのオブジェクト	すべてのオブジェクト
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の処理	ブロック	ブロック	ブロック
検知しないオブジェクト	なし	なし	なし
スキャン時間が次を超えたら停止する(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	20 MB
複合オブジェクトの保護	• 圧縮されたオブジェクト	• 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	• 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

トラフィックセキュリティタスクの既定の設定

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 52. トラフィックセキュリティタスクの既定の設定

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。
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アンチウイルス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 アンチフィッシング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。
保護レベル	推奨	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
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。

管理プラグインからトラフィックセキュリティを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーのタスク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

操作方法

必要なタスクの設定をインターフェイスから操作する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のポリシーの設定ウィンドウ

► Kaspersky Security Center のポリシーからアプリケーション起動コントロールタスクの設定を開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。

   表示されたポリシーのプロパティウィンドウで、[**サーバーのリアルタイム保護**]セクションを選択します。
5. [**トラフィックセキュリティ**]サブセクションの[**設定**]をクリックします。

   [**トラフィックセキュリティ**]ウィンドウが開きます。
6. 必要に応じてポリシーを設定します。

トラフィックセキュリティルールのリスト

► **Kaspersky Security Center からアプリケーション起動コントロールのリストを開くには:**

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**サーバーのリアルタイム保護**]セクションを選択します。
6. [**トラフィックセキュリティ**]サブセクションの[**ルールリスト**]をクリックします。

   [**ウェブコントロールルール**]ウィンドウが開きます。

必要に応じてルールリストを設定します。

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を設定するには:**

1. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**全般**]タブの[**タスクモード**]セクションでタスクの処理モードを選択および設定します(303 ページのセクション「タスクの処理モードの設定」を参照)。
3. [**URL と Web アドレスの処理**]タブで URL のアンチフィッシングおよびアンチウイルススキャンを設定します(309 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)。
4. [**マルウェアからの保護**]タブで、ヒューリスティックアナライザーと保護レベルを設定します(306 ページのセクション「Web 感染型マルウェアからの保護の設定」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の開始を設定します(138 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**]をクリックします。

タスクの設定が保存されます。

このセクションの内容

タスクの処理モードの設定

► **タスクの処理モードを設定するには:**

1. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**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**(303 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**(305 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**
3. 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 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。

   ICAP サービス接続設定を適用するには、タスクを再起動します。
4. 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。
5. [**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

► **ドライバーインターセプターモードを設定するには:**

1. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**全般**]タブで、[**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 プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

- **証明書が無効の Web サーバーを信頼しない**

  [**HTTPS プロトコル経由の安全な接続をスキャンする**]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 感染型の脅威を検知するために Kaspersky Security 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 プロトコル経由の安全な接続をスキャンする**]にリストアップされています。

4. ポートを監視領域に追加する、またはそこから除外するには、[**監視領域の設定**]をクリックします。

   [**監視領域**]ウィンドウが開きます。

5. [**ポートの監視**]タブで次のオプションのいずれかを選択します:
   - **すべて監視する**
   - **指定したポートを監視する**:

     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。

     ポートが監視領域に追加されます。

   既定では、Kaspersky Security 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監視します。

6. 監視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 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**]タブで監視領域から IP アドレスを除外するには:
   a. IP アドレスを IPv4 形式で入力します(短い形式で入力、またはサブネットマスクがあるアドレスを指定)。
   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する**]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、[**開く**]をクリックします。
9. [**監視領域**]ウィンドウで[**OK**]をクリックします。
10. [**トラフィックセキュリティ**]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

► リダイレクターモードを設定するには:

1. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**全般**]タブで、[**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 プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

- **スキャン後にトラフィックをプロキシサーバーにリダイレクトする**

  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社内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 感染型の脅威を検知するために Kaspersky Security 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 プロトコル経由の安全な接続をスキャンする**]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 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。

Web 感染型マルウェアからの保護の設定

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. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**マルウェアからの保護**]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(298 ページのセクション「定義済みの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**
- **最高のパフォーマンス**
- **カスタム**

3. [**設定**]をクリックして[**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**

     すべてのオブジェクトがスキャンされます。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **指定の拡張子リストによってオブジェクトをスキャン**

     ファイル拡張子に基づいて、ファイルがスキャンされます。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。

4. [**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、アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護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、SFX アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護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ファイルが、スキャン時にスキップされます。

既定値は、選択した保護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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

5. [**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。

     Kaspersky Security for Windows Server は、感染した添付ファイルを電子メールから完全に削除します。この場合、検知された脅威に関するイベントが、トラフィックセキュリティタスクのログに記録されます。

   - **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。

     Kaspersky Security for Windows Server は、感染した添付ファイルを電子メールから削除しません。この場合、検知された脅威に関するイベントが、トラフィックセキュリティタスクのログに記録されます。

6. [**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(https://encyclopedia.kaspersky.com/knowledge/classification/)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、指定した検知可能なオブジェクトがスキャン時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、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. [**編集**]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:

     - **スキャン時間が次を超えたら停止する(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、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。

- **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。

  指定したサイズ制限を超える複合オブジェクトが、スキャン時にスキップされます。

  既定では、値は 20 MB に設定されています。

7. [**マルウェアからの保護設定**]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。

メール脅威対策の設定

メール脅威対策を使用するには、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（295 ページのセクション「脅威からのメールの保護」を参照）。

► メール脅威対策を有効にするには:

1. [**トラフィックセキュリティ**]ウィンドウを開きます（301 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ポリシーの設定ウィンドウ」を参照）。
2. [**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 Microsoft Outlook アドインを使用するすべての受信メールでアンチウイルススキャンとアンチフィッシング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。

   メール脅威対策を有効または無効にすると、その設定は短いタイムアウトの後（5 分）、または Microsoft Outlook の再起動後すぐに適用されます。

3. [**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. [**トラフィックセキュリティ**]ウィンドウを開きます（301 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ポリシーの設定ウィンドウ**」を参照）。
2. [**全般**]タブの[**タスクモード**]セクションでタスクの処理モードを選択および設定します（303 ページのセクション「タスクの処理モードの設定」を参照）。
3. [**URL と Web アドレスの処理**]タブ:

- [**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、アンチフィッシングデータベースを使用して各 URL がチェックされます。アンチフィッシング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 のアンチフィッシングスキャンを設定するときは、アンチフィッシング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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

  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:

  - トラフィックセキュリティの設定で[**保護に KSN を使用する**]がオンになっている。
  - KSN 声明に同意している。
  - [**要求した URL に関するデータを送信**](283 ページのセクション「**KSN の使用タスクの管理プラグインからの設定**」を参照)がオンになっている。
  - KSN の使用タスクが開始されている。

4. [**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。

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 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、ブロックしたりできます。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. トラフィックセキュリティタスクを設定します(311 ページのセクション「タスクモードの選択と設定」を参照)。

b. 証明書のルールを追加および適用します(312 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 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. [**トラフィックセキュリティ**]ウィンドウを開きます(301 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ポリシーの設定ウィンドウ」を参照)。
2. [**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**(303 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**(305 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)
3. [**タスクモード設定**]ブロックで次の設定を行います:
   - **HTTPS プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

4. [**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 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. [**ウェブコントロールルール**]ウィンドウを開きます(302 ページのセクション「トラフィックセキュリティルールのリスト」を参照)。
2. [**ウェブコントロール**]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 証明書の一部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ンです。
3. [**追加**]をクリックして新しいルールを追加します。
4. [**追加**]のコンテキストメニューで、[**証明書ベースのルール**]を選択します。
5. [**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**]:[**マスク記号を使用する**]または[**正規表現を使用する**]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。
6. 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。
7. [**ウェブ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。

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. [**ウェブコントロールルール**]ウィンドウを開きます(302 ページのセクション「**トラフィックセキュリティルールの設定ウィンドウ**」を参照)。
2. [**カテゴリ**]タブを開きます。

3. [**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。

4. 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、正規の Web リソースへのアクセスを許可する**
   - **正規の広告へのアクセスを許可する**
5. 使用可能なカテゴリ分類リスト内(295 ページのセクション「カテゴリのリスト」を参照)で次の操作を実行します:
   - 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。

     [**ルールの種別**]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。

     [**ルールの種別**]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)。

6. [**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(283 ページのセクション「KSN の使用タスクの管理プラグインからの設定」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(302 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(486 ページのセクション「非ウイルスマスクの適用」を参照)。

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. [**ウェブコントロールルール**]ウィンドウを開きます(302 ページのセクション「トラフィックセキュリティルールのリスト」を参照)。
2. [**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 URL 拒否ルールの適用により URL の一部がブロックされます。

   チェックボックスをオフにすると、URL 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ンです。
3. [**追加**]をクリックして新しいルールを追加します。
4. [**追加**]のコンテキストメニューで、[**URL ベースのルール**]を選択します。
5. [**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. [**URL**]フィールドで URL を指定します。
   e. [**OK**]をクリックします。
6. 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。
7. [**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。

アプリケーションコンソールからトラフィックセキュリティを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのタスクの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する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の設定ウィンドウ

► **アプリケーションコンソールからトラフィックセキュリティタスクの全般的な設定を開くには:**

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**トラフィックセキュリティ**]サブフォルダーを選択します。
3. [**トラフィックセキュリティ**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。
   [**タスクの設定**]ウィンドウが表示されます。

トラフィックセキュリティルールの設定ウィンドウ

► **アプリケーションコンソールからトラフィックセキュリティルールのリストを開くには:**

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**トラフィックセキュリティ**]サブフォルダーを選択します。
3. [**トラフィックセキュリティ**]フォルダーの詳細ペインで、[**ウェブコントロールルール**]をクリックします。
   [**ウェブコントロールルール**]ウィンドウが開きます。

必要に応じてルールリストを設定します。

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を設定するには:**

1. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**全般**]タブの[タスクモード]セクションでタスクの処理モードを選択および設定します(316 ページのセクション「タスクの処理モードの設定」を参照)。
3. [**URL と Web アドレスの処理**]タブで URL のアンチフィッシングおよびアンチウイルススキャンを設定します(317 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)。
4. [**マルウェアからの保護**]タブで、ヒューリスティックアナライザーと保護レベルを設定します(320 ページのセクション「Web 感染型マルウェアからの保護の設定」を参照)。
5. [**スケジュール**]タブと[**詳細設定**]タブで、スケジュールに基づいてタスクを開始します(138 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。

このセクションの内容

タスクの処理モードの設定

► **タスクの処理モードを設定するには:**

1. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**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**
   - **リダイレクター**
   - **外部プロキシ**
3. **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 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。

ICAP サービス接続設定を適用するには、タスクを再起動します。

4. 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。

5. [**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

► ドライバーインターセプターモードを設定するには:

1. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**全般**]タブで、[**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 プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

     既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

   - **証明書が無効の Web サーバーを信頼しない**

     [**HTTPS プロトコル経由の安全な接続をスキャンする**]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 感染型の脅威を検知するために Kaspersky Security 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 プロトコル経由の安全な接続をスキャンする**]にリストアップされています。

4. ポートを監視領域に追加する、またはそこから除外するには、[**監視領域の設定**]をクリックします。

   [**監視領域**]ウィンドウが開きます。

5. [**ポートの監視**]タブで次のオプションのいずれかを選択します:

   - **すべて監視する**
   - **指定したポートを監視する**:

     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。

     ポートが監視領域に追加されます。

   > 既定では、Kaspersky Security 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監視します。

6. 監視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 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**]タブで監視領域から IP アドレスを除外するには:

   a. IP アドレスを IPv4 形式で入力します(短い形式で入力、またはサブネットマスクがあるアドレスを指定)。

   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する**]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、[**開く**]をクリックします。

9. [**監視領域**]ウィンドウで[**OK**]をクリックします。

10. [**タスクの設定**]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

► リダイレクターモードを設定するには:

1. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**全般**]タブで、[**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 プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

     > 既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

   - **セキュリティポート**

     Web 感染型の脅威を検知するために Kaspersky Security 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 プロトコル経由の安全な接続をスキャンする**]にリストアップされています。

   - **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社内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。

[**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 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。

Web 感染型マルウェアからの保護の設定

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. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**マルウェアからの保護**]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。
   - 保護レベル(298 ページのセクション「定義済みの保護レベルの設定」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**
     - **最高のパフォーマンス**
     - **カスタム**
3. 下部の[**説明**]タブで、選択した保護レベルの設定を確認できます。
4. [**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**

     すべてのオブジェクトがスキャンされます。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
   - **指定の拡張子リストによってオブジェクトをスキャン**

     ファイル拡張子に基づいて、ファイルがスキャンされます。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。

5. [**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、アーカイブがスキャン時にスキップされます。

  既定値は、選択した保護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、SFX アーカイブがスキャン時にスキップされます。

  既定値は、選択した保護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ファイルが、スキャン時にスキップされます。

  既定値は、選択した保護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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

6. [**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。

  Kaspersky Security for Windows Server は、感染した添付ファイルを電子メールから完全に削除します。この場合、検知された脅威に関するイベントが、トラフィックセキュリティタスクのログに記録されます。

- **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。

Kaspersky Security for Windows Server は、感染した添付ファイルを電子メールから削除しません。この場合、検知された脅威に関するイベントが、トラフィックセキュリティタスクのログに記録されます。

7. [**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（https://encyclopedia.kaspersky.com/knowledge/classification/）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、指定した検知可能なオブジェクトがスキャン時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、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:
  - **スキャン時間が次を超えたら停止する（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、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。

  - **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。

指定したサイズ制限を超える複合オブジェクトが、スキャン時にスキップされます。

既定では、値は 20 MB に設定されています。

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

保護レベルの設定が保存されます。

メール脅威対策の設定

► メール脅威対策を有効にするには:

1. [**タスクの設定**]ウィンドウを開きます（315 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ウィンドウ**」を参照）。
2. [**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 Microsoft Outlook アドインを使用するすべての受信メールでアンチウイルススキャンとアンチフィッシング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。

メール脅威対策を有効または無効にすると、その設定は短いタイムアウトの後（5 分）、または Microsoft Outlook の再起動後すぐに適用されます。

3. [**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:

4. [**タスクの設定**]ウィンドウを開きます（315 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ウィンドウ**」を参照）。
5. [**全般**]タブの[**タスクモード**]セクションでタスクの処理モードを選択および設定します（316 ページのセクション「タスクの処理モードの設定」を参照）。
6. [**URL と Web アドレスの処理**]タブ:
   - [**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、アンチフィッシングデータベースを使用して各 URL がチェックされます。アンチフィッシング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 のアンチフィッシングスキャンを設定するときは、アンチフィッシング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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

     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:

- トラフィックセキュリティの設定で[**保護に KSN を使用する**]がオンになっている。
- KSN 声明に同意している。
- [**スキャンした URL に関するデータを送信**](287 ページのセクション「**KSN の使用タスクのアプリケーションコンソールからの設定**」を参照)がオンになっている。
- KSN の使用タスクが開始されている。

7. [**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。

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 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、ブロックしたりできます。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. トラフィックセキュリティタスクを設定します(324 ページのセクション「タスクモードの選択と設定」を参照)。

b. 証明書のルールを追加および適用します(325 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 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. [**タスクの設定**]ウィンドウを開きます(315 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ウィンドウ**」を参照)。
2. [**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**(317 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**
3. [**タスクモード設定**]ブロックで次の設定を行います:
   - **HTTPS プロトコル経由の安全な接続をスキャンする**

     チェックボックスをオンにすると、監視対象の暗号化 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**

既定では、すべてのバージョンが選択されています。この場合、[**TLS 1.0**]をオフにすることはできません。

4. [**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。既定では、Kaspersky Security は証明書の拒否ルールのみを作成します。

► 証明書ルールを追加または設定するには:

1. [**ウェブコントロールルール**]ウィンドウを開きます(315 ページのセクション「トラフィックセキュリティルールの設定ウィンドウ」を参照)。
2. [**ウェブコントロール**]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 証明書の一部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ンです。
3. [**追加**]をクリックして新しいルールを追加します。
4. [**追加**]のコンテキストメニューで、[**証明書ベースのルール**]を選択します。
5. [**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**]:[**マスク記号を使用する**]または[**正規表現を使用する**]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。
6. 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。

7. [**ウェブ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。

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. [**ウェブコントロールルール**]ウィンドウを開きます(315 ページのセクション「**トラフィックセキュリティルールの設定ウィンドウ**」を参照)。
2. [**カテゴリ**]タブを開きます。
3. [**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。
4. 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、正規の Web リソースへのアクセスを許可する**
   - **正規の広告へのアクセスを許可する**
5. 使用可能なカテゴリ分類リスト内(295 ページのセクション「カテゴリのリスト」を参照)で次の操作を実行します:
   - 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)。
6. [**保存**]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. アプリケーションコンソールツリーで、[KSN の使用タスクの設定]を開きます(287 ページのセクション「KSN の使用タスクのアプリケーションコンソールからの設定」を参照)。
2. [**スキャンした 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(317 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)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）マスクの使用が[**信頼ゾーン**]で設定されます。

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. [**ウェブコントロールルール**]ウィンドウを開きます（315 ページのセクション「**トラフィックセキュリティルールの設定ウィンドウ**」を参照）。
2. [**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 URL 拒否ルールの適用により URL の一部がブロックされます。

   チェックボックスをオフにすると、URL 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ンです。
3. [**追加**]をクリックして新しいルールを追加します。
4. [**追加**]のコンテキストメニューで、[**URL ベースのルール**]を選択します。
5. [**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. [**ルールの種別**]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. [**URL**]フィールドで URL を指定します。
   e. [**OK**]をクリックします。
6. 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。
7. [**ウェブ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。

新しいルールが適用されます。

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。

この章の内容

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、このコンピューターの LUID(ローカルで一意な識別子)がブロック対象コンピューターのリストに追加されます。

アンチクリプタータスクは同期モードまたは非同期モードで実行できます。既定では、アンチクリプタータスクは非同期モードで実行され、ファイル操作は並列的に処理されます。ファイル処理の同期モードと非同期モード、およびモードの切り替え方法について詳しくは、カスペルスキーのオンラインナレッジベース(28 ページの「自分で調査する場合の情報源」)を参照してください。

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フォルダー内で行われる場合、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。悪意のある動作を認識するまで一定の時間がかかるため、この間に暗号化プログラムが悪意のある動作を実行する可能性があります。

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統計情報

アンチクリプタータスクが実行中の場合、タスク開始時以降に Kaspersky Security for Windows Server で処理されたオブジェクトの数に関するリアルタイム情報(タスク実行統計)を表示できます。

► アンチクリプタータスクの統計情報を表示するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。

選択したフォルダーの詳細ペインにある[**統計情報**]セクションに、タスクの統計情報が表示されます。

タスクの開始以降、Kaspersky Security for Windows Server によって処理されたオブジェクトに関する情報を表示できます(次の表を参照)。

表 53. アンチクリプタータスクの統計情報

フィールド	説明
検知した悪意のある暗号化の試行	Kaspersky Security for Windows Server が暗号化動作を検知したアクセス試行の数。
処理エラー	タスクのエラーになった、ストレージ領域に対するアプリケーションの要求の数。
処理されたオブジェクト	Kaspersky Security for Windows Server で処理されたアクセス試行の総数。

アンチクリプタータスクの既定の設定

アンチクリプタータスクでは、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 54. アンチクリプタータスクの既定の設定

設定	既定値	説明
作業モード	処理を実行	アンチクリプタータスクは、**処理を実行**モードまたは**統計のみ**モードで開始できます。
保護領域	すべての保護対象サーバーの共有フォルダーに、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。
除外リスト	除外リストは適用されており、Kaspersky Lab のエキスパートによって追加された項目が含まれています。	タスクの保護範囲から除外する領域を指定します。
ヒューリスティックアナライザー	ヒューリスティックアナライザーはオンで、**中レベル**のスキャン詳細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 for Windows Server の起動時に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。

アンチクリプタータスクの管理プラグインからの設定

► **アンチクリプター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。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

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**]サブセクションの[**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. 表示されたウィンドウで、次の設定を行います:

   - [**全般**]タブで作業モードとヒューリスティックアナライザーの使用(331 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(332 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(333 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(138 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、システム監査ログに保存されます。

このセクションの内容

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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

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**]サブセクションの[**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. [**全般**]タブの[**作業モード**]セクションで、[**処理を実行**]モードを選択します。

   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 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。

6. [**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。

7. 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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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。

8. [**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め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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

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**]サブセクションの[**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. [**保護範囲**]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共有フォルダーのみが保護されます。

6. 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**]を選択し、[**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、直接入力します。

   c. [**OK**]をクリックします。

7. [**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:

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. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

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**]サブセクションの[**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. [**除外**]タブで、[**除外リストを適用する**]をオンにします。

   このチェックボックスをオンにすると、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ンで、除外リストには Kaspersky Lab のエキスパートによって次の項目が追加されています。

   - ***.stt**
   - ***.sig**
   - ***.exe**
   - ***.sldprt**

6. [**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。

7. [**参照**]をクリックしてフォルダーを選択するか、直接入力します。

8. [**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。

アンチクリプタータスクのアプリケーションコンソールからの設定

► アンチクリプタータスクを設定するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。
3. [**アンチクリプター**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。

4. 表示されたウィンドウで、次の設定を行います:
   - [**全般**]タブで作業モードとヒューリスティックアナライザーの使用(336 ページのセクション「タスクの全般的な設定」を参照)
   - [**保護領域**]タブで保護領域(335 ページのセクション「保護範囲の作成」を参照)。
   - [**除外リスト**]タブで除外リスト(337 ページのセクション「除外の追加」を参照)
   - [**スケジュール**]タブおよび[**詳細設定**]タブでタスク開始スケジュール設定(138 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、システム監査ログに保存されます。

このセクションの内容

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め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。

定義済み、またはユーザーの保護範囲のいずれかを使用すると、保護範囲から選択したフォルダーを、たとえばこれらのフォルダーのデータがリモート端末にインストールされたプログラムによって暗号化される場合に除外できます。

► アンチクリプタータスクの保護範囲を設定するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。
3. [**アンチクリプター**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
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共有フォルダーのみが保護されます。
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、次のいずれかの方法を使用します:
   - 手動:

     a. 保護対象サーバーの共有フォルダーの名前を入力します。

     b. [**追加**]をクリックします。

フォルダーがリストに追加されます。

- 検索の使用:

  a. [**参照**]をクリックします。

  Microsoft Windows 標準のウィンドウが表示されます。

  b. タスクの保護範囲に追加するフォルダーを選択します。

  c. [**OK**]をクリックします。

6. [**OK**]をクリックします。

指定された設定が保存されます。

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. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。
3. [**アンチクリプター**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. [**全般**]タブの[**作業モード**]セクションで、[**処理を実行**]モードを選択します。

   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 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。このスキャンのレベルによって、脅威の検知の徹底度、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非常に多くの数実行します。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。

除外の追加

► アンチクリプタータスクの保護範囲を設定するには:

1. アプリケーションコンソールツリーで、[**サーバーのリアルタイム保護**]フォルダーを展開します。
2. [**アンチクリプター**]サブフォルダーを選択します。
3. [**アンチクリプター**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. [**除外リスト**]タブで、[**除外リストを適用する**]をオンにします。

   このチェックボックスをオンにすると、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ンで、除外リストには Kaspersky Lab のエキスパートによって次の項目が追加されています。

- *.stt
- *.sig
- *.exe
- *.sldprt

5. フォルダー名またはマスクを指定します。
6. [**追加**]をクリックします。
7. 必要に応じて手順 5 ～ 6 を繰り返し、除外をさらに追加します。
8. [**タスクの設定**]ウィンドウで[**OK**]をクリックします。

保護範囲の除外が追加および適用されます。

アプリケーション起動コントロール

このセクションでは、アプリケーション起動コントロールタスクとその設定方法について説明します。

この章の内容

アプリケーション起動コントロールタスクについて

アプリケーション起動コントロールタスクの実行中に、Kaspersky Security for Windows Server はアプリケーションを起動しようとするユーザーの試行を監視し、これらのアプリケーションの開始を許可または拒否します。アプリケーション起動コントロールタスクは「既定で拒否」の原則に基づいています。これは、タスク設定で許可されていないアプリケーションはすべて自動でブロックされることを意味します。

次のいずれかの方法により、アプリケーションの起動を許可できます:

- 信頼するアプリケーションの許可ルールを設定する。
- 起動時に KSN において信頼するアプリケーションの評価について確認する。

アプリケーションの起動の拒否には最大の優先度が指定されます。いずれかのブロックルールによってアプリケーションの起動が阻止された場合、KSN による信頼の判定には関係なく、アプリケーションの起動が拒否されます。たとえば、アプリケーションが許可ルールの範囲に含まれているにもかかわらず、KSN サービスによって信頼されていない場合、このアプリケーションの起動は拒否されます。

> アプリケーションを開始しようとするすべての試行は、タスク実行ログに記録されます(「タスク実行ログについて」(210 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は、2 つのモードのいずれかで実行できます:

- **処理を実行**:アプリケーション起動コントロールルールの範囲に該当するアプリケーションについて、起動をコントロールするルールを使用します。アプリケーション起動コントロールルールの範囲は、このタスクの設定で指定されます。アプリケーションはアプリケーション起動コントロールルールの適用範囲に該当し、そのタスク設定が指定されたルールに適合していない場合、そのアプリケーションの起動は拒否されます。

  アプリケーション起動コントロールタスクの設定で指定されたルールの範囲に該当しないアプリケーションは、アプリケーション

起動コントロールタスクの設定に関係なく、起動が許可されます。

アプリケーション起動コントロールタスクは、ルールが作成されていない場合、または 1 つのサーバーに対して 65,535 を超えるルールがある場合に、[処理を実行]モードで起動できません。

- **統計のみ**:Kaspersky Security for Windows Server は、アプリケーションの起動を許可まはた拒否するために、アプリケーション起動コントロールルールを使用しません。代わりに、アプリケーションの起動に関する情報、アプリケーションの開始を実行するルール、**処理を実行**モードでタスクを開始した場合に実行される処理に関する情報を記録します。すべてのアプリケーションの起動が許可されます。既定ではこのモードが設定されています。

  このモードを使用すると、実行ログに記録された情報に基づいてアプリケーション起動コントロールルールを作成できます(379 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イベントからの許可ルールの作成」を参照)。

次のいずれかのシナリオに従って、アプリケーション起動コントロールタスクを設定できます:

- 詳細なルール設定(339 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ルールについて」を参照)およびアプリケーション起動コントロールにおけるそのルールの使用。
- アプリケーション起動コントロールにおける基本的なルール設定および KSN の使用(372 ページのセクション「KSN の使用の設定」を参照)。

オペレーティングシステムのファイルがアプリケーション起動コントロールタスクの範囲に該当する場合、アプリケーション起動コントロールルールを作成するとき、そのアプリケーションが新たに作成したルールによって許可されていることを確認してください。許可されていない場合、オペレーティングシステムが起動しないことがあります。

また、Kaspersky Security for Windows Server は、Windows Subsystem for Linux で起動されたプロセスを監視します(UNIX™ シェル、またはコマンドラインインタープリターから実行されたスクリプトを除く)。そのようなプロセスに対して、アプリケーション起動コントロール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。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は、アプリケーションの起動を検出し、Windows Subsystem for Linux で動作するアプリケーションに対して対応するルールを生成します。

アプリケーション起動コントロールルールについて

アプリケーション起動コントロールルールのしくみ

アプリケーション起動コントロールルールの処理は、次のコンポーネントに基づきます:

- ルールの種別

  アプリケーション起動コントロールルールは、アプリケーションの起動を許可または拒否できます。それぞれ**許可**ルールまたは**拒否**ルールと呼ばれています。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作成するには、ルールの自動生成を使用して許可ルールを作成するか、アプリケーション起動コントロールタスクで**統計のみ**モードを使用します。また、許可ルールを手動で追加することもできます。

- ユーザーまたはユーザーグループ

  アプリケーション起動コントロールルールは、ユーザーまたはユーザーグループによって指定されたアプリケーションの起動を制御できます。

- ルールの適用範囲

  アプリケーション起動コントロールルールは、**実行ファイル**や**スクリプト**、**MSI パッケージ**に適用できます。

- ルール有効化の条件

  アプリケーション起動コントロールルールは、ルール設定で指定された基準のいずれかを満たすファイルの起動を制御します。指定された**デジタル証明書**によってファイルが署名されていること、指定された **SHA256 ハッシュ**とファイルが一致しているこ

と、指定された**パス**にファイルがあることが、ルール設定で指定される基準です。

ルール有効化の条件に**デジタル証明書**を設定すると、オペレーティングシステムで信頼されているすべてのアプリケーションの起動が、作成したルールによって制御されます。次のチェックボックスを使用して、より厳しい有効化の条件を設定することもできます:

- **発行先を使用**

  ルール有効化の条件として、デジタル証明書の発行先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、デジタル証明書の指定された発行先が、ルール有効化の条件として使用されます。作成したルールでは、発行先として指定された製造元のアプリケーションに対してのみ起動が制御されます。

  このチェックボックスをオフにすると、ルール有効化の条件にデジタル署名の発行先は使用されません。[**デジタル証明書**]の基準を選択すると、あらゆる発行先のデジタル証明書で署名されたアプリケーションの起動が、作成したルールにより管理されます。

  ファイルの署名に使用されたデジタル証明書の発行先は、[**ルール有効化の条件**]セクションの上にある[**ファイルのプロパティからルール有効化の条件を設定**]を使用して選択されたファイルのプロパティからのみ指定できます。

  既定では、このチェックボックスはオフです。

- **サムプリントを使用**

  ルール有効化の条件として、デジタル証明書の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、デジタル証明書の指定されたサムプリントが、ルール有効化の条件として使用されます。作成したルールでは、指定のサムプリントのデジタル証明書で署名されたアプリケーションの起動が制御されます。

  このチェックボックスをオフにすると、ルール有効化の条件にデジタル証明書のサムプリントは使用されません。[**デジタル証明書**]の基準を選択すると、あらゆるサムプリントのデジタル証明書を使用して署名されたアプリケーションの起動が制御されます。

  ファイルの署名に使用されたデジタル証明書のサムプリントは、[**ルール有効化の条件**]セクションの上にある[**ファイルのプロパティからルール有効化の条件を設定**]を使用して選択されたファイルのプロパティからのみ指定できます。

  既定では、このチェックボックスはオフです。

サムプリントはデジタル証明書を一意に識別し、デジタル証明書の発行先と違って偽造できないため、デジタル証明書に基づくアプリケーション起動ルールの適用では、最も基準が正確になっています。

アプリケーション起動コントロールルールに対して除外対象を指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ルールの除外対象は、ルール有効化の条件と同様、デジタル証明書、SHA256 ハッシュ、ファイルのパスに基づきます。特定の許可ルールのために、アプリケーション起動コントロールルールの除外対象が必要になる場合もあります。たとえば、ユーザーが C:¥Windows のパスからアプリケーションを起動することを許可する一方で、ファイル Regedit.exe の起動をブロックできます。

オペレーティングシステムのファイルがアプリケーション起動コントロールタスクの範囲に該当する場合、アプリケーション起動コントロールルールを作成するとき、そのアプリケーションが新たに作成したルールによって許可されていることを確認してください。許可されていない場合、オペレーティングシステムが起動しないことがあります。

アプリケーション起動コントロールルールの管理

アプリケーション起動コントロールルールを使用して、次の処理を実行できます:

- ルールを手動で追加する
- ルールを自動作成して追加する
- ルールを削除する

- ルールをファイルにエクスポートする
- 選択したファイルの実行を許可するルールに適合しているかどうか、これらのファイルをチェックする
- 指定した基準に従って、リストのルールをフィルタリングする

ソフトウェア配布コントロールについて

保護対象サーバーでのソフトウェア配布も制御する必要がある場合、アプリケーション起動コントロールルールの生成は複雑になる可能性があります。たとえば、サーバー上にインストールされたソフトウェアが定期的に自動アップデートされるなどの特性を考慮する必要があります。この場合、ソフトウェアのアップデート後に毎回、許可ルールのリストをアップデートし、新しく作成されたファイルがアプリケーション起動コントロールタスクの設定に反映されるようにする必要があります。ソフトウェアの配布シナリオで起動コントロールを簡略化するために、ソフトウェア配布コントロールのサブシステムを使用できます。

ソフトウェアの配布パッケージは、サーバーにインストールされるソフトウェアアプリケーションを表します。各パッケージには 1 つ以上のアプリケーションが含まれており、特にソフトウェアアプリケーションまたはアップデートをインストールしている場合は、アプリケーションに加えて個々のファイル、アップデート、さらに個々のコマンドが含まれることもあります。

ソフトウェア配布コントロールのサブシステムは、追加の除外リストとして実装されます。ソフトウェアの配布パッケージをこのリストに追加すると、これらの信頼するパッケージの展開、および信頼するパッケージによってインストールまたは変更されるソフトウェアの自動起動が許可されます。抽出したファイルは、展開元の配布パッケージの信頼する属性を継承することができます。**展開元の配布パッケージ**は、ソフトウェア配布コントロールの除外リストにユーザーが追加して信頼するパッケージとなったものです。

Kaspersky Security for Windows Server は、ソフトウェアの配布のフルサイクルのみを管理します。パッケージが初めて起動されたときにソフトウェア配布コントロールがオフになっている場合、またはアプリケーション起動コントロールコンポーネントがインストールされていない場合、信頼するパッケージによって変更されたファイルの起動を正しく処理できません。

アプリケーション起動コントロールタスクの設定で、[**実行ファイルにルールを適用する**]がオフになっている場合は、ソフトウェア配布コントロールは使用できません。

ソフトウェアの配布のキャッシュ

Kaspersky Security for Windows Server は、動的に生成されたソフトウェア配布のキャッシュ(「配布キャッシュ」とも表記)を使用して、信頼するパッケージとソフトウェアの配布中に作成されたファイルとの関連付けを確立します。パッケージの最初の起動時に、Kaspersky Security for Windows Server はソフトウェアの配布処理中にパッケージから作成したすべてのファイルを検知し、ファイルのチェックサムとパスを配布キャッシュに保存します。その後、既定では、配布キャッシュのすべてのファイルの起動が許可されます。

ユーザーインターフェイスから配布キャッシュを更新、クリア、または手動で変更することはできません。キャッシュは Kaspersky Security for Windows Server によって追加および管理されます。

コマンドラインのオプションを使用して配布キャッシュを設定ファイルに(XML 形式で)エクスポートしたり、キャッシュをクリアできます。

► 配布キャッシュを設定ファイルにエクスポートするには、次のコマンドを実行します:

```
kavshell appcontrol /config /savetofile:<フルパス> /sdc
```

► 配布キャッシュをクリアするには、次のコマンドを実行します:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Security for Windows Server は、配布キャッシュを 24 時間ごとにアップデートします。前に許可されたファイルのチェックサムが変更されると、そのファイルのレコードが配布キャッシュから削除されます。アプリケーション起動コントロールタスクが[処理を実行]モードで開始された場合、このファイルのそれ以降の開始試行はブロックされます。前に許可されたファイルのフルパスが変更された

場合は、チェックサムは配布キャッシュに保存されたまま残るため、それ以降のこのファイルの起動の試行はブロックされません。

抽出したファイルの処理

信頼するパッケージから抽出したすべてのファイルでは、パッケージの最初の起動時に信頼属性が継承されます。最初の起動後にチェックボックスをオフにした場合、このパッケージから抽出されたすべてのファイルでは継承された属性が維持されます。抽出されたすべてのファイルで継承された属性をリセットするには、配布キャッシュをクリアして、[**この配布パッケージを解凍して作成されたファイルすべての起動を許可する**]をオフにしてから信頼する配布パッケージをもう一度起動する必要があります。

信頼する展開元の配布パッケージによって作成・抽出されたファイルとパッケージでは、除外リストに含まれるソフトウェアの配布パッケージを最初に開いてファイルとパッケージのチェックサムが配布キャッシュに追加されたときに、信頼属性が継承されます。このため、配布パッケージ自体とこのパッケージから抽出されたすべてのファイルも信頼されます。既定では、信頼属性を継承するレベルの数に制限はありません。

抽出したファイルは、オペレーティングシステムの再起動後でも信頼属性を維持します。

[**この配布パッケージを解凍して作成されたファイルすべての起動を許可する**]のオンまたはオフによって、ファイルの処理がソフトウェア配布コントロール設定で指定されます(352 ページのセクション「ソフトウェア配布コントロールの設定」を参照)。

たとえば、他のパッケージやアプリケーションをいくつか含むテスト用の .msi パッケージを除外リストに追加してチェックボックスをオンにします。この場合、テスト用の .msi パッケージに含まれるすべてのパッケージとアプリケーションは、他のファイルを含む場合に、実行または抽出が許可されます。このシナリオは、すべてのネストされたレベルで抽出されたファイルに対して有効です。

テスト用の .msi パッケージを除外リストに追加して[**この配布パッケージを解凍して作成されたファイルすべての起動を許可する**]をオフにすると、(最初のレベルでネストされる)展開元の信頼するパッケージから直接抽出したパッケージと実行ファイルにのみ、信頼属性が割り当てられます。そのようなファイルチェックサムは、配布キャッシュに保存されます。2 番目以降のレベルでネストされるすべてのファイルは、「既定で拒否」の原則によってブロックされます。

アプリケーション起動コントロールルールリストとの影響関係

ソフトウェア配布コントロールのサブシステムの信頼するパッケージのリストは、除外のリストであり、アプリケーション起動コントロールルールの全般リストを補完しますが、置き換えるものではありません。

アプリケーション起動コントロールルールによる拒否は、最も優先されます。これらのパッケージとファイルがアプリケーション起動コントロールの拒否ルールによって影響を受けている場合、信頼するパッケージの展開と新しいファイルまたは変更されたファイルの起動がブロックされます。

アプリケーション起動コントロールリストの拒否ルールがこれらのパッケージとファイルに適用されていない場合、ソフトウェア配布コントロールの除外リストが、これらのパッケージによって作成または変更された、信頼するパッケージとファイルの両方に適用されます。

KSN の判定の利用

ファイルを信頼しないという KSN の判定は、ソフトウェア配布コントロールの除外リストよりも優先されます。これらのファイルを信頼しないとの判定を KSN から受け取っている場合、信頼するパッケージの展開、またはこのパッケージによって作成または変更されたファイルの起動はブロックされます。

アプリケーション起動コントロールタスクでの KSN の使用について

KSN の使用タスクを開始するには、KSN 声明に同意する必要があります。

アプリケーションの評価に関する KSN のデータがアプリケーション起動コントロールタスクによって使用される場合、KSN でのアプリケーションの評価は該当するアプリケーションの起動を許可または拒否する際の基準とみなされます。アプリケーション起動の試行時に Kaspersky Security for Windows Server が KSN から信頼しないとの判定を受け取った場合、このアプリケーションの起動は拒否されます。アプリケーション起動の試行時に Kaspersky Security for Windows Server が KSN から信頼するとの判定を受け取った場合、このアプリケーションの起動は許可されます。KSN は、アプリケーション起動コントロールルールとともに使用するか、あるいはアプリ

ケーションの起動を拒否するための独立した 1 つの基準として使用できます。

アプリケーションの起動を拒否するための独立した基準として KSN の判定を使用する

このシナリオでは、ルールリストの詳細な設定を使用しなくても、保護対象サーバーでアプリケーションの起動を安全に管理できます。

Kaspersky Security for Windows Server に対して、KSN の判定と指定したルールのみを適用できます。KSN で信頼されているアプリケーション、あるいは特定のルールで許可されているアプリケーションの起動のみが許可されます。

このようなシナリオでは、デジタル証明書に基づいてアプリケーションの起動を許可するルールを設定してください。

その他のアプリケーションはすべて、「既定で拒否」の原則に従って起動が拒否されます。ルールが適用されていないときに KSN を使用すると、KSN が脅威であるとみなしているアプリケーションからコンピューターが保護されます。

アプリケーション起動コントロールルールと同時に KSN の判定を使用する

KSN の判定をアプリケーション起動コントロールルールと同時に使用すると、次の条件が適用されます:

- アプリケーションが 1 つ以上の拒否ルールの範囲に含まれている場合、Kaspersky Security for Windows Server では常にこのアプリケーションの起動が拒否されます。アプリケーションが KSN によって信頼されるとみなされている場合、この判定の優先度は低く、考慮されません。アプリケーションの起動は拒否されます。これにより、不要なアプリケーションとして起動を拒否するアプリケーションの対象範囲を拡大できます。
- KSN で信頼されていないアプリケーションの起動が禁止されており、アプリケーションが KSN で信頼されていない場合、Kaspersky Security for Windows Server では常にこのアプリケーションの起動が拒否されます。アプリケーションで許可ルールが設定されている場合も、その優先度は低く、考慮されないため、アプリケーションの起動は拒否されます。これにより、ルールの初期設定時には考慮されていなかったが現在では KSN が脅威であるとみなしているアプリケーションからコンピューターが保護されます。

アプリケーション起動コントロールルールの生成

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。共通ルールを作成する上でベースとなるような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の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。アプリケーションコンソールからアプリケーション起動コントロールタスクの自動作成タスクをローカルで実行すると、1 つのサーバーで実行中のアプリケーションに基づいてルールのリストを作成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コンポーネントは、事前設定された 2 つの許可ルールとともにインストールされます:

- オペレーティングシステムの信頼する証明書を使用したスクリプトと MSI ファイルの許可ルール。
- オペレーティングシステムの信頼する証明書を使用した実行ファイルの許可ルール。

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リストを作成するには、次のいずれかの方法で行います:

- 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を使用する。

  このシナリオでは、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。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によって生成される XML ファイルには、タスクを開始する前のタスクの設定で指定した許可ルールが含まれます。指定されたタスクの設定で起動が許可されていないアプリケーションに対してルールは作成されません。そのようなアプリケーションの起動は既定で拒否されます。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。設定で、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ように指定できます。

  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タスクのルールのリストへ自動的にインポートされるように、設定を編集できます。

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、適用される許可ルールに、安全であることがわかっているフォルダーとファイルのみが含まれる場合に限定して設定してください。

ネットワークでアプリケーション起動コントロールタスクを使用する前に、すべての保護対象サーバーが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共有フォルダーを使用できない場合は、テストサーバーグループのサーバー上で、または共通ルールを作成する上でベースとなるような参照マシン上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タスクを開始してください。

- **統計のみ**モードで実行されるアプリケーション起動コントロールタスクにより、Kaspersky Security Center で生成されるタスクイベントのレポートをベースにする。

  このシナリオでは、Kaspersky Security for Windows Server はアプリケーションの起動を拒否しません。代わりに、[**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、実行ログを使用して、アプリケーションの起動が拒否されたイベントの 1 つのリストを生成します。

  タスクの実行期間を編集し、指定された期間中に保護対象サーバーおよびサーバーグループで生じうるすべてのシナリオが実行され、なおかつ再起動が 1 回以上実施されるようにする必要があります。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たあと、保存された Kaspersky Security Center のイベントレポート(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用途種別の異なるサーバー(異なるソフトウェア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に、このシナリオを使用してください。

- 設定ファイルの作成やインポートは行わずに、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をベースにする。

  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された場合、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)。ルールのリストをアップデートする際には、アプリケーション起動コントロールルールの自動作成タスクまたはアプリケーション起動コントロールタスクを、テスト管理グループのサーバー上で**統計のみ**モードで実行してください。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。

許可ルールのリストの XML ファイルは、保護対象サーバーで開始されるタスクの分析を基に作成されます。ルールのリストの作成時にネットワーク上で使用されているすべてのアプリケーションを含めるには、アプリケーション起動コントロールルールの自動作成タスクおよびアプリケーション起動コントロールタスクを、共通ルールを作成する上でベースとなるような参照マシン上で**統計のみ**モードで開始してください。

参照マシン上で起動されたアプリケーションに基づいて許可ルールの作成する前に、参照マシンが安全でマルウェアが存在しないことを確認してください。

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。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。

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

アプリケーション起動コントロールタスクでは、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 55. 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、拒否された起動イベントおよび許可された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あとで、[**処理を実行**]モードを選択できます。
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	適用されます。	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ことができます。
実行するコマンドのないコマンドライン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ラインインタープリターの起動を拒否できます。
ルールの管理	**ローカルルールをポリシールールで上書きする**	ポリシーで指定したルールとローカルコンピューター上のルールを合わせて適用す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 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。
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	適用されません。	設定で指定したインストーラーおよびアプリケーションを使用するソフトウェア配布を許可できます。既定では、ソフトウェア配布は Windows インストーラーサービスを使用する場合のみ許可されます。

設定	既定値	説明
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([**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**]の設定が有効になっている場合のみ変更できます)。	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。
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	適用されません([**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**]の設定が有効になっている場合のみ変更できます)。	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布をオンまたはオフにできます。
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 for Windows Server の起動時に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。

表 56. 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既定の設定

設定	既定値	説明
許可ルール名の接頭辞	Kaspersky Security for Windows Server がインストールされているサーバーの名前と同一にします。	許可ルールの名前の接頭辞を変更できます。
許可ルールの適用範囲	許可ルールの適用範囲には、次の既定のファイルのカテゴリが含まれます: • C:\Windows、C:\Program Files (x86)、および C:\Program Files の各フォルダーにある EXE 拡張子を持つファイル • C:¥Windows フォルダーにある MSI パッケージ • C:¥Windows フォルダーに保存されているスクリプト このタスクは、場所や形式に関係なく、実行中のすべてのアプリケーションのルールも作成します。	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。また、許可ルールを作成するときに、実行中のアプリケーションを無視することもできます。
許可ルールの生成の基準	デジタル証明書の発行先とサムプリントが使用されます。ルールはすべてのユーザーとユーザーグループに対して生成されます。	許可ルールを生成するときに、SHA256 ハッシュを使用できます。 許可ルールを自動的に生成する必要があるユーザーおよびユーザーグループを選択できます。

設定	既定値	説明
タスク完了後の処理	許可ルールが、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。新しいルールが既存のルールに結合され、重複するルールは削除されます。	ルールの結合や重複するルールの削除をしないで既存のルールに追加したり、既存のルールを新しい許可ルールに置き換えたりすることもできます。さらに、許可ルールをファイルへエクスポートする設定も可能です。
権限を指定したタスク開始の設定	タスクがシステムアカウントで起動されます。	システムアカウントや指定したユーザーの権限を使用して、アプリケーション起動コントロールルールの自動作成タスクの起動を許可できます。
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。	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は、Kaspersky Security for Windows Server 起動時に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。

管理プラグインからアプリケーション起動コントロールを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーのタスク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

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

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ポリシーの設定ウィンドウ

► Kaspersky Security Center のポリシーからアプリケーション起動コントロールタスクの設定を開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**ローカルアクティビティの管理**]セクションを選択します。
6. [**アプリケーション起動コントロール**]サブセクションの[**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。

必要に応じてポリシーを設定します。

アプリケーション起動コントロールルールのリスト

► Kaspersky Security Center からアプリケーション起動コントロールのリストを開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**ローカルアクティビティの管理**]セクションを選択します。
6. [**アプリケーション起動コントロール**]サブセクションの[**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。
7. [**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。

必要に応じてルールリストを設定します。

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ウィザードとプロパティウィンドウ

► 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作成を開始するには:

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。
2. タスクを設定する管理グループを選択します。
3. [**タスク**]タブを選択します。
4. [**タスクの作成**]をクリックします。

   [**新規タスクウィザード**]ウィンドウが開きます。
5. [**アプリケーション起動コントロールルールの自動作成**]タスクを選択します。
6. [**次へ**]をクリックします。

   [**設定**]ウィンドウが開きます。

► 既存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タスクの設定を編集するには:

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。
2. タスクを設定する管理グループを選択します。
3. [**タスク**]タブを選択します。
4. Kaspersky Security Center タスクのリストで、タスク名をダブルクリックします。

   [**アプリケーション起動コントロールルールの自動作成**]ウィンドウが開きます。

タスクの設定に関する詳細は、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タスクの設定」を参照してください。

アプリケーション起動コントロールタスクの設定

► 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:

1. [**アプリケーション起動コントロール**]ウィンドウを開きます(348 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ポリシーの設定ウィンドウ**」を参照)。
2. [**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タスクのモードを選択できます:

     - **処理を実行**:指定されたルールを使用して、アプリケーションの起動を管理します。
     - **統計のみ**:アプリケーションの起動を管理するために指定されたルールは使用されません。代わりに、実行ログに起動イベントに関する情報が記録されます。すべてのアプリケーションの起動が許可されます。このモードを使用して、実行ログに記録される拒否されたアプリケーションの起動に関する情報に基づき、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ベント情報に基づく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に関するタスクの判定を基にして、アプリケーションの以降の起動が許可または拒否されます。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、この判定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、アプリケーションが起動を試みる度に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ライン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、インタープリ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プリターの起動が拒否されます。コマンドのないコマンドインタープリターは、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プリターの起動が許可されている。
  - 実行対象の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、コマンドラインインタープリターを起動するときに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が KSN によって信頼されていない場合、起動は拒否されます。許可ルールが適用されているか、プロセスが KSN によって信頼されている場合、コマンドラインインタープリター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 for Windows Server は次のコマンドラインインタープリターを認識します:

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

  既定では、このチェックボックスはオフです。

3. [**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. アプリケーション起動コントロールタスク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 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でのアプリケーション起動コントロールを一元管理するかたちで、ポリシーで指定したルールリストが適用されます。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 for Windows Server は、リストにあるスクリプト、MSI パッケージ、および実行ファイルが信頼できるデジタル署名でサインされている場合、これらのオブジェクトを許可する 2 つのプリセットルールを適用します。

4. [**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**

  このチェックボックスでは、実行ファイルの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、**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実行ファイルの起動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実行ファイルの起動は制御されません。実行ファイルの起動が許可されます。

  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 モジュールの読み込み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 モジュールの読み込みを監視しません。DLL モジュールの読み込みが許可されます。

  [**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に、このチェックボックスを選択できます。

  既定では、このチェックボックスはオフです。

> DLL モジュールの読み込みを監視すると、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。

5. [**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評価データに従って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 で信頼されていない場合に、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 の信頼しないアプリケーションの評価は考慮されず、そのようなアプリケーション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評価データに従って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 で信頼されている場合に、そのアプリケーションの実行を許可します。アプリケーションが KSN で信頼されていても、同じ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拒否ルールの方が、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場合でも、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 の信頼するアプリケーションの評価は考慮されず、そのようなアプリケーション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。

6. [**ソフトウェア配布コントロール**]タブでソフトウェア配布コントロールを設定します(352 ページのセクション「ソフトウェア配布コントロールの設定」を参照)。
7. [**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(139 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、システム監査ログに保存されます。

ソフトウェア配布コントロールの設定

► 信頼する配布パッケージを追加するには:

1. [**アプリケーション起動コントロール**]ウィンドウを開きます(348 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ポリシーの設定ウィンドウ」を参照)。
2. [**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起動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。

3. 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起動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、ファイルの起動は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、配布パッケージから抽出したファイルを起動できなくなったりする場合があります。

4. 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布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、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。ソフトウェア配布は、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。

パッケージ配布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布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本製品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。

5. 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、実行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. [**この配布パッケージを解凍して作成されたファイルすべての起動を許可する**]をオンまたはオフにします。

     c. 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有効化の条件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。

        既定では、このオプションはオンです。

        - **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有効化の条件として指定されます。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。

        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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

        既定では、このオプションはオフです。

- **ハッシュで複数のパッケージを追加**

  実行ファイルおよび配布パッケージを数の制限なく選択して、すべて同時にリストに追加できます。Kaspersky Security 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**

  異なる実行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 for Windows Server によって認識されるファイルは、次の条件を満たす必要があります:

  - ファイル拡張子が TXT である
  - 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>:<SHA256 ハッシュ>
    - <SHA256 ハッシュ>*<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。

6. 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。抽出したファイルの実行が許可されます。

   抽出したファイルの起動を防ぐには、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。

7. [**OK**]をクリックします。

新しい設定が保存されます。

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を設定するには:

1. **アプリケーション起動コントロールルールの自動作成**のプロパティウィンドウを開きます(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ**」を参照)。
2. [**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 のヘルプ**を参照してください。

3. [**設定**]セクションでは、次の設定を行うことができます:
   - ルール名の接頭辞を追加します。
   - 許可ルールの適用範囲を設定します:

- 実行中のアプリケーションに基づいて許可ルールを作成する
- 特定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

4. [**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有効化の条件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。

  既定では、このオプションはオンです。

- **デジタル証明書の発行先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発行先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発行先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を最も正確に適用できます。

  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です。

  - **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有効化の条件として指定されます。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。

  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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

  既定では、このオプションはオフです。

- **次の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です。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制御します。

  既定の選択項目は[**Everyone**]です。

Kaspersky Security 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。

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 のヘルプ**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。

アプリケーション起動コントロールルールの Kaspersky Security Center からの設定

さまざまな条件に基づいてルールのリストを生成する方法、またはアプリケーション起動コントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

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ルールの追加

► アプリケーション起動コントロールルールを追加するには:

1. [**アプリケーション起動コントロールルール**]ウィンドウを開きます(348 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ルールのリスト」を参照)。
2. [**追加**]をクリックします。
3. 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。
4. 次の設定を指定します:
   a. [**名前**]で、ルールの名前を入力します。

b. [**種別**]ドロップダウンリストで、ルールの種別を選択します:

- **許可**:ルール設定で指定された基準に従って、ルールがアプリケーションの起動を許可します。
- **拒否**:ルール設定で指定された基準に従って、ルールがアプリケーションの起動をブロックします。

c. [**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。

d. [**ユーザーまたはユーザーグループ**]で、ルールの種別に従って、プログラムの起動が許可されるユーザーまたは許可されないユーザーを指定します。それには、次の操作を実行します:

iii. [**参照**]をクリックします。

iv. Microsoft Windows 標準の[**ユーザーまたはグループの選択**]ウィンドウが開きます。

v. ユーザーまたはユーザーグループのリストを指定します。

vi. [**OK**]をクリックします。

e. [**ルール有効化の条件**]セクションにリストされたルール有効化の条件の値を、特定のファイルから取得する場合:

vii. [**ファイルのプロパティからルール有効化の条件を設定**]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。

viii. ファイルを選択します。

ix. [**開く**]をクリックします。

ファイルの基準の値が[**ルール有効化の条件**]セクションのフィールドに表示されます。ファイルのプロパティで指定できるデータの基準が既定で選択されています。

f. [**ルール有効化の条件**]セクションで、次のいずれかを選択します:

- **デジタル証明書**:デジタル証明書で署名されたファイルを使用して起動されるアプリケーションの開始が、ルールによって制御されます:
  - 指定したヘッダーを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、[**発行先を使用**]をオンにします。
  - 指定したサムプリントを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、[**サムプリントを使用**]をオンにします。
- **SHA256 ハッシュ**:チェックサムが指定されたものと一致するファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。
- **ファイルのパス**:指定されたパス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、ルールによって制御されます。

> Kaspersky Security 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。

g. ルールの除外対象を追加するには:

x. ［**ルールから除外**］セクションで、［**追加**］をクリックします。

［**ルールから除外**］ウィンドウが開きます。

xi. ［**名前**］で、除外の名前を入力します。

xii. アプリケーション起動コントロールルールからアプリケーションのファイルを除外する設定を指定します。［**ファイルのプロパティに基づいて除外を設定**］をクリックして、ファイルのプロパティから設定フィールドに入力できます。

- **デジタル証明書**

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有効化の条件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。

既定では、このオプションはオンです。

- **発行先を使用**

ルール有効化の条件として、デジタル証明書の発行先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、デジタル証明書の指定された発行先が、ルール有効化の条件として使用されます。作成したルールでは、発行先として指定された製造元のアプリケーションに対してのみ起動が制御されます。

このチェックボックスをオフにすると、ルール有効化の条件にデジタル署名の発行先は使用されません。［**デジタル証明書**］の基準を選択すると、あらゆる発行先のデジタル証明書で署名されたアプリケーションの起動が、作成したルールにより管理されます。

ファイルの署名に使用されたデジタル証明書の発行先は、［**ルール有効化の条件**］セクションの上にある［**ファイルのプロパティからルール有効化の条件を設定**］を使用して選択されたファイルのプロパティからのみ指定できます。

既定では、このチェックボックスはオフです。

- **サムプリントを使用**

ルール有効化の条件として、デジタル証明書の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、デジタル証明書の指定されたサムプリントが、ルール有効化の条件として使用されます。作成したルールでは、指定のサムプリントのデジタル証明書で署名されたアプリケーションの起動が制御されます。

このチェックボックスをオフにすると、ルール有効化の条件にデジタル証明書のサムプリントは使用されません。［**デジタル証明書**］の基準を選択すると、あらゆるサムプリントのデジタル証明書を使用して署名されたアプリケーションの起動が制御されます。

ファイルの署名に使用されたデジタル証明書のサムプリントは、［**ルール有効化の条件**］セクションの上にある［**ファイルのプロパティからルール有効化の条件を設定**］を使用して選択されたファイルのプロパティからのみ指定できます。

既定では、このチェックボックスはオフです。

- **SHA256 ハッシュ**

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有効化の条件として指定されます。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。

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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

既定では、このオプションはオフです。

- **ファイルのパス**

チェックボックスがオンの場合、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

既定では、このチェックボックスはオフです。

xiii. [**OK**]をクリックします。

xiv. 必要に応じて、手順(i)～(iv)を繰り返し、除外を追加します。

5. [**ルール設定**]ウィンドウで[**OK**]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**]ウィンドウのリストに、作成されたルールが表示されます。

「既定で許可」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、「既定で許可」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。「既定で許可」モードは、以下で記載している設定の許可ルールを追加することによって有効にできます。「既定で許可」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。

► 「既定で許可」ルールを追加するには:

1. [**アプリケーション起動コントロールルール**]ウィンドウを開きます(348 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ルールのリスト**」を参照)。
2. [**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。
3. [**名前**]で、ルールの名前を入力します。
4. [**種別**]ドロップダウンリストで、**許可**ルールを選択します。
5. [**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。
6. [**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。
7. 次のマスクを入力します: ?:¥
8. [**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。

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の 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するには:

1. [**アプリケーション起動コントロールルール**]ウィンドウを開きます(348 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ルールのリスト**」を参照)。
2. [**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。
3. 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他のルールと異なる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。
4. 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**
5. ルール作成タスクで使用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**
6. [**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。
7. [**ルールの生成**]をクリックします。
8. [**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タスク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から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反映されます。

   > アプリケーション起動コントロールルールのリストがポリシーですでに指定されている場合、Kaspersky Security 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。

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を確認することができます。

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起動コントロールの許可ルールを指定するには:

1. [**アプリケーション起動コントロール**]ウィンドウを開きます(348 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ポリシーの設定ウィンドウ」を参照)。
2. [**タスクモード**]セクションで、[**統計のみ**]モードを選択します。
3. ポリシーのプロパティの[**イベントの設定**]セクションで、次の内容を確認します:
   - [**緊急イベント**]で、[**アプリケーションの起動が拒否されました**]イベントの実行ログの保管期間が[**統計のみ**]モードのタスクの実行で計画された期間を超えている(既定値は 30 日)。
   - 重要度が[**警告**]のイベントで、[**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**]イベントの実行ログの保管期間が[**統計のみ**]モードのタスクの実行で計画された期間を超えている(既定値は 30 日)。

   イベントの保管期間が経過すると、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期間を超えていないことを確認してください。
4. 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. Kaspersky Security Center の[**管理サーバー**]フォルダーの作業領域で、[**イベント**]タブを選択します。
   b. [**抽出の作成**]をクリックし、[**アプリケーションの起動が拒否されました**]の基準に基づい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**]をクリックして、ブロックされたアプリケーション起動のレポートを TXT ファイルに保存します。

   生成したレポートを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。
5. 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他のルールと異なる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。

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によっ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。

► 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のグループに対してアプリケーション起動コントロールの許可ルールを指定するには:

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、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(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ」を参照)。
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。

     > このセクションでの設定方法の詳細については、**Kaspersky Security Center のヘルプ**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たりして、許可されるアプリケーションを含むフォルダーとして指定するフォルダーを編集できます。
   - [**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、生成される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タスクを使用する前に、すべての保護対象サーバーが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共有フォルダーを使用できない場合は、テストサーバーグループのサーバー上で、または共通ルールを作成する上でベースとなるような参照マシン上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タスクを開始してください。

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するには:

   a. [**アプリケーション起動コントロールルール**]ウィンドウを開きます(348 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ルールのリスト」を参照)。

   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他のルールと異なる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タスクに対して[**処理を実行**]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。

アプリケーション起動のテスト

設定したアプリケーション起動コントロールルールを適用する前に、任意のアプリケーションのテスト起動を試行して、各アプリケーションにどのアプリケーション起動コントロールルールが適用されているかを判断できます。

既定では、起動がいずれかのルールによって許可されないアプリケーションの起動は拒否されます。重要なアプリケーションの起動を拒否しないようにするには、許可ルールを作成する必要があります。

アプリケーションの起動が、種別の異なる複数のルールで管理されている場合、拒否ルールが優先されます。1 つ以上の拒否ルールの対象になっている場合、アプリケーションの起動は拒否されます。

► アプリケーション起動コントロールルールをテストするには:

1. [**アプリケーション起動コントロールルール**]ウィンドウを開きます(348 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

ルールのリスト」を参照)。

2. 表示されたウィンドウで、[**ファイルのルールを表示**]をクリックします。

   Microsoft Windows 標準のウィンドウが表示されます。

3. 起動コントロールをテストするファイルを選択します。

指定されたファイルへのパスが検索フィールドに表示されます。リストには、選択されたファイルの起動時に適用されるルールすべてが含まれます。

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を作成して編集するには:

1. [新規タスクウィザード]で[**設定**]ウィンドウを開きます(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ」を参照)。
2. 以下を設定します:
   - **ルール名の接頭辞**を指定します。

     接頭辞とはルール名の最初の部分です。ルール名の残りの部分は、起動が許可されるオブジェクト名から作成されます。

     既定の接頭辞は、Kaspersky Security for Windows Server がインストールされているサーバーの名前です。許可ルールの名前の接頭辞を変更できます。
   - 許可ルールの適用範囲を設定します(382 ページのセクション「タスクの適用範囲の制限」を参照)。
3. [**次へ**]をクリックします。
4. Kaspersky Security for Windows Server が実行する処理を指定します:
   - 許可ルールの作成時(382 ページのセクション「ルールの自動作成中に実行する処理」を参照)。
   - タスクの完了時(383 ページのセクション「ルールの自動作成の完了時に実行する処理」を参照)。
5. [**スケジュール**]ウィンドウで、タスクの開始スケジュールを設定します。
6. [**次へ**]をクリックします。
7. [**タスクを実行するアカウントの選択**]ウィンドウで、使用するアカウントを指定します。
8. [**次へ**]をクリックします。
9. タスク名を指定します。
10. [**次へ**]をクリックします。

    タスク名は 100 文字以内にする必要があり、次の記号は使用できません:

    " * < > & ¥ : |

    [**タスクの作成を終了**]ウィンドウが開きます。
11. オプションで[**ウィザード完了後にタスクを実行する**]をオンにすると、ウィザードの終了後にタスクを実行することができます。

12. [**完了**]をクリックしてタスクの作成を終了します。

► Kaspersky Security Center で既存のルールを編集するには:

アプリケーション起動コントロールルールの自動作成のプロパティウィンドウを開き、上記の設定を編集します。

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、システム監査ログに保存されます。

このセクションの内容

タスクの適用範囲の制限

► 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範囲を制限するには:

1. **アプリケーション起動コントロールルールの自動作成**のプロパティウィンドウを開きます(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ」を参照)。
2. 次のタスクの設定を指定します:
   - **実行中のアプリケーションに基づいて許可ルールを作成する**

     このチェックボックスでは、すでに実行中のアプリケーションに対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を有効または無効にします。ネットワーク全体または一定の範囲内で共通する許可ルールを作成するためのベースとなるようなアプリケーションの参照セットがサーバーにある場合、このオプションをオンにしてください。

     このチェックボックスをオンにすると、アプリケーション起動コントロールの許可ルールが実行中のアプリケーションに基づいて生成されます。

     このチェックボックスをオフにすると、許可ルールの生成時に実行中のアプリケーションは考慮されません。

     既定では、このチェックボックスはオンです。

     このチェックボックスは、[**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**]テーブルでフォルダーが選択されていない場合はオフにできません。

   - **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**

     タスクの対象フォルダーと、アプリケーション起動コントロールルールの作成時に考慮する実行ファイルの種別を指定できます。指定のフォルダーに格納されている指定の種別のファイルに対して、許可ルールが生成されます。
3. [**OK**]をクリックします。

指定された設定が保存されます。

ルールの自動作成中に実行する処理

► **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実行時に Kaspersky Security for Windows Server が行う処理を設定するには:**

1. **アプリケーション起動コントロールルールの自動作成**のプロパティウィンドウを開きます(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ**」を参照)。
2. [**オプション**]タブを開きます。
3. [**許可ルールの作成**]セクションで、次の設定を行います:
   - **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有効化の条件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。

     既定では、このオプションはオンです。
   - **デジタル証明書の発行先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発行先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発行先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を最も正確に適用できます。

     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です。

     - **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有効化の条件として指定されます。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。

     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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

既定では、このオプションはオフです。

- **次の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です。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制御します。

  既定の選択項目は[**Everyone**]です。

4. [**OK**]をクリックします。

指定された設定が保存されます。

ルールの自動作成の完了時に実行する処理

► 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完了後に Kaspersky Security for Windows Server が行う処理を設定するには:

1. **アプリケーション起動コントロールルールの自動作成**のプロパティウィンドウを開きます(349 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ルールの自動作成タスクのウィザードとプロパティウィンドウ」を参照)。
2. [**オプション**]タブを開きます。
3. [**タスク完了後**]セクションで、次の設定を行います:
   - **アプリケーション起動コントロールルールのリストに許可ルールを追加する**

     新しく作成された許可ルールのアプリケーション起動コントロールルールのリストへの追加を有効または無効にします。アプリケーション起動コントロールルールのリストは、[アプリケーション起動コントロール]フォルダーの詳細ペインの[**アプリケーション起動コントロールルール**]をクリックすると表示されます。

     このチェックボックスをオンにすると、選択した追加方法に基づいて、アプリケーション起動コントロールルールの自動作成タスクによ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。

     このチェックボックスをオフにすると、新しく作成された許可ルールは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せん。作成されたルールは、ファイルにエクスポートされるだけです。

     既定では、このチェックボックスはオンです。

   - **追加方法**

     このドロップダウンリストは、新しく作成された許可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追加する方法の指定に使用されます。

     - **既存のルールに追加する**:ルールが既存のルールのリストに追加されます。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**:ルールがリストの既存のルールを置き換えます。
     - **既存のルールとマージする**:ルールが既存のルールのリストに追加されます。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他のルールと異なる場合にルールが追加されます。

     既定では、[**既存のルールとマージする**]方法が選択されます。

   - **許可ルールをファイルにエクスポートする**
   - **ファイル名にコンピューターの詳細を追加する**

     アプリケーション起動コントロールの許可ルールをエクスポートするファイルの名前に対し、保護対象サーバーに関する情報の追加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、保護対象サーバーの名前、およびファイルの作成日時をエクスポートするファイルの名前に追加します。

このチェックボックスをオフにすると、保護対象のサーバーに関する情報をエクスポートするファイルの名前に追加しません。

既定では、このチェックボックスはオンです。

4. [OK]をクリックします。

指定された設定が保存されます。

アプリケーションコンソールからアプリケーション起動コントロールを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのタスクの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

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ウィンドウ

► アプリケーションコンソールから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開くに

は:

1. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**アプリケーション起動コントロール**]サブフォルダーを選択します。
3. [**アプリケーション起動コントロール**]サブフォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。

アプリケーション起動コントロールルールの設定ウィンドウ

► **アプリケーションコンソールからアプリケーション起動コントロールルールのリストを開くには:**

1. アプリケーションコンソールツリーで、[**ルールの自動作成**]フォルダーを展開します。
2. [**アプリケーション起動コントロール**]サブフォルダーを選択します。
3. [**アプリケーション起動コントロール**]フォルダーの詳細ペインで、[**アプリケーション起動コントロールルール**]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。
4. 必要に応じてルールリストを設定します。

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設定ウィンドウ

► **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:**

1. アプリケーションコンソールツリーで、[**ルールの自動生成**]フォルダーを展開します。
2. [**アプリケーション起動コントロールルールの自動作成**]サブフォルダーを選択します。
3. [**アプリケーション起動コントロールルールの自動作成**]サブフォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. 必要に応じてタスクを設定します。

アプリケーション起動コントロールタスクの設定

► **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:**

1. [**タスクの設定**]ウィンドウを開きます(368 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ウィンドウ」を参照)。
2. 次のタスクの設定を指定します:
   - [**全般**]タブ:
     - アプリケーション起動コントロールタスクモード(370 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モードの選択」を参照)。

- タスクのルールの適用範囲(371 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範囲の設定」を参照)。
- KSN の使用(372 ページのセクション「KSN の使用の設定」を参照)。

- [**ソフトウェア配布コントロール**]タブのソフトウェア配布コントロールの設定(373 ページのセクション「ソフトウェア配布コントロール」を参照)。
- [**スケジュール**]タブおよび[**詳細設定**]タブのタスク開始スケジュール設定(156 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)。

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

   変更された設定が保存されます。

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、システム監査ログに保存されます。

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モードの選択

► アプリケーション起動コントロールタスクのモードを設定するには:

1. [**タスクの設定**]ウィンドウを開きます(368 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ウィンドウ**」を参照)。
2. [**全般**]タブの[**タスクモード**]ドロップダウンリストで、タスク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:

   - **処理を実行**:指定されたルールを使用して、起動されたアプリケーションを管理します。
   - **統計のみ**:アプリケーションの起動を管理するために指定されたルールは使用されません。代わりに、実行ログに起動に関する情報を記録します。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、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。
3. [**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ベント情報に基づく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に関するタスクの判定を基にして、アプリケーションの以降の起動が許可または拒否されます。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、この判定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、アプリケーションが起動を試みる度に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。

Kaspersky Security for Windows Server では、アプリケーション起動コントロールタスク設定を変更するたびに、キャッシュイベントの新しいリストが作成されます。これは、現在のセキュリティ設定に従って、アプリケーション起動コントロールが実行されることを意味します。

4. [**実行するコマンドのないコマンドライン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、インタープリ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プリターの起動が拒否されます。コマンドのないコマンドインタープリターは、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プリターの起動が許可されている。
   - 実行対象の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、コマンドラインインタープリターを起動するときに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が KSN によって信頼されていない場合、起動は拒否されます。許可ルールが適用されているか、プロセスが KSN によって信頼されている場合、コマンドラインインタープリター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 for Windows Server は次のコマンドラインインタープリターを認識します:

   - cmd.exe
   - powershell.exe
   - python.exe
   - perl.exe

   既定では、このチェックボックスはオフです。

5. [**OK**]をクリックします。

指定された設定が保存されます。

アプリケーションを起動しようとするすべての試行は、実行ログに記録されます。

アプリケーション起動コントロールタスクの範囲の設定

► アプリケーション起動コントロールタスクの範囲を定義するには:

1. [**タスクの設定**]ウィンドウを開きます(368 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ウィンドウ**」を参照)。
2. [**ルールの適用範囲**]セクションの[**全般**]タブで、次の設定を行います:
   - **実行ファイルにルールを適用する**

     このチェックボックスでは、実行ファイルの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、**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実行ファイルの起動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実行ファイルの起動は制御されません。実行ファイルの起動が許可されます。

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 モジュールの読み込み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 モジュールの読み込みを監視しません。DLL モジュールの読み込みが許可されます。

  [**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に、このチェックボックスを選択できます。

  既定では、このチェックボックスはオフです。

  > DLL モジュールの読み込みを監視すると、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。

3. [**OK**]をクリックします。

指定された設定が保存されます。

KSN の使用の設定

► アプリケーション起動コントロールタスクで KSN サービスの使用を設定するには:

1. [**タスクの設定**]ウィンドウを開きます(368 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ウィンドウ**」を参照)。
2. [**全般**]タブの[**KSN の使用**]セクションで、KSN サービスの使用の設定を行います:
   - 必要に応じて、[**KSN で信頼されていないアプリケーションを拒否する**]をオンにします。

     このチェックボックスでは、KSN でのアプリケーション評価データに従って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 で信頼されていない場合に、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 の信頼しないアプリケーションの評価は考慮されず、そのようなアプリケーション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。

   - 必要に応じて、[**KSN で信頼されているアプリケーションを許可する**]をオンにします。

     このチェックボックスでは、KSN でのアプリケーション評価データに従って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 で信頼されている場合に、そのアプリケーションの実行を許可します。アプリケーションが KSN で信頼されていても、同じ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拒否ルールの方が、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場合でも、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 の信頼するアプリケーションの評価は考慮されず、そのようなアプリケーション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**]をオンにする場合、KSN で信頼されているアプリケーションの起動が許可されるユーザーまたはユーザーグループを指定します。それには、次の操作を実行します:

  a. [**編集**]をクリックします。

  Microsoft Windows 標準の[**ユーザーまたはグループの選択**]ウィンドウが開きます。

  b. ユーザーまたはユーザーグループのリストを指定します。

  c. [**OK**]をクリックします。

3. [**タスクの設定**]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。

ソフトウェア配布コントロール

► 信頼する配布パッケージを追加するには:

1. [**タスクの設定**]ウィンドウを開きます(368 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ウィンドウ**」を参照)。
2. [**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起動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。

3. 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起動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、ファイルの起動は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、配布パッケージから抽出したファイルを起動できなくなったりする場合があります。

4. 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布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、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。ソフトウェア配布は、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。

パッケージ配布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布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本製品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。

5. 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、実行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. [**この配布パッケージを解凍して作成されたファイルすべての起動を許可する**]をオンまたはオフにします。

     c. 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有効化の条件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。

     既定では、このオプションはオンです。

        - **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有効化の条件として指定されます。

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。

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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

既定では、このオプションはオフです。

- **ハッシュで複数のパッケージを追加**

  実行ファイルおよび配布パッケージを数の制限なく選択して、すべて同時にリストに追加できます。Kaspersky Security 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**

  異なる実行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 for Windows Server によって認識されるファイルは、次の条件を満たす必要があります:

  - ファイル拡張子が TXT である
  - 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>:<SHA256 ハッシュ>
    - <SHA256 ハッシュ>*<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。

6. 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。抽出したファイルの実行が許可されます。

   抽出したファイルの起動を防ぐには、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。

7. [**OK**]をクリックします。

新しい設定が保存されます。

アプリケーション起動コントロールルールの設定

ルールのリストを生成やインポート / エクスポートする方法、またはアプリケーション起動コントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

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ルールの追加

► **アプリケーション起動コントロールルールを追加するには、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ルール**]のウィンドウを開きます。
2. [**追加**]をクリックします。
3. 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。
4. 次の設定を指定します:

   a. [**名前**]で、ルールの名前を入力します。

   b. [**種別**]ドロップダウンリストで、ルールの種別を選択します:

   - **許可**:ルール設定で指定された基準に従って、ルールがアプリケーションの起動を許可します。
   - **拒否**:ルール設定で指定された基準に従って、ルールがアプリケーションの起動をブロックします。

   c. [**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。

   d. [**ユーザーまたはユーザーグループ**]で、ルールの種別に従って、プログラムの起動が許可されるユーザーまたは許可されないユーザーを指定します。それには、次の操作を実行します:

   xv. [**参照**]をクリックします。

   xvi. Microsoft Windows 標準の[**ユーザーまたはグループの選択**]ウィンドウが開きます。

   xvii. ユーザーまたはユーザーグループのリストを指定します。

   xviii. [**OK**]をクリックします。

   e. [**ルール有効化の条件**]セクションにリストされたルール有効化の条件の値を、特定のファイルから取得する場合:

xix. [**ファイルのプロパティからルール有効化の条件を設定**]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。

xx. ファイルを選択します。

xxi. [**開く**]をクリックします。

ファイルの基準の値が[**ルール有効化の条件**]セクションのフィールドに表示されます。ファイルのプロパティで指定できるデータの基準が既定で選択されています。

f. [**ルール有効化の条件**]セクションで、次のいずれかを選択します:

- **デジタル証明書**:デジタル証明書で署名されたファイルを使用して起動されるアプリケーションの開始が、ルールによって制御されます:
  - 指定したヘッダーを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、[**発行先を使用**]をオンにします。
  - 指定したサムプリントを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、[**サムプリントを使用**]をオンにします。
- **SHA256 ハッシュ**:チェックサムが指定されたものと一致するファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。
- **ファイルのパス**:指定されたパス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、ルールによって制御されます。

> Kaspersky Security 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。

g. ルールの除外対象を追加するには:

xxii. [**ルールから除外**]セクションで、[**追加**]をクリックします。

[**ルールから除外**]ウィンドウが開きます。

xxiii. [**名前**]で、除外の名前を入力します。

xxiv. アプリケーション起動コントロールルールからアプリケーションのファイルを除外する設定を指定します。[**ファイルのプロパティに基づいて除外を設定**]をクリックして、ファイルのプロパティから設定フィールドに入力できます。

- **デジタル証明書**

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有効化の条件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。

既定では、このオプションはオンです。

- **発行先を使用**

ルール有効化の条件として、デジタル証明書の発行先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、デジタル証明書の指定された発行先が、ルール有効化の条件として使用されます。作成したルールでは、発行先として指定された製造元のアプリケーションに対してのみ起動

が制御されます。

このチェックボックスをオフにすると、ルール有効化の条件にデジタル署名の発行先は使用されません。[**デジタル証明書**]の基準を選択すると、あらゆる発行先のデジタル証明書で署名されたアプリケーションの起動が、作成したルールにより管理されます。

ファイルの署名に使用されたデジタル証明書の発行先は、[**ルール有効化の条件**]セクションの上にある[**ファイルのプロパティからルール有効化の条件を設定**]を使用して選択されたファイルのプロパティからのみ指定できます。

既定では、このチェックボックスはオフです。

- **サムプリントを使用**

ルール有効化の条件として、デジタル証明書の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、デジタル証明書の指定されたサムプリントが、ルール有効化の条件として使用されます。作成したルールでは、指定のサムプリントのデジタル証明書で署名されたアプリケーションの起動が制御されます。

このチェックボックスをオフにすると、ルール有効化の条件にデジタル証明書のサムプリントは使用されません。[**デジタル証明書**]の基準を選択すると、あらゆるサムプリントのデジタル証明書を使用して署名されたアプリケーションの起動が制御されます。

ファイルの署名に使用されたデジタル証明書のサムプリントは、[**ルール有効化の条件**]セクションの上にある[**ファイルのプロパティからルール有効化の条件を設定**]を使用して選択されたファイルのプロパティからのみ指定できます。

既定では、このチェックボックスはオフです。

- **SHA256 ハッシュ**

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有効化の条件として指定されます。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。

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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

既定では、このオプションはオフです。

- **ファイルのパス**

チェックボックスがオンの場合、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

既定では、このチェックボックスはオフです。

XXV. [**OK**]をクリックします。

XXVi. 必要に応じて、手順(i)～(iv)を繰り返し、除外を追加します。

5. [**ルール設定**]ウィンドウで[**OK**]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**]ウィンドウのリストに、作成されたルールが表示されます。

「既定で許可」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、「既定で許可」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。「既定で許可」モードは、以下で記載している設定の許可ルールを追加することによって有効にできます。「既定で許可」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。

► 「既定で許可」ルールを追加するには:

1. [**アプリケーション起動コントロールルール**]のウィンドウを開きます。
2. [**追加**]をクリックします。
3. 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。
4. [**名前**]で、ルールの名前を入力します。
5. [**種別**]ドロップダウンリストで、**許可**ルールを選択します。
6. [**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。
7. [**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。
8. 次のマスクを入力します: ?:¥
9. [**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。

アプリケーション起動コントロールタスク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タスクイベントから生成された許可ルールを含む設定ファイルを作成するには:

1. アプリケーション起動コントロールタスクを**統計のみ**モードで開始し(370 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モードの選択」を参照)、保護対象サーバーでのすべてのアプリケーション起動に関する情報を実行ログに記録します。
2. **統計のみ**モードで実行しているタスクの完了後、[**アプリケーション起動コントロール**]フォルダーの詳細ペインの[**管理**]セクションにある[**実行ログを開く**]をクリックして、実行ログを開きます。
3. [**ログ**]ウィンドウで、[**イベントに基づいてルールを作成する**]をクリックします。

統計のみモードのアプリケーション起動コントロールタスクで発生したイベントに基づくルールリストを含んだ XML 設定ファイルが作成されます。アプリケーション起動コントロールタスクで、このルールリストを適用できます(380 ページのセクション「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」を参照)。

記録されたタスクイベントから作成されたルールリストを適用する前に、リストを確認して手動で処理し、指定したルールにより重要なファイル(たとえば、システムファイルなど)の実行が許可されていることを確認してください。

すべてのタスクイベントが、タスクモードに関係なく実行ログに記録されます。**処理を実行**モードでタスクが実行中に作成されたログに基づいたルールリストが含まれる設定ファイルを作成できます。タスクが適切に動作するには、タスクが[**処理を実行**]モードで実行される前に最終的なルールのリストを作成しておく必要があります。そのため、緊急の場合を除いてこのシナリオは推奨されません。

アプリケーション起動コントロールルールのエクスポート

► **アプリケーション起動コントロールルールを設定ファイルにエクスポートするには:**

1. [**アプリケーション起動コントロールルール**]のウィンドウを開きます。
2. [**ファイルにエクスポート**]をクリックします。

   Microsoft Windows 標準のウィンドウが表示されます。
3. 表示されたウィンドウで、ルールをエクスポートするファイルを指定します。ファイルが存在しない場合は作成されます。指定した名前のファイルがすでに存在する場合、ルールをエクスポートするとファイルの内容が上書きされます。
4. [**保存**]をクリックします。

ルール設定が指定されたファイルにエクスポートされます。

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をインポートするには:**

1. [**アプリケーション起動コントロールルール**]のウィンドウを開きます。
2. [**追加**]をクリックします。
3. 表示されるコンテキストメニューで、[**XML ファイルからルールをインポート**]を選択します。
4. インポートされるルールを追加する方法を指定します。そのためには、[**XML ファイルからルールをインポート**]のコンテキストメニューからいずれかのオプションを選択します:
   - **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他のルールと異なる場合にルールが追加されます。

   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. [**ファイルを開く**]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を含む XML ファイルを選択します。
6. [**開く**]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**]ウィンドウのリストに、インポートされたルールが表示されます。

アプリケーション起動コントロールルールの削除

► **アプリケーション起動コントロールルールを削除するには:**

1. [**アプリケーション起動コントロールルール**]のウィンドウを開きます。
2. リストで削除するルールを 1 つ以上選択します。

3. [**選択項目の削除**]をクリックします。
4. [**保存**]をクリックします。

選択したアプリケーション起動コントロールルールが削除されます。

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を編集するには:

1. **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[**タスクの設定**]ウィンドウを開きます(369 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ルールの自動作成タスクの設定ウィンドウ**」を参照)。
2. 次の設定を指定します:
   - [**全般**]タブ:
     - **ルール名の接頭辞**を指定します。

       接頭辞とはルール名の最初の部分です。ルール名の残りの部分は、起動が許可されるオブジェクト名から作成されます。

       既定の接頭辞は、Kaspersky Security for Windows Server がインストールされているサーバーの名前です。許可ルールの名前の接頭辞を変更できます。
     - 許可ルールの適用範囲を設定します(382 ページのセクション「タスクの適用範囲の制限」を参照)。
   - [**処理**]タブで、Kaspersky Security for Windows Server が実行する処理を指定します:
     - 許可ルールの作成時(382 ページのセクション「ルールの自動作成中に実行する処理」を参照)。
     - タスクの完了時(383 ページのセクション「ルールの自動作成の完了時に実行する処理」を参照)。
   - [**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの開始スケジュールを設定します(「タスク開始スケジュールの設定」(156 ページ)を参照)。
   - [**実行用アカウント**]タブで、アカウント権限を使用して起動するタスクを設定します(「タスクを実行するユーザーアカウントの指定」(158 ページ)を参照)。
3. [**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、システム監査ログに保存されます。

このセクションの内容

タスクの適用範囲の制限

► **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範囲を制限するには:**

1. **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[**タスクの設定**]ウィンドウを開きます(369 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ルールの自動作成タスクの設定ウィンドウ**」を参照)。
2. 次のタスクの設定を指定します:
   - **実行中のアプリケーションに基づいて許可ルールを作成する**

     このチェックボックスでは、すでに実行中のアプリケーションに対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を有効または無効にします。ネットワーク全体または一定の範囲内で共通する許可ルールを作成するためのベースとなるようなアプリケーションの参照セットがサーバーにある場合、このオプションをオンにしてください。

     このチェックボックスをオンにすると、アプリケーション起動コントロールの許可ルールが実行中のアプリケーションに基づいて生成されます。

     このチェックボックスをオフにすると、許可ルールの生成時に実行中のアプリケーションは考慮されません。

     既定では、このチェックボックスはオンです。

     このチェックボックスは、[**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**]テーブルでフォルダーが選択されていない場合はオフにできません。

   - **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**

     タスクの対象フォルダーと、アプリケーション起動コントロールルールの作成時に考慮する実行ファイルの種別を指定できます。指定のフォルダーに格納されている指定の種別のファイルに対して、許可ルールが生成されます。
3. [**OK**]をクリックします。

指定された設定が保存されます。

ルールの自動作成中に実行する処理

► **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実行時に Kaspersky Security for Windows Server が行う処理を設定するには:**

1. **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[**タスクの設定**]ウィンドウを開きます(369 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ルールの自動作成タスクの設定ウィンドウ**」を参照)。
2. [**オプション**]タブを開きます。
3. [**許可ルールの作成**]セクションで、次の設定を行います:
   - **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有効化の条件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。

     既定では、このオプションはオンです。

   - **デジタル証明書の発行先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発行先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発行先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を最も正確に適用できます。

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です。

  - **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有効化の条件として指定されます。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。

  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必要がある場合に推奨され、SHA256 チェックサムが各ファイルに固有の識別子として使用されます。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、ルールの適用範囲を 1 つのファイルに絞り込むことができます。

  既定では、このオプションはオフです。

- **次の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です。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制御します。

  既定の選択項目は[**Everyone**]です。

4. [**OK**]をクリックします。

指定された設定が保存されます。

ルールの自動作成の完了時に実行する処理

► 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完了後に Kaspersky Security for Windows Server が行う処理を設定するには:

1. **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[**タスクの設定**]ウィンドウを開きます(369 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ルールの自動作成タスクの設定ウィンドウ**」を参照)。

2. [**オプション**]タブを開きます。
3. [**タスク完了後**]セクションで、次の設定を行います:
   - **アプリケーション起動コントロールルールのリストに許可ルールを追加する**

     新しく作成された許可ルールのアプリケーション起動コントロールルールのリストへの追加を有効または無効にします。アプリケーション起動コントロールルールのリストは、[アプリケーション起動コントロール]フォルダーの詳細ペインの[**アプリケーション起動コントロールルール**]をクリックすると表示されます。

     このチェックボックスをオンにすると、選択した追加方法に基づいて、アプリケーション起動コントロールルールの自動作成タスクによ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。

     このチェックボックスをオフにすると、新しく作成された許可ルールは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せん。作成されたルールは、ファイルにエクスポートされるだけです。

     既定では、このチェックボックスはオンです。
   - **追加方法**

     このドロップダウンリストは、新しく作成された許可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追加する方法の指定に使用されます。

     - **既存のルールに追加する**: ルールが既存のルールのリストに追加されます。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**: ルールがリストの既存のルールを置き換えます。
     - **既存のルールとマージする**: ルールが既存のルールのリストに追加されます。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他のルールと異なる場合にルールが追加されます。

     既定では、[**既存のルールとマージする**]方法が選択されます。
   - **許可ルールをファイルにエクスポートする**
   - **ファイル名にコンピューターの詳細を追加する**

     アプリケーション起動コントロールの許可ルールをエクスポートするファイルの名前に対し、保護対象サーバーに関する情報の追加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、保護対象サーバーの名前、およびファイルの作成日時をエクスポートするファイルの名前に追加します。

     このチェックボックスをオフにすると、保護対象のサーバーに関する情報をエクスポートするファイルの名前に追加しません。

     既定では、このチェックボックスはオンです。
4. [**OK**]をクリックします。

指定された設定が保存されます。

デバイスコントロール

このセクションでは、デバイスコントロールタスクおよびタスクを設定する手順について説明します。

この章の内容

デバイスコントロールタスクについて

Kaspersky Security 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 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/DVD 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 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 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 の通知の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。

本製品は、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を付与します:

- **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、1 つ以上のルールに対して**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 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 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:

- **処理を実行**:Kaspersky Security 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、「既定で拒否」の原則と個別に指定した許可ルールに従って、各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[**処理を実行**]モードで実行される前に、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た場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、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「既定で拒否」の原則は適用されません。

- **統計のみ**:Kaspersky Security 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ブロックに関する情報を基にしてルールを作成する際に適用できます(404 ページのセクション「デバイスコントロールタスクイベントに基づいたルールリストの入力」を参照)。

デバイスコントロールルールについて

このルールは、現在保護対象サーバーに接続されているデバイスまたは接続されていたことがあるデバイスごとに一意に作成されます。ただし、このデバイスに関する情報がシステムレジストリに格納されている場合です。

デバイスコントロールの許可ルールを作成するには、次の処理を実行します:

- デバイスコントロールルールの自動作成タスクの適用(「デバイスコントロールルールの自動作成タスクについて」(389 ページ)を参照)。
- デバイスコントロールタスクの統計のみモードでの実行(「デバイスコントロールタスクイベントに基づいたルールリストの入力」(404 ページ)を参照)。
- 以前接続されていたデバイスに関するシステム情報の適用(「1 台以上の外部デバイスへの許可ルールの追加」(404 ページ)を参照)。
- すでに指定されているルールの適用範囲の拡張(「デバイスコントロールルールの適用範囲の拡張」(406 ページ)を参照)。

Kaspersky Security for Windows Server でサポートされるデバイスコントロールルールの最大数は 3072 です。

デバイスコントロールルールの説明を以下に記載します。

ルールの種別

ルールの種別は常に[**許可**]です。既定では、デバイスが許可ルールの適用範囲に含まれていない場合、デバイスコントロールタスクにより、すべてのフラッシュドライブおよびその他の外部デバイスの接続がブロックされます。

ルール有効化の条件とルールの適用範囲

デバイスコントロールルールでは、**デバイスインスタンスパス**に基づいてフラッシュドライブおよびその他の外部デバイスが識別されます。デバイスインスタンスパスは、デバイスが接続されて大容量記憶デバイスまたは CD / DVD ドライブ(たとえば、IDE または SCSI)として登録されたときに、システムによってデバイスに割り当てられる一意の基準です。

> Kaspersky Security for Windows Server では、接続に使用されているバスには関係なく、CD / DVD ドライブの接続が制御されます。このようなデバイスを USB 経由でマウントする際には、オペレーティングシステムにより、大容量記憶デバイスおよび CD / DVD ドライブ(たとえば、IDE または SCSI)という 2 つのデバイスインスタンスのパス値が登録されます。このようなデバイスを正常に接続するには、インスタンスの各パス値に対して許可ルールを設定する必要があります。

Kaspersky Security for Windows Server ではデバイスインスタンスパスが自動的に定義され、得られた値が次の要素に構文解析されます:

- デバイスの製造元(VID)
- デバイスコントローラーの種別(PID)
- デバイスのシリアルナンバー

デバイスインスタンスパスは手動では設定できません。許可ルールの有効化の条件では、ルールの適用範囲が定義されます。既定では、新しく作成されたルールの適用範囲には、Kaspersky Security for Windows Server がルール作成の基準としてプロパティを参照した初期デバイスが 1 台含まれています。作成したルールの値を設定するには、ルールの適用範囲を拡張するマスクを使用します(「デバイスコントロールルールの適用範囲の拡張」(406 ページ)を参照)。

初期デバイス値

Kaspersky Security for Windows Server で許可ルールの作成に使用され、接続されているデバイスごとに Windows デバイスマネージャーに表示されるデバイスプロパティ。

初期デバイス値には次の情報が含まれています:

- **デバイスインスタンスパス**:Kaspersky Security for Windows Server は、このプロパティに基づいてルール有効化の条件を定義し、次のフィールドに記入します:[**製造元(VID)**]、[**コントローラーの種別(PID)**]、[**ルールのプロパティ**]ウィンドウの[**ルールの適用範囲**]セクションにある[**シリアルナンバー**]。
- **説明的名称**:製造元がデバイスのプロパティで設定するデバイスの説明的名称。

Kaspersky Security for Windows Server では、ルールの作成時に初期デバイス値が自動的に定義されます。あとでこれらの値を使用して、ルール作成の基本として使用されたデバイスを認識できます。初期デバイス値は編集できません。
説明

作成したデバイスコントロールルールごとに、[**説明**]で情報を追加できます。たとえば、接続されているフラッシュドライブの名前を記録したり、その所有者を定義したりできます。この説明は、[**デバイスコントロールルール**]ウィンドウの対応する図に表示されます。

> 説明と初期デバイス値はルール適用での使用は許可されず、ユーザーがデバイスを簡単に識別する目的のみで規定されます。

デバイスコントロールルールのリストの入力について

デバイスコントロール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の実行時に自動的に作成された XML ファイルからデバイスコントロールの許可ルールをインポートできます。

既定では、Kaspersky Security for Windows Server ではフラッシュドライブおよびその他の外部デバイスが、指定したデバイスコント

ロールルールの適用範囲に含まれていない場合、それらのドライブやデバイスの接続が制限されます。

表 57. デバイスコントロールルールのリスト作成の対象とシナリオ

ルール作成シナリオ	対象
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タスクの初回開始前に、以前接続されていた信頼するデバイスに許可ルールを追加します。 • 保護対象サーバーネットワークで信頼されるデバイスのルールリストを作成します。
システムデータに基づいてルールを作成	新しく接続された 1 台以上のデバイスに許可ルールを追加します。
統計のみモードのデバイスコントロールタスク	大量の信頼するデバイスの許可ルールを生成します。

デバイスコントロールルールの自動作成タスクの使用

デバイスコントロールルールの自動作成タスクの完了時に作成された XML ファイルには、システムレジストリにデータが格納されているフラッシュドライブおよびその他の外部デバイスの許可ルールが含まれています。

タスクの実行時に、Kaspersky Security for Windows Server では保護対象サーバーに以前接続されていたことがあるまたは現在接続されているすべての大容量記憶デバイスに関するシステムデータが受信され、検知されたデバイスのシステムデータに基づいて許可ルールリストが作成されます。アプリケーションではタスクの完了時に、タスク設定で指定されたパスによって場所が決められたフォルダー内に XML ファイルが作成されます。作成したルールに対して、デバイスコントロールタスクのルールのリストへの自動インポートを設定できます。

デバイスコントロールタスクの初回開始前に許可ルールリストを作成する場合はこのシナリオを使用し、作成した許可ルールにより保護対象サーバーで使用されているすべての信頼する外部デバイスに対応するようにしてください。

接続されているすべてのデバイスに関するシステムデータの使用

タスクの実行時に、Kaspersky Security for Windows Server では保護対象サーバーに以前接続されていたことがあるまたは現在接続されているすべての外部デバイスに関するシステムデータが受信され、[**システム情報に基づいてルールを生成する**]ウィンドウのリストに検知されたデバイスが表示されます。

Kaspersky Security for Windows Server では、検知された各デバイスの製造元(VID)、コントローラーの種別(PID)、説明的名称、シリアルナンバー、およびデバイスインスタンスパスが構文解析されます。システムにデータが格納されている大容量記憶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リストに新しく作成されたルールを追加できます。

少数の新しい大容量記憶デバイスを信頼する必要がある際に、すでに指定されているルールリストを更新する場合はこのシナリオを使用してください。

Kaspersky Security 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。MTP 接続したモバイルデバイスの許可ルールは生成できません。

統計のみモードのデバイスコントロールタスクの使用

統計のみモードのデバイスコントロールタスクの完了時に受信した XML ファイルは、実行ログに基づいて作成されます。

タスクの実行時に、Kaspersky Security for Windows Server では保護対象サーバーに接続されたすべてのフラッシュドライブおよびその他の大容量記憶デバイスに関する情報が記録されます。タスクのイベントに基づいて許可ルールを作成し、XML ファイルにエクスポートすることができます。**統計のみ**モードでタスクを開始する前にタスク実行期間を設定し、指定した期間中に保護対象サーバーにすべての使用可能なデバイスが接続されるようにしてください。

大量の新しい外部デバイスを許可する必要があり、すでに生成されているルールリストを更新する場合は、このシナリオを使用してください。

テンプレートマシンでこのシナリオに従ってルールリストを作成する場合は、Kaspersky Security Center でデバイスコントロールタスクを設定する際に、作成された許可ルールリストを適用できます。この方法により、保護対象ネットワークに含まれているすべてのコンピュー

ターでテンプレートマシンに接続されている外部デバイスの使用を許可できます。

デバイスコントロールルールの自動作成タスクについて

デバイスコントロールルールの自動作成では、保護対象サーバーに以前接続されていたことがあるすべての外部デバイスに関するシステムデータに基づいて、接続されているフラッシュドライブおよびその他の大容量記憶デバイスの許可ルールのリストを自動的に作成できます。

Kaspersky Security 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。MTP 接続したモバイルデバイスの許可ルールは生成できません。

デバイスコントロールルールの自動作成設定に応じて、タスクの完了時に、検知されたすべての外部デバイスの許可ルールリストを含む XML 設定ファイルが作成されるかあるいはデバイスコントロールタスクに作成されたルールが直接追加されます。自動的に生成された許可ルールでデバイスが許可されます。

タスクで作成されて追加されたルールは、[**デバイスコントロールルール**]ウィンドウに表示されます。

デバイスコントロールルールの作成のシナリオ

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記憶デバイスに関する 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(394 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」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を使用:ネットワーク内のすべてのサーバ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記憶デバイス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。
- [**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サーバーのシステムによって登録されている、すべての大容量記憶デバイス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ルール**]ウィンドウおよびデバイスコントロールルールの自動作成タスクの設定で、[**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 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。

デバイスコントロールの既定のタスク設定

デバイスコントロールタスクでは、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 58. 既定のデバイスコントロールタスクの設定

設定	既定値	説明
タスクモード	**統計のみ**	指定したルールに従ってブロックまたは許可された外部デバイスに関するタスク実行ログ情報。外部デバイスは実際にはブロックされません。 外部デバイスの使用を実際にブロックするには、サーバー保護として**処理を実行**モードを選択します。
デバイスコントロールタスクを実行していない時にすべての大容量ストレージデバイスの使用を許可する	オフ	Kaspersky Security for Windows Server ではデバイスコントロールタスクの状態に関係なく、外部デバイスの使用がブロックされます。これにより、外部デバイスとファイルを交換する際に発生するコンピューターのセキュリティ脅威に対して、最大の保護レベルが実現されます。 デバイスコントロールタスクが実行されていないときに、Kaspersky Security for Windows Server がすべての外部デバイスの使用を許可するように設定を編集できます。
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。	デバイスコントロールタスクは、Kaspersky Security for Windows Server の起動時に自動的には開始されません。 この場合、タスク開始スケジュールを設定できます。

表 59. デバイスコントロールルールの自動作成タスクの既定の設定

設定	既定値	説明
タスクモード	**過去に接続されたすべての大容量ストレージについてシステムデータを考慮する**	
タスク完了後の処理	処理は実行されません。	ルールを結合しないで既存のルールに追加して重複したルールを削除しないようにしたり、既存のルールを新しい許可ルールに置き換えたりすることができます。許可ルールのファイルへのエクスポートを設定することも可能です。
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。	デバイスコントロールルールの自動作成タスクは、Kaspersky Security for Windows Server の起動時に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。

管理プラグインからデバイスコントロールを管理する

このセクションでは、管理プラグインインターフェイスを操作し、サーバーのグループに対して Kaspersky Security Center を介してルールのリストを作成することによって、ネットワーク上のすべてのサーバーへの大容量記憶デバイスの接続を管理する方法について説明し

ます。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

デバイスコントロールタスクのポリシーの設定ウィンドウ

► Kaspersky Security Center のポリシーからデバイスコントロールタスクの設定を開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**ローカルアクティビティの管理**]セクションを選択します。
6. [**デバイスコントロール**]サブセクションの[**設定**]をクリックします。
   [**デバイスコントロール**]ウィンドウが開きます。
7. 必要に応じてポリシーを設定します。

デバイスコントロールルールのリスト

► **Kaspersky Security Center からデバイスコントロールルールのリストを開くには:**

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**ローカルアクティビティの管理**]セクションを選択します。
6. [**デバイスコントロール**]サブセクションの[**設定**]をクリックします。
   [**デバイスコントロール**]ウィンドウが開きます。
7. [**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。
8. 必要に応じてポリシーを設定します。

デバイスコントロールルールの自動作成タスクのウィザードとプロパティウィンドウ

► **デバイスコントロールルールの自動作成タスクの作成を初期化するには:**

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。
2. タスクを設定する管理グループを選択します。
3. [**タスク**]タブを選択します。
4. [**タスクの作成**]をクリックします。
   [**新規タスクウィザード**]ウィンドウが開きます。
5. [**デバイスコントロールルールの自動作成**]タスクを選択します。
6. [**次へ**]をクリックします。
   [**設定**]ウィンドウが開きます。

► **既存のデバイスコントロールルールの自動作成タスクの設定を編集するには:**

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。
2. タスクを設定する管理グループを選択します。
3. [**タスク**]タブを選択します。
4. Kaspersky Security Center タスクのリストで、タスク名をダブルクリックします。
   [**デバイスコントロールルールの自動作成**]ウィンドウが開きます。

タスクの設定に関する詳細は、セクション「デバイスコントロールルールの自動作成タスクの設定」を参照してください。

デバイスコントロールタスクの設定

► デバイスコントロールタスクの設定を行うには:

1. [**デバイスコントロール**]ウィンドウを開きます(391 ページのセクション「デバイスコントロールタスクのポリシーの設定ウィンドウ」を参照)。
2. [**全般**]タブで、次のタスク設定を行います:
   - [**タスクモード**]セクションで、次のいずれかのタスクモードを選択します:
     - **処理を実行**:

       Kaspersky Security 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、「既定で拒否」の原則と個別に指定した許可ルールに従って、各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[処理を実行]モードで実行される前に、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た場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、コンピュータ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「既定で拒否」の原則は適用されません。

     - **統計のみ**:

       Kaspersky Security 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。

   - [**デバイスコントロールタスクを実行していない時にすべての大容量ストレージデバイスの使用を許可する**]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、デバイスコントロールタスクが実行されていないときに大容量記憶デバイスの使用が許可またはブロックされます。

     このチェックボックスがオンにされており、デバイスコントロールタスクが実行されていない場合、保護対象サーバー上のすべての大容量記憶デバイスの使用が許可されます。

     このチェックボックスがオフにされており、デバイスコントロールタスクが実行されていない、あるいは Kaspersky Security サービスがオフの場合、保護対象サーバー上の信頼しない大容量記憶デバイスの使用がブロックされます。これにより、外部デバイスとファイルを交換する際に発生するコンピューターのセキュリティ脅威に対して、最大の保護レベルが実現されます。

     既定では、このチェックボックスはオフです。

3. [**ルールリスト**]をクリックして、デバイスコントロールルールのリストを編集します(395 ページのセクション「デバイスコントロールルールの Kaspersky Security Center からの設定」を参照)。
4. 必要に応じて、[**タスク管理**]タブでタスク開始スケジュールを設定します。
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、システム監査ログに保存されます。

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

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には、次の方法で行います:

- 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を使用:

  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ストレージ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ストレージデバイスが考慮されます。グループタスク完了時に、Kaspersky Security 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タスク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、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タスクをルールの適用時に処理を実行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コントロール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 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、ネットワーク内のすべてのサーバ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[**管理サーバー**]フォルダーの[**イベント**]タブにあります。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、大容量記憶デバイスの統一リストを作成します。

  すべての大容量ストレージ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記憶デバイス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。

- 接続された大容量記憶デバイスに関するシステムデータをベースにする(デバイスコントロールタスクの設定内の[**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 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記憶デバイス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サーバーにある、少数の信頼する新しい大容量ストレージ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をベースにする(**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 for Windows Server は現在接続しているデバイスのみを対象とする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 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。

デバイスコントロールルールの自動作成タスクの設定

► **デバイスコントロールルールの自動作成タスクを設定するには:**

1. **デバイスコントロールルールの自動作成**のプロパティを開きます(392 ページのセクション「**デバイスコントロールルールの自動作成タスクのウィザードとプロパティウィンドウ**」を参照)。
2. [**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 のヘルプ**を参照してください。
3. [**設定**]セクションでは、次の設定を行うことができます:
   - 処理モードを[過去に接続されたすべての大容量ストレージについてシステムデータを考慮する]と[現在接続している大容量ストレージだけを考慮する]から選択します。
   - Kaspersky Security for Windows Server がタスク完了時に作成する許可ルールリストで、設定ファイルを設定します。
4. [**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)。
5. [**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。
6. 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 のヘルプ**を参照してください。
7. 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。

デバイスコントロールルールの Kaspersky Security Center からの設定

さまざまな条件に基づいてルールのリストを生成する方法、またはデバイスコントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

このセクションの内容

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タスクの[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指定するには:

1. 必要に応じて、信頼する新しい大容量記憶デバイスを、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に接続します。
2. [**デバイスコントロールルール**]ウィンドウを開きます(392 ページのセクション「デバイスコントロールルールのリスト」を参照)。
3. [**追加**]をクリックし、表示されたコンテキストメニューで、[**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**]ウィンドウのデバイスリストで、デバイスを選択します。
   - [**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。
4. [**デバイス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。

デバイスコントロールタスク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反映されます。

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タスクの[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指定するには:

1. [**デバイスコントロールルール**]ウィンドウを開きます(392 ページのセクション「デバイスコントロールルールのリスト」を参照)。
2. [**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。
3. 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。
4. [**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。
5. [**デバイス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。

デバイスコントロールタスク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反映されます。

ブロックされたデバイスに関する Kaspersky Security Center のレポート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ブロックされたデバイスの接続のデータをインポートできます(393 ページのセクション「デバイスコントロールタスクの設定」を参照)。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を確認することができます。

► ブロック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に対してデバイス接続のための許可ルールを指定するには:

1. ポリシーのプロパティの[**イベントの設定**]セクションで、次の内容を確認します:
   - 重要度が[**緊急イベント**]のイベントに対して、[**大容量ストレージの制限**]イベントの実行ログを保存する期間が、**統計のみ**モードのタスクの実行で計画された期間を超えている(既定値は 30 日)。
   - 重要度が[**警告**]のイベントに対して、[**統計のみ:信頼しない大容量ストレージが検出されました**]イベントの実行ログを保存する期間が、**統計のみ**モードのタスクの実行で予定された期間を超えている(既定値は 30 日)。

   イベントの保管期間が経過すると、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。
2. **統計のみ**モードのデバイスコントロールタスクを開始します。Kaspersky Security Center の[**管理サーバー**]フォルダーの作業領域で、[**イベント**]タブを選択します。[**抽出の作成**]をクリックし、[**信頼しない大容量ストレージが検出されました**]の基準に基づいて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]ドロップダウンリストで、[**イベントをファイルにエクスポート**]をクリックして、制限された接続のレポートを 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。
3. 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タスクにインポートします:
   a. [**デバイスコントロールルール**]ウィンドウを開きます(392 ページのセクション「デバイスコントロールルールのリスト」を参照)。
   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他のルールと異なる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**]ウィンドウで、[**保存**]をクリックします。

4. [**デバイスコントロール**]ウィンドウで、[**OK**]をクリックします。

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。

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:

1. [**新規タスクウィザード**]で[**設定**]ウィンドウを開きます(392 ページのセクション「**デバイスコントロールルールの自動作成タスクのウィザードとプロパティウィンドウ**」を参照)。
2. 以下を設定します:
   - [**モード**]セクション:
     - **過去に接続されたすべての大容量ストレージについてシステムデータを考慮する**
     - **現在接続している大容量ストレージだけを考慮する**
   - [**タスク完了後**]セクション:
     - **デバイスコントロールルールのリストに許可ルールを追加する**

       新しく作成された許可ルールのデバイスコントロールルールのリストへの追加を有効または無効にします。デバイスコントロールルールのリストは、[**デバイスコントロール**]フォルダーの詳細ペインの[**デバイスコントロールルール**]をクリックすると表示されます。

       このチェックボックスをオンにすると、選択した追加方法に基づいて、デバイスコントロールルールの自動作成タスクによ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。

       このチェックボックスをオフにすると、新しく作成された許可ルールはデバイスコントロールルールのリストに追加されません。作成されたルールは、ファイルにエクスポートされるだけです。

       既定では、このチェックボックスはオフです。

     - **追加方法**

       このドロップダウンリストは、新しく作成された許可ルールをデバイスコントロールルールのリストに追加する方法の指定に使用されます。

       - **既存のルールに追加する**:ルールが既存のルールのリストに追加されます。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**:ルールがリストの既存のルールを置き換えます。
       - **既存のルールとマージする**:ルールが既存のルールのリストに追加されます。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他のルールと異なる場合にルールが追加されます。

       既定では、[**既存のルールとマージする**]方法が選択されます。

     - **許可ルールをファイルにエクスポートする**

       作成されたデバイスコントロールの許可ルールのファイルへのエクスポート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、デバイスコントロールルールの自動作成タスクの終了時に、下にあるフィールドで指定されたファイルに許可ルールがエクスポートされます。

このチェックボックスをオフにすると、デバイスコントロールルールの自動作成タスクの終了時に、作成された許可ルールはファイルにエクスポートされません。代わりに、デバイスコントロールルールのリストにのみ追加されます。

既定では、このチェックボックスはオフです。

- **ファイル名にコンピューターの詳細を追加する**

  デバイスコントロールの許可ルールをエクスポートするファイルの名前に対し、保護対象サーバーに関する情報の追加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、保護対象サーバーの名前、およびファイルの作成日時をエクスポートするファイルの名前に追加します。

  このチェックボックスをオフにすると、保護対象のサーバーに関する情報をエクスポートするファイルの名前に追加しません。

  既定では、このチェックボックスはオンです。

3. [**次へ**]をクリックします。
4. [**スケジュール**]ウィンドウで、タスクの開始スケジュールを設定します。
5. [**次へ**]をクリックします。
6. [**タスクを実行するアカウントの選択**]ウィンドウで、使用するアカウントを指定します。
7. [**次へ**]をクリックします。
8. タスク名を指定します。
9. [**次へ**]をクリックします。

   タスク名は 100 文字以内にする必要があり、次の記号は使用できません:

   " * < > & ¥ : |

   [**タスクの作成を終了**]ウィンドウが開きます。
10. オプションで[**ウィザード完了後にタスクを実行する**]をオンにすると、ウィザードの終了後にタスクを実行することができます。
11. [**完了**]をクリックしてタスクの作成を終了します。
12. 設定中のサーバーグループの作業領域にある、[**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タスクを選択します。
13. [**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コントロールルールを作成することをお勧めします。

デバイスコントロールルールのリストに生成されたルールを追加する

► **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するには:**

1. [**デバイスコントロールルール**]ウィンドウを開きます(392 ページのセクション「デバイスコントロールルールのリスト」を参照)。
2. [**追加**]をクリックします。
3. [**追加**]をクリックし、コンテキストメニューで[**XML ファイルからルールをインポート**]を選択します。
4. 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他のルールと異なる場合にルールが追加されます。
5. 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。
6. [**ファイルを開く**]をクリックします。

   XML ファイルから生成されたすべてのルールは、選択した方法に応じてリストに追加されます。
7. [**デバイス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。
8. 作成したデバイスコントロールルールを適用する場合、ポリシー設定の[**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[**処理を実行**]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。

アプリケーションコンソールからデバイスコントロールを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのタスクの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

デバイスコントロールタスクの設定ウィンドウ

► アプリケーションコンソールからデバイスコントロールタスクの設定を開くには:

1. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**デバイスコントロール**]サブフォルダーを選択します。
3. [**デバイスコントロール**]サブフォルダーの詳細ペインで、[**プロパティ**]をクリックします。
   [**タスクの設定**]ウィンドウが表示されます。
4. 必要に応じてタスクを設定します。

デバイスコントロールルールの設定ウィンドウ

► アプリケーションコンソールからデバイスコントロールルールのリストを開くには:

1. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**デバイスコントロール**]サブフォルダーを選択します。
3. [**デバイスコントロール**]フォルダーの詳細ペインで、[**デバイスコントロールルール**]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。
4. 必要に応じてルールリストを設定します。

デバイスコントロールルールの自動作成タスクの設定ウィンドウ

► デバイスコントロールルールの自動作成タスクを設定するには:

1. アプリケーションコンソールツリーで、[**ルールの自動生成**]フォルダーを展開します。

2. [**デバイスコントロールルールの自動作成**]サブフォルダーを選択します。
3. [**デバイスコントロールルールの自動作成**]サブフォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. 必要に応じてタスクを設定します。

デバイスコントロールタスクの設定

► デバイスコントロールタスクの設定を行うには:

1. [**タスクの設定**]ウィンドウを開きます(401 ページのセクション「デバイスコントロールタスクの設定ウィンドウ」を参照)。
2. [**全般**]タブで、次のタスク設定を行います:
   - [**タスクモード**]セクションで、次のいずれかのタスクモードを選択します:
     - **処理を実行**:

       Kaspersky Security 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、「既定で拒否」の原則と個別に指定した許可ルールに従って、各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[処理を実行]モードで実行される前に、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た場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、コンピュータ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「既定で拒否」の原則は適用されません。
     - **統計のみ**:

       Kaspersky Security 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。
   - [**デバイスコントロールタスクを実行していない時にすべての大容量ストレージデバイスの使用を許可する**]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、デバイスコントロールタスクが実行されていないときに大容量記憶デバイスの使用が許可またはブロックされます。

     このチェックボックスがオンにされており、デバイスコントロールタスクが実行されていない場合、保護対象サーバー上のすべての大容量記憶デバイスの使用が許可されます。

     このチェックボックスがオフにされており、デバイスコントロールタスクが実行されていない、あるいは Kaspersky Security サービスがオフの場合、保護対象サーバー上の信頼しない大容量記憶デバイスの使用がブロックされます。これにより、外部デバイスとファイルを交換する際に発生するコンピューターのセキュリティ脅威に対して、最大の保護レベルが実現されます。

     既定では、このチェックボックスはオフです。
3. 必要に応じて、[**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの起動スケジュールを設定します(「タスク開始スケジュールの設定」(156 ページ)を参照)。
4. デバイスコントロールルールのリストを編集するには(387 ページのセクション「デバイスコントロールルールのリストの入力について」を参照)、[**デバイスコントロール**]フォルダーの詳細ペインの下部にある[**デバイスコントロールルール**]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、システム監査ログに保存されます。

デバイスコントロールルールの設定

ルールのリストを生成やインポート / エクスポートする方法、またはデバイスコントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

このセクションの内容

XML ファイルからのデバイスコントロールルールのインポート

► デバイスコントロールルールをインポートするには、次の手順を実行します:

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「**デバイスコントロールルールの設定ウィンドウ**」を参照)。
2. [**追加**]をクリックします。
3. 表示されるコンテキストメニューで、[**XML ファイルからルールをインポート**]を選択します。
4. インポートされるルールを追加する方法を指定します。そのためには、[**XML ファイルからルールをインポート**]のコンテキストメニューからいずれかのオプションを選択します:
   - **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他のルールと異なる場合にルールが追加されます。

   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. [**ファイルを開く**]ウィンドウで、[デバイスコントロールルール]の設定を含む XML ファイルを選択します。
6. [**開く**]をクリックします。

[**デバイスコントロールルール**]ウィンドウのリストに、インポートされたルールが表示されます。

デバイスコントロールタスクイベントに基づいたルールリストの入力

► **デバイスコントロールルールのリストが含まれている設定ファイルを、デバイスコントロールタスクイベントに基づいて作成するには:**

1. デバイスコントロールタスクを**統計のみ**モードで開始し(「**デバイスコントロールタスクの設定**」(402 ページ)を参照)、保護対象サーバーに接続されているフラッシュドライブおよびその他の外部デバイスのすべてのイベントを記録します。
2. **統計のみ**モードで実行したタスクの完了後、[**デバイスコントロール**]フォルダーの詳細ペインの[**管理**]セクションにある[**実行ログを開く**]をクリックして、実行ログを開きます。
3. [**ログ**]ウィンドウで、[**イベントに基づいてルールを作成する**]をクリックします。

統計のみモードのデバイスコントロールタスクで発生したイベントに基づくルールリストを含んだ XML 設定ファイルが作成されます。このリストはデバイスコントロールタスクで適用できます(「XML ファイルからのデバイスコントロールルールのインポート」(403 ページ)を参照)。

タスクイベントに基づいて作成されたルールリストを適用する前に、このルールリストを確認してから手動で処理し、指定されたルールで許可された信頼しないデバイスが存在しないことを確認してください。

アプリケーションでは、タスクイベントにより XML ファイルをルールリストに変換する際に、登録されたすべてのイベントの許可ルール(デバイスの制限を含む)が作成されます。

すべてのタスクイベントが、タスクモードに関係なくタスク実行ログに登録されます。**処理を実行**モードで実行したタスクで発生したイベントに基づくルールリストを含んだ設定ファイルが作成されます。タスクが適切に動作するには、タスクが「処理を実行」モードで実行される前にルールリストの最終バージョンを作成しておく必要があります。そのため、緊急の場合を除いてこのシナリオは推奨されません。

1 台以上の外部デバイスへの許可ルールの追加

デバイスコントロールタスクでは、ルールを 1 つずつ手動で追加する機能はサポートされていません。ただし、1 台以上の新しい外部デバイスにルールを追加する必要がある場合は、[**システムデータに基づいてルールを作成**]を使用できます。このシナリオを適用すると、アプリケーションでは以前接続されていたすべての外部デバイスに関する Windows データが使用され、現在接続されているデバイスに対しても許可ルールリストを入力できます。

Kaspersky Security 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。MTP 接続したモバイルデバイスの許可ルールは生成できません。

► **現在接続されている 1 台以上の外部デバイスに許可ルールを追加するには:**

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「デバイスコントロールルールの設定ウィンドウ」を参照)。
2. [**追加**]をクリックします。
3. 表示されたコンテキストメニューで、[**システムデータに基づいてルールを作成**]をオンにします。
4. 表示されたウィンドウで検知されたデバイスのリストを確認し、保護対象サーバーで信頼する 1 台以上のデバイスを選択しま

す。

5. [**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。

新しいルールが作成され、デバイスコントロールルールのリストに追加されます。

デバイスコントロールルールの削除

► **デバイスコントロールルールを削除するには:**

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「**デバイスコントロールルールの設定ウィンドウ**」を参照)。
2. リストで削除するルールを 1 つ以上選択します。
3. [**選択項目の削除**]をクリックします。
4. [**保存**]をクリックします。

選択したデバイスコントロールルールが削除されます。

デバイスコントロールルールのエクスポート

► **デバイスコントロールルールを設定ファイルにエクスポートするには:**

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「**デバイスコントロールルールの設定ウィンドウ**」を参照)。
2. [**ファイルにエクスポート**]をクリックします。

   Microsoft Windows 標準のウィンドウが表示されます。
3. 表示されたウィンドウで、ルールをエクスポートするファイルを指定します。ファイルが存在しない場合は作成されます。指定した名前のファイルがすでに存在する場合、ルールをエクスポートするとファイルの内容が書き換えられます。
4. [**保存**]をクリックします。

ルールとその設定が指定されたファイルにエクスポートされます。

デバイスコントロールルールのアクティベートとアクティベート解除

作成したデバイスコントロールルールは、削除しなくてもアクティベートおよびアクティベート解除できます。

► **作成したデバイスコントロールルールをアクティベートまたはアクティベート解除するには、次の手順を実行します:**

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「**デバイスコントロールルールの設定ウィンドウ**」を参照)。
2. 指定したルールのリストで、プロパティを設定するルールをダブルクリックして[**ルールのプロパティ**]ウィンドウを開きます。

3. 表示されたウィンドウで、[**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では、デバイスコントロールルールを有効または無効にできます。

   このチェックボックスがオンのルールはアクティベートされます。ルールの適用範囲に含まれる外部デバイスへの接続は許可されます。

   ルールのプロパティでこのチェックボックスがオフのルールはアクティベート解除されます。ルールの適用範囲に含まれる外部デバイスへの接続はブロックされます。

   既定では、作成した各ルールの設定においてこのチェックボックスはオンです。

4. [**OK**]をクリックします。

ルールの適用ステータスが保存され、指定したルールに表示されます。

デバイスコントロールルールの適用範囲の拡張

自動作成された各デバイスコントロールルールが対応しているのは、1 台の外部デバイスのみです。ルールの適用範囲を手動で拡張するには、指定したルールのプロパティでデバイスインスタンスパスのマスクを設定します。

デバイスインスタンスパスのマスクを適用すると、指定するルールの合計数を減らすことができ、ルールの処理の複雑さを低減できます。ただし、ルールの適用範囲を拡張すると、大容量記憶デバイスの制御効率が低下する可能性があります。

► デバイスコントロールルールのプロパティでデバイスインスタンスパスのマスクを適用するには:

1. [**デバイスコントロールルール**]ウィンドウを開きます(401 ページのセクション「**デバイスコントロールルールの設定ウィンドウ**」を参照)。
2. 表示されたウィンドウでルールを選択し、マスク適用でそのプロパティを使用します。
3. 選択したデバイスコントロールルールをダブルクリックして、[**ルールのプロパティ**]ウィンドウを開きます。
4. 表示されたウィンドウで、次の操作を行います:
   - 選択したルールにより、デバイスの製造元とデバイスのシリアルナンバーで指定された情報に適合するすべての大容量記憶デバイスへの接続を許可する場合は、[**コントローラーの種別(PID)**]の横にある[**マスクを使用**]をオンにします。
   - 選択したルールにより、デバイスの製造元とコントローラーの種別で指定された情報に適合するすべての大容量記憶デバイスへの接続を許可する場合は、[**シリアルナンバー**]の横にある[**マスクを使用**]をオンにします。
   - 選択したルールにより、デバイスの製造元で指定された情報に適合するすべての大容量記憶デバイスへの接続を許可する場合は、[**コントローラーの種別(PID)**]および[**シリアルナンバー**]の横にある[**マスクを使用**]をオンにします。

   1 つ以上のフィールドで[**マスクを使用**]をオンにすると、チェックボックスがオンのフィールドのデータが「*」記号で置き換えられ、ルールの適用時に考慮されなくなります。
5. 必要に応じて、ルールに関する追加情報を[**説明**]に入力します。たとえば、ルールによって影響を受けるデバイスの情報を入力します。
6. [**OK**]をクリックします。

新しく設定されたルールのプロパティが保存されます。ルールの適用範囲は、指定されたデバイスインスタンスパスのマスクに従って拡張されます。

デバイスコントロールルールの自動作成タスクの設定

► デバイスコントロールルールの自動作成タスクを設定するには:

1. アプリケーションコンソールツリーで、[**ルールの自動生成**]フォルダーを展開します。
2. [**デバイスコントロールルールの自動作成**]サブフォルダーを選択します。
3. [**デバイスコントロールルールの自動作成**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. [**全般**]タブの[**タスクモード**]セクションで、タスクの処理モードを選択します:
   - **過去に接続されたすべての大容量ストレージについてシステムデータを考慮する**
   - **現在接続している大容量ストレージだけを考慮する**
5. [**タスク完了後**]セクションで、タスクの完了時に Kaspersky Security for Windows Server が実行する処理を指定します:
   - **デバイスコントロールルールのリストに許可ルールを追加する**

     新しく作成された許可ルールのデバイスコントロールルールのリストへの追加を有効または無効にします。デバイスコントロールルールのリストは、[**デバイスコントロール**]フォルダーの詳細ペインの[**デバイスコントロールルール**]をクリックすると表示されます。

     このチェックボックスをオンにすると、選択した追加方法に基づいて、デバイスコントロールルールの自動作成タスクによ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。

     このチェックボックスをオフにすると、新しく作成された許可ルールはデバイスコントロールルールのリストに追加されません。作成されたルールは、ファイルにエクスポートされるだけです。

     既定では、このチェックボックスはオフです。
   - **追加方法**

     このドロップダウンリストは、新しく作成された許可ルールをデバイスコントロールルールのリストに追加する方法の指定に使用されます。

     - **既存のルールに追加する**: ルールが既存のルールのリストに追加されます。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**: ルールがリストの既存のルールを置き換えます。
     - **既存のルールとマージする**: ルールが既存のルールのリストに追加されます。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他のルールと異なる場合にルールが追加されます。

     既定では、[**既存のルールとマージする**]方法が選択されます。
   - **許可ルールをファイルにエクスポートする**

     作成されたデバイスコントロールの許可ルールのファイルへのエクスポート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、デバイスコントロールルールの自動作成タスクの終了時に、下にあるフィールドで指定されたファイルに許可ルールがエクスポートされます。

     このチェックボックスをオフにすると、デバイスコントロールルールの自動作成タスクの終了時に、作成された許可ルールはファイルにエクスポートされません。代わりに、デバイスコントロールルールのリストにのみ追加されます。

既定では、このチェックボックスはオフです。

- **ファイル名にコンピューターの詳細を追加する**

  デバイスコントロールの許可ルールをエクスポートするファイルの名前に対し、保護対象サーバーに関する情報の追加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、保護対象サーバーの名前、およびファイルの作成日時をエクスポートするファイルの名前に追加します。

  このチェックボックスをオフにすると、保護対象のサーバーに関する情報をエクスポートするファイルの名前に追加しません。

  既定では、このチェックボックスはオンです。

6. [**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの開始スケジュールを設定します(「タスク開始スケジュールの設定」(156ページ)を参照)。
7. [**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、システム監査ログに保存されます。

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。

この章の内容

ファイアウォール管理タスクについて

Kaspersky Security 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性と操作性にすぐれた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 for Windows Server グラフィックインターフェイスを介して Windows ファイアウォールを管理できます。ファイアウォール管理タスク時に Kaspersky Security 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、外部からファイアウォール設定が編集される可能性をすべてブロックします。

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 ファイアウォール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 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 ファイアウォールが Kaspersky Security 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 ファイアウォールをオンにした場合、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 ファイアウォール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 for Windows Server が Windows ファイアウォール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 ファイアウォールを 1 分ごとにポーリングすることで、Kaspersky Security for Windows Server は次を監視します:

- Windows ファイアウォールの動作状況。

- Kaspersky Security 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 ファイアウォールに新しいルールを適用すると、Kaspersky Security for Windows Server は［**Windows ファイアウォール**］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 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 for Windows Server ファイアウォール管理タスクを再起動します。

Windows ファイアウォール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 ファイアウォールが 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 ファイアウォール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 for Windows Server は Windows ファイアウォール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 ファイアウォール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 for Windows Server はそのルールを削除します。
- Windows ファイアウォール設定から既存のルールが削除された場合、タスクが再起動されたときに Kaspersky Security for Windows Server はそのルールを復元します。
- Windows ファイアウォール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 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 for Windows Server は Windows ファイアウォール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 for Windows Server は Windows ファイアウォール設定からルールを強制的に削除します。

Kaspersky Security 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 for Windows Server は Windows ファイアウォール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 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。

ファイアウォール管理タスクの既定の設定

ファイアウォール管理タスクでは、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 60. ファイアウォール管理タスクの既定の設定

設定	既定値	説明
アプリケーションを対象とするファイアウォールのルール	アプリケーションを対象とする 2 つの既定のルールが有効です	既定のルールを無効にしたり、新しいツールを追加できます。
ポートを対象とするファイアウォールのルール	ポートを対象とする 6 つの既定のルールが有効です	既定のルールを無効にしたり、新しいツールを追加できます。
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。	ファイアウォール管理タスクは、Kaspersky Security for Windows Server の起動時に自動的には開始されません。 この場合、タスク開始スケジュールを設定できます。

管理プラグインからファイアウォールのルールを管理する

このセクションでは、管理プラグインからファイアウォールのルールを管理する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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129

ページ）参照）。

> Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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**]サブセクションの[**設定**]をクリックします。
5. 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。
6. 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。
7. 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。
8. [**ファイアウォールのルール**]ウィンドウで[**OK**]をクリックします。
9. [**ファイアウォール管理**]ウィンドウで[**OK**]をクリックします。
10. ポリシーのプロパティウィンドウで、[**OK**]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 ファイアウォールに送信されます。

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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます（「ポリシーの設定」（125 ページ）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には、[**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（「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」（129 ページ）参照）。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。

4. [**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**]サブセクションの[**設定**]をクリックします。
5. 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。
6. 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。
7. 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。
8. [**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。
9. [**ファイアウォール管理**]ウィンドウで[**OK**]をクリックします。
10. ポリシーのプロパティウィンドウで、[**OK**]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 ファイアウォールに送信されます。

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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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**]サブセクションの[**設定**]をクリックします。
5. 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。
6. 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。
7. ルールリストで、削除するルールを選択します。
8. [**削除**]をクリックします。

   選択したルールが削除されます。
9. [**ファイアウォールのルール**]ウィンドウで[**OK**]をクリックします。
10. [**ファイアウォール管理**]ウィンドウで[**OK**]をクリックします。
11. ポリシーのプロパティウィンドウで、[**OK**]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 ファイアウォールに送信されます。

アプリケーションコンソールからファイアウォールのルールを管理する

このセクションでは、アプリケーションコンソールインターフェイスからファイアウォールのルールを管理する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. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**ファイアウォール管理**]サブフォルダーを選択します。
3. [**ファイアウォール管理**]フォルダーの詳細ペインで、[**ファイアウォールのルール**]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。
4. 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。
5. 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。
6. [**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 ファイアウォールに送信されます。

ファイアウォールルールの手動での追加

► **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. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**ファイアウォール管理**]サブフォルダーを選択します。
3. [**ファイアウォール管理**]フォルダーの詳細ペインで、[**ファイアウォールのルール**]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。
4. 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。

5. 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。

6. [**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。
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 ファイアウォールに送信されます。

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. アプリケーションコンソールツリーで、[**サーバーコントロール**]フォルダーを展開します。
2. [**ファイアウォール管理**]サブフォルダーを選択します。
3. [**ファイアウォール管理**]フォルダーの詳細ペインで、[**ファイアウォールのルール**]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。
4. 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。

5. ルールリストで、削除するルールを選択します。
6. [**削除**]をクリックします。

   選択したルールが削除されます。
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 ファイアウォールに送信されます。

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。

この章の内容

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、大容量記憶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 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大容量記憶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(424 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。各ルールに対して個数の制限なく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 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 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 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 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 61. 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
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
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

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
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既定の設定

ファイル変更監視タスクでは、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 62. ファイル変更監視タスクの既定の設定

設定	既定値	説明
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	指定したフォルダー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	オン	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。
次のフォルダーをコントロールから除外する	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 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。
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。

設定	既定値	説明
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 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。

管理プラグインからファイル変更監視を管理する

このセクションでは、管理プラグインからファイル変更監視タスク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

ファイル変更監視タスクの設定

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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**システム監査**]セクションの[**ファイル変更監視**]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。
5. 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 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（424 ページのセクション「監視ルールの設定」を参照）。

6. [**タスク管理**]タブで、スケジュールに基づいてタスクの開始を設定します（138 ページのセクション「タスクスケジュールの管理」を参照）。

7. [**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

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 63. ファイル変更監視タスクの既定の設定

設定	既定値	説明
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	指定したフォルダー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	オン	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。
次のフォルダーをコントロールから除外する	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 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。
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 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。

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**システム監査**]セクションの[**ファイル変更監視**]ブロックで、[**設定**]をクリックします。

   [**ファイル変更監視**]のプロパティウィンドウが開きます。

5. [**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。

6. 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¥*> - フォルダー <¥dir> にあるすべてのファイル。
     - <¥dir¥*¥name.ext> - フォルダー <¥dir> とそのすべてのサブフォルダーにある、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:<ボリューム文字>:¥<マスク>。ボリューム文字がない場合、Kaspersky Security for Windows Server は指定した監視範囲を追加しません。

7. [**信頼するユーザー**]タブで、[**追加**]をクリックします。

   Microsoft Windows 標準の[**ユーザーまたはグループの選択**]ウィンドウが開きます。

8. 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 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(420 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。

9. [**ファイル操作マーカー**]タブを選択します。

10. 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」(420 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 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。

11. 操作の実行後に Kaspersky Security 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. [**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、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、変更したファイルのチェックサムが計算されます。

    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、変更したファイルのチェックサムは計算されません。

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**

12. 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(420 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)。

13. 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**]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、除外リストで指定した監視範囲がスキップされます。

チェックボックスがオフの場合、指定したすべての監視範囲のイベントが記録されます。

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。

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[**OK**]をクリックします。

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。

14. [**ファイル変更監視ルール**]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。

アプリケーションコンソールからファイル変更監視を管理する

このセクションでは、アプリケーションコンソールからファイル変更監視タスク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

ファイル変更監視タスクの設定

► **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. アプリケーションコンソールツリーで、[**システム監査**]フォルダーを展開します。
2. [**ファイル変更監視**]サブフォルダーを選択します。
3. [**ファイル変更監視**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。

   [**タスクの設定**]ウィンドウが表示されます。
4. 表示されたウィンドウの[**全般**]タブで、[**監視中断期間におけるファイル操作の情報を記録する**]をオフまたはオンにします。

   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 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。
5. [**スケジュール**]タブおよび[**詳細設定**]タブで、タスクの起動スケジュールを設定します(「タスクスケジュールの管理」(138 ページ)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

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 64. ファイル変更監視タスクの既定の設定

設定	既定値	説明
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	指定したフォルダー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。

設定	既定値	説明
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	オン	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。
次のフォルダーをコントロールから除外する	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 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。
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 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。

► 監視範囲を追加するには、次の手順を実行します:

1. アプリケーションコンソールツリーで、[**システム監査**]フォルダーを展開します。
2. [**ファイル変更監視**]サブフォルダーを選択します。
3. [**ファイル変更監視**]フォルダーの詳細ペインで、[**ファイル変更監視ルール**]をクリックします。

   [**ファイル変更監視**]ウィンドウが表示されます。
4. 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. ウィンドウの左側にある[**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。

     c. [**追加**]をクリックし、指定した監視範囲で Kaspersky Security for Windows Server によるファイル操作の監視を開始します。
   - 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¥*> - フォルダー <¥dir> にあるすべてのファイル。
     - <¥dir¥*¥name.ext> - フォルダー <¥dir> とそのすべてのサブフォルダーにある、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：<ボリューム文字>:¥<マスク>。ボリューム文字がない場合、Kaspersky Security for Windows Server は指定した監視範囲を追加しません。

ウィンドウの右側にある[**ルールの説明**]タブに、この監視範囲で選択した信頼するユーザーとファイル操作マーカーが表示されます。

5. 追加した監視範囲のリストで、設定を実行する範囲を選択します。
6. [**信頼するユーザー**]タブを選択します。
7. [**追加**]をクリックします。

   Microsoft Windows 標準の[**ユーザーまたはグループの選択**]ウィンドウが開きます。
8. 選択した監視範囲で Kaspersky Security for Windows Server が信頼するとみなすユーザーまたはユーザーグループを選択します。
9. [**OK**]をクリックします。

既定では、Kaspersky Security 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（420 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。

10. [**ファイル操作マーカーの設定**]タブを選択します。
11. 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」（420 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 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。

12. 操作の実行後に Kaspersky Security 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、ファイルの変更後にファイル最終版のチェックサムを計算する。チェックサムは実行ログに表示されます**]をオンにします。

       チェックボックスがオンの場合、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、変更したファイルのチェックサムが計算されます。

       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、変更したファイルのチェックサムは計算されません。

       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. [**アルゴリズムを使用してチェックサムを計算する**]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**:

13. 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. [**除外の設定**]タブを選択します。

b. [**除外された監視範囲を検討する**]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、除外リストで指定した監視範囲がスキップされます。

チェックボックスがオフの場合、指定したすべての監視範囲のイベントが記録されます。

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。

c. [**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。

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[**OK**]をクリックします。

e. [**OK**]をクリックします。

f. [**追加**]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。

> また、監視範囲の指定に使用されたのと同じマスクを使用して、除外された監視範囲を手動で追加することもできます。

14. [**保存**]をクリックして、新しいルール設定を適用します。

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。

この章の内容

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 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有効化の条件を設定できます:

- 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 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 ログの監視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 ID のリスト

  ルールに対して指定されたイベント ID 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 ID 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指定できます。このサブログ内のみで、指定されたイベント ID 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、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。

既定では、Windows イベントログ監視タスクでカスタムルールが適用されます。

> 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/en-us/library/cc952128.aspx)を参照してください。

Windows イベントログ監視タスクの既定の設定

Windows イベントログ監視タスクでは、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 65. ファイル変更監視タスクの既定の設定

設定	既定値	説明
Windows イベントログ監視にカスタムルールを適用する	適用されます。	カスタムルールの追加や変更を行ったり、各ルールの有効と無効を切り替えることができます。
Windows イベントログ監視に定義済みのルールを適用する	適用されます。	保護対象サーバーで通常とは異なるふるまいを検知する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。
ブルートフォース攻撃の検知	300 秒でログオンの失敗回数が 10 回	適用基準となる試行の数と期間を指定し、その期間内に指定した回数以上の試行が発生した場合にヒューリスティックアナライザーを適用するように設定します。
ネットワークログオン	午前 12 時	Kaspersky Security for Windows Server がサインインの試行を異常なふるまいとして扱う時間帯の開始と終了を指定します。
除外	適用されません。	ヒューリスティックアナライザーを適用しないユーザーと IP アドレスを指定できます。

設定	既定値	説明
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。

管理プラグインから Windows イベントログ監視のルールを管理する

このセクションでは、管理プラグインから Windows イベントログ監視のルールを追加または編集する方法について説明します。

このセクションの内容

管理プラグインから定義済みのタスクルールを管理する

► 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ます。
2. アプリケーションの設定を行う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、**ポリシーのプロパティ**ウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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。

5. [**定義済みのルール**]タブを選択します。
6. [**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。

   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。

7. 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
8. 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。
9. [**ブルートフォース攻撃の検知**]セクションで、適用基準となる試行の数と期間を指定し、その期間内に指定した回数以上の試行が発生した場合にヒューリスティックアナライザーを適用するように設定します。
10. [**ネットワークログオンの検知**]セクションで、Kaspersky Security 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指定します。
11. [**除外**]タブを選択します。
12. 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。
13. 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。
14. 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。
15. [**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(139 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)。
16. [**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。

管理プラグインから Windows イベントログ監視のルールを追加する

► **新しい Windows イベントログ監視の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ます。
2. アプリケーションの設定を行う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、ポリシーのプロパティウィンドウを開きます(「ポリシーの設定」(125 ページ)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には、[**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(「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」(129 ページ)参照)。

   > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、このポリシーによりアプリケーションの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設定**]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。
4. [**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。
5. [**カスタムルール**]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 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。ポップアップ検出ルールのみがアクティブです。

   > 事前設定ルールを Windows イベントログ監視のルール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。
6. 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。
7. [**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。

8. [**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。各ルールに対して個数の制限なく ID 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。

アプリケーションコンソールから Windows イベントログ監視のルールを管理する

このセクションでは、アプリケーションコンソールから Windows イベントログ監視のルールを追加または編集する方法について説明します。

このセクションの内容

アプリケーションコンソールから定義済みのタスクルールを管理する

► **ヒューリスティックアナライザーを Windows イベントログ監視タスクに対して設定する次の処理を行います:**

1. アプリケーションコンソールツリーで、[**システム監査**]フォルダーを展開します。
2. [**Windows イベントログ監視**]サブフォルダーを選択します。
3. [**Windows イベントログ監視**]フォルダーの詳細ペインで、[**プロパティ**]をクリックします。
   [**タスクの設定**]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カスタムルールを適用する**]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、[**拡張**]タブに移動します。
8. [**ブルートフォース攻撃の検知**]で、適用基準となる試行の数と期間を指定し、その期間内に指定した回数以上の試行が発生した場合にヒューリスティック分析を適用するように設定します。
9. [**ネットワークログオン**]セクションで、Kaspersky Security 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指定します。
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。

    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。
13. [**スケジュール**]タブと[**詳細設定**]タブを選択し、タスクの開始スケジュールを設定します。
14. [**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 イベントログ監視の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. アプリケーションコンソールツリーで、[**システム監査**]フォルダーを展開します。
2. [**Windows イベントログ監視**]サブフォルダーを選択します。
3. [**Windows イベントログ監視**]フォルダーの詳細ペインで、[**Windows イベントログ監視のルール**]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。
4. [**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 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。ポップアップ検出ルールのみがアクティブです。

   定義済みのルールを Windows イベントログ監視タスク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作成するには、次のようにします。
   a. 新しいルール名を入力します。
   b. [**追加**]をクリックします。

   作成されたルールは、一般ルールリストに追加されます。
6. ルールの設定を行うには、次の手順を実行します:
   a. リストでルールをクリックして選択します。

   ウィンドウの右の領域にある[**説明**]タブに、ルールに関する一般情報が表示されます。

   新しいルールの説明は空白です。

   b. [**ルールの説明**]タブを選択します。
   c. [**全般**]セクションで、必要に応じてルール名を編集します。
   d. [**ソース**]を選択します。
7. [**イベント 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。各ルールに対して個数の制限なく ID を追加できます。

   c. [**保存**]をクリックします。

   設定された Windows イベントログ監視ルールが適用されます。

オンデマンドスキャン

このセクションでは、オンデマンドスキャンタスク、および保護対象サーバー上でのオンデマンドスキャンタスクとセキュリティの設定手順について説明します。

この章の内容

オンデマンドスキャンタスクについて

Kaspersky Security 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がないかをスキャンします。Kaspersky Security for Windows Server ではサーバーのファイル、メモリ、および自動実行オブジェクトがスキャン対象になります。

Kaspersky Security for Windows Server では、オンデマンドスキャンの以下のシステムタスクを提供します:

- [オペレーティングシステムの起動時にスキャン]タスクは、Kaspersky Security for Windows Server の起動のたびに実行されます。ハードディスクやリムーバブルドライブのブートセクターやマスターブートレコード、システムメモリ、およびプロセスのメモリがスキャンされます。このタスクが実行されるたびに、感染していないブートセクターのコピーが作成されます。次回のタスク起動時にこれらのセクターで脅威が検知された場合は、バックアップコピーと置き換えられます。
- 既定では、簡易スキャンタスクがスケジュールに従って週単位で実行されます。オペレーティングシステムの重要な領域のオブジェクト(自動実行オブジェクト、ハードディスクやリムーバブルドライブのブートセクターやマスターブートレコード、システムメモリやプロセスのメモリなど)がスキャンされます。%windir%¥system32 などのシステムフォルダーのファイルがスキャンされます。Kaspersky Security for Windows Server は、[推奨]レベルに対応する値をセキュリティ設定に適用します(「オンデマンドスキャンタスクの定義済みセキュリティレベルについて」(444 ページ)を参照)。簡易スキャンタスクの設定は変更できます。
- 隔離のスキャンタスクは、定義データベースのアップデートのたびに、スケジュールに従って既定で実行されます。隔離のスキャンタスクの対象範囲は変更できません。
- アプリケーションの整合性チェックタスクは毎日実行されます。Kaspersky Security for Windows Server モジュールの破損または変更を確認するオプションを提供します。アプリケーションのインストールフォルダーが確認されます。タスク実行の統計情報には、確認したモジュールと破損したモジュールの数に関する情報が含まれます。タスクの設定の値は既定で定義され、編

集できません。タスク開始スケジュール設定は編集できます。

さらに、カスタムのオンデマンドスキャンタスク(サーバー上の共有フォルダーをスキャンするタスクなど)を作成できます。

複数のオンデマンドスキャンタスクが同時に実行される場合があります。

スキャン範囲について

オペレーティングシステムの起動時にスキャンタスク、簡易スキャンタスク、およびカスタムのオンデマンドスキャンタスクに対して、スキャン範囲を設定できます。

既定では、オンデマンドスキャンタスクはサーバーファイルシステムのすべてのオブジェクトをスキャンします。ファイルシステムのすべてのオブジェクトをスキャンするセキュリティ要件がない場合は、スキャンをスキャン範囲に制限することができます。

アプリケーションコンソールでは、スキャン範囲は、Kaspersky Security for Windows Server が操作できるサーバーのファイルリソースのツリーまたはリストとして表示されます。既定では、保護対象サーバーのネットワークファイルリソースがリストビューモードで表示されます。

► ネットワークファイルリソースをツリービューモードで表示するには:

[**スキャン範囲の設定**]ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。

次のように、サーバーファイルリソースのリストビューまたはツリービューモードでフォルダーが表示されます:

☑ フォルダーがスキャン範囲に含まれています。

☐ フォルダーがスキャン範囲から除外されています。

▣ このフォルダーの 1 つ以上のサブフォルダーがスキャン範囲から除外されます。または、このサブフォルダーとフォルダーのセキュリティ設定が異なります(ツリービューモードの場合のみ)。

> ▣ アイコンは、親フォルダーを除くすべてのサブフォルダーが選択されている場合に表示されます。この場合、親フォルダーのファイルとフォルダーの構成の変更は、選択したサブフォルダーのスキャン範囲の変更中は自動的に無視されます。

スキャン範囲の仮想フォルダーの名前は、青色のフォントで表示されます。

定義済みのスキャン範囲

選択したオンデマンドスキャンタスクのコンピューターファイルリソースのツリーまたはリストが、[**スキャン範囲の設定**]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 for Windows Server には次の定義済みスキャン範囲が含まれています:

- **マイコンピューター**:Kaspersky Security for Windows Server はサーバー全体をスキャンします。
- **ローカルハードディスク**:Kaspersky Security for Windows Server はサーバーのハードディスク上のオブジェクトをスキャンします。すべてのハードディスク、個々のディスク、フォルダー、ファイルをスキャン範囲に含めたりスキャン範囲から除外したりすることができます。

- **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スキャンされます。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、ファイルをスキャン範囲に含めたりスキャン範囲から除外したりすることができます。
- **ネットワーク**:ネットワーク上のフォルダーやファイルのパスを UNC(ユニバーサルネーミング規約)フォーマットで指定して、スキャン範囲に追加できます。タスクの開始に使用するアカウントには、追加するネットワーク上のフォルダーやファイルのアクセス権がある必要があります。既定では、オンデマンドスキャンタスクはシステムアカウントで実行されます。

  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のオブジェクトをスキャン範囲に含めるには、このネットワークドライブに対応するフォルダーのパスを、UNC フォーマットで指定します。

- **システムメモリ**:スキャンの開始時にオペレーティングシステムで実行されているプロセスの実行ファイルおよびモジュールがスキャンされます。
- **スタートアップオブジェクト**:レジストリキーや設定ファイルによって参照されるオブジェクトがスキャンされます。たとえば、WIN.INI や SYSTEM.INI、およびコンピューターの起動時に自動的に起動されるアプリケーションのモジュールなどです。
- **共有フォルダー**:保護対象サーバーにある共有フォルダーをスキャン範囲に含めることができます。
- **仮想ドライブ**:共有のクラスタードライブなどの、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、およびドライブをスキャン範囲に含めることができます。

  SUBST コマンドを使用して作成した仮想ドライブは、アプリケーション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。仮想ドライブのオブジェクトをスキャンするには、この仮想ドライブが関連付けられているサーバーフォルダーをスキャン範囲に含めます。

既定では、ネットワークファイルリソースツリーで定義済みスキャン範囲を表示して設定できます。また、その構成時にスキャン範囲設定のネットワークファイルリソースリストに定義済みの範囲を追加することもできます。

既定では、オンデマンドスキャンタスクは次の範囲で実行されます:

- オペレーティングシステムの起動時にスキャン:
  - **ローカルハードディスク**
  - **リムーバブルドライブ**
  - **システムメモリ**
- 簡易スキャン:
  - **ローカルハードディスク**(Windows フォルダーを除く)
  - **リムーバブルドライブ**
  - **システムメモリ**
  - **スタートアップオブジェクト**
- その他のタスク:
  - **ローカルハードディスク**(Windows フォルダーを除く)
  - **リムーバブルドライブ**
  - **システムメモリ**
  - **スタートアップオブジェクト**
  - **共有フォルダー**

クラウドストレージのファイルのスキャン

クラウドファイルについて

Kaspersky Security for Windows Server は、Microsoft OneDrive のクラウドファイルを対象とした操作を実行できます。新機能である、OneDrive のファイルオンデマンド機能をサポートします。

> Kaspersky Security for Windows Server は、他のクラウドストレージをサポートしません。

OneDrive のファイルオンデマンド機能では、OneDrive のファイルをダウンロードすることなく、すべてのファイルにアクセスできるので、デバイスのストレージ容量を消費しません。必要に応じて、ファイルをハードディスクにダウンロードできます。

OneDrive のファイルオンデマンド機能が有効になっている場合、エクスプローラーの[**ステータス**]列の各ファイルの横にステータスアイコンが表示されます。ファイルにはそれぞれ次のいずれかのステータスが表示されます:

このステータスアイコンは、ファイルが**オンラインでのみ利用できる**ことを示します。オンライン専用ファイルは、ハードディスクに物理的に保存されません。オンライン専用ファイルは、デバイスがインターネットに接続していないときは開くことができません。

このステータスアイコンは、ファイルが**ローカルで利用できる**ことを示します。これは、オンライン専用ファイルを開いてデバイスにダウンロードした場合に発生します。インターネットにアクセスしていない場合でも、ローカルで利用できるファイルはいつでも開くことができます。容量を確保するために、ファイルを （オンライン専用）に変更できます。

このステータスアイコンは、ファイルが**ハードディスクに保存されており、いつでも利用できる**ことを示しています。

クラウドファイルのスキャン

Kaspersky Security for Windows Server は、保護対象サーバーのローカルに保存されているクラウドファイルのみをスキャンできます。そのような OneDrive ファイルは と のステータスになっています。 ファイルは物理的に保護対象サーバー上にないため、スキャン中はスキップされます。

> Kaspersky Security for Windows Server は、ファイルがスキャン範囲に含まれていても、スキャン中に ファイルをクラウドから自動的にダウンロードすることはありません。

クラウドファイルはタスク種別に応じて、いくつかの Kaspersky Security for Windows Server タスクによってさまざまなシナリオで処理されます:

- クラウドファイルのリアルタイムスキャン:クラウドファイルを含むフォルダーをファイルのリアルタイム保護タスクの保護範囲に追加できます。ユーザーがファイルにアクセスするとスキャンされます。 ファイルにユーザーがアクセスすると、ダウンロードされてローカルで利用できるようになり、ステータスが に変更されます。これにより、ファイルのリアルタイム保護タスクによるファイルの処理が可能になります。
- クラウドファイルのオンデマンドスキャン:クラウドファイルを含むフォルダーをオンデマンドスキャンタスクのスキャン範囲に追加できます。このタスクでは、 と のステータスのファイルをスキャンします。 ファイルが範囲内で見つかった場合、スキャン中はスキップされます。スキャンされたファイルはクラウドファイルの単なるプレースホルダーであり、ローカルディスクには存在しないことを示す情報イベントが実行ログに記録されます。
- アプリケーションコントロールルールの作成と利用: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使用して、 と のファイルの許可および拒否のルールを作成できます。アプリケーション起動コントロールタスクは、プロセスに対しては「既定で拒否」の原則と個別に作成したルールを適用し、クラウドファイルに対してはこれをブロックします。

アプリケーション起動コントロールタスクは、ステータスに関係なく、すべてのクラウドファイルの起動をブロックします。 ファイルはハードディスクに物理的に保存されていないため、ルール作成の範囲に含まれません。そのようなファイルに対して許可ルールを作成できないため、「既定で拒否」の原則が適用されます。

OneDrive のクラウドファイルで脅威が検知された場合、スキャンを実行するタスクの設定で指定された処理を適用します。この方法で、ファイルを削除、駆除、隔離、またはバックアップすることができます。

変更されたローカルファイルは、関連する Microsoft OneDrive の資料で説明されている仕様に従い、OneDrive に保存されているコピーと同期されます。

オンデマンドスキャンタスクの選択したフォルダーのセキュリティ設定

選択したオンデマンドスキャンタスクでは、セキュリティ設定の既定値は、スキャン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ツリーまたはリストのフォルダーや項目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。

選択した親フォルダーに対するセキュリティ設定は、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。

次のいずれかの方法を使用して、選択したスキャン範囲または保護範囲の設定を実行できます:

- 3 つの定義済みセキュリティレベル(**最高のパフォーマンス**、**推奨**、**最大の保護**)のいずれかを選択する。
- サーバーのファイルリソースのツリーまたはリストで、選択したフォルダーや項目のセキュリティ設定を手動で変更する(セキュリティレベルが**カスタム**に変更されます)。

フォルダーの一連の設定をテンプレートに保存して、後で他のフォルダーに適用することができます。

オンデマンドスキャンタスクの定義済みセキュリティレベルについて

[**iChecker テクノロジーを使用する**]、[**iSwift テクノロジーを使用する**]、[**ヒューリスティックアナライザーを使用する**]、[**ファイルの Microsoft の署名をチェックする**]などのセキュリティ設定は、事前設定のセキュリティレベルには含まれません。[**iChecker テクノロジーを使用する**]、[**iSwift テクノロジーを使用する**]、[**ヒューリスティックアナライザーを使用する**]、[**ファイルの Microsoft の署名をチェックする**]などの設定のステータスが変更されても、選択した事前設定のセキュリティレベルは変更されません。

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)。

最高のパフォーマンス

サーバーおよびワークステーションでの Kaspersky Security for Windows Server の使用に加えて、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(ファイアウォールや既存のセキュリティポリシーなど)を適用している場合、[**最高のパフォーマンス**]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、保護レベルと保護対象のサーバーのパフォーマンスへの影響とのバランスが最適化されます。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で高い水準のコンピューターセキュリティ要件が求められる場合、[**最大の保護**]セキュリティレベルを推奨します。

表 66. 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値

オプション	セキュリティレベル		
	最高のパフォーマンス	推奨	最大の保護
オブジェクトのスキャン	形式に基づく	すべてのオブジェクト	すべてのオブジェクト
作成または変更されたファイルのみをスキャン	有効	無効	無効
感染などの問題があるオブジェクトの処理	駆除、駆除できない場合は削除	推奨処理を実行(駆除、駆除できない場合は削除)	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	隔離	推奨処理を実行(隔離)	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
スキャン時間が次を超えたら停止する(秒)	60 秒	なし	なし
スキャンする複合オブジェクトの最大サイズ(MB)	8 MB	なし	なし
NTFS 代替データストリームをスキャン	有効	有効	有効
ディスクのブートセクターと MBR をスキャン	有効	有効	有効

オプション	セキュリティレベル		
複合オブジェクトのスキャン	• 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	• アーカイブ* • SFX アーカイブ* • メールデータベース* • 通常のメール* • 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

リムーバブルドライブスキャンについて

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 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。一時的な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 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 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 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 67. 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、コンポーネントの対象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、リムーバブルドライブスキャンは実行されません。
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。

オンデマンドスキャンタスクの既定の設定

オンデマンドスキャンタスクでは、次の表の既定の設定が使用されます。システムおよびユーザーのオンデマンドスキャンタスクを設定できます。

表 68. オンデマンドスキャンタスクの既定の設定

設定	値	説明
スキャン範囲	システムタスクとカスタムタスクに適用されます: • **オペレーティングシステムの起動時にスキャン**:共有フォルダーと自動実行オブジェクトを除いたサーバー全体が対象です。 • **簡易スキャン**:共有フォルダーと特定のオペレーティングシステムファイルを除いたサーバー全体が対象です。 • カスタムの**オンデマンドスキャン**タスク:サーバー全体が対象です。	スキャン範囲を変更することができます。スキャン範囲は、**隔離のスキャン**および**アプリケーションの整合性チェック**のシステムタスクでは設定できません。

設定	値	説明
セキュリティ設定	スキャン範囲全体に共通する設定として、セキュリティレベルの[**推奨**]に相当する設定。	コンピューターのファイルリソースリストまたは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: • 別の定義済みセキュリティレベルを選択する • 手動でセキュリティ設定を変更する あとで異なるフォルダーに使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一連のセキュリティ設定を保存できます。
ヒューリスティックアナライザーを使用する	簡易スキャン、オペレーティングシステムの起動時のスキャン、カスタムタスクでは**中**の分析レベルで使用されます。 隔離のスキャンタスクでは**高**の分析レベルで使用されます。	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。隔離のスキャンタスクの分析レベルは変更できません。 ヒューリスティックアナライザーは、アプリケーションの整合性チェックタスクでは使用されません。
信頼ゾーンを適用する	適用されます(隔離のスキャンタスクには適用されません)。	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。
スキャンに KSN を使用する	適用されます。	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、サーバーの保護を改善することができます。
権限を指定したタスクの開始設定	タスクがシステムアカウントで起動されます。	隔離のスキャンタスクとアプリケーションの整合性チェックタスクを除き、すべてのシステムおよびユーザーのオンデマンドスキャンタスクに対して、アカウントの権限を使用して開始の設定を編集できます。
バックグラウンドモードでタスクを実行する(優先度「低」)	オフ	オンデマンドスキャンタスクのレベルの優先度を設定できます。
タスク開始スケジュール	システムタスクに適用されます: • オペレーティングシステムの起動時にスキャン - **アプリケーションの起動時** • 簡易スキャン - **週単位** • 隔離のスキャン - **定義データベースのアップデート後** • アプリケーションの整合性チェック - **日単位** 新しく作成されたカスタムタスクでは使用されません。	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。
スキャンの実行の登録とサーバーの保護ステータスの更新	サーバーの保護ステータスは、簡易スキャンを実行したタイミングで週単位で更新されます。	簡易スキャンの実行の登録は、次の方法で設定できます: • 簡易スキャンタスクの開始スケジュール設定を編集する。 • 簡易スキャンタスクのスキャン範囲を編集する。 • ユーザーのオンデマンドスキャンタスクを作成する。

管理プラグインからオンデマンドスキャンタスクを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーのタスク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

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

オンデマンドスキャンタスクウィザード

► 新しいカスタムオンデマンドスキャンタスクの作成を開始するには:

1. ローカルタスクを作成するには:
   a. Kaspersky Security Center の管理コンソールで[**管理対象デバイス**]フォルダーを展開します。
   b. サーバーが所属する管理グループを選択します。
   c. 詳細ペインの[**デバイス**]タブで、保護対象のサーバーのコンテキストメニューを開きます。
   d. [**プロパティ**]メニューオプションを選択します。

e. 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。

[**新規タスクウィザード**]ウィンドウが開きます。

2. 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ます。

   b. タスクを作成する管理グループを選択します。

   c. [**タスク**]タブを開きます。

   d. [**タスクの作成**]をクリックします。

   [**新規タスクウィザード**]ウィンドウが開きます。

3. カスタマイズ可能な条件を指定して、1 台以上のサーバーを対象に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の[**デバイスの抽出**]フォルダーで、[**抽出を実行**]をクリックしてデバイスの抽出を実行します。

   b. [**抽出結果 "抽出名"**]タブを開きます。

   c. [**処理を実行**]ドロップダウンリストで、[**タスクの作成**]オプションを選択します。

   [**新規タスクウィザード**]ウィンドウが開きます。

4. Kaspersky Security for Windows Server で使用可能なタスクの一覧から、[**オンデマンドスキャン**]タスクを選択します。

5. [**次へ**]をクリックします。

   [**設定**]ウィンドウが開きます。

必要に応じてタスクを設定します。

► 既存のオンデマンドスキャンタスクの設定を編集するには:

Kaspersky Security Center タスクのリストで、タスク名をダブルクリックします。

オンデマンドスキャンのプロパティウィンドウが表示されます。

オンデマンドスキャンタスクのプロパティウィンドウ

► 単一のサーバーでオンデマンドスキャンタスクのプロパティを開くには:

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. 保護対象サーバーが所属する管理グループを選択します。
3. [**デバイス**]タブを選択します。
4. スキャン範囲を設定するサーバーの名前をダブルクリックします。

   サーバーのプロパティウィンドウが表示されます。
5. [**タスク**]セクションを選択します。
6. デバイス用に作成されたタスクのリストで、作成したオンデマンドスキャンタスクを選択します。
7. [**プロパティ**]をクリックします。

   オンデマンドスキャンのプロパティウィンドウが表示されます。

必要に応じてタスクを設定します。

オンデマンドスキャンタスクの作成

► カスタムオンデマンドスキャンタスクを作成するには:

1. [**新規タスクウィザード**]で[**設定**]ウィンドウを開きます(449 ページのセクション「**オンデマンドスキャンタスクウィザード**」を参照)。
2. 目的の[**タスクの作成方法**]を選択します。
3. [**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**]を選択するか、[**追加**]をクリックします。

     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、いずれかの定義済みのセキュリティレベルを選択するか、[**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。

     セキュリティ設定は、ファイルのリアルタイム保護と同じ方法で設定されます(254 ページのセクション「手動でのセキュリティの設定」を参照)。

   - 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連携を設定します。

- ヒューリスティックアナライザーの使用を設定します（251 ページのセクション「ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの連携の設定」を参照）。
- 信頼ゾーンのリストに追加されたオブジェクトをタスクのスキャン範囲から除外する場合は、[**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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

  既定では、このチェックボックスはオンです。

- Kaspersky Security 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 for Windows Server タスクおよびアプリケーションによる CPU とサーバーの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 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 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。

- 作成したタスクを簡易スキャンタスクとして使用する場合、[**オプション**]ウィンドウで[**タスクを簡易スキャンとする**]をオンにしてください。

  このチェックボックスでは、**簡易スキャン**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、**簡易スキャン**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 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、簡易スキャン完了が記録され、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。

カスタムオンデマンドスキャンタスクでは、このチェックボックスは既定でオフです。

6. [**次へ**]をクリックします。
7. [**スケジュール**]ウィンドウで、タスクの開始スケジュールを設定します。
8. [**次へ**]をクリックします。
9. [**タスクを実行するアカウントの選択**]ウィンドウで、使用するアカウントを指定します。
10. [**次へ**]をクリックします。
11. タスク名を指定します。
12. [**次へ**]をクリックします。

    タスク名は 100 文字以内にする必要があり、次の記号は使用できません:

    " * < > & ¥ : |

    [**タスクの作成を終了**]ウィンドウが開きます。
13. オプションで[**ウィザード完了後にタスクを実行する**]をオンにすると、ウィザードの終了後にタスクを実行することができます。
14. [**完了**]をクリックしてタスクの作成を終了します。

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。

このセクションの内容

オンデマンドスキャンタスクへの簡易スキャンタスクのステータスの割り当て

既定では、簡易スキャンタスクの実行頻度が Kaspersky Security for Windows Server のイベント生成しきい値の[**簡易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(451 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)。
2. タスクウィザードの[**オプション**]ウィンドウで、[**タスクを簡易スキャンとする**]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サーバーに適用されます。タスクのスケジュールを設定します。

［**タスクを簡易スキャンとする**］は、サーバーのグループに対してオンデマンドスキャンタスクを作成するとき、またはタスクのプロパティウィンドウでオンにできます（450 ページのセクション「オンデマンドスキャンタスクのプロパティウィンドウ」を参照）。

3. 新しいポリシーまたは既存のポリシーを使用して、システムのオンデマンド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（109 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、**簡易スキャン**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簡易スキャンの状態に基づいて、その状態が通知されます。

簡易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。

アプリケーションコンソールを使用して、オンデマンドスキャンタスクが簡易スキャンタスクであるかを確認できます。

アプリケーションコンソールで、タスク設定に［**タスクを簡易スキャンとする**］チェックボックスが表示されますが、この設定を編集することはできません。

バックグラウンドでのオンデマンドスキャンタスクの実行

既定では、Kaspersky Security for Windows Server タスクが実行されるプロセスは、基本の優先度［**中**］（［標準］）に割り当てられます。

オンデマンドスキャンタスクを実行するプロセスは、優先度［**低**］に割り当てることができます。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。

複数のバックグラウンドタスクを、優先度［低］で 1 つの処理対象プロセスで実行できます。バックグラウンドのオンデマンドスキャンタスクのプロセスの最大数を指定できます。

► 既存のオンデマンドスキャンタスクの優先度を変更するには：

1. **オンデマンドスキャン**のプロパティウィンドウを開きます（449 ページのセクション「オンデマンドスキャンタスクウィザード」を参照）。
2. ［**バックグラウンドモードでタスクを実行する**］をオンまたはオフにします。

   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 for Windows Server タスクおよびアプリケーションによる CPU とサーバーの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 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。

3. ［**OK**］をクリックします。

構成されたタスクの設定が保存され、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。

簡易スキャンの実行の登録

既定では、サーバーの保護ステータスが[**Kaspersky Security**]フォルダーの詳細ペインに表示され、簡易スキャンを実行したタイミングで週単位で更新されます。

サーバーの保護ステータスを更新する時間は、[**タスクを簡易スキャンとする**]がオンに設定されたオンデマンドスキャンタスクのスケジュールに紐付いています。既定では、このチェックボックスは簡易スキャンタスクでのみオンになっており、このタスクでは変更できません。

サーバーの保護ステータスに結果を反映させるオンデマンドスキャンタスクの選択は、Kaspersky Security Center からのみ実行できます。

タスクのスキャン範囲の設定

オペレーティングシステム起動時のスキャンタスクおよび簡易スキャンタスクのスキャン範囲を変更する場合は、Kaspersky Security for Windows Server 自体を復元することにより、これらのタスクの既定のスキャン範囲を復元できます([**スタート**] - [**すべてのプログラム**] - [**Kaspersky Security 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で、[**インストール済みコンポーネントの修復**]を選択して[**次へ**]をクリックし、[**製品の推奨設定を復元する**]をオンにします。

► 既存のオンデマンドスキャンタスクのスキャン範囲を編集するには:

1. **オンデマンドスキャンのプロパティウィンドウを開きます**(450 ページのセクション「オンデマンドスキャンタスクのプロパティウィンドウ」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. スキャン範囲に項目を含めるには:
   a. スキャン範囲のリストの空白部分でコンテキストメニューを開きます。
   b. [**範囲の追加**]コンテキストメニューオプションを選択します。
   c. 表示された[**スキャン範囲にオブジェクトを追加**]ウィンドウで、追加するオブジェクトの種別を選択します:
   - **定義済みの範囲**:保護対象サーバーでいずれかの定義済み範囲を追加します。ドロップダウンリストで、必要なスキャン範囲を選択します。
   - **ディスク、フォルダー、またはネットワークの場所**:個別のドライブ、フォルダー、またはネットワークオブジェクトをスキャン範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。
   - **ファイル**:個別のファイルをスキャン範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。

   オブジェクトがすでにスキャン範囲からの除外対象として追加されている場合、スキャン範囲には追加できません。
4. スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにするか、次の手順を実行します:
   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。
   b. コンテキストメニューで、[**除外の追加**]を選択します。
   c. [**除外の追加**]ウィンドウで、スキャン範囲にオブジェクトを追加する手順と同様に、スキャン範囲からの除外対象とし

て追加するオブジェクトの種別を選択します。

5. スキャン範囲または追加する除外対象を変更するには、該当するスキャン範囲のコンテキストメニューで[**範囲の編集**]を選択します。
6. ネットワークファイルリソースのリストに以前追加したスキャン範囲または除外対象を非表示にするには、該当するスキャン範囲のコンテキストメニューで[**範囲の削除**]を選択します。

   スキャン範囲がネットワークファイルリソースリストから削除されたときに、オンデマンドスキャンタスクの範囲から除外されます。

7. [**OK**]をクリックします。

スキャン範囲設定ウィンドウが終了します。これで新しい設定が保存されました。

オンデマンドスキャンタスクの定義済みセキュリティレベルの選択

サーバーのネットワークファイルリソースのリストで選択した項目に対して、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**]。

► 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:

1. **オンデマンドスキャン**のプロパティウィンドウを開きます(450 ページのセクション「**オンデマンドスキャンタスクのプロパティウィンドウ**」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. サーバーのリストでスキャン範囲に含まれる項目を選択して、定義済みセキュリティレベルを設定します。
4. [**設定**]をクリックします。

   [**オンデマンドスキャンの設定**]ウィンドウが開きます。
5. [**セキュリティレベル**]タブで、適用するセキュリティレベルを選択します。

   選択したセキュリティレベルに対応するセキュリティ設定のリストが表示されます。
6. [**OK**]をクリックします。
7. **オンデマンドスキャン**のプロパティウィンドウで、[**OK**]をクリックします。

   構成されたタスクの設定が保存され、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。

手動でのセキュリティの設定

オンデマンドスキャンタスクでは、既定でスキャン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、定義済みセキュリティレベルの[**推奨**]に対応します(242 ページのセクション「定義済みのセキュリティレベル」を参照)。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはサーバーのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定することができます。

► 手動でセキュリティを設定するには:

1. **オンデマンドスキャンのプロパティウィンドウを開きます**(450 ページのセクション「オンデマンドスキャンタスクのプロパティウィンドウ」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. セキュリティ設定を行うスキャン範囲のリストから項目を選択します。

   セキュリティ設定を含む定義済みのテンプレート(「セキュリティ設定テンプレートについて」(162 ページ)を参照)は、スキャン範囲内の選択したフォルダーや項目に適用できます。

4. [**設定**]をクリックします。

   [**オンデマンドスキャンの設定**]ウィンドウが開きます。

5. 要件に従って、選択したフォルダーや項目に必要なセキュリティを設定します:
   - **全般**設定(457 ページのセクション「タスクの全般的な設定」を参照)
   - **処理**(460 ページのセクション「**処理の設定**」を参照)
   - **パフォーマンス**(461 ページのセクション「**パフォーマンスの設定**」を参照)
6. [**オンデマンドスキャンの設定**]ウィンドウで[**OK**]をクリックします。
7. [**スキャン範囲**]ウィンドウで、[**OK**]をクリックします。

新しいスキャン範囲の設定が保存されます。

このセクションの内容

タスクの全般的な設定

► オンデマンドスキャンタスクの全般的な設定を行うには:

1. **オンデマンドスキャン**のプロパティウィンドウを開きます(450 ページのセクション「**オンデマンドスキャンタスクのプロパティウィンドウ**」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. [**設定**]をクリックします。

   [**オンデマンドスキャンの設定**]ウィンドウが開きます。
4. [**設定**]をクリックします。
5. [**全般**]タブの[**オブジェクトのスキャン**]セクションで、スキャンの範囲に含めるオブジェクト種別を指定します:

- **スキャン対象オブジェクト**
  - **すべてのオブジェクト**

    すべてのオブジェクトがスキャンされます。
  - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
  - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
  - **指定の拡張子リストによってオブジェクトをスキャン**

    ファイル拡張子に基づいて、ファイルがスキャンされます。拡張子のリストは、[**編集**]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。
- **サブフォルダー**
- **サブファイル**
- **ディスクのブートセクターと MBR をスキャン**

  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、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トリームをスキャンします。

  このチェックボックスをオンにすると、感染の可能性があるオブジェクトと、そのオブジェクトに関連するすべての NTFS ストリーム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、検知され、感染の可能性があると判断されたオブジェクトのみ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. [**パフォーマンス**]セクションで、[**作成または変更されたファイルのみをスキャン**]をオンまたはオフにします。

   このチェックボックスでは、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、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、スキャンおよび保護する対象を、新規ファイルまたはすべてのファイル(変更されたかどうかを問わず)のいずれかから選択できます。

   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**]と[**推奨**]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。

> チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の[**すべての / 新しい(～のみ)**]をクリックします。

7. [**複合オブジェクトのスキャン**]セクションで、スキャンの範囲に含める複合オブジェクトを指定します:

- **すべてのアーカイブ / 新しいアーカイブのみ / 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、アーカイブがスキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

- **すべての SFX アーカイブ / 新しい SFX アーカイブのみ / 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、SFX アーカイブがスキャン時にスキップされます。

  既定値は、選択した保護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。

- **すべてのメールデータベース / 新しいメールデータベースのみ / メールデータベース**

  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、メールデータベースファイルがスキャン時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。

- **すべての圧縮されたオブジェクト / 新しい圧縮されたオブジェクトのみ / 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ファイルが、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

- **すべての通常のメール / 新しい通常のメールのみ / 通常のメール**

  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、メール形式のファイルがスキャン時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 / 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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

8. [**OK**]をクリックします。

新しいタスクの設定が保存されます。

処理の設定

► オンデマンドスキャンタスク実行中の、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する処理を設定するには:

1. **オンデマンドスキャン**のプロパティウィンドウを開きます(450 ページのセクション「**オンデマンドスキャンタスクのプロパティウィンドウ**」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. [**設定**]をクリックします。

   [**オンデマンドスキャンの設定**]ウィンドウが開きます。
4. [**設定**]をクリックします。
5. [**処理**]タブを選択します。
6. 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:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **駆除**
   - **駆除、駆除できない場合は削除**
   - **削除**
   - **推奨処理を実行**
7. 感染の可能性があるオブジェクトの処理を選択します:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **隔離**
   - **削除**
   - **推奨処理を実行**
8. 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:

   a. [**検知したオブジェクトの種別に応じて処理を実行**]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、チェックボックスの横にある[**設定**]をクリックして、検知したオブジェク

トの種別ごとに最初の処理と 2 番目の処理を独立して設定できます。この場合、選択したオプションに関わらず、感染したオブジェクトを開いたり実行することは許可されません。

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種別ごとに[**感染などの問題があるオブジェクトの処理**]および[**感染の可能性があるオブジェクトの処理**]セクションで選択された処理が実行されます。

既定では、このチェックボックスはオフです。

b. [**設定**]をクリックします。

c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理(最初の処理が失敗した場合)を選択します。

d. [**OK**]をクリックします。

9. 修正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:[**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**]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、感染の可能性がある子オブジェクト、またはその他の検知された埋め込み子オブジェクトが検知された場合に、その親の複合ファイルの強制削除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していて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、悪意のあるオブジェクト、またはその他の埋め込みオブジェクトが検知されたときに、親の複合オブジェクト全体が強制的に削除されます。親ファイルおよびそこに含まれるすべてのコンテンツの強制削除は、検知された子オブジェクトを単独で削除できない場合に発生します(たとえば親オブジェクトを修正できない場合)。

このチェックボックスをオフにしていて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、親オブジェクトを修正できないときは選択した処理は実行されません。

10. [**OK**]をクリックします。

新しいタスクの設定が保存されます。

パフォーマンスの設定

► オンデマンドスキャンタスクの実行を設定するには:

1. **オンデマンドスキャン**のプロパティウィンドウを開きます(450 ページのセクション「**オンデマンドスキャンタスクのプロパティウィンドウ**」を参照)。
2. [**スキャン範囲**]タブを選択します。
3. [**設定**]をクリックします。

   [**オンデマンドスキャンの設定**]ウィンドウが開きます。
4. [**設定**]をクリックします。
5. [**パフォーマンス**]タブを選択します。
6. [**除外リスト**]セクション:
   - [**除外するファイル**]をオフまたはオンにします。

     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、指定したオブジェクトがスキャン時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、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**]をオフまたはオンにします。

  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（https://encyclopedia.kaspersky.com/knowledge/classification/）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、指定した検知可能なオブジェクトがスキャン時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、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。

- 除外リストを追加する設定ごとに[**編集**]をクリックします。

7. [**詳細設定**]セクション:

   - **スキャン時間が次を超えたら停止する（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、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。

   - **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、スキャン時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。

     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。

   - **iSwift テクノロジーを使用する**

     iSwift は、データベースに保管されている NTFS 識別子と、現在の識別子を比較します。スキャンは、識別子が変更されたファイル（新規ファイルと、最後に実行した NTFS システムオブジェクトのスキャン以降に変更されたファイル）に対してのみ実行されます。

     このチェックボックスをオンにすると、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、ネットワークフォルダーのファイル以外では、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 ファイルシステム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ンです。

   - **iChecker テクノロジーを使用する**

     iChecker は、スキャンしたファイルのチェックサムを計算し、記憶します。オブジェクトが変更されると、チェックサムも変更されます。スキャンタスク中に、すべてのチェックサムが比較され、最後に実行したファイルスキャン以降に新規作成または更新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ンにすると、新規作成または更新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、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。

8. [**OK**]をクリックします。

新しいタスクの設定が保存されます。

リムーバブルドライブスキャンの設定

► 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。
2. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。

   表示されたポリシーのプロパティウィンドウで、[**詳細設定**]セクションを選択します。
5. [**リムーバブルドライブスキャン**]サブセクションの、[**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。
6. [**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。
7. [**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。

アプリケーションコンソールからオンデマンドスキャンタスクを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのタスクの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

オンデマンドスキャンタスクの設定ウィンドウ

► アプリケーションコンソールからオンデマンドスキャンタスクの全般的な設定を開くには:

1. アプリケーション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. 設定するタスクに該当するサブフォルダーを選択します。
3. サブフォルダーの詳細ペインで、[**プロパティ**]をクリックします。
   [**タスクの設定**]ウィンドウが表示されます。

► アプリケーションコンソールからスキャン範囲の設定ウィンドウを開くには:

1. アプリケーション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. 設定するオンデマンドスキャンタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの詳細ペインで、[**スキャン範囲の設定**]をクリックします。
   [**スキャン範囲の設定**]ウィンドウが開きます。

オンデマンドスキャンタスクの作成と編集

単一のサーバーを対象とするカスタムタスクは、[**オンデマンドスキャン**]フォルダーで作成できます。その他の Kaspersky Security for Windows Server の機能コンポーネントでは、カスタムタスクの作成を行うことはできません。

► 新規のオンデマンドスキャンタスクを作成して編集するには:

1. アプリケーションコンソールツリーで、[**オンデマンドスキャン**]フォルダーのコンテキストメニューを開きます。
2. [**タスクの追加**]を選択します。

   [**タスクの追加**]ウィンドウが開きます。
3. 次のタスクの設定を指定します:
   - **名前** - 100 文字以内のタスク名。次の記号を除くすべての記号を使用できます: **" * < > & ¥ : |**

     タスク名が指定されていないと、[**スケジュール**]タブ、[**詳細設定**]タブ、および[**実行用アカウント**]タブで、タスクの保存および新しいタスクの設定は行えません。
   - **説明** - 2000 文字以内のタスクに関する追加情報。この情報は、タスクのプロパティウィンドウに表示されます。
   - **ヒューリスティックアナライザーを使用する**

     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。
   - **バックグラウンドモードでタスクを実行する**

     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 for Windows Server タスクおよびアプリケーションによる CPU とサーバーの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 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。
   - **信頼ゾーンを適用する**

     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、信頼する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、タスクの保護範囲を判定するときに、信頼するプロセスのファイル操作が無視されます。

     既定では、このチェックボックスはオンです。
   - **タスクを簡易スキャンとする**

     このチェックボックスでは、**簡易スキャン**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、**簡易スキャン**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 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、簡易スキャン完了が記録され、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。

カスタムオンデマンドスキャンタスクでは、このチェックボックスは既定でオフです。

- **スキャンに KSN を使用する**

  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。

4. [**スケジュール**]タブおよび[**詳細設定**]タブでタスク開始スケジュールを設定します（156 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）。
5. [**実行用アカウント**]タブで、アカウント権限を使用して起動するタスクを設定します（「タスクを実行するユーザーアカウントの指定」（158 ページ）を参照）。
6. [**タスクの追加**]ウィンドウで[**OK**]をクリックします。

   新しいカスタムオンデマンドスキャンタスクが作成されます。新しいタスクの名前が付いたフォルダーがアプリケーションコンソールツリーに表示されます。操作が、システム監査ログに登録されます（208 ページ）。
7. 必要に応じて、選択したフォルダーの詳細ペインで、[**スキャン範囲の設定**]を選択します。

   [**スキャン範囲の設定**]ウィンドウが開きます。
8. サーバーのファイルリソースツリーまたはリストで、スキャンの範囲に含めるフォルダーや項目を選択します。
9. 定義済みのセキュリティレベルの 1 つを選択するか（「オンデマンドスキャンタスクの定義済みセキュリティレベルについて」（444 ページ）を参照）、またはスキャンの設定を手動で行います（「手動でのセキュリティの設定」（470 ページ）を参照）。
10. [**スキャン範囲の設定**]ウィンドウで、[**保存**]をクリックします。

設定の内容は、次回のタスク開始時に適用されます。

オンデマンドスキャンタスクのスキャン範囲

このセクションでは、オンデマンドスキャンタスクのスキャン範囲の作成と使用について説明します。

このセクションの内容

ネットワークファイルリソースのビューモードの設定

► スキャン範囲設定時のネットワークファイルリソースのビューモードを選択するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開きます。次のいずれかの処理を実行します:
   - [**ツリービュー**]を選択し、ネットワークファイルリソースをツリービューモードで表示する。
   - [**リストビュー**]を選択し、ネットワークファイルリソースをリストビューモードで表示する。

   既定では、保護対象サーバーのネットワークファイルリソースがリストビューモードで表示されます。
3. [**保存**]をクリックします。

スキャン範囲設定ウィンドウが終了します。新しい設定が適用されます。

スキャン範囲の作成

管理者のワークステーションにインストールされているアプリケーションコンソールを使用して、保護対象のサーバー上の Kaspersky Security for Windows Server をリモートで管理している場合は、保護対象のサーバー上のフォルダーを表示できるように、保護対象のサーバーの管理者グループのメンバーである必要があります。

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。

オペレーティングシステム起動時のスキャンタスクおよび簡易スキャンタスクのスキャン範囲を変更する場合は、Kaspersky Security for Windows Server 自体を復元することにより、これらのタスクの既定のスキャン範囲を復元できます([**スタート**] - [**すべてのプログラム**] - [**Kaspersky Security 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で、[**インストール済みコンポーネントの修復**]を選択して[**次へ**]をクリックし、[**製品の推奨設定を復元する**]をオンにします。

オンデマンドスキャンタスク範囲を作成する手順は、ネットワークファイルリソースのビューモードに応じて異なります(「ネットワークファイルリソースのビューモードの設定」(467 ページ)を参照)。ネットワークファイルリソースのビューモードは、ツリーまたはリスト(既定の設定)として設定できます。

► ネットワークファイルリソースツリーを使用してスキャン範囲を作成するには:

1. [**スキャン範囲の設定**]ウィンドウを開きます(464 ページ)。
2. ウィンドウの左側のセクションでネットワークファイルリソースツリーを開き、すべてのフォルダーとサブフォルダーを表示します。
3. 次の操作を行います:
   - スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにします。
   - 個別のフォルダーをスキャン範囲に含めるには、[**マイコンピューター**]をオフにして、次の操作を行います:
     - 同じ種別のすべてのドライブをスキャン範囲に含める場合は、対象のドライブ種別の名前の横にあるチェックボックスをオンにします。たとえば、サーバー上のすべてのリムーバブルドライブを追加する場合は、[**リムーバブルドライブ**]をオンにします。
     - 特定の種別の個々のドライブをスキャン範囲に含める場合は、その種別のドライブのリストを含むフォルダーを展開し、

対象のドライブの名前の横にあるチェックボックスをオンにします。たとえば、リムーバブルドライブの **F:** ドライブを選択する場合は、[**リムーバブルドライブ**]フォルダーを展開し、**F:** ドライブのチェックボックスをオンにします。

- ドライブ上のフォルダーまたはファイルを 1 つのみ含める場合は、そのフォルダーまたはファイルの名前の横にあるチェックボックスをオンにします。

4. [**保存**]をクリックします。

スキャン範囲設定ウィンドウが終了します。新しい設定が保存されます。

► ネットワークファイルリソースリストを使用してスキャン範囲を作成するには:

1. [**スキャン範囲の設定**]ウィンドウを開きます(464 ページ)。
2. 個別のフォルダーをスキャン範囲に含めるには、[**マイコンピューター**]をオフにして、次の操作を行います:
   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。
   b. ボタンのコンテキストメニューで、[**スキャン範囲を追加**]を選択します。
   c. 表示された[**スキャン範囲を追加**]ウィンドウで、追加するオブジェクトの種別を選択します:
   - **定義済みの範囲**:保護対象サーバーでいずれかの定義済み範囲を追加します。ドロップダウンリストで、必要なスキャン範囲を選択します。
   - **ディスク、フォルダー、またはネットワークの場所**:個別のドライブ、フォルダー、またはネットワークオブジェクトをスキャン範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。
   - **ファイル**:個別のファイルをスキャン範囲に含めます。[**参照**]をクリックして必要な範囲を選択します。

   オブジェクトがすでにスキャン範囲からの除外対象として追加されている場合、スキャン範囲には追加できません。
3. スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにするか、次の手順を実行します:
   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。
   b. コンテキストメニューで、[**除外の追加**]を選択します。
   c. [**除外の追加**]ウィンドウで、スキャン範囲にオブジェクトを追加する手順と同様に、スキャン範囲からの除外対象として追加するオブジェクトの種別を選択します。
4. スキャン範囲または追加する除外対象を変更するには、該当するスキャン範囲のコンテキストメニューで[**範囲の編集**]を選択します。
5. ネットワークファイルリソースのリストに以前追加したスキャン範囲または除外対象を非表示にするには、該当するスキャン範囲のコンテキストメニューで[**リストから削除**]を選択します。

   スキャン範囲がネットワークファイルリソースリストから削除されたときに、オンデマンドスキャンタスクの範囲から除外されます。
6. [**保存**]をクリックします。

スキャン範囲設定ウィンドウが終了します。新しい設定が保存されます。

スキャン範囲にネットワークオブジェクトを含める

UNC(ユニバーサルネーミング規約)フォーマットでパスを指定して、ネットワークドライブ、フォルダー、またはファイルをスキャン範囲に

追加することができます。

システムアカウントでネットワークフォルダーをスキャンできます。

► ネットワーク上の場所をスキャン範囲に追加するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。
3. [**ネットワーク**]フォルダーのコンテキストメニューを開きます:
   - スキャン範囲にネットワークフォルダーを追加する場合は、[**ネットワークフォルダーの追加**]を選択します。
   - スキャン範囲にネットワークファイルを追加する場合は、[**ネットワークファイルの追加**]を選択します。
4. ネットワークフォルダーまたはネットワークファイルへのパスを UNC フォーマットで入力して、**ENTER** キーを押します。
5. 新しく追加されたネットワークオブジェクトの横にあるチェックボックスをオンにして、スキャン範囲に含めます。
6. 必要に応じて、追加したネットワークオブジェクトのセキュリティ設定を変更します。
7. [**保存**]をクリックします。

変更されたタスクの設定が保存されます。

仮想スキャン範囲の作成

ダイナミックドライブ、フォルダー、およびファイルは、仮想スキャン範囲を作成するためにスキャン範囲に含めることができます。

ファイルリソースのツリーとして保護範囲またはスキャン範囲が表示されている場合に限り、個別の仮想ドライブ、フォルダー、またはファイルを追加して、保護範囲またはスキャン範囲を拡張することができます(「ネットワークファイルリソースのビューモードの設定」(467 ページ)を参照)。

► 仮想ドライブをスキャン範囲に追加するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。
3. サーバーファイルリソースのツリーで、[**仮想ドライブ**]フォルダーのコンテキストメニューを開き、[**仮想ドライブの追加**]をクリックして、使用可能な名前のリストから仮想ドライブ名を選択します。
4. 追加したドライブの横のチェックボックスをオンにして、ドライブをスキャン範囲に含めます。
5. [**保存**]をクリックします。

変更されたタスクの設定が保存されます。

► 仮想フォルダーまたは仮想ファイルをスキャン範囲に追加するには:

1. [**スキャン範囲の設定**]ウィンドウを開きます(464 ページ)。
2. ウィンドウの左上部にあるドロップダウンリストより、[**ツリービュー**]を選択します。

3. サーバーのファイルリソースツリーでフォルダーまたはファイルを追加するフォルダーのコンテキストメニューを開き、次のいずれかを選択します:
   - **仮想フォルダーの追加**:スキャン範囲に仮想フォルダーを追加する場合に選択します。
   - **仮想ファイルの追加**:スキャン範囲に仮想ファイルを追加する場合に選択します。
4. 入力フィールドに、フォルダーまたはファイルの名前を指定します。
5. 作成されたフォルダーまたはファイルの名前と同じチェックボックスをオンにして、このフォルダーまたはファイルをスキャン範囲に追加します。
6. [**保存**]をクリックします。

変更されたタスクの設定が保存されます。

オンデマンドスキャンタスクの定義済みセキュリティレベルの選択

サーバーのネットワークファイルリソースのツリーまたはリストで選択したフォルダーや項目に対して、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**]。

► 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:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. サーバーのネットワークファイルリソースのツリーまたはリストで、定義済みのセキュリティレベルを設定するフォルダーや項目を選択します。
3. 選択したフォルダーや項目がスキャン範囲に含まれることを確認します。
4. ウィンドウの右側の[**セキュリティレベル**]タブで、適用するセキュリティレベルを選択します。

   選択したセキュリティレベルに対応するセキュリティ設定のリストが表示されます。
5. [**保存**]をクリックします。

   構成されたタスクの設定が保存され、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。

手動でのセキュリティの設定

オンデマンドスキャンタスクでは、既定でスキャン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、定義済みセキュリティレベルの[**推奨**]に対応します(242 ページのセクション「定義済みのセキュリティレベル」を参照)。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはサーバーのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定することができます。

ネットワーク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。

► 手動でセキュリティを設定するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。

2. ウィンドウの左側のセクションで、セキュリティ設定を行うフォルダーまたは項目を選択します。

   セキュリティ設定を含む定義済みのテンプレート(「セキュリティ設定テンプレートについて」(162 ページ)を参照)は、スキャン範囲内の選択したフォルダーや項目に適用できます。

3. 要件に従って、次のタブで、選択したフォルダーや項目に必要なセキュリティを設定します:
   - 全般設定(471 ページのセクション「タスクの全般的な設定」を参照)
   - 処理(473 ページのセクション「処理の設定」を参照)
   - パフォーマンス(475 ページのセクション「パフォーマンスの設定」を参照)
   - 階層型ストレージ
4. [**スキャン範囲の設定**]ウィンドウで、[**保存**]をクリックします。

新しいスキャン範囲の設定が保存されます。

このセクションの内容

タスクの全般的な設定

► オンデマンドスキャンタスクのセキュリティの全般設定を行うには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. [**全般**]タブを選択します。
3. [**オブジェクトのスキャン**]セクションで、スキャンの範囲に含めるオブジェクト種別を指定します:
   - **スキャン対象オブジェクト**
     - **すべてのオブジェクト**

       すべてのオブジェクトがスキャンされます。
     - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
     - **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。リストは、Kaspersky Security for Windows Server の定義データベースに含まれています。
     - **指定の拡張子リストによってオブジェクトをスキャン**

       ファイル拡張子に基づいて、ファイルがスキャンされます。拡張子のリストは、[**編集**]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**

  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、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トリームをスキャンします。

  このチェックボックスをオンにすると、感染の可能性があるオブジェクトと、そのオブジェクトに関連するすべての NTFS ストリーム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、検知され、感染の可能性があると判断されたオブジェクトのみ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。

4. [**パフォーマンス**]セクションで、[**作成または変更されたファイルのみをスキャン**]をオンまたはオフにします。

   このチェックボックスでは、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、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、スキャンおよび保護する対象を、新規ファイルまたはすべてのファイル(変更されたかどうかを問わず)のいずれかから選択できます。

   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**]と[**推奨**]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。

> チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の[**すべての / 新しい(～のみ)**]をクリックします。

5. [**複合オブジェクトのスキャン**]セクションで、スキャンの範囲に含める複合オブジェクトを指定します:

   - **すべてのアーカイブ / 新しいアーカイブのみ / 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、アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護レベルによって異なります。

   - **すべての SFX アーカイブ / 新しい SFX アーカイブのみ / 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、SFX アーカイブがスキャン時にスキップされます。

     既定値は、選択した保護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。

   - **すべてのメールデータベース / 新しいメールデータベースのみ / メールデータベース**

     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、メールデータベースファイルがスキャン時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。

- **すべての圧縮されたオブジェクト / 新しい圧縮されたオブジェクトのみ / 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ファイルが、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

- **すべての通常のメール / 新しい通常のメールのみ / 通常のメール**

  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、メール形式のファイルがスキャン時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 / 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、スキャン時にスキップされます。

  既定値は、選択した保護レベルによって異なります。

6. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

処理の設定

► オンデマンドスキャンタスクで、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の処理を設定するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. [**処理**]タブを選択します。
3. 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:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモー

ドは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。

- **駆除**
- **駆除、駆除できない場合は削除**
- **削除**
- **推奨処理を実行**

4. 感染の可能性があるオブジェクトの処理を選択します:
   - **通知のみ**

     このモードを選択すると、検知されたオブジェクトやその他の検知されたオブジェクトへのアクセスがブロックされず、処理も実行されません。次のイベントがタスク実行ログに追記されます:**オブジェクトが駆除されませんでした。理由:ユーザー定義の設定により、検知したオブジェクトを無害化する処理は実行されませんでした。**このイベントは、検知されたオブジェクトに関する入手可能なすべての情報を示します。

     [**通知のみ**]モードは、保護領域ごとまたはスキャン領域ごとに個別に設定する必要があります。このモードは、既定ではどのセキュリティレベルでも使用されません。このモードを選択すると、セキュリティレベルが[**カスタム**]に自動的に変更されます。
   - **隔離**
   - **削除**
   - **推奨処理を実行**
5. 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:
   a. [**検知したオブジェクトの種別に応じて処理を実行**]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、チェックボックスの横にある[**設定**]をクリックして、検知したオブジェクトの種別ごとに最初の処理と 2 番目の処理を独立して設定できます。この場合、選択したオプションに関わらず、感染したオブジェクトを開いたり実行することは許可されません。

      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種別ごとに[**感染などの問題があるオブジェクトの処理**]および[**感染の可能性があるオブジェクトの処理**]セクションで選択された処理が実行されます。

      既定では、このチェックボックスはオフです。

   b. [**設定**]をクリックします。

   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理(最初の処理が失敗した場合)を選択します。

   d. [**OK**]をクリックします。
6. 修正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:[**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**]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、感染の可能性がある子オブジェクト、またはその他の検知された埋め込み子オブジェクトが検知された場合に、その親の複合ファイルの強制削除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していて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、悪意のあるオブジェクト、またはその他の埋め込みオブジェクトが検知されたときに、親の複合オブジェクト全体が強制的に削除されます。親ファイルおよびそこに含まれるすべてのコンテンツの強制削除は、検知された子オブジェクトを単独で削除できない場合に発生します(たとえば親オブジェクトを修正できない場合)。

   このチェックボックスをオフにしていて、なおかつ感染したオブジェクトおよび感染の可能性があるオブジェクトを削除するようにタスクが設定されている場合、親オブジェクトを修正できないときは選択した処理は実行されません。

7. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

パフォーマンスの設定

► オンデマンドスキャンタスクの実行を設定するには:

1. [**スキャン範囲の設定**](464 ページ)ウィンドウを開きます。
2. [**パフォーマンス**]タブを選択します。
3. [**除外リスト**]セクション:
   - [**除外するファイル**]をオフまたはオンにします。

     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、指定したオブジェクトがスキャン時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、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**]をオフまたはオンにします。

     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(https://encyclopedia.kaspersky.com/knowledge/classification/)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、指定した検知可能なオブジェクトがスキャン時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、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。
   - 除外リストを追加する設定ごとに[**編集**]をクリックします。
4. [**詳細設定**]セクション:
   - **スキャン時間が次を超えたら停止する(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、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。
   - **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、スキャン時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。

     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。
   - **iSwift テクノロジーを使用する**

     iSwift は、データベースに保管されている NTFS 識別子と、現在の識別子を比較します。スキャンは、識別子が変更されたファイル(新規ファイルと、最後に実行した NTFS システムオブジェクトのスキャン以降

に変更されたファイル）に対してのみ実行されます。

このチェックボックスをオンにすると、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、ネットワークフォルダーのファイル以外では、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 ファイルシステム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ンです。

- **iChecker テクノロジーを使用する**

  iChecker は、スキャンしたファイルのチェックサムを計算し、記憶します。オブジェクトが変更されると、チェックサムも変更されます。スキャンタスク中に、すべてのチェックサムが比較され、最後に実行したファイルスキャン以降に新規作成または更新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ンにすると、新規作成または更新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、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。

5. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

階層型ストレージの設定

► オンデマンドスキャンタスクで、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の処理を設定するには:

1. [**スキャン範囲の設定**]（464 ページ）ウィンドウを開きます。
2. [**階層型ストレージ**]タブを選択します。
3. オフラインファイルの処理を選択します:
   - **スキャンしない**
   - **ファイルの常駐部分のみスキャン**
   - **ファイル全体をスキャンする**

     この処理を選択すると、次のオプションを指定できます:

     - [**指定した期間（日数）にアクセスされた場合のみ**]をオンまたはオフにして、オンの場合は日数を指定します。
     - [**可能な場合はローカルのハードディスクにファイルをコピーしない**]をオンまたはオフにします。
4. [**保存**]をクリックします。

新しいタスクの設定が保存されます。

リムーバブルドライブのスキャン

► アプリケーションコンソールから、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を設定するには:

1. アプリケーション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、[**リムーバブルドライブ**

スキャンを設定]を選択します。

[**リムーバブルドライブスキャン**]ウィンドウが開きます。

2. [**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。
3. [**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。

オンデマンドスキャンタスクの統計情報

オンデマンドスキャンタスクの実行中は、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数に関する情報を表示できます。

タスクが一時停止中であっても、この情報は使用できます。実行ログで、タスクの統計情報を表示できます(「タスク実行ログでの Kaspersky Security for Windows Server のタスクに関する統計と情報の表示」(212 ページ)を参照)。

► オンデマンドスキャンタスクの統計情報を表示するには、次の手順を実行します:

1. アプリケーション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. 統計情報を表示するオンデマンドスキャンタスクを選択します。

選択したフォルダーの詳細ペインにある[**統計情報**]セクションに、タスクの統計情報が表示されます。

タスクが開始されてから現在までに Kaspersky Security for Windows Server によって処理されたオブジェクトに関する情報を表示できます(次の表を参照)。

表 69. オンデマンドスキャンタスクの統計情報

フィールド	説明
検知	検知されたオブジェクトの数。たとえば、5 つのファイルから 1 つのマルウェアが検知された場合、このフィールドの値が 1 つ加算されます。
感染などの問題があるオブジェクトの検知	検知され、感染として分類されたオブジェクトの数、または侵入者がコンピューターや個人情報に損害を与える目的で使用する可能性がある正規のソフトウェアとして分類されたファイルの検知数(リアルタイム保護タスクとオンデマンドスキャンタスクの範囲から除外されていない場合)。
感染の可能性があるオブジェクトの検知	Kaspersky Security for Windows Server が感染の可能性を検知したオブジェクトの数。
駆除されていないオブジェクト	次の理由により、駆除されなかったオブジェクトの数: • 検知したオブジェクトが、駆除できない種別である。 • 駆除中にエラーが発生した。

フィールド	説明
隔離されていないオブジェクト	隔離に移動しようとしたが、ディスク容量不足などにより移動できなかったオブジェクトの数。
削除されていないオブジェクト	削除しようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由で削除できなかったオブジェクトの数。
スキャンされていないオブジェクト	スキャンしようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由でスキャンできなかったオブジェクトの数。
バックアップされていないオブジェクト	バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存できなかったオブジェクトの数。
処理エラー	処理がエラーになったオブジェクトの数。
駆除されたオブジェクト	駆除されたオブジェクトの数。
隔離済み	隔離されたオブジェクトの数。
バックアップ済み	バックアップに保存されたオブジェクトコピーの数。
削除されたオブジェクト	削除されたオブジェクトの数。
パスワードで保護されているオブジェクト	パスワードで保護されていたため、スキップされたオブジェクト（アーカイブなど）の数。
破損しているオブジェクト	フォーマットが破損していたため、スキップされたオブジェクトの数。
処理されたオブジェクト	処理されたオブジェクトの合計数。

オンデマンドスキャンタスクの統計情報を選択したタスク実行ログに表示するには、詳細ペインの［**管理**］セクションにある［**実行ログを開く**］をクリックします。

タスクの完了時には、［**イベント**］タブの実行ログに登録されているイベントを手動で処理してください。

信頼ゾーン

このセクションでは、Kaspersky Security for Windows Server の信頼ゾーンに関する情報、およびタスク実行時に信頼ゾーンにオブジェクトを追加する手順について説明します。

この章の内容

信頼ゾーンについて

信頼ゾーンは、オンデマンドスキャン、ファイルのリアルタイム保護、トラフィックセキュリティ、スクリプト監視、RPC ネットワークストレージの保護の各タスクに対して生成して適用できる、保護またはスキャン範囲から除外するリストです。

Kaspersky Security for Windows Server のインストール時に[**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**]と[**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**]をオンにしていた場合、ファイルのリアルタイム保護タスクで、Microsoft およびカスペルスキーによって推奨されているファイルが信頼ゾーンに追加されます。

次のルールに従い、Kaspersky Security for Windows Server で信頼ゾーンを作成できます:

- 信頼するプロセス:ファイルの監視の影響を受けやすいアプリケーションのプロセスによってアクセスされるオブジェクトは、信頼ゾーンに配置されます。
- バックアップ処理:ハードディスクを外部デバイスにバックアップするためにシステムによってアクセスされるオブジェクトは、信頼ゾーンに配置されます。
- 除外リスト:場所によって指定されたオブジェクト、または指定したオブジェクトの内部で検知されたオブジェクトは、信頼ゾーンに配置されます。

信頼ゾーンは、ファイルのリアルタイム保護、トラフィックセキュリティ、スクリプト監視、RPC ネットワークストレージの保護の各タスク、新しく作成されたカスタムオンデマンドスキャンタスク、すべてのシステムのオンデマンドスキャンタスク(隔離のスキャンタスクを除く)に適用できます。

既定では、ファイルのリアルタイム保護タスクおよびオンデマンドスキャンタスクに適用されます。

信頼ゾーンを生成するためのルールのリストは、XML 形式で設定ファイルにエクスポートして、別のサーバーで実行されている Kaspersky Security for Windows Server にインポートできます。

信頼するプロセス

ファイルのリアルタイム保護タスクとトラフィックセキュリティタスクに適用されます。

一部のサーバー上のアプリケーションでは、アクセスするファイルの情報が Kaspersky Security for Windows Server によって途中で取得されると、不安定になる場合があります。そのようなアプリケーションには、システムドメインコントローラーアプリケーションなどがあります。

そのようなアプリケーションの動作を妨害しないように、それらのアプリケーションが実行するプロセスによってアクセスされるファイルの保護を無効にすることができます(これにより、信頼ゾーン内に信頼するプロセスのリストが作成されます)。

Microsoft の推奨事項に基づいて、ファイルのリアルタイム保護から、一部の Microsoft Windows オペレーティングシステムファイルと Microsoft アプリケーションファイルを、感染しないプログラムとして除外してください。これらの一部は、Microsoft の Web サイト https://www.microsoft.com/ja-jp/ に名前が記載されています(記事コード:KB822158)。

信頼ゾーンの信頼するプロセスの使用は、有効にすることも無効にすることもできます。

更新などで実行可能プロセスファイルが変更された場合、信頼するプロセスのリストからそのファイルが除外されます。

本製品では、プロセスを信頼するために保護対象サーバーのファイルのパスの値を適用することはありません。保護対象サーバーのファイルへのパスは、ファイルの検索、チェックサムの計算、およびユーザーに対する実行ファイルのソースに関する情報の提供のみに使用されます。

バックアップ処理

サーバーのリアルタイム保護タスクに適用されます。

ハードディスクに格納されているデータを外部デバイスにバックアップする際には、バックアップ処理時にアクセスされるオブジェクトの保護を無効にできます。Kaspersky Security for Windows Server では、バックアップのコピーアプリケーションで開いて読み取られる FILE_FLAG_BACKUP_SEMANTICS 属性のオブジェクトがスキャンされます。

除外

ファイルのリアルタイム保護タスク、トラフィックセキュリティタスク、RPC ネットワークストレージの保護タスク、オンデマンドスキャンタスクに適用されます。

信頼ゾーンに追加されたすべての除外対象を使用するタスクを選択できます。Kaspersky Security for Windows Server の個々のタスクのセキュリティレベルの設定で、オブジェクトをスキャン対象から除外することもできます。

サーバー上の場所、そのオブジェクト内で検知されたオブジェクトの名前または名前マスク、またはその両方の条件を使用して、信頼ゾーンにオブジェクトを追加できます。

除外するオブジェクトに基づいて、指定されたタスクの実行時に Kaspersky Security for Windows Server で次のオブジェクトをスキップできます:

- サーバーまたはネットワーク接続ストレージの指定された領域内で、名前または名前マスクで指定された検知可能なオブジェクト。
- サーバーまたはネットワーク接続ストレージの指定された領域内で、検知可能なすべてのオブジェクト。
- 保護範囲またはスキャン範囲全体で、名前または名前マスクで指定された検知可能なオブジェクト

管理プラグインから信頼ゾーンを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーの信頼ゾーン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

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

Kaspersky Security Center からのアプリケーションの管理

► Kaspersky Security Center のポリシーから信頼ゾーンを開くには:

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**詳細設定**]セクションを選択します。
6. [**信頼ゾーン**]サブセクションの[**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。

必要に応じてポリシーを設定します。

サーバーが 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、アプリケーションコンソールでこれらの設定を編集することはできません。

信頼ゾーンのプロパティウィンドウ

► [アプリケーションのプロパティ]ウィンドウで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ます。
2. タスクを設定する管理グループを選択します。
3. [**デバイス**]タブを選択します。
4. 次のいずれかの方法で、サーバ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。
   - 保護対象サーバーのコンテキストメニューで[**プロパティ**]を選択します。

サーバーのプロパティウィンドウが表示されます。

5. [**アプリケーション**]セクションで、[**Kaspersky Security for Windows Server**]を選択します。
6. [**プロパティ**]をクリックします。

   Kaspersky Security for Windows Server のアプリケーション設定ウィンドウが開きます。
7. [**詳細設定**]セクションを選択します。
8. [**信頼ゾーン**]サブセクションの[**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。

必要に応じて信頼ゾーンを設定します。

信頼ゾーンの管理プラグインからの設定

既定では、新しく作成されたすべての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、次の手順を実行します:

1. [**除外**]タブで、タスクの実行時にスキップするオブジェクトを指定できます(482 ページのセクション「除外の追加」を参照)。
2. [**信頼するプロセス**]タブで、タスクの実行時にスキップするプロセスを指定できます(484 ページのセクション「信頼するプロセスの追加」を参照)。
3. not-a-virus(非ウイルス)マスクを適用します(486 ページのセクション「not-a-virus(非ウイルス)マスクの適用」を参照)。

このセクションの内容

除外の追加

► Kaspersky Security Center のポリシーから信頼ゾーンに除外を追加するには:

1. [**信頼ゾーン**]ウィンドウを開きます(481 ページの「**Kaspersky Security Center からのアプリケーションの管理**」を参照)。
2. [**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 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。

     [**除外**]ウィンドウが開きます。
3. [**次の条件が満たされた場合はオブジェクトをスキャンしない**]セクションで、保護範囲またはスキャン範囲から除外するオブ

ジェクトと、検知可能なオブジェクトから除外するオブジェクトを指定します:

- 保護範囲またはスキャン範囲からオブジェクトを除外するには:

  a. [**スキャン対象オブジェクト**]をオンにします。

  ファイル、フォルダー、ドライブ、スクリプトファイルが除外対象に追加されます。

  このチェックボックスをオンにすると、[**ルールの適用範囲**]で選択した Kaspersky Security for Windows Server のコンポーネントを使用してスキャンを実行する場合に、指定した定義済みの範囲、ファイル、フォルダー、ドライブ、スクリプトファイルがスキップされます。

  既定では、このチェックボックスはオフです。

  b. [**編集**]をクリックします。

  [**オブジェクトを選択**]ウィンドウが開きます。

  c. スキャンの範囲から除外するオブジェクトを指定します。

  > オブジェクトを指定するときに、特殊記号 ? と * を使用できます。

  d. [**OK**]をクリックします。

  e. 指定されたオブジェクトの下位に置かれているすべてのファイルとフォルダーを保護範囲またはスキャン範囲から除外する場合は、[**サブフォルダーにも適用**]をオンにします。

- 検知可能なオブジェクトの名前を指定するには:

  a. [**検知対象オブジェクト**]をオンにします。

  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（https://encyclopedia.kaspersky.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、指定した検知可能なオブジェクトがスキャン時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、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。

  b. [**編集**]をクリックします。

  [**オブジェクトのリスト**]ウィンドウが開きます。

  c. ウイルス百科事典の分類に従い、検知可能なオブジェクトの名前または名前のマスクを指定します。

  d. [**追加**]をクリックします。

  e. [**OK**]をクリックします。

4. [**ルールの適用範囲**]セクションで、除外を適用するタスクの名前の横にあるチェックボックスをオンにします。

   ルールが使用される Kaspersky Security for Windows Server タスクの名前。

5. [**OK**]をクリックします。

[**信頼ゾーン**]ウィンドウの[**除外リスト**]タブのリストに、除外対象オブジェクトが表示されます。

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. [**信頼ゾーン**]ウィンドウを開きます(481 ページの「Kaspersky Security Center からのアプリケーションの管理」を参照)。
2. [**信頼するプロセス**]タブを選択します。
3. ファイルの読み取り操作のスキャンをスキップするには、[**ファイルのバックアップ処理を確認しない**]をオンにします。

   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の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、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。
4. 信頼するプロセスのファイル操作のスキャンをスキップするには、[**指定したプロセスでのファイルの処理をチェックしない**]をオンにします。

   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、信頼するプロセスの操作の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、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。
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. **信頼対象と判断する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、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

     チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

     既定では、このチェックボックスはオフです。

     b. **信頼対象と判断する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、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が決定されます。

     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判定する基準として、ファイルのハッシュは使

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。

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 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、プロセス識別子(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。ローカルサーバーでアプリケーションコンソールを使用するか、あるいは指定されたホスト設定で Kaspersky Security Center を使用している場合のみ、[**プロセス**]をクリックして実行中のプロセスを選択できます。

- **ファイル名とパスに基づく 1 つのプロセス**

  [**プロセスの追加**]ウィンドウで、次を実行します:

  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**

  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. [**参照**]をクリックしてプロセスを選択します。

  b. **信頼対象と判断する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、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

  チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

  既定では、このチェックボックスはオフです。

  c. **信頼対象と判断する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、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が決定されます。

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判定する基準として、ファイルのハッシュは使用されません。

既定では、このチェックボックスはオンです。

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. [**信頼するプロセスの追加**]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正規の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 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. [**信頼ゾーン**]ウィンドウを開きます(481 ページの「Kaspersky Security Center からのアプリケーションの管理」を参照)。
2. チェックボックスがオフの場合、[**除外リスト**]タブの[**検知対象オブジェクト**]列でリストをスクロールして、「**not-a-virus:***」(非ウイルス)という値の行を選択します。
3. [**OK**]をクリックします。

新しい設定が適用されます。

アプリケーションコンソールから信頼ゾーンを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーの信頼ゾーン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

アプリケーションコンソールでタスクに信頼ゾーンを適用する

既定では、信頼ゾーンは、ファイルのリアルタイム保護タスク、新しく作成されたカスタムオンデマンドスキャンタスク、すべてのシステムのオンデマンドスキャンタスク（隔離のスキャンタスクを除く）に適用されます。

信頼ゾーンを有効化または無効化すると、指定された除外対象オブジェクトに即座に適用されるか、あるいは実行中のタスクでの適用が終了します。

► Kaspersky Security for Windows Server タスクで信頼ゾーンの使用を有効または無効にするには:

1. アプリケーションコンソールツリーで、信頼ゾーンの使用を設定するタスクの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。

   [**タスクの設定**]ウィンドウが表示されます。
3. ウィンドウが表示されたら[**全般**]タブを選択し、次のいずれかの操作を実行します:
   - タスクで信頼ゾーンを適用するには、[**信頼ゾーンを適用する**]をオンにします。
   - タスクで信頼ゾーンを無効にするには、[**信頼ゾーンを適用する**]をオフにします。
4. 信頼ゾーンを設定するには、[**信頼ゾーンを適用する**]のリンク部分をクリックします。

   [**信頼ゾーン**]ウィンドウが開きます。
5. [**タスクの設定**]ウィンドウで、[**OK**]をクリックして変更を保存します。

アプリケーションコンソールでの信頼ゾーンの設定

信頼ゾーンを設定するには、次の手順を実行します:

1. [**除外**]タブで、タスクの実行時にスキップするオブジェクトを指定できます（488 ページのセクション「除外対象オブジェクトの信頼ゾーンへの追加」を参照）。
2. [**信頼するプロセス**]タブで、タスクの実行時にスキップするプロセスを指定できます（489 ページのセクション「信頼するプロセス」を参照）。
3. 製品のタスクに信頼ゾーンを適用します（487 ページのセクション「アプリケーションコンソールでタスクに信頼ゾーンを適用する」を参照）。
4. not-a-virus（非ウイルス）マスクを適用します（492 ページのセクション「not-a-virus（非ウイルス）マスクの適用」を参照）。

このセクションの内容

除外対象オブジェクトの信頼ゾーンへの追加

► アプリケーションコンソールを使用して、除外するオブジェクトを信頼ゾーンに手動で追加するには：

1. アプリケーション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. [**信頼ゾーンの設定**]メニューオプションを選択します。

   [**信頼ゾーン**]ウィンドウが開きます。
3. [**除外**]タブを選択します。
4. [**追加**]をクリックします。

   [**除外**]ウィンドウが開きます。
5. [**次の条件が満たされた場合はオブジェクトをスキャンしない**]セクションで、保護範囲またはスキャン範囲から除外するオブジェクトと、検知可能なオブジェクトから除外するオブジェクトを指定します：
   - 保護範囲またはスキャン範囲からオブジェクトを除外するには：

     a. [**スキャン対象オブジェクト**]をオンにします。

     ファイル、フォルダー、ドライブ、スクリプトファイルが除外対象に追加されます。

     このチェックボックスをオンにすると、[**ルールの適用範囲**]で選択した Kaspersky Security for Windows Server のコンポーネントを使用してスキャンを実行する場合に、指定した定義済みの範囲、ファイル、フォルダー、ドライブ、スクリプトファイルがスキップされます。

     既定では、このチェックボックスはオフです。

     b. [**編集**]をクリックします。

     [**オブジェクトを選択**]ウィンドウが開きます。

     c. スキャンの範囲から除外するオブジェクトを指定します。

     > オブジェクトを指定するときに、特殊記号 ？ と * を使用できます。

     d. [**OK**]をクリックします。

     e. 指定されたオブジェクトの下位に置かれているすべてのファイルとフォルダーを保護範囲またはスキャン範囲から除外する場合は、[**サブフォルダーにも適用**]をオンにします。

- 検知可能なオブジェクトの名前を指定するには:

  a. [**検知対象オブジェクト**]をオンにします。

  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（https://encyclopedia.kaspersky.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、指定した検知可能なオブジェクトがスキャン時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、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。

  b. [**編集**]をクリックします。

  [**オブジェクトのリスト**]ウィンドウが開きます。

  c. ウイルス百科事典の分類に従い、検知可能なオブジェクトの名前または名前のマスクを指定します。

  d. [**追加**]をクリックします。

  e. [**OK**]をクリックします。

6. [**ルールの適用範囲**]セクションで、除外を適用するタスクの名前の横にあるチェックボックスをオンにします。

   ルールが使用される Kaspersky Security for Windows Server タスクの名前。

7. [**OK**]をクリックします。

[**信頼ゾーン**]ウィンドウの[**除外リスト**]タブのリストに、除外対象オブジェクトが表示されます。

信頼するプロセス

次のいずれかの方法を使用して、信頼するプロセスのリストにプロセスを追加できます:

- 保護対象のサーバーで実行中のプロセスのリストから、対象のプロセスを選択する方法。
- プロセスの実行ファイルを選択する方法。この方法では、プロセスが現在実行されているかどうかは関係ありません。

  プロセスの実行ファイルが変更されている場合、信頼するプロセスのリストからこのプロセスが除外されます。

► 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. アプリケーション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. [**信頼ゾーンの設定**]メニューオプションを選択します。

   [**信頼ゾーン**]ウィンドウが開きます。
3. [**信頼するプロセス**]タブを選択します。
4. ファイルの読み取り操作のスキャンをスキップするには、[**ファイルのバックアップ処理を確認しない**]をオンにします。

   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の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、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。

5. 信頼するプロセスのファイル操作のスキャンをスキップするには、[**指定したプロセスでのファイルの処理をチェックしない**]をオンにします。

   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、信頼するプロセスの操作の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、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. [**追加**]をクリックします。

7. 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. **信頼対象と判断する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、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

        チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

        既定では、このチェックボックスはオフです。

     b. **信頼対象と判断する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、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が決定されます。

        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判定する基準として、ファイルのハッシュは使用されません。

        既定では、このチェックボックスはオンです。

     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 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、プロセス識別子(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。ローカルサーバーでアプリケーションコンソールを使用するか、あるいは指定されたホスト設定で Kaspersky Security Center を使用している場合のみ、[**プロセス**]をクリックして実行中のプロセスを選択できます。

- **ファイル名とパスに基づく 1 つのプロセス**

  [**プロセスの追加**]ウィンドウで、次を実行します:

  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**

  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. [**参照**]をクリックしてプロセスを選択します。

  b. **信頼対象と判断する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、ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。

  チェックボックスがオフの場合、プロセスを信頼するかどうかを判定する基準として、ファイルのパスは使用されません。

  既定では、このチェックボックスはオフです。

  c. **信頼対象と判断する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、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が決定されます。

  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判定する基準として、ファイルのハッシュは使用されません。

  既定では、このチェックボックスはオンです。

  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。

8. [**信頼するプロセスの追加**]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正規の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 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. アプリケーション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. [**信頼ゾーンの設定**]メニューオプションを選択します。

   [**信頼ゾーン**]ウィンドウが開きます。
3. [**除外**]タブを選択します。
4. チェックボックスがオフの場合、リストをスクロールして、「**not-a-virus:***」（非ウイルス）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。

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について

Kaspersky Security 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、保護対象プロセスに外部のプロセス保護エージェント(「エージェント」)を挿入することによってプロセスメモリを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 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軽減できます。

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 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、プロセスを終了する。
- プロセスが危険にさらされている事実を報告する。

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 脆弱性攻撃ブロックサービス

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 脆弱性攻撃ブロック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 脆弱性攻撃ブロックサービスが停止したあと、Kaspersky Security 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ブロック技術を適用してプロセスメモリを保護します。

Kaspersky Security 脆弱性攻撃ブロック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 for Windows Server はプロセスを終了しません。

- **通知のみ**:このモードを適用すると、セキュリティログ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の試行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 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。

管理プラグインから脆弱性攻撃ブロックを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべてのサーバーのコンポーネントの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

脆弱性攻撃ブロックのポリシーの設定ウィンドウ

► **脆弱性攻撃ブロックの設定を Kaspersky Security Center のポリシーから開くには:**

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. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**サーバーのリアルタイム保護**]セクションを選択します。
6. [**脆弱性攻撃ブロック**]サブセクションの[**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。

必要に応じて脆弱性攻撃ブロックを設定します。

脆弱性攻撃ブロックのプロパティウィンドウ

► **サーバーのプロパティウィンドウで、脆弱性攻撃ブロックのセクションを開くには:**

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. タスクを設定する管理グループを選択します。
3. [**デバイス**]タブを選択します。
4. 次のいずれかの方法で、サーバ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。
   - 保護対象サーバーのコンテキストメニューで[**プロパティ**]を選択します。

   サーバーのプロパティウィンドウが表示されます。
5. [**アプリケーション**]セクションで、[**Kaspersky Security for Windows Server**]を選択します。
6. [**プロパティ**]をクリックします。

   Kaspersky Security for Windows Server のアプリケーション設定ウィンドウが開きます。
7. [**サーバーのリアルタイム保護**]セクションを選択します。
8. [**脆弱性攻撃ブロック**]サブセクションの[**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。

必要に応じて脆弱性攻撃ブロックを設定します。

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. **脆弱性攻撃ブロック**ウィンドウを開きます(495 ページのセクション「**脆弱性攻撃ブロックのポリシーの設定ウィンドウ**」を参照)。
2. [**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、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軽減できます。

     このチェックボックスがオフの場合、サーバープロセスを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、脆弱性攻撃試行を検知すると保護対象プロセスが終了します。
   - **通知のみ**

     このモードを選択すると、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されます。危険にさらされたプロセスは実行され続けます。

     [**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が検知された場合、コンポーネントが強制的に[**通知のみ**]モードに切り替わります。
3. [**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、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が、ターミナルウィンドウに表示されます。

     チェックボックスがオフの場合、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が、ターミナルウィンドウに表示されます。ターミナルウィンドウは、Kaspersky Security 脆弱性攻撃ブロック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 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軽減できます。Kaspersky Security 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 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。
4. [**OK**]をクリックします。

Kaspersky Security 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。リストの該当するチェックボックスをオフにすることで、処理を保護範囲から

除外できます。

► 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. **脆弱性攻撃ブロック**ウィンドウを開きます(495 ページのセクション「**脆弱性攻撃ブロックのポリシーの設定ウィンドウ**」を参照)。
2. [**保護対象プロセス**]タブで、[**参照**]をクリックします。

   Microsoft Windows のエクスプローラーのウィンドウが表示されます。
3. リストに追加するプロセスを選択します。
4. [**開く**]をクリックします。

   プロセス名が表示されます。
5. [**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。
6. 追加したプロセスを選択します。
7. [**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技術**]ウィンドウが開きます。
8. 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。既定では、プロセスに使用できる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する**

     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 技術を適用する**]をオンまたはオフにします。
9. Attack Surface Reduction 技術を設定します:
   - [**次のモジュールを拒否する**]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、モジュールを拒否しない**]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。
10. [**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。

アプリケーションコンソールから脆弱性攻撃ブロックを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、ローカルサーバーのコンポーネントの設定を行う方法について説明します。

このセクションの内容

操作方法

必要なタスクの設定をインターフェイスから操作する方法について説明します。

このセクションの内容

脆弱性攻撃ブロックの全般的な設定ウィンドウ

► [脆弱性攻撃ブロックの設定]ウィンドウを開くには:

1. アプリケーションコンソールツリーで、[**Kaspersky Security**]フォルダーを選択します。
2. コンテキストメニューを開いて[**脆弱性攻撃ブロック:一般設定**]メニューオプションを選択します。

   [**脆弱性攻撃ブロックの設定**]ウィンドウが開きます。

必要に応じて脆弱性攻撃ブロックの全般的な設定を指定します。

脆弱性攻撃ブロックのプロセス保護設定ウィンドウ

► [プロセス保護設定]ウィンドウを開くには:

1. アプリケーションコンソールツリーで、[**Kaspersky Security**]フォルダーを選択します。
2. コンテキストメニューを開いて[**脆弱性攻撃ブロック:プロセス保護設定**]メニューオプションを選択します。

[**プロセス保護設定**]ウィンドウが表示されます。

必要に応じて脆弱性攻撃ブロックのプロセス保護設定を指定します。

プロセスメモリ保護の設定

► 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. [脆弱性攻撃ブロックの設定]ウィンドウを開きます。
2. [**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、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軽減できます。

     このチェックボックスがオフの場合、サーバープロセスを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、脆弱性攻撃試行を検知すると保護対象プロセスが終了します。

   - **通知のみ**

     このモードを選択すると、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されます。危険にさらされたプロセスは実行され続けます。

     [**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が検知された場合、コンポーネントが強制的に[**通知のみ**]モードに切り替わります。
3. [**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、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が、ターミナルウィンドウに表示されます。

     チェックボックスがオフの場合、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が、ターミナルウィンドウに表示されます。ターミナルウィンドウは、Kaspersky Security 脆弱性攻撃ブロック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 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軽減できます。Kaspersky Security 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 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。
4. [**脆弱性攻撃ブロックの設定**]ウィンドウで[**OK**]をクリックします。

Kaspersky Security 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. [プロセス保護設定]ウィンドウを開きます。
2. プロセスを追加して悪用から保護し、脆弱性攻撃の影響を軽減するには、次の処理を実行します:
   a. [**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。
   b. 表示されたウィンドウで、リストに追加するプロセスを選択します。
   c. [**開く**]をクリックします。
   d. [**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。
3. リストでプロセスを選択します。
4. [**プロセス保護設定**]に、現在の設定が表示されます:
   - **プロセス名**
   - **実行中**
   - **適用される脆弱性攻撃ブロック技術**
   - **Attack Surface Reduction の設定**
5. プロセスに適用される脆弱性攻撃ブロック技術を変更するには、[**脆弱性攻撃ブロック技術**]タブを選択します。
6. 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。既定では、プロセスに使用できるすべての技術が適用されます。
   - **プロセスに対してリストされ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。
7. Attack Surface Reduction 技術を設定します:
   - [**次のモジュールを拒否する**]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、モジュールを拒否しない**]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。

8. [**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。

脆弱性攻撃ブロック技術

表 70. 脆弱性攻撃ブロック技術

脆弱性攻撃ブロック技術	説明
Data Execution Prevention（DEP）	Data Execution Prevention は、保護されたメモリ領域でのすべて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 ページの割り当て	NULL ポインタのリダイレクト防止。
LoadLibrary のネットワークコールチェック（Anti ROP）	ネットワークパスからの DLL ロードに対する保護。
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。
アンチスタックピボット（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。
単純な 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（Heapspray）	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 におけるすべてのコードの実行）。
Attack Surface Reduction（ASR）	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。
Anti Process Hollowing（Hollowing）	信頼するプロセスの悪意のあるコピーの作成と実行に対する保護。
Anti AtomBombing（APC）	非同期プロシージャーコールを経由したグローバルアトムテーブルの悪用（APC）。

脆弱性攻撃ブロック技術	説明
Anti CreateRemoteThread（RThreadLocal）	保護対象のプロセスに、別のプロセスがスレッドを作成しました。
Anti CreateRemoteThread（RThreadRemote）	保護対象のプロセスが、別のプロセスにスレッドを作成しました。

階層型ストレージの管理

このセクションでは、階層型ストレージ領域とバックアップシステムに配置されているファイルのスキャンを実行する方法について説明します。

この章の内容

階層型ストレージについて

階層型ストレージ管理システム(以降「HSM システム」)によって、高速なローカルドライブと長期データ保存用の低速なストレージデバイスとの間で、データを再配置できます。高速なストレージデバイスの利点は明らかですが、ほとんどの組織にとって、かなり高額なものです。HSM システムでは、使用されないデータが低価格のリモートのストレージデバイスに転送されるため、企業のコストを最小限に抑えることができます。

HSM システムでは、一部のデータをリモート保管領域に保存し、必要に応じて情報を復元できます。HSM システムでは、ファイルアクセスが定期的に監視され、リモート保管領域に安全に移動できるファイルと、ローカルに保存する必要があるファイルが検出されます。指定した一定期間にアクセス要求がないファイルは、リモート保管領域に再配置されます。リモートに保存されたファイルにユーザーがアクセスすると、そのファイルはローカルドライブに転送し直されます。このため、使用可能なディスク容量を大幅に超える大量のデータに迅速にアクセスできます。

HSM システムでは、ローカルドライブからリモート保管領域にファイルを移動する間に、ファイルの実際の場所のリンクが保存されます。リンクが含まれるファイルにアクセスすると、バックアップデバイス上のデータの場所が特定されます。リンクが含まれる実際のファイルを、実際の保存場所に移動すると、実質的に無制限のサイズの保管領域を作成できます。

一部の HSM システムは、ファイル部分のローカル保管領域をサポートしています。この場合、ファイルデータの大きい部分はリモート保管領域に転送され、ローカル保管領域には元のファイルの小さい部分だけが残ります。

HSM システムで階層型ストレージのデータにアクセスするには、2 つの方法があります:

- 再解析ポイント
- 拡張ファイル属性

HSM システムの管理プラグインからの設定

HSM システムを使用しない場合は、[HSM システムの設定]の設定を既定値([HSM システムを使用しない])のままにします。

階層型ストレージへのアクセスを設定するには、HSM システムでスキャン対象ファイルの場所を特定する方法を指定する必要があります。この情報については、ご使用の HSM システムのマニュアルを参照してください。

► 階層型ストレージのアクセス種別を定義するには:

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。
2. タスクを設定する管理グループを選択します。
3. [**ポリシー**]タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示されたポリシーのプロパティウィンドウで、[**アプリケーションの設定**]セクションを選択します。
6. [**スケーラビリティとインターフェイス**]サブセクションで、[**設定**]をクリックします。

   [**製品の詳細設定**]ウィンドウが表示されます。
7. [**階層型ストレージ**]タブを開きます。
8. HSM システムへのアクセスのオプションを選択します:
   - **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**

     オンデマンドスキャンタスクの実行中に、拡張ファイル属性を使用して、リモート保管領域にあるファイルがスキャンされます。
   - **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。

     正しくないバージョンを指定したり、[**不明な HSM システム**]を選択したりすると、オブジェクトの場所が正しく特定されず、オブジェクトの処理時間が長くなる場合があります。
9. [**OK**]をクリックします。

HSM システムの設定内容が保存されます。

HSM システムのアプリケーションコンソールからの設定

HSM システムを使用しない場合は、[HSM システムの設定]の設定を既定値([HSM システムを使用しない])のままにします。

階層型ストレージへのアクセスを設定するには、HSM システムでスキャン対象ファイルの場所を特定する方法を指定する必要があります。この情報については、ご使用の HSM システムのマニュアルを参照してください。

► 階層型ストレージのアクセス種別を定義するには:

1. アプリケーション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. [**階層型ストレージ**]を選択します。

   [**HSM システムの設定**]ウィンドウが開きます。
3. [**階層型ストレージ**]タブで HSM システムの次の設定を指定します:
   - **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**

     オンデマンドスキャンタスクの実行中に、拡張ファイル属性を使用して、リモート保管領域にあるファイルがスキャンされます。
   - **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。

     正しくないバージョンを指定したり、[**不明な HSM システム**]を選択したりすると、オブジェクトの場所が正しく特定されず、オブジェクトの処理時間が長くなる場合があります。
4. [**OK**]をクリックします。

HSM システムの設定内容が保存されます。

サードパーティ製システムとの連携

このセクションでは、Kaspersky Security for Windows Server とサードパーティ製の機能およびテクノロジーとの連携について説明します。

この章の内容

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

このセクションでは、Kaspersky Security 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。

このセクションの内容

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 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 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 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 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 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 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 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 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 71. 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 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 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 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 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 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 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 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 for Windows Server の再起動

スキップされた要求の合計数

表 72. 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 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 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 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 73. 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（メモリなど）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 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 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 for Windows Server 処理対象プロセスが要求を処理するために、より多くのメモリ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メモリ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 74. 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 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トリームの平均数

表 75. 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

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 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 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 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 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トリームの最大

数

表 76. 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

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 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 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 77. 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 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 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 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 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 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)。 • 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 78. 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 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 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 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 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 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 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 for Windows Server の再起動

Kaspersky Security 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 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 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 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 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 for Windows Server の SNMP カウンター

このセクションでは Kaspersky Security 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 79. 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（509 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（511 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（512 ページを参照）
currentWorkProcessesNumber	Kaspersky Security for Windows Server で現在動作中のプロセスの数

隔離カウンター

表 80. 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 81. 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 82. 標準カウンター

カウンター	定義

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**簡易スキャンタスク**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が追加されている場合、予備のライセンス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 for Windows Server の実行時間(100 分の 1 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 83. 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 分の 1 秒単位))。

リアルタイム保護カウンター

表 84. 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

カウンター	定義
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
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

Kaspersky Security for Windows Server の SNMP トラップ

Kaspersky Security for Windows Server の SNMP トラップのオプションについて、以下に概要を示します:

- eventThreatDetected:オブジェクトが検知されました。

  トラップのオプションは、次のとおりです:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- 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。

  トラップのオプションは、次のとおりです:

  - 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。

トラップのオプションは、次のとおりです:

- eventDateAndTime
- eventSeverity
- eventSource

- 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。

  トラップのオプションは、次のとおりです:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined:隔離中にエラーが発生しました。

  トラップのオプションは、次のとおりです:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason
- eventObjectNotBackuped:バックアップ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。

  トラップのオプションは、次のとおりです:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError:隔離中に内部エラーが発生しました。

  トラップのオプションは、次のとおりです:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError:バックアップでエラーが発生しました。

  トラップのオプションは、次のとおりです:

  - 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。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- 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。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted：Kaspersky Security for Windows Server が実行中です。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown：Kaspersky Security for Windows Server が停止しました。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime：重要領域の簡易スキャンが長期間実行されていません。前回の簡易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。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired：ライセンスの有効期間が終了しました。

  トラップのオプションは、次のとおりです：

  - 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。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError：タスクの実行中にエラーが発生しました。

  トラップのオプションは、次のとおりです：

  - 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た。

  トラップのオプションは、次のとおりです：

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

トラップオプションとその可能なパラメータ値は、次のとおりです：

- eventDateAndTime：イベントの発生日時。
- eventSeverity：重要度。

  オプションとして、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）。
- eventSource：イベントが生成された機能コンポーネント。

  オプションとして、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 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。

  オプションとして、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。
- 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（https://encyclopedia.kaspersky.com/knowledge/classification/）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 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（113 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。

  オプションとして、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正規アプリケーション。
- detectCertainty：検知された脅威が実際の脅威であるかの検知の信頼度。

  オプションとして、次の値が使用されます：

  - Suspicion（感染の可能性あり） - Kaspersky Security 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 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。

  オプションとして、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。
- 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。

- 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。

  オプションとして、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 for Windows Server を復元する必要があります。
  - reasonStorageReadOnly - データベースが読み取り専用になっている。Kaspersky Security for Windows Server を復元する必要があります。
  - reasonStorageIOError - 入力-出力エラー：a) Kaspersky Security for Windows Server が破損している。Kaspersky Security for Windows Server を復元する必要があります。b) Kaspersky Security for Windows Server ファイルのディスクが破損している。
  - reasonStorageCorrupted - 保管領域が破損している。Kaspersky Security for Windows Server を復元する必要があります。
  - 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 for Windows Server を復元する必要があります。
  - reasonStorageOSFeatureError - 一部のオペレーティングシステム機能が Kaspersky Security for Windows Server の要件を満たしていない。
  - 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。

WMI との連携

Kaspersky Security for Windows Server は、Windows Management Instrumentation（WMI）との連携をサポートしています：Web-Based Enterprise Management（WBEM）標準でデータを受信し、Kaspersky Security for Windows Server とそのコンポーネントの情報を収集する目的で WMI を使用するクライアントシステムを使用できます。

Kaspersky Security for Windows Server のインストール時に、システムに専用モジュールが登録されます。このモジュールは、ローカルコンピューターの WMI 名前空間 root への Kaspersky Security for Windows Server の名前空間の作成を支援します。Kaspersky Security for Windows Server の名前空間により、Kaspersky Security for Windows Server のクラス、インスタンス、プロパティが使用できるようになります。

一部のインスタンスのプロパティの値は、タスク種別に依存します。

定期的でないタスクは、時間の制約がないタスクで、常に実行させておくことも停止することも可能です。これらのタスクには、実行時の進捗がありません。タスクの実行結果は、タスクが単一のイベントとして実行されている間（例：任意のサーバーのリアルタイム保護タスクで感染したオブジェクトを検知した場合など）は、ノンストップでログに記録されます。この種別のタスクは、Kaspersky Security Center のポリシーで管理されます。

定期的なタスクは、時間の制約があるタスクで、実行時の進捗がパーセンテージで表示されます。タスクの結果は、タスクの完了時に生成され、単一のアイテムまたは変更されたアプリケーションのステータスとして表示されます（例：定義データベースのアップデートの完了、ルールの自動生成タスクの設定ファイルの生成など）。同じ種別の定期的なタスクの多くが、単一のコンピューター上で同時に実行されています（例：オンデマンドスキャンを異なるタスク範囲で 3 つ実行するなど）。定期的なタスクは、Kaspersky Security Center のグループタスクとして管理されます。

WMI 名前空間のクエリの生成や、企業ネットワークの WMI 名前空間からの動的データの受信にツールを使用する場合、現在の本製品の状態に関する情報を受信できます（次の表を参照）。

表 85. 本製品の状態に関する情報

インスタンスのプロパティ	説明	値
ProductName	インストールされた本製品の名前。	本製品の名前（バージョン番号なし）。
ProductVersion	インストールされた本製品のバージョン。	本製品のバージョン番号（ビルド番号を含む）。
InstalledPatches	本製品に導入されたパッチの表示名。	本製品にインストールされた重要な修正のリスト。
IsLicenseInstalled	本製品のアクティベーションの状態。	本製品のアクティベーションに使用されたライセンスの状態。 取りうる値： • False - ライセンス情報ファイルまたはアクティベーションコードが本製品に適用されていません。 • True - ライセンス情報ファイルまたはアクティベーションコードが本製品に適用されています。

インスタンスのプロパティ	説明	値
LicenseDaysLeft	現在のライセンスの有効期間が終了するまでの日数を表示します。	現在のライセンスの有効期間が終了するまでの日数。 取りうる 0 以下の値: • 0 - ライセンスの有効期間が終了しています。 • -1 - 現在のライセンスに関する情報が取得できないか、指定されたライセンス情報が本製品のアクティベーションに使用できません(例:ブラックリストに掲載されているため、ブロックされているなど)。
AVBasesDatetime	現在の定義データベースのバージョンのタイムスタンプ。	現在使用されている定義データベースの作成日時。 インストール済みの本製品が定義データベースを使用していない場合、フィールドの値は「未インストール」になります。
IsExploitPreventionEnabled	脆弱性攻撃ブロックコンポーネントの状態。	脆弱性攻撃ブロックコンポーネントの状態。 取りうる値: • True - 脆弱性攻撃ブロックコンポーネントが有効で、保護を提供しています。 • False - 脆弱性攻撃ブロックコンポーネントが保護を提供していません。例:無効にされている、未インストールである、使用許諾契約書に違反している、など。
ProtectionTasksRunning	現在実行中の保護タスク。	現在実行中の保護、管理、監視などのタスク。このフィールドには、実行中のすべての定期的でないタスクが表示されます。 定期的でないタスクが 1 つも実行されていない場合は、フィールドの値は「No」になります。
IsAppControlRunning	アプリケーション起動コントロールタスクの状態。	アプリケーション起動コントロールタスクの状態。 • True - アプリケーション起動コントロールタスクが現在実行中です。 • False - アプリケーション起動コントロールタスクが現在実行されていないか、コンポーネントがインストールされていません。
AppControlMode	アプリケーション起動コントロールタスクのモード。	アプリケーション起動コントロールコンポーネントの現在の状態の説明と、そのタスクで選択されたモードの説明。 取りうる値: • Active - **処理を実行**モードがタスク設定で選択されています。 • Statistics Only - **統計のみ**モードがタスク設定で洗濯されています。 • Not installed - アプリケーション起動コントロールコンポーネントが未インストールです。

インスタンスのプロパティ	説明	値
AppControlRulesNumber	アプリケーション起動コントロールルールの総数。	アプリケーション起動コントロールルールタスクの設定で現在指定されているルールの数。
AppControlLastBlocking	アプリケーション起動コントロールタスクが任意のモードで起動をブロックした最後のタイムスタンプ。	アプリケーション起動コントロールコンポーネントがアプリケーションの起動を最後にブロックした日時。このフィールドには、ブロックされたアプリケーションのすべてが、タスクのモードに関係なく表示されます。 WMI クエリが処理された時点でアプリケーションの起動のブロックの実行が記録されていない場合、このフィールドの値は「No」になります。
PeriodicTasksRunning	現在実行中の定期的なタスク。	現在実行中のオンデマンドスキャン、アップデート、インベントリを使用するタスクのリスト。このフィールドには、実行中のすべての定期的なタスクが表示されます。 定期的なタスクが 1 つも実行されていない場合は、フィールドの値は「No」になります。
ConnectionState	WMI プロバイダーコンポーネントと Kaspersky Security サービス（KAVFS）間の接続の状態。	WMI プロバイダーモジュールと Kaspersky Security サービス間の接続に関する情報。 取りうる値： • Success - 接続が正常に確立されています：WMI クライアントがアプリケーションの状態に関する情報を受信可能な状態です。 • Failed.Error Code: <コード> - 特定のコードを持つエラーにより、接続が確立されていません。

このデータは、次のインスタンスのプロパティで表示されます：KasperskySecurity_ProductInfo.ProductName=Kaspersky Security

- KasperskySecurity_ProductInfo：Kaspersky Security for Windows Server のクラスの名前
- .ProductName=Kaspersky Security：Kaspersky Security for Windows Server のキーパラメータ

インスタンスは、名前空間 ROOT\Kaspersky\Security に作成されます。

コマンドラインからの Kaspersky Security 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 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 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 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 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 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 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 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 86. Kaspersky Security for Windows Server のコマンド

コマンド	説明

コマンド	説明
KAVSHELL APPCONTROL（「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」（538 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（「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」（535 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。
KAVSHELL APPCONTROL /GENERATE（「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」（536 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（「Kaspersky Security for Windows Server ログファイルのデフラグ：KAVSHELL VACUUM」（546 ページ）を参照）	Kaspersky Security for Windows Server ログファイルのデフラグ。
KAVSHELL PASSWORD	パスワードによる保護の設定の管理。
KAVSHELL HELP（「Kaspersky Security for Windows Server コマンドヘルプの表示：KAVSHELL HELP」（527 ページ）を参照）	Kaspersky Security for Windows Server コマンドヘルプの表示。
KAVSHELL START（「Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP」（528 ページ）を参照）	Kaspersky Security for Windows Server サービスの開始。
KAVSHELL STOP（「Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP」（528 ページ）を参照）	Kaspersky Security for Windows Server サービスの停止。
KAVSHELL SCAN（「選択した領域のスキャン：KAVSHELL SCAN」（528 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（「簡易スキャンタスクの開始：KAVSHELL SCANCRITICAL」（532 ページ）を参照）	簡易スキャンのシステムタスクの開始。
KAVSHELL TASK（「指定されたタスクの非同期での管理：KAVSHELL TASK」（533 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。

コマンド	説明
KAVSHELL RTP（「リアルタイム保護タスクの開始と停止：KAVSHELL RTP」（535 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（「Kaspersky Security 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」（540 ページ）を参照）	Kaspersky Security 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）。
KAVSHELL ROLLBACK（「Kaspersky Security for Windows Server 定義データベースのロールバック：KAVSHELL ROLLBACK」（543 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（「製品のアクティベート：KAVSHELL LICENSE」（544 ページ）を参照）	ライセンスまたはアクティベーションコードの追加と削除。追加されたライセンスとアクティベーションコードに関する情報を表示します。
KAVSHELL TRACE（「トレースログの有効化、設定、無効化： KAVSHELL TRACE」（545 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（「ダンプファイル作成の有効化と無効化：KAVSHELL DUMP」（548 ページ）を参照）	プロセスが不正に終了した場合の Kaspersky Security 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（「設定のインポート：KAVSHELL IMPORT」（549 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 for Windows Server 設定、機能、およびタスクのインポート。
KAVSHELL EXPORT（「設定のエクスポート：KAVSHELL EXPORT」（549 ページ）を参照）	Kaspersky Security 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。
KAVSHELL DEVCONTROL（「デバイスコントロールルールのリストの入力：KAVSHELL DEVCONTROL」（539 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 for Windows Server コマンドヘルプの表示：KAVSHELL HELP

すべての Kaspersky Security 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アプリケーションコンソールに表示されます(タスク設定をアプリケーションコンソールで確認することはできません)。タスク実行ログが同時に生成されます。ログは、アプリケーションコンソールの[**実行ログ**]に表示されます。

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(「指定されたタスクの非同期での管理: KAVSHELL TASK」(533 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 87. KAVSHELL SCAN コマンドの修飾子

キー	説明
スキャン範囲:必須の修飾子	
<ファイル> <フォルダー> <ネットワークパス>	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。 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	メモリ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	自動実行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。

キー	説明
/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
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。 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 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。
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 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
/AS: **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。	
QUARANTINE	隔離
DELETE	削除

キー	説明
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 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。
/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。 以下のヒューリスティック分析レベルを設定できます： 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。

キー	説明
/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 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)。アプリケーションコンソールで、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)	
/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 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 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、アプリケーションコンソールの[実行ログ]に表示されます。 Kaspersky Security 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。

簡易スキャンの開始:KAVSHELL SCANCRITICAL

アプリケーション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簡易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簡易スキャンを実行し、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 88. KAVSHELL SCANCRITICAL コマンドの /W 修飾子の構文

キー	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 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、アプリケーションコンソールの[**実行ログ**]に表示されます。 Kaspersky Security 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 コマンドの例

```
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 89. KAVSHELL TASK コマンドの修飾子

キー	説明

キー	説明
キーの指定なし	既存のすべての Kaspersky Security 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 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 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。
/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（553 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）。

システムの保護対象プロセスとしての KAVFS の登録：KAVSHELL CONFIG

KAVSHELL CONFIG コマンドを使用することで、アプリケーションのインストール中にオペレーティングシステムにインストールされている ELAM ドライバーを使用して、Kaspersky Security Service のシステム保護対象プロセス（Protected Process Light）としての登録を制御できます。

KAVSHELL CONFIG コマンドの構文

```
KAVSHELL CONFIG /PPL:<ON|OFF>
```

表 90. KAVSHELL CONFIG コマンドのキー

キー	説明

キー	説明
/PPL:ON	Kaspersky Security Service を PPL として登録します。
/PPL:OFF	Kaspersky Security Service の PPL 属性を削除します。

次の操作のいずれかが実行されると、アプリケーションはサービスの登録解除を自動的に実行します:

- アプリケーションのアンインストール
- アプリケーションのアップグレード
- パッチのインストール
- アプリケーションコンポーネントの修復

KAVSHELL CONFIG コマンドのリターンコード

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 91. KAVSHELL RTP コマンドの修飾子

キー	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[処理を実行]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
```

コマンドラインの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 92. KAVSHELL APPCONTROL /GENERATE コマンドスイッチ

キー	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 93. KAVSHELL APPCONTROL /GENERATE コマンドキー

キー	説明
許可ルールの適用範囲	
<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、デジタル証明書の発行先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。なくとも 1 つのルールパラメータが他のルールと異なる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。なくとも 1 つのルールパラメータが他のルールと異なる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 94. KAVSHELL APPCONTROL コマンドキー

キー	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。なくとも 1 つのルールパラメータが他のルールと異なる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 95. KAVSHELL DEVCONTROL コマンドキー

キー	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。なくとも 1 つのルールパラメータが他のルールと異なる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 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 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 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。実行中にのみアプリケーションコンソールに表示されます。タスク実行ログが同時に生成されます。ログは、アプリケーションコンソールの[**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アプリケーション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 for Windows Server の管理については、「Kaspersky Security Center を使用した Kaspersky Security 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 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 96. KAVSHELL UPDATE コマンドのキー

キー	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 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。
<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 for Windows Server によって自動的に検出されます。

キー	説明
/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 for Windows Server がプロキシサーバーに接続します。 **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 for Windows Server がプロキシサーバーに接続します。 **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。
/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 for Windows Server は FTP のアクティブモードを使用します。このキーを指定しないと、Kaspersky Security for Windows Server は FTP のパッシブ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。
/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 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、アプリケーション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。

キー	説明
/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 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)。アプリケーションコンソールで、タスクに「Update-databases <日時>」という名前が割り当てられます(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 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 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。 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、アプリケーションコンソールの[**実行ログ**]に表示されます。 Kaspersky Security 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(554 ページを参照)

Kaspersky Security 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 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 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(555 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 97. KAVSHELL TASK LOG-INSPECTOR コマンドの修飾子

キー	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(553 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 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 LICENSE 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:<ライセンス情報 | アクティベーションコード番号>]
```

KAVSHELL LICENSE 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: <アクティベーションコードまたはライセンス情報>
```

► 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 98. KAVSHELL LICENSE コマンドのキー

キー	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: • ライセンス情報 • ライセンスの種別(製品版) • ライセンスの期間 • ライセンスのステータス(現在のライセンスまたは予備のライセンス)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。
/DEL:<ライセンス情報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(555 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 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 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トレースログの設定を指定します(次の表を参照)。

表 99. KAVSHELL TRACE コマンドのキー

キー	説明
/ON	トレースログの有効化。

キー	説明
/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。保護対象でない他のサーバーのネットワークドライブ上のフォルダーへ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 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「注意が必要なイベント」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（556 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 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。アプリケーションのイベントに基づいて生成された多数のログファイルの保管によるシステムエラーおよびアプリケーションエラーを回避することができます。

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 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 for Windows Server\10.1\Reports に保存されます。ログの保管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 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コントロールタスクは、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 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 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 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**）。

フォルダー %SYSTEMDRIVE%¥System Volume Information にファイル klamfb.dat および klamfb2.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 klamfb.dat（klamfb2.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、klamfb.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 klamfb.dat をクリーニングする場合、（klamfb.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。

- klamfb.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、すべてのファイルに対して、klamfb.dat をクリアした後の最初のアクセス時にスキャンが実行されます。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 klamfb.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 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 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>
```

表 100. KAVSHELL DUMP コマンドのキー

キー	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。保護対象でない他のサーバーのネットワークドライブ上のフォルダーへ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	指定した PID で進行中の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（557 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）。

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 /F: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
```

設定のインポート:KAVSHELL IMPORT

KAVSHELL IMPORT コマンドを使用すると、Kaspersky Security 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 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 101. KAVSHELL IMPORT コマンドのキー

キー	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(557 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 for Windows Server のコピーにあとでインポートするために、Kaspersky Security 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 102. KAVSHELL EXPORT コマンドのキー

キー	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(558 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)。

Microsoft Operations Management Suite との連携: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 103. KAVSHELL OMSINFO コマンドのキー

キー	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 104. 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

リターンコード	説明
-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 105. 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	感染などの問題があるオブジェクトの検知
-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 106. 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 107. 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 108. 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 109. 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

リターンコード	説明
-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 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 110. 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 111. 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

リターンコード	説明
-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 112. 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
-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 113. 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 114. 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 115. 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

リターンコード	説明
-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（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 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 116. 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）

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。

テクニカルサポートサービスの内容については、サポートセンターのご案内を参照してください。

- テクニカルサポートに電話する
- カスペルスキーカンパニーアカウントポータルから依頼を送信する（https://companyaccount.kaspersky.com）

電話によるテクニカルサポート

世界中のほとんどの地域から、テクニカルサポートのスペシャリストに電話できます。お住まいの地域おけるテクニカルサポートのご利用方法、およびテクニカルサポートへのお問い合わせ方法については、カスペルスキーのテクニカルサポートサイトをご確認ください（https://support.kaspersky.co.jp/b2b）。

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（https://support.kaspersky.co.jp/support/rules）。

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 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ごとに追跡し、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グ目的で、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編集します。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。

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 埋め込みオブジェクト

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 埋め込み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

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。

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。

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点で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。

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反映します。

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。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。

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://encyclopedia.kaspersky.com/
カスペルスキーウイルスデスク：	https://virusdesk.kaspersky.co.jp（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 コミュニティ：	https://community.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。

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。

Dropbox は Dropbox, Inc. の商標です。

EMC、Celerra、Isilon、OneFS、および 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。

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。

Microsoft、Active Directory、Internet Explorer、Excel、Hyper-V、JScript、MultiPoint、Outlook、PowerShell、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。

Oracle は Oracle およびその関連会社の登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited により独占的に認可されています。

索引

F

H

I

N

あ

い

お

こ

し

す

た

は

ふ

め

り

る

ろ

漢字