

**kaspersky**

# **Kaspersky Endpoint Security for Windows 11.7.0**

© 2023 AO Kaspersky Lab

# 目次

## [よくある質問 \(FAQ\)](#)

## [新機能](#)

### [Kaspersky Endpoint Security for Windows](#)

#### [製品の購入](#)

#### [システム要件](#)

#### [オペレーティングシステムの種別に応じて利用できる本製品の機能の比較](#)

#### [管理用コンソールの種別に応じて利用できる製品機能の比較表](#)

#### [その他の製品との互換性情報](#)

## [本製品のインストールと削除](#)

### [Kaspersky Security Center による導入](#)

#### [製品の標準インストール](#)

#### [インストールパッケージの作成](#)

#### [インストールパッケージ内の定義データベースのアップデート](#)

#### [リモートインストールタスクの作成](#)

### [ウィザードを使用したローカルへの製品のインストール](#)

### [System Center Configuration Manager を使用しての製品のリモートインストール](#)

### [ファイル setup.ini のインストール設定の説明](#)

### [コンポーネントの変更](#)

### [旧バージョンの製品からのアップグレード](#)

### [製品の削除](#)

#### [Kaspersky Security Center を使用したアンインストール](#)

#### [ウィザードを使用しての製品のアンインストール](#)

## [製品のライセンス](#)

### [使用許諾契約書について](#)

### [ライセンスの概要](#)

### [ライセンスの証明書について](#)

### [月額制サービスについて](#)

### [ライセンスについて](#)

### [About activation code](#)

### [ライセンス情報ファイルについて](#)

## [製品のアクティベーション](#)

### [Kaspersky Security Center を使用した製品のアクティベーション](#)

### [アクティベーションウィザードを使用した製品のアクティベーション](#)

### [ライセンス情報の表示](#)

### [ライセンスの更新または購入](#)

### [月額制サービスの更新](#)

## [データ提供](#)

### [使用許諾契約書におけるデータ提供](#)

### [Kaspersky Security Network 使用時のデータ提供](#)

### [欧州連合の規則 \(GDPR\) の順守](#)

## [使用開始時に行う設定](#)

### [Kaspersky Endpoint Security for Windows の管理プラグインについて](#)

### [異なるバージョンの管理プラグインを使用する場合の留意点](#)

### [外部サービスと相互作用する暗号化プロトコルを使用する場合の留意点](#)

## [製品のインターフェイス](#)

### [タスクバーの通知領域の製品アイコン](#)

[簡略化したアプリケーションインターフェイス](#)

[製品インターフェイスの表示の設定](#)

[使用開始時に行う設定](#)

[ポリシーの管理](#)

[タスクの管理](#)

[個別のローカル環境用の製品設定](#)

[Kaspersky Endpoint Security の起動と終了](#)

[プロテクションとコントロールの一時停止と再開](#)

[コンピューターのウイルススキャン](#)

[コンピューターのスキャン](#)

[Scanning removable drives when they are connected to the computer](#)

[バックグラウンドスキャン](#)

[コンテキストメニューからのスキャン](#)

[本製品の整合性の確認](#)

[スキャン範囲の編集](#)

[スケジュールされたスキャンの実行](#)

[異なるユーザーとしてスキャンを実行する](#)

[スキャンの最適化](#)

[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](#)

[データベースと製品モジュールのアップデートシナリオ](#)

[サーバーリポジトリからアップデート](#)

[共有フォルダーからアップデート](#)

[Kaspersky Update Utility を使用してのアップデート](#)

[モバイルモードでのアップデート](#)

[アップデートタスクの開始と停止](#)

[別のユーザーアカウントの権限でのアップデートタスクの開始](#)

[アップデートタスクの実行方法の選択](#)

[Adding an update source](#)

[共有フォルダーからのアップデートの設定](#)

[製品モジュールのアップデート](#)

[プロキシサーバーを使用してのアップデート](#)

[前回のアップデートのロールバック](#)

[アクティブな脅威に対する操作](#)

[コンピューターの保護](#)

[ファイル脅威対策](#)

[ファイル脅威対策の有効化と無効化](#)

[ファイル脅威対策の自動的な一時停止](#)

[感染したファイルに対してファイル脅威対策が行う処理の変更](#)

[ファイル脅威対策の保護範囲の設定](#)

[スキャン方法の使用](#)

[ファイル脅威対策で使用するスキャン技術の設定](#)

[スキャンの最適化](#)

[複合ファイルのスキャン](#)

[スキャン方法の変更](#)

[ウェブ脅威対策](#)

[ウェブ脅威対策の有効化と無効化](#)

[悪意のある Web トラフィックオブジェクトに対する処理の変更](#)

[フィッシングサイトまたは悪意のある Web サイトのデータベースで URL をチェックする](#)

[ウェブ脅威対策でのヒューリスティック分析の使用](#)

[信頼する URL のリストの作成](#)

[信頼する URL のリストのエクスポート/インポート](#)

## メール脅威対策

[メール脅威対策の有効化と無効化](#)

[感染したメールに対する処理の変更](#)

[メール脅威対策の保護範囲の設定](#)

[メールに添付されている複合ファイルのスキャン](#)

[メール添付ファイルのフィルター](#)

[添付ファイルのフィルターの拡張子のエクスポートおよびインポート](#)

[Microsoft Office Outlook におけるメールのスキャン](#)

## ネットワーク脅威対策

[ネットワーク脅威対策の有効化と無効化](#)

[攻撃元コンピューターのブロック](#)

[ブロックから除外するアドレスの設定](#)

[ブロックの除外対象のリストのエクスポート/インポート](#)

[ネットワーク攻撃の種別に対応した保護を設定する](#)

## ファイアウォール

[ファイアウォールの有効化または無効化](#)

[ネットワーク接続種別の変更](#)

[ネットワークパケットルールの管理](#)

[ネットワークパケットルールの作成](#)

[ネットワークパケットルールの有効化または無効化](#)

[ネットワークパケットルールに対するファイアウォール処理の変更](#)

[ネットワークパケットルールの優先順位の変更](#)

[ネットワークパケットルールのエクスポートおよびインポート](#)

[アプリケーションネットワークルールの管理](#)

[アプリケーションネットワークルールの作成](#)

[アプリケーションネットワークルールの有効化と無効化](#)

[アプリケーションネットワークルールのファイアウォール処理の変更](#)

[アプリケーションネットワークルールの優先度の変更](#)

[ネットワークモニター](#)

## 有害 USB 攻撃ブロック

[有害 USB 攻撃ブロックの有効化と無効化](#)

[USB デバイスの認証時のセキュリティキーボードの使用](#)

## AMSI 保護

[AMSI 保護の有効化と無効化](#)

[AMSI 保護機能を使用した複合ファイルのスキャン](#)

## 脆弱性攻撃ブロック

[脆弱性攻撃ブロックの有効化と無効化](#)

[攻撃を検知した場合に行う処理の選択](#)

[システムプロセスのメモリ保護](#)

## ふるまい検知

[ふるまい検知の有効化と無効化](#)

[マルウェアの動作を検知したときに実行する処理の選択](#)

[外部からの暗号化に対する共有フォルダーの保護](#)

[外部からの暗号化に対する共有フォルダーの保護の有効化または無効化](#)

[外部からの共有フォルダーの暗号化を検知した場合に行う処理の選択](#)

[外部からの暗号化に対する共有フォルダーの保護から除外するアドレスの設定](#)

[外部からの暗号化に対する共有フォルダーの保護の除外リストのエクスポートおよびインポート](#)

## [ホスト侵入防止](#)

[ホスト侵入防止の有効化と無効化](#)

[アプリケーション許可グループの管理](#)

[アプリケーションの許可グループを変更する](#)

[許可グループの権限の設定](#)

[Kaspersky Endpoint Security の前に起動したアプリケーションの許可グループを選択する](#)

[不明なアプリケーションに許可グループを選択する](#)

[デジタル署名されたアプリケーションに許可グループを選択する](#)

[アプリケーション権限の管理](#)

[オペレーティングシステムのリソースと個人データの保護](#)

[未使用のアプリケーションに関する情報の削除](#)

[ホスト侵入防止の監視](#)

[音声、映像へのアクセスの保護](#)

## [修復エンジン](#)

[Kaspersky Security Network](#)

[Kaspersky Security Network の使用の有効化と無効化](#)

[プライベート KSN の制限事項](#)

[保護機能のクラウドモードの有効化と無効化](#)

[Kaspersky Security Network でのファイルの評価の確認](#)

[暗号化された接続のスキャン](#)

[暗号化された接続のスキャンの設定](#)

[Scanning encrypted connections in Firefox and Thunderbird](#)

[暗号化された接続をスキャンから除外する](#)

## [コンピューターのコントロール](#)

[ウェブコントロール](#)

[ウェブコントロールの有効化と無効化](#)

[Web リソースアクセスルールを使用した処理](#)

[Web リソースへのアクセスルールの追加](#)

[Web リソースアクセスルールの優先度の割り当て](#)

[Web リソースへのアクセスルールの有効化と無効化](#)

[信頼する URL のリストのエクスポート / インポート](#)

[Web リソースへのアクセスルールのテスト](#)

[Web リソースアドレスのリストのエクスポート / インポート](#)

[ユーザーが行っているインターネット活動の監視](#)

[ウェブコントロールメッセージのテンプレートの編集](#)

[Web リソースアドレスマスクの編集](#)

[以前のバージョンの製品から Web リソースのアクセスルールの移行](#)

[デバイスコントロール](#)

[デバイスコントロールの有効化と無効化](#)

[アクセスルールの概要](#)

[デバイスアクセスルールの編集](#)

[接続バスアクセスルールの編集](#)

[信頼する Wi-Fi ネットワークの追加](#)

[リムーバブルドライブの使用状況の監視](#)

[キャッシュ期間の変更](#)

[信頼するデバイスを使用した処理](#)

[アプリケーションインターフェイスから信頼リストへのデバイスの追加](#)

[Kaspersky Security Center から信頼リストへのデバイスの追加](#)

[信頼するデバイスのリストのエクスポート / インポート](#)

[ブロックされたデバイスへのアクセスの取得](#)

[オンラインモードでのアクセス権の付与](#)

[オフラインモードでのアクセス権の付与](#)

[デバイスコントロールメッセージのテンプレートの編集](#)

[アンチブリッジ](#)

[アンチブリッジを有効にする](#)

[接続ルールのステータスの変更](#)

[接続ルールの優先度の変更](#)

[アダプティブアノマリーコントロール](#)

[アダプティブアノマリーコントロールの有効化と無効化](#)

[アダプティブアノマリーコントロールルールの有効化と無効化](#)

[アダプティブアノマリーコントロールルールが適用されたときに実行する処理の変更](#)

[Creating an exclusion for an Adaptive Anomaly Control rule](#)

[アダプティブアノマリーコントロールルールの除外のエクスポートとインポート](#)

[アダプティブアノマリーコントロールルールへのアップデートの適用](#)

[アダプティブアノマリーコントロールのメッセージテンプレートの編集](#)

[アダプティブアノマリーコントロールのレポートの表示](#)

[アプリケーションコントロール](#)

[アプリケーションコントロールの機能の制限](#)

[アプリケーションコントロールの有効化と無効化](#)

[アプリケーションコントロールモードの選択](#)

[製品インターフェイスでのアプリケーションコントロールルールの操作](#)

[アプリケーションコントロールルールを追加する](#)

[アプリケーションコントロールルールの適用条件の追加](#)

[アプリケーションコントロールルールのステータスの変更](#)

[Kaspersky Security Center でのアプリケーションコントロールルールの管理](#)

[クライアン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についての情報の取得](#)

[アプリケーションカテゴリの作成](#)

[実行ファイルフォルダーからアプリケーションカテゴリへの実行ファイルの追加](#)

[イベントに関連した実行ファイルのアプリケーションカテゴリへの追加](#)

[Kaspersky Security Center を使用したアプリケーションコントロールルールの追加と変更](#)

[Kaspersky Security Center を使用したアプリケーションコントロールルールのステータス変更](#)

[アプリケーションコントロールルールのエクスポートおよびインポート](#)

[Kaspersky Security Center を使用したアプリケーションコントロールルールのテスト](#)

[アプリケーションコントロールのテスト動作によるイベントの表示](#)

[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の表示](#)

[アプリケーションコントロールの動作によるイベントの表示](#)

[ブロックされたアプリケーションに関するレポートの表示](#)

[アプリケーションコントロールルールのテスト](#)

[Application activity monitor](#)

[Rules for creating name masks for files or folders](#)

[アプリケーションコントロールのメッセージテンプレートの編集](#)

[許可されるアプリケーションのリストの実装のベストプラクティス](#)

[アプリケーションの許可リストモードの設定](#)

[許可リストモードのテスト](#)

[許可リストモードのサポート](#)

[ネットワークポートの監視](#)

[すべてのネットワークポートの監視の有効化](#)

[監視対象ネットワークポートのリストの作成](#)

[すべてのネットワークポートを監視するアプリケーションのリストの作成](#)

[監視対象のポートのリストのエクスポートまたはインポート](#)

[データの消去](#)

[パスワードによる保護](#)

[パスワードによる保護を有効にする](#)

[個別のユーザーまたはグループへの権限付与](#)

[一時パスワードを使用した権限の付与](#)

[パスワードによる保護で付与する権限に関する留意事項](#)

[信頼ゾーン](#)

[信頼するオブジェクトの作成](#)

[信頼するオブジェクトの有効化と無効化](#)

[Editing the list of trusted applications](#)

[信頼するアプリケーションのリストでのアプリケーションに対する信頼ゾーンルールの有効化と無効化](#)

[信頼するシステム証明書ストアの使用](#)

[バックアップの管理](#)

[バックアップファイルの最大保管期間の設定](#)

[バックアップの最大サイズの設定](#)

[バックアップからのファイルの復元](#)

[バックアップからのファイルのバックアップコピーの削除](#)

[通知サービス](#)

[イベントログ設定の指定](#)

[通知の表示と配信の設定](#)

[製品のステータスに関する通知領域での警告の表示設定](#)

[レポートの管理](#)

[レポートの表示](#)

[レポート最長保管期間の設定](#)

[レポートファイルの最大サイズの設定](#)

[レポートのファイルへの保存](#)

[レポートの削除](#)

[Kaspersky Endpoint Security Self-Defense](#)

[セルフディフェンスの有効化と無効化](#)

[AM-PPL のサポートの有効化と無効化](#)

[外部からの管理に対する防御の有効化と無効化](#)

[リモート管理アプリケーションのサポート](#)

[Kaspersky Endpoint Security のパフォーマンスと他のアプリケーションとの互換性](#)

[検知可能なオブジェクトの選択](#)

[サーバー向けの特別な駆除の有効化または無効化](#)

[省エネモードの有効化または無効化](#)

[他のアプリケーションへのリソースの供与の有効化または無効化](#)

[設定ファイルの作成と使用](#)

[既定の設定の復元](#)

[ユーザーと管理者間のメッセージ](#)

[データ暗号化](#)

[暗号化機能の制限](#)

## [暗号鍵 \(AES56 / AES256\) の鍵長の変更](#)

### [Kaspersky Disk Encryption](#)

[SSD ドライブ暗号化の特別な機能](#)

[Kaspersky Disk Encryption 技術を使用したディスク全体の暗号化](#)

[暗号化から除外するハードディスクのリスト作成](#)

[暗号化から除外するハードディスクのリストのエクスポートおよびインポート](#)

[シングルサインオン \(SSO\) 技術の有効化](#)

[認証エージェントアカウントの管理](#)

[認証エージェントでのトークンまたはスマートカードの使用](#)

[ハードディスクの復号化](#)

[Kaspersky Disk Encryption 技術で保護されたドライブへのアクセスの復元](#)

[オペレーティングシステムのアップデート](#)

[暗号化機能のアップデートのエラーの解決](#)

[認証エージェントのトレースレベルの選択](#)

[認証エージェントのヘルプテキストの編集](#)

[認証エージェントの動作テスト後に残存するオブジェクトとデータの削除](#)

### [BitLocker の管理](#)

[BitLocker ドライブ暗号化の開始](#)

[BitLocker で保護されたハードドライブの復号化](#)

[BitLocker で保護されたハードドライブへのアクセスの復元](#)

[ソフトウェアアップデート時の BitLocker 保護の一時停止](#)

### [ローカルコンピュータドライブでのファイルレベルの暗号化](#)

[ローカルコンピュータドライブのファイルの暗号化](#)

[アプリケーションを対象にした暗号化ファイルへのアクセスルールの策定](#)

[特定のアプリケーションによって作成または変更されたファイルの暗号化](#)

[復号化ルールの作成](#)

[ローカルコンピュータドライブでのファイルの復号化](#)

[暗号化されたパッケージへの追加](#)

[暗号化されたファイルへのアクセスの復元処理](#)

[オペレーティングシステム障害が発生した後の暗号化されたデータへのアクセスの復元](#)

[暗号化ファイルアクセスメッセージのテンプレートの編集](#)

### [リムーバブルドライブの暗号化](#)

[リムーバブルドライブの暗号化の開始](#)

[リムーバブルドライブの暗号化ルールの追加](#)

[リムーバブルドライブの暗号化ルールのリストのエクスポートまたはインポート](#)

[リムーバブルドライブ上の暗号化ファイルにアクセスするためのポータブルモード](#)

[リムーバブルドライブの復号化](#)

### [データ暗号化の詳細の表示](#)

[暗号化ステータスの表示](#)

[Kaspersky Security Center ダッシュボードで暗号化の統計情報の表示](#)

[ローカルコンピュータドライブでのファイル暗号化エラーの表示](#)

[データ暗号化レポートの表示](#)

### [暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用](#)

[FDERT 復元ツールを使用してデータを復元する](#)

[オペレーティングシステムのレスキューディスクの作成](#)

### [Detection and Response](#)

[Kaspersky Endpoint Agent](#)

[\[KES+KEA\] 設定から \[KES11.7.0\] への移行](#)



## Managed Detection and Response

### Endpoint Detection and Response

セキュリティ侵害インジケータ (IOC) のスキャン

ファイルを隔離する

ファイルを取得する

ファイルを削除する

プロセスの開始

プロセスの終了

実行防止

コンピューターのネットワーク分離

### Kaspersky Sandbox

## コマンドラインを使用しての製品の管理

本製品のインストール

製品のアクティベーション

製品の削除

### AVP コマンド

SCAN : スキャン

UPDATE : 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

ROLLBACK : 前回のアップデートのロールバック

TRACES : トレース

START : 指定した機能の起動

STOP : 指定した機能の停止

STATUS : 指定した機能のステータス

STATISTICS : 指定した機能の動作の統計情報

RESTORE : バックアップからのファイルの復元

EXPORT : 本製品の設定のエクスポート

IMPORT : 本製品の設定のインポート

ADDKEY : ライセンス情報ファイルの適用

LICENSE : ライセンス管理

RENEW : ライセンスの更新または購入

PBATESTRESET : 暗号化前のディスクチェックの結果のリセット

EXIT : 本製品の終了

EXITPOLICY : ポリシーの無効化

STARTPOLICY : ポリシーの有効化

DISABLE : 保護の無効化

SPYWARE : スパイウェアの検知の切り替え

KSN : グローバル/プライベート KSN の切り替え

### KESCLI コマンド

Scan : スキャン

GetScanState : スキャン完了のステータス

GetLastScanTime : スキャン完了時刻の判断

GetThreats : 検知した脅威に関するデータの取得

UpdateDefinitions : 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

GetDefinitionState : アップデート完了時刻の判断

EnableRTP : 保護の有効化

GetRealTimeProtectionState : ファイル脅威対策のステータス

Version : 本製品のバージョンの識別

## Detection and Response management commands

[SANDBOX : Kaspersky Sandbox の管理](#)

[PREVENTION : 実行防止の管理](#)

[ISOLATION : ネットワーク分離の管理](#)

[RESTORE : 隔離からのファイルの復元](#)

[start locScanTask. Scan for indicators of compromise \(IOC\)](#)

[MDRLICENSE : MDR のアクティベーション](#)

[エラーコード](#)

[補足資料 : コマンド指定用の機能名](#)

[REST API を使用した製品の管理](#)

[REST API の使用を有効にしての本製品のインストール](#)

[API の使用](#)

[製品の情報源](#)

[Contacting Technical Support](#)

[トレースファイルの内容と保存場所](#)

[アプリケーションの動作のトレース](#)

[製品のパフォーマンスのトレース](#)

[ダンプ書き込み](#)

[ダンプファイルとトレースファイルの保護](#)

[制限と警告](#)

[用語解説](#)

[IOC](#)

[IOC ファイル](#)

[OLE オブジェクト](#)

[OpenIOC](#)

[Trusted Platform Module](#)

[Web リソースアドレスの正規化された形式](#)

[アーカイブ](#)

[悪意のある URL のデータベース](#)

[感染可能なファイル](#)

[感染したファイル](#)

[管理グループ](#)

[駆除](#)

[現在のライセンス](#)

[誤検知](#)

[証明書の発行元](#)

[スキャン範囲](#)

[タスク](#)

[定義データベース](#)

[認証エージェント](#)

[ネットワークエージェント](#)

[フィッシングサイトの URL のデータベース](#)

[ポータブルファイルマネージャー](#)

[保護範囲](#)

[マスク](#)

[予備のライセンス](#)

[ライセンス証明書](#)

[補足資料](#)

[補足資料1: 製品設定](#)

[File Threat Protection](#)  
[ウェブ脅威対策](#)  
[メール脅威対策](#)  
[ネットワーク脅威対策](#)  
[ファイアウォール](#)  
[有害 USB 攻撃ブロック](#)  
[AMSI 保護](#)  
[脆弱性攻撃ブロック](#)  
[ふるまい検知](#)  
[ホスト侵入防止](#)  
[修復エンジン](#)  
[Kaspersky Security Network](#)  
[ウェブコントロール](#)  
[デバイスコントロール](#)  
[アプリケーションコントロール](#)  
[アダプティブアノマリーコントロール](#)  
[Endpoint Sensor](#)  
[Kaspersky Sandbox](#)  
[Endpoint Detection and Response](#)  
[ディスク全体の暗号化](#)  
[ファイルレベルの暗号化](#)  
[リムーバブルドライブの暗号化](#)  
[テンプレート \(データの暗号化\)](#)  
[除外リスト](#)  
[製品設定](#)  
[レポートと保管領域](#)  
[ネットワークの設定](#)  
[インターフェイス](#)  
[設定の管理](#)  
[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](#)  
[補足資料 2 : アプリケーション許可グループ](#)  
[補足資料 3 : リムーバブルドライブの簡易スキャンのファイル拡張子](#)  
[補足資料 4 : メール脅威対策用の添付ファイルフィルターのファイル種別](#)  
[補足資料 5 : 外部サービスとの相互作用のためのネットワーク設定](#)  
[補足資料 6 : Windows イベントログのアプリケーションイベントログ](#)  
[補足資料 7 : Kaspersky Security Center イベントログ内の製品イベント](#)  
[補足資料 8 : 実行防止でサポートされるファイルの拡張子](#)  
[補足資料 9 : サポートされるスクリプトインタープリター](#)  
[補足資料 10 : レジストリ内の IOC スキャン範囲 \(RegistryItem\)](#)  
[補足資料 11 : IOC ファイルの要件](#)  
[サードパーティ製のコードに関する情報](#)  
[商標に関する通知](#)

## よくある質問 (FAQ)



### 全般

Kaspersky Endpoint Security を使用するには、コンピュータがどのような要件を満たす必要がありますか？

以前のバージョンと比べて、どのような機能が追加されたり変更されましたか？

Kaspersky Endpoint Security と競合せずに動作できるのは、どのカスペルスキー製品ですか？

Kaspersky Endpoint Security の動作中に、メモリなどのリソース消費量を抑えるにはどうすればよいですか？



### 製品の導入

社内のすべてのコンピュータに Kaspersky Endpoint Security を簡単にインストールするにはどうすればよいですか？

コマンドラインを使用したインストールではどのような設定を指定できますか？

Kaspersky Endpoint Security をリモートからアンインストールするにはどうすればよいですか？



### アップデート

定義データベースをアップデートするにはどのような方法がありますか？

アップデートの実行後に問題が発生したら、どのように対応すればよいですか？

ユーザーがコンピュータを社内ネットワークの外で使用している場合、どのようにすれば定義データベースをアップデートできますか？

アップデート元からのアップデートのダウンロード時に、プロキシサーバーを使用することはできますか？



### セキュリティ

Kaspersky Endpoint Security はどのような仕組みでメールをスキャンしていますか？

信頼できるファイルをスキャン対象から除外するにはどうすればよいですか？

リムーバブルドライブ経由でのウイルス感染を防ぐにはどのように設定すればよいですか？

ユーザーへの通知などを特に表示せずにスキャンを実行するにはどうすればよいですか？



### インターネット

Kaspersky Endpoint Security では、暗号化された接続 (HTTPS) をスキャンできますか？

ユーザーに対して信頼できる Wi-Fi ネットワークへの接続のみを許可するにはどうすればよいですか？

SNS へのアクセスをブロックするにはどうすればよいですか？



### アプリケーション

ユーザーのコンピュータにインストールされているアプリケーションを、インベントリタスクを使用して確認するにはどうすればよいですか？

コンピュータゲームの実行を禁止するにはどうすればよいですか？

指定したアプリケーションコントロールルールが意図した通りに動作するか確認するにはどうすればよいですか？

信頼するアプリケーションのリストにアプリケーションを追加するにはどうすればよいですか？



### デバイス

外付けドライブの使用をブロックするにはどうすればよいですか？

信頼リストにデバイスを追加するにはどうすればよいですか？

業務上必要なデバイスへのアクセスがブロックされた場合、ユーザーがアクセス権を要求することはできますか？



### 暗号化

ハードディスクなどの使用状況などからくる制限で、暗号化機能を使用できないことはありますか？

暗号化したパッケージへのアクセスをパスワードを使用して制限するにはどうすればよいですか？

暗号化されたハードディスクへのアクセスの認証に、スマートカードやトークンを使用できますか？

コンピュータが Kaspersky Security Center に接続されていない状況で、暗号化されたデータにアクセスする方法はありますか？

オペレーティングシステムでの機能エラーが発生した後に、暗号化されたまま残ってしまったデータにアクセスするにはどうすればよいですか？

Kaspersky Endpoint Security の保護機能を一時的に停止させるにはどうすればよいですか？

Kaspersky Endpoint Security によって誤って削除されたファイルを復元するにはどうすればよいですか？

Kaspersky Endpoint Security をユーザーが勝手にアンインストールできないように設定するにはどうすればよいですか？



サポート

レポートファイルはどこに保存されていますか？

トレースファイルを作成するにはどうすればよいですか？

ダンプの書き込みを有効にするにはどうすればよいですか？

# 新機能

## 11.7.0 のアップデート

Kaspersky Endpoint Security for Windows 11.7.0 の新機能と改良点は次の通りです：

1. [Kaspersky Endpoint Security for Windows のインターフェイス](#)が更新されました。
2. [Windows 11、Windows Server 10 21H2 および Windows Server 2022 をサポート](#)するようになりました。
3. 追加された新機能：
  - [Kaspersky Sandbox との連携用の組み込みエージェント](#)が追加されました。Kaspersky Sandbox ソリューションはコンピューター上の高度な脅威を検知し、自動的にブロックします。Kaspersky Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Kaspersky Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Kaspersky Sandbox サーバー）上でオブジェクトを分析およびスキャンします。このソリューションについて詳しくは、[Kaspersky Sandbox](#) のヘルプを参照してください。

Kaspersky Sandbox を使用する際に Kaspersky Endpoint Agent が不要になりました。Kaspersky Endpoint Security はすべての Kaspersky Endpoint Agent の機能を実行できます。Kaspersky Endpoint Agent のポリシーを移行するには、[移行ウィザード](#)を使用してください。Kaspersky Sandbox のすべての機能が動作するためには Kaspersky Security Center 13.2 が必要です。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行に関して詳しくは、[製品のヘルプ](#)を参照してください。
  - [Kaspersky Endpoint Detection and Response Optimum ソリューションの操作をサポートする組み込みエージェント](#)が追加されました。Kaspersky Endpoint Detection and Response Optimum は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

Kaspersky Endpoint Detection and Response を使用する際に Kaspersky Endpoint Agent が不要になりました。Kaspersky Endpoint Security はすべての Kaspersky Endpoint Agent の機能を実行できます。Kaspersky Endpoint Agent のポリシーおよびタスクを移行するには、[移行ウィザード](#)を使用してください。Kaspersky Endpoint Detection and Response Optimum のすべての機能を使用するには、Kaspersky Security Center 13.2 が必要です。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行に関して詳しくは、[製品のヘルプ](#)を参照してください。
4. Kaspersky Endpoint Agent のポリシーおよびタスクを移行する[移行ウィザード](#)が追加されました。移行ウィザードは、Kaspersky Endpoint Security for Windows の新しく統合されたポリシーおよびタスクを作成します。ウィザードを使用すると、Detection and Response ソリューションを Kaspersky Endpoint Agent から Kaspersky Endpoint Security に移行できます。Detection and Response solutions には、Kaspersky Sandbox、Kaspersky Endpoint Detection and Response Optimum（EDR Optimum）および Kaspersky Managed Detection and Response（MDR）が含まれます。
5. 配信キットに含まれている [Kaspersky Endpoint Agent](#) がバージョン 3.11 にアップデートされました。



Kaspersky Endpoint Security のアップグレード時に、本製品は Kaspersky Endpoint Agent のバージョンおよび設計を検出します。Kaspersky Endpoint Agent が Kaspersky Sandbox、Kaspersky Managed Detection and Response (MDR) および Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) の操作用に設計されていた場合、Kaspersky Endpoint Security はこれらのソリューションの動作を本製品の組み込みエージェントに切り替えます。Kaspersky Sandbox および EDR Optimum の場合は、本製品は自動的に Kaspersky Endpoint Agent をアンインストールします。MDR については、Kaspersky Endpoint Agent を手動でアンインストールできます。アプリケーションが Kaspersky Endpoint Detection and Response Expert (EDR Expert) 用に設計されていた場合は、Kaspersky Endpoint Security は Kaspersky Endpoint Agent のバージョンをアップグレードします。製品の詳細については、Kaspersky Endpoint Agent をサポートするカスペルスキー製品のガイドを参照してください。

#### 6. BitLocker 暗号化機能が改善されました :

- [BitLocker ドライブ暗号化](#)で拡張 PIN が使用できるようになりました。拡張 PIN を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります。
- [オペレーティングシステムのアップグレードやアップグレードパッケージのインストール用に BitLocker 認証を無効にする](#)機能が追加されました。アップデートのインストールには、コンピューターの再起動が複数回必要になることがあります。正常にアップデートをインストールするために一時的に BitLocker 認証をオフにして、アップデートのインストール後に再度認証を有効にすることができます。
- [BitLocker 暗号化パスワードまたは PIN に有効期限を設定](#)できるようになりました。パスワードまたは PIN の有効期間が終了すると、Kaspersky Endpoint Security はユーザーに新しいパスワードの入力を要求します。

#### 7. 有害 USB 攻撃ブロックのため、キーボード認証試行回数の最大数を設定できるようになりました。 [認証コードの入力の失敗が指定した回数に到達すると](#)、USB デバイスは一時的にロックされます。

#### 8. ファイアウォール機能が改善されました :

- [ファイアウォールのパケットルール](#)の IP アドレスの範囲を設定できるようになりました。アドレスの範囲は IPv4 または IPv6 形式で入力できます。たとえば、「192.168.1.1-192.168.1.100」または「12:34::2-12:34::99」のように入力します。
- [ファイアウォールのパケットルール](#)に IP アドレスの代わりに DNS 名を入力できるようになりました。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。

#### 9. [ウェブコントロールルール](#)の検索が改善されました。Web リソースのアクセスルールを検索する際、ルール名に加えて Web サイトの URL、ユーザー名、コンテンツカテゴリ、データ種別を使用できるようになりました。

#### 10. ウィルススキャンタスクが改善されました :

- [ウィルススキャン](#)タスクが改善されました : スキャン中にコンピューターを再起動すると、Kaspersky Endpoint Security は自動的にスキャンが中断された箇所からタスクを継続して実行します。
- [ウィルススキャン](#)タスクが最適化されました。既定では、Kaspersky Endpoint Security はコンピューターが使用されていないときにのみスキャンを実行します。タスクのプロパティからコンピューターのスキャンをいつ実行するか設定できます。

#### 11. [アプリケーション動作モニター](#)が提供するデータへのユーザーのアクセスを制限できるようになりました。アプリケーション動作モニターは、ユーザーのコンピューターのアプリケーションの動作に関する情報をリアルタイムで表示するように設計されたツールです。管理者は、アプリケーションポリシーのプロパティでアプリケーション動作モニターをユーザーに対して非表示にすることができます。

12. [REST API を使用した製品の管理のセキュリティが向上しました](#)。Kaspersky Endpoint Security が REST API 経由で送信された要求の署名を検証するようになりました。プログラムを管理するには、要求の識別用の証明書をインストールする必要があります。

## 11.6.0 のアップデート

Kaspersky Endpoint Security 11.6.0 for Windows の新機能と改良点は次の通りです：

1. [Windows 10 21H1 のサポート](#)。Microsoft Windows 10 オペレーティングシステムのサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#)を参照してください。
2. [Managed Detection and Response](#) が追加されました。この機能は、Kaspersky Managed Detection and Response と呼ばれるソリューションとのやり取りをサポートします。Kaspersky Managed Detection and Response (MDR) は、24 時間体制で日々増加していく脅威に対抗する保護を提供します。企業側で専門知識や技術を確認するために限られたリソースの時間や労力を費やす必要はありません。ソリューションの詳細については、Kaspersky Managed Detection and Response のヘルプを参照してください。
3. 配信キットに含まれている [Kaspersky Endpoint Agent](#) がバージョン 3.10 にアップデートされました。Kaspersky Endpoint Agent 3.10 は新機能を実装し、また一部の既知の問題を修正し、安定性が向上しました。製品の詳細については、Kaspersky Endpoint Agent をサポートするカスペルスキー製品のガイドを参照してください。
4. [ネットワーク脅威対策の設定](#)で、ポートのスキャンおよびネットワークフラッディングのような攻撃に対する保護を管理する機能を提供できるようになりました。
5. ファイアウォールのネットワークルールを作成する方法が新しく追加されました。[ネットワークモニター](#) ウィンドウで表示される接続の[パケットルール](#)および[アプリケーションルール](#)を追加できます。ネットワークルールの接続設定は自動で設定されます。
6. [ネットワークモニター](#)のインターフェイスが改善されました。ネットワークでの操作に関する次の情報を追加しました：ネットワーク操作を開始したプロセス ID、ネットワーク種別（ローカルネットワークまたはインターネット）、ローカルポート。既定では、ネットワーク種別に関する情報は非表示です。
7. 新規 Windows ユーザーに対して自動で認証エージェントアカウントを作成できるようになりました。エージェントを使用して、ユーザーが[Kaspersky Disk Encryption 技術を使用して暗号化された](#)ドライブにアクセスするための認証を完了し、オペレーティングシステムを読み込むことができます。本製品はコンピューター上の Windows ユーザーアカウントに関する情報を確認します。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。そのため、すでに暗号化されたドライブを持つコンピューター用に[認証エージェントを手動で追加](#)する必要はありません。
8. ユーザーのコンピューター上の製品インターフェイスでディスクの暗号化プロセスを確認できるようになりました（Kaspersky Disk Encryption および BitLocker）。暗号化モニターツールは製品の[メインウィンドウ](#)から実行できます。

## [11.5.0 のアップデート](#)








Kaspersky Endpoint Security 11.5.0 for Windows の新機能と改良点は次の通りです：

1. [Windows 10 20H2 のサポート](#)。Microsoft Windows 10 オペレーティングシステムのサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#)を参照してください。
2. [アプリケーションインターフェイスのアップデート](#)。また、[通知エリアの製品アイコン](#)、製品の通知、ダイアログボックスもアップデートされました。
3. アプリケーションコントロール、デバイスコントロール、アダプティブアノマリーコントロールの Web プラグインのインターフェイスの向上。
4. ルールおよび除外リストの一覧を XML 形式でインポートおよびエクスポートする機能の追加。エクスポート後に XML 形式のリストを編集できます。Kaspersky Security Center コンソールでのみリストを管理できます。次のリストのエクスポートおよびインポートが可能です：
  - [ふるまい検知（除外リスト）](#)
  - [ウェブ脅威対策（信頼する URL のリスト）](#)
  - [メール脅威対策（添付ファイルの拡張子のフィルターのリスト）](#)
  - [ネットワーク脅威対策（除外リスト）](#)
  - [ファイアウォール（ネットワークパケットルールのリスト）](#)
  - [アプリケーションコントロール（ルールのリスト）](#)
  - [ウェブコントロール（ルールのリスト）](#)
  - [ネットワークポートの監視（Kaspersky Endpoint Security の監視対象のポートおよびアプリケーションのリスト）](#)
  - [Kaspersky Disk Encryption（除外リスト）](#)
  - [リムーバブルドライブの暗号化（ルールのリスト）](#)
5. [脅威の検知レポート](#)にオブジェクトの MD5 情報が追加されました。以前のバージョンの Kaspersky Endpoint Security では、オブジェクトの SHA256 のみが表示されていました。
6. デバイスコントロールの設定で、[デバイスアクセスルールに優先度を割り当て](#)られるようになりました。優先度を割り当てることにより、ユーザーのデバイスへのアクセスをより柔軟に設定できるようになりました。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 0 を設定し、Everyone グループには 1 を設定します。優先度は、ファイルシステムを持つデバイスにのみ設定できます。これには、ハードディスク、リムーバブルドライブ、フロッピーディスク、CD/DVD ドライブ、およびポータブルデバイス（MTP）が含まれます。
7. 追加された新機能：
  - [サウンドの管理](#)。
  - ネットワークにかかる費用の対策で、モバイル接続時などインターネット接続が制限されている場合に Kaspersky Endpoint Security のネットワークトラフィックを制限します。

- [信頼するリモートアクセスアプリケーションでの Kaspersky Endpoint Security 設定の管理](#)  
(TeamViewer、LogMeIn Pro および Remotely Anywhere など)。リモート管理アプリケーションを使用して Kaspersky Endpoint Security を開始したり製品インターフェイスで Kaspersky Endpoint Security 設定を管理できます。
  - [Firefox および Thunderbird で保護されたトラフィックのスキャン設定の管理](#)。Mozilla により使用される証明書ストアを選択できます：Windows 証明書ストアまたは Mozilla 証明書ストア。この機能はポリシーが適用されていないコンピューターのみ利用可能です。ポリシーがコンピューターに適用されていた場合、Kaspersky Endpoint Security は Firefox および Thunderbird に対して自動的に Windows 証明書ストアの使用を有効にします。
8. [保護されたトラフィックのスキャンモードを設定](#)できるようになりました：保護機能が無効になった場合でも常にトラフィックをスキャンする、または保護機能が要求したときにのみトラフィックをスキャンします。
  9. [レポートの情報を削除する](#)手順を見直しました。ユーザーはすべてのレポートを削除することのみ可能です。以前のバージョンでは、ユーザーはレポートからその情報を削除されるアプリケーションコンポーネントを選択していました。
  10. [Kaspersky Endpoint Security の設定を含む設定ファイルのインポート](#)の手順および[製品設定の復元](#)の手順を見直しました。インポートまたは復元前に、Kaspersky Endpoint Security は警告のみを表示します。以前のバージョンでは、新しい設定が適用される前に新しい設定の値を表示できました。
  11. [BitLocker により暗号化されたドライブへのアクセスの復元の手順](#)を簡素化しました。アクセス復元の手順の完了後、Kaspersky Endpoint Security は新しいパスワードまたは PIN コードを設定するよう通知します。新しいパスワードの設定後、BitLocker はドライブを暗号化します。以前のバージョンでは、ユーザーは BitLocker の設定で手動でパスワードをリセットする必要がありました。
  12. ユーザーは特定のコンピューターにローカルの[信頼ゾーン](#)を作成できるようになりました。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの[除外リスト](#)と[信頼するアプリケーション](#)のリストを作成することができます。管理者はローカルの除外リストまたはローカルの信頼するアプリケーションの使用を許可またはブロックできます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変更または削除することができます。
  13. [信頼するアプリケーションのプロパティにコメントを入力](#)できるようになりました。コメントは信頼するアプリケーションの検索や並べ替えに役に立ちます。
  14. [REST API を使用した製品の管理](#)：
    - メール脅威対策の Outlook 用機能拡張を設定できるようになりました。
    - ウイルスやワーム、トロイの木馬の検出を無効にすることは禁止されています。

## 11.4.0 のアップデート

Kaspersky Endpoint Security 11.4.0 for Windows の新機能と改良点は次の通りです：

1. [タスクバーの通知エリアの製品アイコン](#)のデザインが新しくなりました。古いアイコン (  ) の代わりに新しいアイコン (  ) が表示されます。本製品のアップデート後に再起動が必要な場合など、ユーザーが操作を実行する必要がある場合はアイコンが  に変わります。本製品の保護機能が無効になっている、または問題がある場合はアイコンが  または  に変わります。アイコンにマウスオーバーすると、コンピューターの保護についての説明が表示されます。
2. 配布キットに含まれている Kaspersky Endpoint Agent がバージョン 3.9 にアップデートされました。Kaspersky Endpoint Agent 3.9 は新しい Kaspersky ソリューションとの統合をサポートします。製品の詳細については、Kaspersky Endpoint Agent をサポートするカスペルスキー製品のガイドを参照してください。
3. Kaspersky Endpoint Security コンポーネントのステータスに「ライセンスが対応していない」が追加されました。[メインアプリケーションウィンドウ](#)の「[保護コンポーネント](#)」をクリックしてコンポーネントのステータスを表示できます。
4. [脆弱性攻撃ブロック](#)からの新しいイベントが[レポート](#)に追加されました。
5. 暗号化が開始されると、[Kaspersky Disk Encryption](#)技術向けのドライバーが自動的に Windows 回復環境 (WinRE) に追加されるようになりました。以前のバージョンの Kaspersky Endpoint Security では、本製品のインストール時にドライバーが追加されていました。WinRE へのドライバーの追加により、Kaspersky Disk Encryption 技術で保護されたコンピューターのオペレーティングシステムの回復時に、アプリケーションの動作がより安定します。

Endpoint Sensor は Kaspersky Endpoint Security から削除されました。Kaspersky Endpoint Security のバージョン 11.0.0 から 11.3.0 がコンピューターにインストールされている場合は Endpoint Sensor の設定をポリシー内で設定できます。

# Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows（以降、「Kaspersky Endpoint Security」とも記載）は、さまざまな脅威、ネットワーク攻撃とフィッシング攻撃からコンピューターを包括的に保護します。

## 脅威検知技術



### 機械学習

機械学習に基づいたモデルを使用します。このモデルはカスペルスキーによって開発されました。それ以降、このモデルは継続的に KSN からの脅威データを取得します（モデルのトレーニング）。



### クラウド分析

Kaspersky Endpoint Security は [Kaspersky Security Network](#) から脅威のデータを受け取ります。KSN (Kaspersky Security Network) はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。



### エキスパートによる分析

カスペルスキーのウイルスアナリストにより追加された脅威のデータを使用します。ウイルスアナリストは、自動でオブジェクトの評価が決定できない場合にオブジェクトを評価します。



### ふるまい分析

リアルタイムでオブジェクトの活動を分析します。



### 自動分析

オブジェクトの自動解析システムからデータを受け取ります。システムはカスペルスキーに送られたすべてのオブジェクトを処理します。次に、システムはオブジェクトの評価を決定し、定義データベースにそのデータを追加します。システムがオブジェクトを評価できない場合は、システムはカスペルスキーのウイルスアナリストにクエリを送ります。



### Kaspersky Sandbox

Kaspersky Endpoint Security は仮想マシンでオブジェクトを処理します。Kaspersky Sandbox がオブジェクトのふるまいを分析し、その評価を決定します。この技術は [Kaspersky Sandbox ソリューション](#) を使用している場合のみ利用可能です。

## 選択ツリー

各種の脅威が専用のコンポーネントによって処理されます。各コンポーネントは個別に有効または無効にすることができ、設定も個別に行うことができます。

### 選択ツリー

セクション	コンポーネント
脅威対策	<b>ファイル脅威対策</b> ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターの RAM に常駐します。このコンポーネントは、コンピューターのすべてのドライブと接続されたドライブのファイルをスキャンします。このコンポーネントは、定義データベース、 <a href="#">Kaspersky Security Network クラウドサービス</a> 、およびヒューリスティック分析を使用してコンピューターを保護します。  <b>ウェブ脅威対策</b>

ウェブ脅威対策は、インターネットからの悪意のあるファイルのダウンロードを防ぎ、悪意のある Web サイトやフィッシングサイトをブロックします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

### メール脅威対策

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、悪意のあるリンクやフィッシングリンクのメッセージもスキャンします。既定では、メール脅威対策はコンピューターの RAM に常駐し、POP3、SMTP、IMAP、NNTP プロトコル、または Microsoft Office Outlook メールクライアント (MAPI) を使用して送受信されるすべてのメッセージをスキャンします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

### ネットワーク脅威対策

ネットワーク脅威対策は、受信ネットワークトラフィックをスキャンし、典型的なネットワーク攻撃の活動をチェックします。Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、Kaspersky Endpoint Security データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、[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](#)時にアップデートされます。

### ファイアウォール

ファイアウォールは、インターネットまたはローカルネットワークでの作業中に、コンピューターへの不正な接続をブロックします。ファイアウォールは、コンピューター上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義されたネットワークルールを使用してコンピューターを保護します。

### 有害 USB 攻撃ブロック

有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。

### AMSI 保護

AMSI 保護機能は Microsoft 社の AMSI (Antimalware Scan Interface) をサポートすることを目的とした機能です。AMSI (Antimalware Scan Interface) により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト (たとえば、PowerShell スクリプトなど) のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。

## 先進の脅威対策



### Kaspersky Security Network

KSN (Kaspersky Security Network) はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。

### ふるまい検知



	<p>ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures (BSS) を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されず。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。</p> <p><b>脆弱性攻撃ブロック</b></p> <p>脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとする、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。</p> <p><b>ホスト侵入防止</b></p> <p>ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。</p> <p><b>修復エンジン</b></p> <p>修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。</p>
<p>セキュリティコントロール</p> <p>中</p>	<p><b>アプリケーションコントロール</b></p> <p>アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。</p> <p><b>デバイスコントロール</b></p> <p>デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。</p> <p><b>ウェブコントロール</b></p> <p>ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します。</p> <p><b>アダプティブアノマリーコントロール</b></p> <p>アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「Office アプリケーションによる Microsoft PowerShell の起動」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートするとともに、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。</p>
<p>暗号化</p>	<p><b>ファイルレベルの暗号化</b></p>



この機能を使用してファイルの暗号化ルールを作成できます。暗号化のための事前定義されたフォルダーを指定したり、手動でフォルダーを指定したり、または拡張子で個別のファイルを指定したりできます。

### ディスク全体の暗号化

この機能を使用すると、Kaspersky Disk Encryption または BitLocker ドライブ暗号化を使用してハードドライブを暗号化できます。

### リムーバブルドライブの暗号化

この機能を使用してリムーバブルドライブのデータを保護します。ディスク全体の暗号化 (FDE) またはファイルレベルの暗号化 (FLE) を使用できます。

Detection  
and  
Response



### Endpoint Detection and Response

Kaspersky Endpoint Detection and Response Optimum ソリューション (以降「EDR Optimum」とします) の組み込みエージェントです。Kaspersky Endpoint Detection and Response Optimum は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のオンラインヘルプを参照してください。

### Kaspersky Sandbox

この機能は Kaspersky Sandbox ソリューションとの連携を有効にします。Kaspersky Sandbox ソリューションはコンピューター上の高度な脅威を検知し、自動的にブロックします。Kaspersky Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Kaspersky Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー (Kaspersky Sandbox サーバー) 上でオブジェクトを分析およびスキャンします。このソリューションについて詳しくは、[Kaspersky Sandbox](#) のヘルプを参照してください。

### Managed Detection and Response

Kaspersky Managed Detection and Response ソリューションの操作をサポートする組み込みエージェントです。Kaspersky Managed Detection and Response (MDR) ソリューションはお客様のインフラストラクチャ内のセキュリティインシデントを自動で検知し分析します。MDR はエンドポイントから取得する遠隔測定したデータと機械学習を使用します。MDR はカスペルスキーのエキスパートにインシデントのデータを送信します。エキスパートはインシデントを処理し、新しい項目を定義データベースに追加するなどの対応をします。また、エキスパートたちはインシデントの処理に対して、コンピューターをネットワークから分離するなど、推奨事項を提示することもあります。ソリューションについて詳しくは、[Kaspersky Managed Detection and Response のヘルプ](#) を参照してください。

本製品が提供するリアルタイム保護の機能に加えて、ウイルスやその他の脅威がないかどうか、定期的にコンピューターをスキャンすることを推奨します。これにより、セキュリティレベルが低く設定されていたなどの理由でマルウェアが保護機能によって検知されなくても、マルウェアを拡散してしまわずに済みます。

コンピューターの保護を最新の状態に維持するには、この製品が使用する定義データベースおよびモジュールをアップデートする必要があります。製品は既定で自動的にアップデートされますが、必要に応じて、定義データベースとソフトウェアモジュールを手動でアップデートすることができます。

Kaspersky Endpoint Security では、次のタスクを実行できます：

- **整合性チェック**：Kaspersky Endpoint Security は、製品のインストールフォルダーにあるソフトウェアモジュールに破損や変更がないかチェックします。ソフトウェアモジュールのデジタル署名が正しくない場合、そのモジュールは破損していると考えられます。
- **完全スキャン**：Kaspersky Endpoint Security は、カーネルメモリ、オペレーティングシステムの起動時に読み込まれるオブジェクト、ディスクのブートセクター、オペレーティングシステムのバックアップ記憶領域

域、すべてのハードディスクおよびリムーバブルドライブを含め、オペレーティングシステムをスキャンします。

- **オブジェクトスキャン**：Kaspersky Endpoint Security はユーザーが選択したオブジェクトをスキャンします。
- **簡易スキャン**：Kaspersky Endpoint Security は、カーネルメモリ、オペレーティングシステムの起動時に読み込まれるオブジェクト、ディスクのブートセクターをスキャンします。
- **アップデート**：アップデートされた定義データベースおよびソフトウェアモジュールをダウンロードします。アップデートにより、コンピューターは新しいウイルスや脅威から保護されます。
- **前回のアップデートのロールバック**：前回アップデートした定義データベースとソフトウェアモジュールを元に戻します。これにより、必要に応じて、定義データベースとソフトウェアモジュールを前のバージョンにロールバックすることができます。この機能は、たとえば新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。

## 製品の支援機能

Kaspersky Endpoint Security には多数の支援機能が備わっています。支援機能は製品を最新の状態に維持し、製品の機能を拡張して、製品操作時にユーザーを支援することを目的としています。

- **レポート**：動作中に、製品は各コンポーネントに関するレポートを保持します。完了したタスクの結果に関する情報の確認にもレポートを使用できます。このレポートには、Kaspersky Endpoint Security の動作中に発生したイベントと製品が実行したすべての処理のリストが含まれています。インシデントが発生した場合は、カスペルスキーにレポートを送信できます。これにより、テクニカルサポートのスペシャリストが問題を詳細に調査できます。
- **バックアップ**：コンピューターのウイルスや他の脅威をスキャンしているときに、感染したファイルが検知されると、それらのファイルがブロックされます。また、駆除および削除されたファイルのコピーが、「バックアップ」に保存されます。何らかの理由で処理されなかったファイルは、アクティブな脅威のリストに移動されます。ユーザーはファイルをスキャンしたり、ファイルを元のフォルダーに戻したり、データ保管領域を空にしたりできます。
- **通知**：ユーザーは通知サービスを使用することで、コンピューターの保護ステータスに影響を与えるイベントと Kaspersky Endpoint Security の動作を監視できます。通知は画面に表示したり、メールで受信したりできます。
- **Kaspersky Security Network**：ユーザーが Kaspersky Security Network に参加することにより、ファイル、Web リソースおよびソフトウェアの評価に関して全世界のユーザーから取得された情報をリアルタイムで使用できるため、コンピューター保護の効率が向上します。
- **ライセンス**：ライセンスを購入することで、製品の全機能の制限が解除され、定義データベースとモジュールアップデートにアクセスできるようになり、製品のインストールと設定に関する問題点、およびその使用方法について、テクニカルサポートへ問い合わせることもできるようになります。
- **サポート**：Kaspersky Endpoint Security の登録ユーザーはすべて、テクニカルサポートスペシャリストによるサポートを受けることができます。カスペルスキーカンパニーアカウントポータルからテクニカルサポートへサポート依頼を送信するか、電話で問い合わせを行うことができます。

製品がエラーを返す場合や、操作中にフリーズする場合、自動的に再起動することがあります。

クラッシュを引き起こすエラーが繰り返し発生する場合、製品は以下の動作を行います：

1. コントロールとプロテクションの機能を無効にします（暗号化機能は有効のままです）。



- 機能が無効になったことをユーザーに通知します。
- 定義データベースをアップデートしたり、ソフトウェアモジュールのアップデートを適用したりした後で、製品を動作する状態に復元しようとします。

## 製品の購入

配信キットには、次の配布パッケージが含まれています：

- **強力な暗号化アルゴリズムを使用する暗号化モジュール（AES256）**

この配布パッケージには、AES（Advanced Encryption Standard）暗号化アルゴリズムによる暗号化を実効鍵長 256 ビットで実行できる暗号化ツールが含まれています。

- **相対的に強度の低い暗号化アルゴリズムを使用する暗号化モジュール（AES56）**

この配布パッケージには、AES 暗号化アルゴリズムによる暗号化を実効鍵長 56 ビットで実行できる暗号化ツールが含まれています。

各配布パッケージには次のファイルが含まれています：

kes_win.msi	Kaspersky Endpoint Security のインストールパッケージ。
setup_ks.exe	いずれの <a href="#">製品インストール</a> の方法でも必要となるファイル。
kes_win.kud	<a href="#">Kaspersky Endpoint Security のインストールパッケージの作成</a> で必要となるファイル。
klcfginst.msi	Kaspersky Security Center に Kaspersky Endpoint Security 管理プラグインをインストールするインストールパッケージ。
bases.cab	インストール中に使用されるアップデートパッケージファイル。
cleaner.cab	競合するソフトウェアをアンインストールするためのファイル。
incompatible.txt	共存できないソフトウェアのリストが含まれるファイル。
ksn_<言語 ID>.txt	Kaspersky Security Network への参加条件が記載されたファイル。
license.txt	<a href="#">使用許諾契約書</a> とプライバシーポリシーの内容が記載されたファイル。
installer.ini	配信キットの内部設定を含むファイル。
endpointagent.msi	<a href="#">Kaspersky Endpoint Agent</a> のインストールパッケージ。その他のカスペルスキーのソリューション（例えば Kaspersky Sandbox）との統合に必要です。
NDP<バージョン>-<パッケージのプロパティ>	Microsoft .NET Framework のインストールパッケージ。
keswin_web_plugin.zip	アーカイブには <a href="#">Kaspersky Endpoint Security Web プラグイン</a> のインストールに必要なファイルが含まれています。

この設定の値は変更しないでください。インストールオプションを変更する場合は、[setup.ini ファイル](#)を使用してください。

## システム要件

Kaspersky Endpoint Security が正常に動作することを保証するためには、コンピューターが次の要件を満たしている必要があります：

全般的な最小要件：

- 2 GB以上のディスク空き容量
- CPU：
  - ワークステーション：1 GHz
  - サーバー：1.4 GHz
  - SSE2 命令セット対応
- メモリ：
  - ワークステーション (x86)：1 GB
  - ワークステーション (x64)：2 GB
  - サーバー：2 GB
- Microsoft .NET Framework 4.0 以降

サポート対象のワークステーション用オペレーティングシステム：

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 以降
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11

Microsoft は SHA-1 モジュールの署名アルゴリズムを推奨していません。アップデート KB4474419 は Kaspersky Endpoint Security を Microsoft Windows 7 オペレーティングシステムを実行しているコンピューターに正常にインストールするために必要です。このアップデートに関する詳細については、[Microsoft のテクニカルサポートの Web サイト](#) を参照してください。

Microsoft Windows 10 オペレーティングシステムのサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#) を参照してください。

Microsoft Windows 11 オペレーティングシステムのサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#) を参照してください。

## サポート対象のサーバー用オペレーティングシステム :

- Windows Small Business Server 2011 Essentials / Standard (64 ビット)

Microsoft Small Business Server 2011 Standard (64-bit) は Microsoft Windows Server 2008 R2 の Service Pack 1 がインストールされている場合のみサポート対象です。

- Windows MultiPoint Server 2011 (64 ビット)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1以降
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2022

Microsoft は SHA-1 モジュールの署名アルゴリズムを推奨していません。アップデート KB4474419 は Kaspersky Endpoint Security を Microsoft Windows 2008 R2 オペレーティングシステムを実行しているコンピューターに正常にインストールするために必要です。このアップデートに関する詳細については、[Microsoft のテクニカルサポートの Web サイト](#) を参照してください。

Microsoft Windows Server 2016 および Microsoft Windows Server 2019 サポートについては、[テクニカルサポートサイトのナレッジベースの記事](#) を参照してください。

Microsoft Windows Server 2022 オペレーティングシステムのサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#) を参照してください。

## サポートされるターミナルサーバーの種別 :

- Windows Server 2008 R2 SP1 の Microsoft Remote Desktop Services
- Windows Server 2012 の Microsoft Remote Desktop Services
- Windows Server 2012 R2 の Microsoft Remote Desktop Services
- Windows Server 2016 の Microsoft Remote Desktop Services
- Windows Server 2019 の Microsoft Remote Desktop Services

## サポートされる仮想プラットフォーム :

- VMware Workstation 16.1.1 Pro
- VMware ESXi 7.0 Update 2a

- Microsoft Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2103
- Citrix Provisioning 2012
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security は次のバージョンの Kaspersky Security Center をサポートしています：

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B
- Kaspersky Security Center 13
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2。

## オペレーティングシステムの種別に応じて利用できる本製品の機能の比較

Kaspersky Endpoint Security で利用できる機能の組合せは、オペレーティングシステムの種別（ワークステーションまたはサーバー）によって異なります（下記の表を参照）。

Kaspersky Endpoint Security の機能の比較表

機能	ワークステーション	サーバー
<b>先進の脅威対策</b>		
Kaspersky Security Network	✓	✓
ふるまい検知	✓	✓
脆弱性攻撃ブロック	✓	✓
ホスト侵入防止	✓	-
修復エンジン	✓	✓
<b>脅威対策</b>		
ファイル脅威対策	✓	✓
ウェブ脅威対策	✓	-
メール脅威対策	✓	-
ファイアウォール	✓	✓
ネットワーク脅威対策	✓	✓
有害 USB 攻撃ブロック	✓	✓

AMSI 保護	✓	✓
<b>セキュリティコントロール</b>		
アプリケーションコントロール	✓	✓
デバイスコントロール	✓	-
ウェブコントロール	✓	-
アダプティブアノマリーコントロール	✓	-
<b>データ暗号化</b>		
Kaspersky Disk Encryption	✓	-
BitLocker ドライブ暗号化	✓	✓
ファイルレベルの暗号化	✓	-
リムーバブルドライブの暗号化	✓	-
<b>Detection and Response</b>		
Kaspersky Endpoint Agent	✓	✓
Endpoint Detection and Response Optimum	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response	✓	✓

## 管理用コンソールの種別に応じて利用できる製品機能の比較表

Kaspersky Endpoint Security で利用できる機能の組み合わせは管理用コンソールの種別に応じて異なります（下記の表を参照）。

Kaspersky Security Center の次のコンソールを使用して、本製品を管理できます。

- 管理コンソール：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 Microsoft 管理コンソール (MMC) スナップイン。
- Web コンソール：管理サーバーにインストールされている Kaspersky Security Center のコンポーネント。管理サーバーにアクセスできる任意のコンピューターのブラウザから Web コンソールを操作できます。

Kaspersky Security Center Cloud コンソールを使用して製品を管理することもできます。Kaspersky Security Center Cloud コンソールは、Kaspersky Security Center のクラウドバージョンです。これは、Kaspersky Security Center の管理サーバーと他のコンポーネントがカスペルスキーのクラウドインフラストラクチャにインストールされていることを意味します。Kaspersky Security Center Cloud コンソールを使用した本製品の管理について詳しくは、[Kaspersky Security Center Cloud コンソールのオンラインヘルプ](#) を参照してください。

Kaspersky Endpoint Security の機能の比較表

機能	Kaspersky Security Center		Kaspersky Security Center
	管理コンソール	Web コンソール	Cloud コンソール
先進の脅威対策			

Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	-
ふるまい検知	✓	✓	✓
脆弱性攻撃ブロック	✓	✓	✓
ホスト侵入防止	✓	✓	✓
修復エンジン	✓	✓	✓
<b>脅威対策</b>			
ファイル脅威対策	✓	✓	✓
ウェブ脅威対策	✓	✓	✓
メール脅威対策	✓	✓	✓
ファイアウォール	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓
有害 USB 攻撃ブロック	✓	✓	✓
Managed Detection and Response	✓	✓	✓
AMSI 保護	✓	✓	✓
<b>セキュリティコントロール</b>			
アプリケーションコントロール	✓	✓	✓
デバイスコントロール	✓	✓	✓
ウェブコントロール	✓	✓	✓
アダプティブアノマリーコントロール	✓	✓	✓
<b>データ暗号化</b>			
Kaspersky Disk Encryption	✓	✓	-
BitLocker ドライブ暗号化	✓	✓	✓
ファイルレベルの暗号化	✓	✓	-
リムーバブルドライブの暗号化	✓	✓	-
<b>Detection and Response</b>			
Kaspersky Endpoint Agent	✓	✓	✓
Endpoint Detection and Response Optimum (EDR)	-	✓	✓
Kaspersky Sandbox	-	✓	✓
Managed Detection and Response	✓	✓	✓
<b>タスク</b>			
ライセンスの追加	✓	✓	✓
コンポーネントの変更	✓	✓	✓
インベントリ	✓	✓	✓
アップデート	✓	✓	✓
アップデートのロールバック	✓	✓	✓

スキャン	✓	✓	✓
整合性チェック	✓	✓	-
データの消去	✓	✓	✓
認証エージェントアカウントの管理 (Kaspersky Disk Encryption)	✓	✓	-
IOC スキャン (EDR)	-	✓	✓
ファイルを隔離する (EDR)	-	✓	✓
ファイルの取得 (EDR)	-	✓	✓
ファイルの削除 (EDR)	-	✓	✓
プロセスの開始 (EDR)	-	✓	✓
プロセスの終了 (EDR)	-	✓	✓

## その他の製品との互換性情報

インストール前に、Kaspersky Endpoint Security はコンピューターにカスペルスキー製品が存在するかどうかを確認します。また互換性のないソフトウェアがコンピューター上にあるかどうか確認します。競合する製品のリストは、[配信キット](#)に含まれている incompatible.txt ファイルで参照できます。

 [こちらのリンクから incompatible.txt ファイルをダウンロードできます](#)

Kaspersky Endpoint Security は、次のカスペルスキー製品との互換性がありません：

- カスペルスキー スモール オフィス セキュリティ
- カスペルスキー インターネット セキュリティ
- Kaspersky Anti-Virus
- Kaspersky Total Security
- Kaspersky Safe Kids
- カスペルスキー フリー
- Kaspersky Anti-Ransomware Tool
- Kaspersky Anti Targeted Attack Platform (Endpoint Sensor を含む)
- Kaspersky Sandbox (Kaspersky Endpoint Agent を含む)
- Kaspersky Endpoint Detection and Response (Endpoint Sensor コンポーネントを含む)

その他のカスペルスキー製品の導入ツールを使用して Endpoint Agent がコンピューターにインストールされていた場合、Kaspersky Endpoint Security のインストール中にコンポーネントは自動的に削除されます。製品コンポーネントのリストで Endpoint Agent を選択した場合、Kaspersky Endpoint Security には Endpoint Sensor / Kaspersky Endpoint Agent も含まれる場合があります。

- Kaspersky Security for Virtualization Light Agent
- Kaspersky Fraud Prevention for Endpoint
- Kaspersky Security for Windows Server
- Kaspersky Embedded Systems Security

このリストのカスペルスキー製品がコンピューターにインストールされている場合、Kaspersky Endpoint Security はこれらのアプリケーションを削除します。この処理が終わるまで待機してから、Kaspersky Endpoint Security のインストールを続行してください。



## 本製品のインストールと削除

Kaspersky Endpoint Security のインストールでは、次の方法を使用できます：

- クライアントデバイスのローカルで、[セットアップウィザード](#)を使用。
- クライアントデバイスのローカルで、[コマンドライン](#)を使用。
- Kaspersky Security Center を使用してリモートで実行。
- Microsoft Windows のグループポリシー管理エディターを使用してリモートで実行（詳しい手順については、[Microsoft のテクニカルサポートサイト](#)を参照してください）
- [System Center Configuration Manager](#)を使用してリモートで実行。

本製品のインストール設定は複数の方法で指定できます。複数の設定方法を同時に使用してインストール設定を指定した場合、最も優先度が高い方法で指定した設定が Kaspersky Endpoint Security によって適用されます。Kaspersky Endpoint Security での優先度の順番は次の通りです：

1. ファイル「[setup.ini](#)」で指定した設定。
2. ファイル「[installer.ini](#)」で指定した設定。
3. [コマンドライン](#)で指定した設定。

リモートインストールを含め、Kaspersky Endpoint Security のインストールを開始する前に、実行中のアプリケーションをすべて終了してください。

## Kaspersky Security Center による導入

企業ネットワーク内のコンピューターへの Kaspersky Endpoint Security の導入には、複数の方法を使用できます。組織のニーズに最適な導入シナリオを選択するか、いくつかの導入シナリオを同時に組み合わせて使用できます。Kaspersky Security Center は、次の主要な導入方法をサポートしています：

- 製品導入ウィザードを使用した製品のインストール  
Kaspersky Endpoint Security の既定の設定で組織のニーズを満たすことができ、組織のインフラストラクチャの構成もシンプルで特別な設定が必要ない場合、[標準インストール](#)での導入が便利です。
- リモートインストールタスクを使用した製品のインストール  
Kaspersky Endpoint Security 設定を指定し、リモートインストールタスク自体にも柔軟に管理設定を行える一般的なインストール方法です。Kaspersky Endpoint Security をインストールするには、次の手順を実行します：
  1. [インストールパッケージの作成](#)
  2. [リモートインストールタスクの作成](#)

Kaspersky Security Center では、上記以外の Kaspersky Endpoint Security のインストール方法として、製品導入済みのオペレーティングシステムイメージの使用などがサポートされています。その他の導入方法については、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。

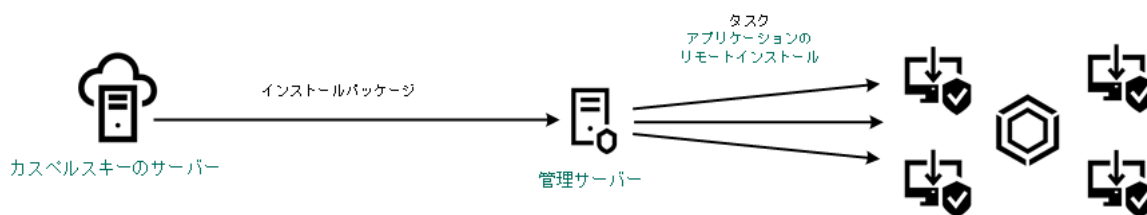
## 製品の標準インストール

Kaspersky Security Center は、企業のコンピューターにアプリケーションをインストールするための製品導入ウィザードを提供します。製品導入ウィザードでは、主な処理として次の操作を実行できます：

### 1. Kaspersky Endpoint Security for Windows のインストールパッケージの選択

インストールパッケージには、Kaspersky Security Center を使用してカスペルスキー製品のリモートインストールを行うために必要なファイルがまとめられています。インストールパッケージには、製品のインストールに必要な設定と、インストール後すぐに製品を動作させるために必要な設定が含まれています。インストールパッケージは、配布キット内に含まれている拡張子が kpd と kud のファイルを使用して作成されます。Kaspersky Endpoint Security のインストールパッケージは、すべての Windows のバージョンおよびプロセッサアーキテクチャの種別で共通です。

### 2. Kaspersky Security Center 管理サーバーの [アプリケーションのリモートインストール] タスクの作成



Kaspersky Endpoint Security の導入

## [管理コンソール \(MMC\) で製品導入ウィザードを実行する方法](#)

1. 管理コンソールで、[管理サーバー] → [詳細] → [リモートインストール] フォルダーに移動します。
2. [管理対象デバイス（ワークステーション）にインストールパッケージを配布] をクリックします。

製品導入ウィザードが開始されます。ウィザードの指示に従います。

クライアントコンピューターで、TCP ポート 139 とポート 445、UDP ポート 137 とポート 138 を開いている必要があります。

## ステップ 1：インストールパッケージの選択

リストから Kaspersky Endpoint Security インストールパッケージを選択します。リストに Kaspersky Endpoint Security のインストールパッケージが含まれていない場合は、ウィザードでパッケージを作成できます。

Kaspersky Security Center で [インストールパッケージの設定](#) を設定できます。たとえば、コンピューターにインストールする製品コンポーネントを選択できます。

ネットワークエージェントも、Kaspersky Endpoint Security と合わせてインストールされます。ネットワークエージェントは、管理サーバーとクライアントコンピューターのやり取りをサポートします。ネットワークエージェントが既にコンピューター上にインストールされている場合、再インストールは行われません。

## ステップ 2：インストール先のデバイスの選択

Kaspersky Endpoint Security をインストールするコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。未割り当てデバイスにはネットワークエージェントがまだインストールされていません。この方法を使用する場合、タスクは特定のデバイスに割り当てられます。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 3：リモートインストールタスク設定の定義

次の追加のアプリケーション設定を設定します：

- **インストールパッケージの強制ダウンロード**：製品インストールの方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。
- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。
- **別の管理サーバーの管理対象デバイスに対する処理**：Kaspersky Endpoint Security のインストール方法を選択します。ネットワーク内に複数の管理サーバーがインストールされている場合、同じクライアントコンピューターが複数の管理サーバーで可視になる場合があります。これにより、たとえば同じクライアントコンピューターへの同じ製品のリモートインストールが複数の管理サーバーから重複して実行されるなどの競合が発生する場合があります。
- **アプリケーションが既にインストールされている場合再インストールしない**：古いバージョンの製品をインストールする場合などには、このオプションをオフにします。
- **Active Directory のグループポリシーにネットワークエージェントのインストールを割り当てる**：Active Directory リソースを使用してネットワークエージェントを手動でインストールします。ネットワークエージェントをインストールするには、リモートインストールタスクはドメイン管理者権限で実行する必要があります。

## ステップ 4：ライセンスの選択

製品をアクティベートするためのライセンスをインストールパッケージに追加します。この手順は省略可能です。管理サーバーの保管領域に自動配信可能なライセンスがある場合、ライセンスが後で自動的に追加されます。また、[ライセンスの追加] タスクを使用して、後から[製品のアクティベーション](#)を行うこともできます。

## ステップ 5：オペレーティングシステムの再起動設定の選択

コンピューターの再起動が必要な場合に実行するアクションを選択します。Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。

## ステップ 6：製品のインストール前の互換性のない製品の削除

互換性のない製品のリストを注意深く読んで、これらの製品の削除を許可してください。コンピューターに競合するアプリケーションがインストールされていると、Kaspersky Endpoint Security のインストールはエラーで終了します。

## ステップ 7：コンピューターへのアクセス用のアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときに利用するユーザーアカウントを選択します。この場合、コンピューターへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をインストールする場合は、アカウントを選択する必要はありません。

## ステップ 8 : インストールの開始

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

[Web コンソールおよび Cloud コンソールで製品導入ウィザードを開始する方法](#) 

Web コンソールのメインウィンドウで [検出と製品の導入] → [導入と割り当て] → [製品導入ウィザード] の順に選択します。

製品導入ウィザードが開始されます。ウィザードの指示に従います。

クライアントコンピューターで、TCP ポート 139 とポート 445、UDP ポート 137 とポート 138 を開いている必要があります。

## ステップ 1: インストールパッケージの選択

リストから Kaspersky Endpoint Security インストールパッケージを選択します。リストに Kaspersky Endpoint Security のインストールパッケージが含まれていない場合は、ウィザードでパッケージを作成できます。インストールパッケージを作成する上で、製品の配布パッケージを検索してコンピューター上に保存する必要はありません。Kaspersky Security Center では、カスペルスキーのサーバーにある配布パッケージのリストを表示することができ、インストールパッケージが自動的に作成されます。新しいバージョンの製品がリリースされると、このリストが更新されます。

Kaspersky Security Center で [インストールパッケージの設定](#) を設定できます。たとえば、コンピューターにインストールする製品コンポーネントを選択できます。

## ステップ 2: ライセンスの選択

製品をアクティベートするためのライセンスをインストールパッケージに追加します。この手順は省略可能です。管理サーバーの保管領域に自動配信可能なライセンスがある場合、ライセンスが後で自動的に追加されます。また、[ライセンスの追加] タスクを使用して、後から [製品のアクティベーション](#) を行うこともできます。

## ステップ 3: ネットワークエージェントの選択

Kaspersky Endpoint Security と合わせてインストールされるネットワークエージェントのバージョンを選択します。ネットワークエージェントは、管理サーバーとクライアントコンピューターのやり取りをサポートします。ネットワークエージェントが既にコンピューター上にインストールされている場合、再インストールは行われません。

## ステップ 4: インストール先のデバイスの選択

Kaspersky Endpoint Security をインストールするコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。未割り当てデバイスにはネットワークエージェントがまだインストールされていません。この方法を使用する場合、タスクは特定のデバイスに割り当てられます。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。



## ステップ 5：詳細設定

次の追加のアプリケーション設定を設定します：

- **インストールパッケージの強制ダウンロード**：製品インストールの方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。
  - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。
- **アプリケーションが既にインストールされている場合再インストールしない**：古いバージョンの製品をインストールする場合などには、このオプションをオフにします。
- **Active Directory のグループポリシーにパッケージのインストールを割り当てる**：Kaspersky Endpoint Security はネットワークエージェントを使用して、あるいは Active Directory を使用して手動でインストールされます。ネットワークエージェントをインストールするには、リモートインストールタスクはドメイン管理者権限で実行する必要があります。

## ステップ 6：オペレーティングシステムの再起動設定の選択

コンピューターの再起動が必要な場合に実行するアクションを選択します。Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。

## ステップ 7：製品のインストール前の互換性のない製品の削除

互換性のない製品のリストを注意深く読んで、これらの製品の削除を許可してください。コンピューターに競合するアプリケーションがインストールされていると、Kaspersky Endpoint Security のインストールはエラーで終了します。

## ステップ 8：管理グループへの割り当て

ネットワークエージェントのインストール後にコンピューターを移動する管理グループを選択します。[ポリシー](#)および[グループタスク](#)を適用できるように、コンピューターを管理グループに移動する必要があります。コンピューターが既に管理グループにある場合、コンピューターは移動されません。管理グループを選択しなかった場合、コンピューターは **[未割り当てデバイス]** グループに追加されます。

## ステップ 9 : コンピューターへのアクセス用のアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときに利用するユーザーアカウントを選択します。この場合、コンピューターへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をインストールする場合は、アカウントを選択する必要はありません。

## ステップ 10 : インストールの開始

ウィザードを終了します。必要に応じて、**「ウィザードの完了後にタスクを実行」** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

## インストールパッケージの作成

インストールパッケージには、Kaspersky Security Center を使用してカスペルスキー製品のリモートインストールを行うために必要なファイルがまとめられています。インストールパッケージには、製品のインストールに必要な設定と、インストール後すぐに製品を動作させるために必要な設定が含まれています。インストールパッケージは、配布キット内に含まれている拡張子が kpd と kud のファイルを使用して作成されます。Kaspersky Endpoint Security のインストールパッケージは、すべての Windows のバージョンおよびプロセッサアーキテクチャの種別で共通です。

### [管理コンソール \(MMC\) でインストールパッケージを作成する方法](#)



1. 管理コンソールで、**管理サーバー** - **詳細** - **リモートインストール** - **インストールパッケージ** のフォルダーに移動します。

これにより、Kaspersky Security Center にダウンロードされたインストールパッケージのリストが開きます。

2. **インストールパッケージの作成** をクリックします。

新規パッケージウィザードが表示されます。ウィザードの指示に従います。

## ステップ 1: インストールパッケージの種別の選択

**カスペルスキー製品のインストールパッケージの作成** を選択します。

## ステップ 2: インストールパッケージ名の定義

Kaspersky Endpoint Security for Windows 11.7.0などのインストールパッケージの名前を入力します。

## ステップ 3: インストールする配布パッケージの選択

**参照** をクリックし、**配信キット**に含まれている kes\_win.kud ファイルを選択します。

必要に応じて、**アップデートをリポジトリからインストールパッケージへコピーする** チェックボックスを使用して、インストールパッケージ内の定義データベースをアップデートします。

## ステップ 4: 使用許諾契約書とプライバシーポリシー

使用許諾契約書およびプライバシーポリシーの条項を読んで同意します。

インストールパッケージが作成され、Kaspersky Security Center に追加されます。インストールパッケージを使用して、組織ネットワーク内のコンピューターへの Kaspersky Endpoint Security のインストールまたはインストール済みの製品のバージョンのアップデートを実行できます。インストールパッケージの設定で、インストールする製品コンポーネントを選択したり製品のインストール設定を編集することもできます（下記の表を参照）。インストールパッケージには、管理サーバーリポジトリの定義データベースが含まれます。**インストールパッケージのデータベースをアップデート**することで、Kaspersky Endpoint Security をインストールした後にデータベースをアップデートすることにより生じるトラフィック量を削減できます。

## [Web コンソールと Cloud コンソールでインストールパッケージを作成する方法](#)

1. Web コンソールのメインウィンドウで [検出と製品の導入] → [導入と割り当て] → [インストールパッケージ] の順に選択します。

これにより、Kaspersky Security Center にダウンロードされたインストールパッケージのリストが開きます。

2. [追加] をクリックします。

新規パッケージウィザードが表示されます。ウィザードの指示に従います。

## ステップ 1: インストールパッケージの種別の選択

[カスペルスキー製品のインストールパッケージの作成] を選択します。

ウィザードによって、カスペルスキーのサーバーにある配布パッケージからインストールパッケージが作成されます。新しいバージョンの製品がリリースされると、このリストは自動的に更新されます。Kaspersky Endpoint Security のインストールを行う場合は、このオプションをオンにする作成方法が推奨されます。

インストールパッケージをファイルから作成することもできます。

## ステップ 2: インストールパッケージ

Kaspersky Endpoint Security for Windows インストールパッケージを選択します。インストールパッケージの作成プロセスが開始されます。インストールパッケージの作成中に、エンドユーザーライセンス契約とプライバシーポリシーの条件に同意する必要があります。

インストールパッケージが作成され、Kaspersky Security Center に追加されます。インストールパッケージを使用して、組織ネットワーク内のコンピューターへの Kaspersky Endpoint Security のインストールまたはインストール済みの製品のバージョンのアップデートを実行できます。インストールパッケージの設定で、インストールする製品コンポーネントを選択したり製品のインストール設定を編集することもできます（下記の表を参照）。インストールパッケージには、管理サーバーリポジトリの定義データベースが含まれます。[インストールパッケージのデータベースをアップデート](#)することで、Kaspersky Endpoint Security をインストールした後にデータベースをアップデートすることにより生じるトラフィック量を削減できます。

### インストールパッケージの設定

セクション	説明
保護機能	このセクションでは、ユーザーに提供する製品コンポーネントを選択できます。[コンポーネントの変更] タスクを使用して、 <a href="#">後からコンポーネントのセットを変更</a> できます。既定の設定では、有害 USB 攻撃ブロック、Endpoint Agent、データ暗号化はインストールされません。これらのコンポーネントは、インストールパッケージの設定で追加できます。
インストール設定	<b>アプリケーションの場所を環境変数 %PATH% に追加する：</b> <a href="#">コマンドラインインターフェイスの使用</a> で便利のように、%PATH% 変数にインストール先のパスを追加できます。 <b>インストールプロセスを保護しない：</b> インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Endpoint Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります（たとえば、Windows Remote Desktop でリモートインストールを実行するとき）。

**Citrix Provisioning Services との互換性を確保する** : Kaspersky Endpoint Security を仮想マシンにインストールするために、Citrix Provisioning Services のサポートを有効にすることができます。

**アプリケーションのインストールフォルダーのパス** : クライアントコンピューター上での Kaspersky Endpoint Security のインストール先のパスを変更できます。既定では、アプリケーションは %Program Files%\Kaspersky Lab\ Kaspersky Endpoint Security for Windows フォルダーにインストールされます。

**設定ファイル** : Kaspersky Endpoint Security の設定を定義した設定ファイルをアップロードできます。 [製品のローカルインターフェイスで、設定ファイルを作成](#) できます。

## インストールパッケージ内の定義データベースのアップデート

インストールパッケージには、管理サーバーのリポジトリに保存されている定義データベースが含まれます。これらの定義データベースは、インストールパッケージを作成した時点での最新の定義データベースです。インストールパッケージを作成した後で、インストールパッケージ内の定義データベースをアップデートできます。これにより、Kaspersky Endpoint Security をインストールした後で定義データベースをアップデートすることで生じるトラフィック量を削減できます。

管理サーバーのリポジトリの定義データベースをアップデートするには、「管理サーバーのリポジトリへのアップデートのダウンロード」タスクを管理サーバーで使用します。管理サーバーのリポジトリの定義データベースをアップデートする方法については、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

インストールパッケージ内の定義データベースは、管理コンソールと Kaspersky Security Center Web コンソールでのみアップデートできます。Kaspersky Security Center Cloud コンソールでは、インストールパッケージ内の定義データベースをアップデートできません。

### [管理コンソール \(MMC\) を使用してインストールパッケージ内の定義データベースをアップデートする方法](#)

1. 管理コンソールで、**[管理サーバー]** - **[詳細]** - **[リモートインストール]** - **[インストールパッケージ]** のフォルダーに移動します。

これにより、Kaspersky Security Center にダウンロードされたインストールパッケージのリストが開きます。

2. インストールパッケージのプロパティを開きます。
3. **[全般]** セクションの **[定義データベースのアップデート]** をクリックします。

これにより、管理サーバーのリポジトリからインストールパッケージ内の定義データベースがアップデートされます。[配信キット](#)に含まれている bases.cab ファイルは、bases フォルダーに置き換えられます。このフォルダー内にアップデートパッケージが保存されています。

### [Web コンソールを使用してインストールパッケージ内の定義データベースをアップデートする方法](#)

1. Web コンソールのメインウィンドウで **[検出と製品の導入]** → **[導入と割り当て]** → **[インストールパッケージ]** の順に選択します。

Web コンソールにダウンロードされたインストールパッケージのリストが表示されます。

2. 定義データベースをアップデートする Kaspersky Endpoint Security のインストールパッケージの名前をクリックします。

インストールパッケージのプロパティウィンドウが表示されます。

3. **[一般情報]** タブで **[定義データベースのアップデート]** をクリックします。

これにより、管理サーバーのリポジトリからインストールパッケージ内の定義データベースがアップデートされます。[配信キット](#)に含まれている bases.cab ファイルは、bases フォルダに置き換えられます。このフォルダ内にアップデートパッケージが保存されています。

## リモートインストールタスクの作成

アプリケーションのリモートインストールタスクは、Kaspersky Endpoint Security のリモートインストール用に設計されています。アプリケーションのリモートインストールタスクを使用すると、[アプリケーションのインストールパッケージ](#)を組織内のすべてのコンピューターに導入できます。インストールパッケージを導入する前に、パッケージ内の[定義データベースをアップデート](#)し、インストールパッケージのプロパティで使用可能なコンポーネントを選択できます。

### [管理コンソール \(MMC\) でリモートインストールタスクを作成する方法](#)

1. 管理コンソールで、[管理サーバー] → [タスク] のフォルダーに移動します。

タスクのリストが表示されます。

2. [新規タスク] をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

[Kaspersky Security Center 管理サーバー] → [アプリケーションのリモートインストール] を選択します。

## ステップ 2：インストールパッケージの選択

リストから Kaspersky Endpoint Security インストールパッケージを選択します。リストに Kaspersky Endpoint Security のインストールパッケージが含まれていない場合は、ウィザードでパッケージを作成できます。

Kaspersky Security Center で [インストールパッケージの設定](#) を設定できます。たとえば、コンピューターにインストールする製品コンポーネントを選択できます。

ネットワークエージェントも、Kaspersky Endpoint Security と合わせてインストールされます。ネットワークエージェントは、管理サーバーとクライアントコンピューターのやり取りをサポートします。ネットワークエージェントが既にコンピューター上にインストールされている場合、再インストールは行われません。

## ステップ 3：追加

ネットワークエージェントのインストールパッケージを選択します。選択したバージョンのネットワークエージェントが Kaspersky Endpoint Security と合わせてインストールされます。

## ステップ 4：設定

次の追加のアプリケーション設定を設定します：

- **インストールパッケージの強制ダウンロード**：製品インストールの方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピュータに配布されます。クライアントコンピュータにネットワークエージェントがインストールされていないが、クライアントコンピュータが管理サーバーと同じネットワーク内に存在する場合にはこのオプションを選択できます。
- **別の管理サーバーの管理対象デバイスに対する処理**：Kaspersky Endpoint Security のインストール方法を選択します。ネットワーク内に複数の管理サーバーがインストールされている場合、同じクライアントコンピュータが複数の管理サーバーで可視になる場合があります。これにより、たとえば同じクライアントコンピュータへの同じ製品のリモートインストールが複数の管理サーバーから重複して実行されるなどの競合が発生する場合があります。
- **アプリケーションが既にインストールされている場合再インストールしない**：古いバージョンの製品をインストールする場合などには、このオプションをオフにします。

## ステップ 5：オペレーティングシステムの再起動設定の選択

コンピュータの再起動が必要な場合に実行するアクションを選択します。Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。

## ステップ 6：タスクを割り当てるデバイスの選択

Kaspersky Endpoint Security をインストールするコンピュータを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピュータにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。未割り当てデバイスにはネットワークエージェントがまだインストールされていません。この方法を使用する場合、タスクは特定のデバイスに割り当てられます。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 7：タスクを実行するアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときを利用するユーザーアカウントを選択します。この場合、コンピュータへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をインストールする場合は、アカウントを選択する必要はありません。

## ステップ 8：タスク開始スケジュールの設定

たとえば、手動で、またはコンピュータを使用していないときに、タスクを開始するスケジュールを設定します。

## ステップ 9 : タスク名の定義

タスクの名前を入力します。たとえば、Kaspersky Endpoint Security 11.7.0 のインストールなど。

## ステップ 10 : タスク作成の終了

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。本製品がサイレントモードでインストールされます。インストールが完了すると、**k** アイコンがユーザーのコンピューターの通知領域に追加されます。**k** というアイコンが表示された場合、[製品のアクティベーションが完了していることを確認してください。](#)

## [Web コンソールと Cloud コンソールでリモートインストールタスクを作成する方法](#)



1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **[アプリケーション]** ドロップダウンリストで、**Kaspersky Security Center** を選択します。
2. **[タスク種別]** で、**[アプリケーションのリモートインストール]** を選択します。
3. **[タスク名]** に「管理者用の Kaspersky Endpoint Security のインストール」などの簡潔な名前を付けます。
4. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。

## ステップ 2：インストール先のコンピューターの選択

選択したタスク範囲の指定方法に応じて、Kaspersky Endpoint Security をインストールするコンピューターを選択します。

## ステップ 3：インストールパッケージの設定

インストールパッケージを設定します：

1. **[Kaspersky Endpoint Security for Windows (11.7.0)]** インストールパッケージを選択します。
2. ネットワークエージェントのインストールパッケージを選択します。  
選択したバージョンのネットワークエージェントが Kaspersky Endpoint Security と合わせてインストールされます。ネットワークエージェントは、管理サーバーとクライアントコンピューターのやり取りをサポートします。ネットワークエージェントが既にコンピューター上にインストールされている場合、再インストールは行われません。
3. **[インストールパッケージの強制ダウンロード]** で、製品のインストール方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピュータに配布されます。クライアントコンピュータにネットワークエージェントがインストールされていないが、クライアントコンピュータが管理サーバーと同じネットワーク内に存在する場合にはこのオプションを選択できます。
4. **【同時ダウンロード数の上限】**で、管理サーバーに送信されるインストールパッケージのダウンロード要求数の上限を設定します。要求数の上限を設定することで、ネットワークに過剰な負荷を与えずに済みます。
  5. **【インストール試行回数の上限】**で、製品のインストールの試行を繰り返す回数の上限を設定します。Kaspersky Endpoint Security のインストールがエラーで終了した場合、タスクは自動的にインストールをもう一度開始します。
  6. 必要に応じて、**【アプリケーションが既にインストールされている場合再インストールしない】**をオフにします。これにより、以前のバージョンの製品をインストールすることなどが可能になります。
  7. 必要に応じて、**【ダウンロード前に OS の種別を確認する】**をオフにします。このオプションがオンの場合、コンピュータのオペレーティングシステムが製品のインストール要件を満たさないのに製品の配布パッケージを誤ってダウンロードしてしまうことを防ぐことができます。コンピュータのオペレーティングシステムが製品のインストール要件を確実に満たしている場合は、この検証をスキップできます。
  8. 必要に応じて、**【Active Directory のグループポリシーにパッケージのインストールを割り当てる】**をオンにします。Kaspersky Endpoint Security はネットワークエージェントを使用して、あるいは Active Directory を使用して手動でインストールされます。ネットワークエージェントをインストールするには、リモートインストールタスクはドメイン管理者権限で実行する必要があります。
  9. 必要に応じて、**【実行中のアプリケーションを終了するよう告知する】**をオンにします。Kaspersky Endpoint Security のインストールはコンピュータのリソースを消費します。このオプションをオンにすると、ユーザーの利便性のために、製品のインストールウィザードで、インストールを開始する前に実行中のアプリケーションを終了するようにメッセージが表示されます。これにより、他のアプリケーションの動作でのエラーやコンピュータでのエラーの発生を防ぐことができます。
  10. **【別の管理サーバーの管理対象デバイスに対する処理】**セクションで、Kaspersky Endpoint Security のインストール方法を選択します。ネットワーク内に複数の管理サーバーがインストールされている場合、同じクライアントコンピュータが複数の管理サーバーで可視になる場合があります。これにより、たとえば同じクライアントコンピュータへの同じ製品のリモートインストールが複数の管理サーバーから重複して実行されるなどの競合が発生する場合があります。

## ステップ 4：タスクを実行するアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときには利用するユーザーアカウントを選択します。この場合、コンピュータへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をインストールする場合は、アカウントを選択する必要はありません。

## ステップ 5：タスク作成の完了

**【終了】**をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。タスクを実行するには、タスクのチェックボックスをオンにし、**【開始】**をクリックします。本製品がサイレントモードでインストールされます。インストールが完了すると、**k** アイコンがユーザーのコンピュータの通知領域に追加されます。**k** というアイコンが表示された場合、**製品のアクティベーションが完了していること**を確認してください。

## ウィザードを使用したローカルへの製品のインストール

セットアップウィザードのインターフェイスは、製品のインストール手順に対応した一連のウィンドウで構成されています。

セットアップウィザードを使用して、製品をインストールしたり、製品を以前のバージョンからアップグレードしたりするには：

1. ユーザーのコンピューターに[配信キット](#)フォルダーをコピーします。
2. Setup\_kes.exe を実行します。

セットアップウィザードが起動します。

### インストールの準備

Kaspersky Endpoint Security をコンピューターにインストールしたり旧バージョンからアップグレードしたりする前に、次の条件が満たされていることを確認してください：

- 競合するソフトウェアがインストールされているかどうか（競合する製品のリストは、[配信キット](#)に含まれている incompatible.txt ファイルで参照できます）
- [システム要件](#)が満たされているかどうか
- ユーザーがソフトウェア製品をインストールできる権限を持っているかどうか

上記のいずれかの要件が満たされていない場合は、該当する通知が画面に表示されます。

コンピューターが上記の要件を満たしている場合、セットアップウィザードは、インストールする製品と同時に実行されたときに競合する可能性があるカスペルスキー製品がないか検索します。このようなアプリケーションが見つかった場合は、手動で削除するよう要求されます。

検出されたアプリケーションに以前のバージョンの Kaspersky Endpoint Security が含まれている場合、移行可能なすべてのデータ（アクティベーションのデータ、製品設定など）は保持され、Kaspersky Endpoint Security 11.7.0 for Windows のインストール時に使用されます。本製品の以前のバージョンは自動的に削除されます。該当する製品バージョンは次の通りです：

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows（ビルド 10.3.3.275）
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows（ビルド 10.3.3.304）
- Kaspersky Endpoint Security 11.0.0 for Windows（ビルド 11.0.0.6499）
- Kaspersky Endpoint Security 11.0.1 for Windows（ビルド 11.0.1.90）
- Kaspersky Endpoint Security 11.0.1 for Windows SF1（ビルド 11.0.1.90）
- Kaspersky Endpoint Security 11.1.0 for Windows（ビルド 11.1.0.15919）
- Kaspersky Endpoint Security 11.1.1 for Windows（ビルド 11.1.1.126）

- Kaspersky Endpoint Security 11.2.0 for Windows (ビルド 11.2.0.2254)
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (ビルド 11.2.0.2254)
- Kaspersky Endpoint Security 11.3.0 for Windows (ビルド 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 for Windows (ビルド 11.4.0.233)
- Kaspersky Endpoint Security 11.5.0 for Windows (ビルド 11.5.0.590)
- Kaspersky Endpoint Security 11.6.0 for Windows (ビルド 11.6.0.394)

## Kaspersky Endpoint Security の各コンポーネント

インストールプロセスでは、インストールする Kaspersky Endpoint Security のコンポーネントを選択できます。ファイル脅威対策は必ずインストールする必要があります。このインストールはキャンセルできません。

既定では、以下を除くすべてのコンポーネントが選択されています：

- [有害 USB 攻撃ブロック](#)
- [データ暗号化コンポーネント](#)
- [Detection and Response コンポーネント](#)

[アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更](#)できます。これを行うには、セットアップウィザードを再度実行し、使用可能なコンポーネントの変更を選択する必要があります。

## 詳細設定

**本製品のインストールのプロセスを保護する**：インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Endpoint Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります（たとえば、Windows Remote Desktop でリモートインストールを実行するとき）。

**Citrix Provisioning Services との互換性を確保する**：Kaspersky Endpoint Security を仮想マシンにインストールするために、Citrix Provisioning Services のサポートを有効にすることができます。

**アプリケーションの場所を環境変数 %PATH% に追加する**：[コマンドラインインターフェイスの使用](#)で便利のように、%PATH% 変数にインストール先のパスを追加できます。

## System Center Configuration Manager を使用しての製品のリモートインストール

以下の手順は、System Center Configuration Manager 2012 R2 で実行できます。

System Center Configuration Manager を使用して製品をリモートインストールするには：

1. Configuration Manager コンソールを開きます。
2. コンソールの右側の **【アプリケーション管理】** セクションで、 **【パッケージ】** を選択します。
3. コンソール上部のコントロールパネルで **【パッケージの作成】** をクリックします。  
パッケージとプログラムの作成ウィザードが開始します。
4. パッケージとプログラムの作成ウィザードで、次の操作を実行します：
  - a. **【パッケージ】** セクションで次の操作を実行します：
    - **【名前】** にインストールパッケージの名前を入力します。
    - **【ソースフォルダー】** で、Kaspersky Endpoint Security の配布パッケージを含むフォルダーのパスを指定します。
  - b. **【アプリケーション種別】** セクションで **【標準プログラム】** を選択します。
  - c. **【標準プログラム】** セクションで次の操作を実行します：
    - **【名前】** に、インストールパッケージの一意的名前（たとえばアプリケーション名とバージョン）を入力します。
    - **【コマンドライン】** で、コマンドラインから Kaspersky Endpoint Security をインストールする際のオプションを指定します。
    - **【参照】** をクリックして、製品の実行ファイルのパスを指定します。
    - **【実行モード】** リストで **【管理者の権限で実行】** が選択されていることを確認してください。
  - d. **【要件】** セクションで次の操作を実行します：
    - Kaspersky Endpoint Security をインストールする前に別のアプリケーションを起動するには、 **【別のプログラムを最初に実行】** をオンにします。  
 **【アプリケーション】** からアプリケーションを選択するか、 **【参照】** をクリックしてアプリケーションの実行ファイルのパスを指定します。
    - 製品を特定のオペレーティングシステムにのみインストールするには、 **【プラットフォームの要件】** セクションで **【このプログラムは、指定したプラットフォームでのみ実行できます】** をオンにします。  
 下のリストで、Kaspersky Endpoint Security をインストールするオペレーティングシステムの横にあるチェックボックスをオンにします。  
  
この手順は省略可能です。
  - e. **【概要】** セクションで、入力したすべての設定値を確認し、 **【次へ】** をクリックします。  
  
作成されたインストールパッケージが、 **【パッケージ】** セクションの使用可能なインストールパッケージのリストに表示されます。
5. インストールパッケージのコンテキストメニューから **【展開】** を選択します。  
展開ウィザードが開始します。
6. 展開ウィザードで次の操作を実行します：

a. **[全般]** セクションで次の操作を実行します：

- **[ソフトウェア]** にインストールパッケージの一意の名前を入力するか、**[参照]** をクリックしてリストからインストールパッケージを選択します。
- **[コレクション]** に製品をインストールするコンピューターのコレクションの名前を入力するか、**[参照]** をクリックしてコレクションを選択します。

b. **[コンテンツ]** セクションで、ディストリビューションポイントを追加します（詳しくは、System Center Configuration Manager のヘルプを参照してください）。

c. 必要に応じて、展開ウィザードの他の設定の値を指定します。これらの設定は、Kaspersky Endpoint Security のリモートインストールでは任意です。

d. **[概要]** セクションで、入力したすべての設定値を確認し、**[次へ]** をクリックします。

展開ウィザードが完了すると、Kaspersky Endpoint Security をリモートインストールするタスクが作成されます。

## ファイル setup.ini のインストール設定の説明

setup.ini ファイルは、コマンドラインまたは Microsoft Windows のグループポリシーエディターから製品をインストールする場合に使用します。setup.ini ファイルの設定を適用するには、これらのファイルを Kaspersky Endpoint Security の配布パッケージを同じフォルダーに配置します。

 [こちらのリンクから setup.ini ファイルをダウンロードできます](#)

setup.ini ファイルには次のセクションが含まれています：

- **[Setup]**：製品のインストールの全般設定。
- **[Components]**：インストールするコンポーネントの選択。コンポーネントが1つも指定されていない場合は、オペレーティングシステムで利用できるコンポーネントがすべてインストールされます。ファイル脅威対策は必須のコンポーネントです。このセクションで表示される設定に関係なくコンピューターにインストールされます。Managed Detection and Response もこのセクションでは表示されません。この機能をインストールするには、[Kaspersky Security Center コンソールで Managed Detection and Response をアクティベート](#)します。
- **[Tasks]**：Kaspersky Endpoint Security タスクのリストに含まれるタスクを選択します。タスクが1つも指定されていない場合は、すべてのタスクが Kaspersky Endpoint Security のタスクリストに含まれます。

1 を設定する代わりに **yes**、**on**、**enable**、**enabled** も指定できます。

0 を設定する代わりに **no**、**off**、**disable**、**disabled** も指定できます。

setup.ini ファイルの設定

セクション	パラメータ	説明
[Setup]	InstallDir	アプリケーションのインストールフォルダーのパス。
	ActivationCode	Kaspersky Endpoint Security のアクティベーションコ



		ード
	EULA=1	<p>使用許諾契約書の条項に同意する。使用許諾契約書のテキストは、<a href="#">Kaspersky Endpoint Security の配信キット</a>に含まれています。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>製品をインストールまたはアップグレードするには、使用許諾契約書に同意する必要があります。</p> </div>
	PrivacyPolicy=1	<p>プライバシーポリシーに同意する。プライバシーポリシーのテキストは、<a href="#">Kaspersky Endpoint Security の配信キット</a>に含まれています。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>本製品のインストールおよびバージョンのアップグレードには、プライバシーポリシーに同意する必要があります。</p> </div>
	KSN	<p>Kaspersky Security Network への参加に同意するかどうか。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security を最初に起動したときに、KSN への参加に同意するかどうかの確認画面が表示されます。次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1：KSN への参加に同意する</li> <li>• 0：KSN への参加に同意しない（既定値）</li> </ul> <p>Kaspersky Endpoint Security の配布パッケージは、Kaspersky Security Network とともに使用するように最適化されています。Kaspersky Security Network に参加しない場合、インストール後すぐに Kaspersky Endpoint Security をアップデートしてください。</p>
	Login	<p>Kaspersky Endpoint Security の機能と設定にアクセスできるユーザー名の指定（<a href="#">パスワードによる保護機能</a>）。ユーザー名は、「Password」および「PasswordArea」の設定と合わせて指定します。既定では、ユーザー名 KLAdmin が使用されます。</p>
	Password	<p>Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワード（パスワードは「Login」および「PasswordArea」パラメータと合わせて指定します）。</p> <p>「Login」パラメータでユーザー名を指定せずにパスワードを指定した場合、KLAdmin が既定のユーザー名として使用されます。</p>
	PasswordArea	<p>Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワードが必要になる操作の範囲。この範囲内に含まれている操作をユーザーが実行しようとした場合、Kaspersky Endpoint Security でアカウントの認証情報の入力を要求されます（「Login」と「Password」パラメータ）。複数の値を指定するには、区切り文字として「;」を使用してください。</p> <p>次の値を設定できます：</p>



		<ul style="list-style-type: none"> <li>• SET : 製品設定の変更</li> <li>• EXIT : 製品の終了</li> <li>• DISPROTECT : 保護機能の停止とスキャンタスクの停止</li> <li>• DISPOLICY : Kaspersky Security Center ポリシーの無効化</li> <li>• UNINST : コンピューターからの製品の削除</li> <li>• DISCTRL : 管理コンポーネントの停止</li> <li>• REMOVELIC : ライセンスの削除</li> <li>• REPORTS : レポートの表示</li> </ul>
	SelfProtection	<p>製品のインストール保護メカニズムを有効にするかどうか。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : 製品のインストール保護メカニズムを有効にする (既定値)</li> <li>• 0 : 製品のインストール保護メカニズムを無効にする</li> </ul> <p>インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Endpoint Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります (たとえば、Windows Remote Desktop でリモートインストールを実行するとき)。</p>
	Reboot=1	<p>製品のインストール後またはアップグレード後にコンピューターの再起動が必要な場合に自動再起動を行うかどうか。このパラメータの値が指定されていない場合、コンピューターの自動再起動はブロックされません。</p> <p>Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。</p>
	AddEnvironment	<p>%PATH% システム変数に、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスを追加するかどうか。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : %PATH% システム変数を、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスで補完する</li> </ul>

		<ul style="list-style-type: none"> <li>• 0 : %PATH% システム変数を、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスで補完しない</li> </ul>
	AMPPL	<p>AM-PPL 技術 (Antimalware Protected Process Light) を使用した Kaspersky Endpoint Security プロセスの保護を有効にするかどうか。AM-PPL 技術については、<a href="#">Microsoft の Web サイトの情報</a> を参照してください。</p> <p>AM-PPL 技術は Windows 10 バージョン 1703 (RS2) 以降および Windows Server 2019 で利用できます。</p> <p>次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を有効にする</li> <li>• 0 : AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を無効にする</li> </ul>
	SetupReg	<p>setup.reg ファイルに含まれるレジストリキーをレジストリに書き込む。SetupReg: setup.reg パラメータ値。</p>
	EnableTraces	<p>本製品のトレース記録を有効にするかどうか。Kaspersky Endpoint Security は、起動後にトレースファイルを「%ProgramData%\Kaspersky Lab\KES\Traces」フォルダーに保存します。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : トレース記録をオンにする</li> <li>• 0 : トレース記録をオフにする (既定値)</li> </ul>
	TracesLevel	<p>トレース記録の詳細度。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 100 (緊急) : 深刻なエラーに関するメッセージのみ。</li> <li>• 200 (高) : 深刻なエラーを含めたすべてのエラーに関するメッセージ。</li> <li>• 300 (診断) : すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。</li> <li>• 400 (重要) : すべてのエラーに関するメッセージとすべての警告および詳細情報。</li> <li>• 500 (通常) : すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ (既定値)。</li> <li>• 600 (低) : すべてのメッセージ。</li> </ul>
	RESTAPI	<p>REST API を使用した製品の管理。REST API を使用して製品を管理するには、ユーザー名 (RESTAPI_User パラメータ) を指定する必要があります。</p>

		<p>次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1 – REST API による管理を許可する</li> <li>• 0 – REST API による管理をブロックする（既定値）</li> </ul> <p>REST API を使用して製品を管理するには、管理システムを使用した管理を許可する必要があります。許可するには、AdminKitConnector=1 パラメータを設定します。REST API を使用して製品を管理する場合、カスペルスキーの管理システムを使用して製品を管理することはできません。</p>
	RESTAPI_User	<p>REST API による製品の管理に使用する Windows ドメインアカウントのユーザー名。REST API による製品の管理はこのユーザーのみ実行できます。ユーザー名は、&lt;ドメイン&gt;\&lt;ユーザー名&gt; の形式で入力します（例：RESTAPI_User=COMPANY\Administrator）。REST API を利用するユーザーは1人しか選択できません。</p> <p>REST API を使用して製品を管理するには、ユーザー名の追加は必須です。</p>
	RESTAPI_Port	<p>REST API による製品の管理に使用するポート。既定ではポート 6782 が使用されます。</p>
	RESTAPI_Certificate	<p>リクエストを識別するための証明書（例：RESTAPI_Certificate=C:\cert.pem）。REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。</p>
[Components]	ALL	<p>すべてのコンポーネントのインストール。このパラメータの値を 1 に設定すると、個々のコンポーネントのインストール設定にかかわらず、すべてのコンポーネントがインストールされます。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Detection and Response ソリューションをサポートする方法により、Endpoint Detection and Response Optimum および Kaspersky Sandbox コンポーネントがコンピューターにインストールされます。本製品のこの設定では、Endpoint Agent コンポーネントは設定されません。</p> </div>
	MailThreatProtection	メール脅威対策
	WebThreatProtection	ウェブ脅威対策
	AMSI	AMSI 保護
	HostIntrusionPrevention	ホスト侵入防止
	BehaviorDetection	ふるまい検知
	ExploitPrevention	脆弱性攻撃ブロック
	RemediationEngine	修復エンジン

	Firewall	ファイアウォール。
	NetworkThreatProtection	ネットワーク脅威対策
	WebControl	ウェブコントロール
	DeviceControl	デバイスコントロール
	ApplicationControl	アプリケーションコントロール
	AdaptiveAnomaliesControl	アダプティブアノマリーコントロール
	FileEncryption	ファイルレベルの暗号化ライブラリ
	DiskEncryption	ディスク全体の暗号化ライブラリ
	BadUSBAttackPrevention	有害 USB 攻撃ブロック
	AntiAPT	Endpoint Agent Endpoint Agent は本製品と Kaspersky Sandbox などの <a href="#">カスペルスキーのソリューション</a> との連携をサポートして先進の脅威を検知するため、Kaspersky Endpoint Agent をインストールします。  このコンポーネントは Endpoint Detection and Response Optimum (EDR) および Kaspersky Sandbox (SB) コンポーネントとは互換性はありません。
	EDR	Endpoint Detection and Response Optimum (EDR Optimum) :  このコンポーネントには Endpoint Agent コンポーネント (AntiAPT) との互換性はありません。
	SB	Kaspersky Sandbox :  このコンポーネントには Endpoint Agent コンポーネント (AntiAPT) との互換性はありません。
	AdminKitConnector	管理システムを使用した製品管理。管理システムには、Kaspersky Security Center などが含まれます。カスペルスキーの管理システムに加えて、サードパーティ製ソリューションを使用することもできます。Kaspersky Endpoint Security はそのための API を提供します。 次の値を設定できます： <ul style="list-style-type: none"> <li>• 1 – 管理システムを利用した製品管理を許可します (既定値)。</li> <li>• 0 – ローカルインターフェイスを利用した製品管理のみを許可します。</li> </ul>
[Tasks]	ScanMyComputer	完全スキャンタスク。次の値を設定できます：

		<ul style="list-style-type: none"> <li>• 1 : タスクを Kaspersky Endpoint Security のタスクリストに含める</li> <li>• 0 : タスクを Kaspersky Endpoint Security のタスクリストに含めない</li> </ul>
	ScanCritical	<p>簡易スキャンタスク。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : タスクを Kaspersky Endpoint Security のタスクリストに含める</li> <li>• 0 : タスクを Kaspersky Endpoint Security のタスクリストに含めない</li> </ul>
	Updater	<p>アップデートタスク。次の値を設定できます :</p> <ul style="list-style-type: none"> <li>• 1 : タスクを Kaspersky Endpoint Security のタスクリストに含める</li> <li>• 0 : タスクを Kaspersky Endpoint Security のタスクリストに含めない</li> </ul>

## コンポーネントの変更

製品のインストール中に、使用可能なコンポーネントを選択できます。使用可能な製品コンポーネントは、次の方法で変更できます :

- クライアントデバイスのローカルで、セットアップウィザードを使用。  
製品コンポーネントは、Windows オペレーティングシステムの通常の方法で、コントロールパネルを使用して変更されます。セットアップウィザードを実行して、利用可能な製品コンポーネントを変更するオプションを選択します。画面に表示される指示に従って操作します。
- Kaspersky Security Center を使用してリモートで実行。  
[コンポーネントの変更] タスクを使用すると、インストール後でも Kaspersky Endpoint Security のコンポーネントを変更できます。

製品コンポーネントを変更する際は、次の事項に留意してください :

- Windows Server を実行しているコンピューターでは、[Kaspersky Endpoint Security のすべてのコンポーネントをインストール](#)できません (たとえば、アダプティブアノマリーコントロールコンポーネントは使用できません)。
- コンピューターのハードディスクが[ディスク全体の暗号化 \(FDE\)](#) で保護されている場合、ディスク全体の暗号化コンポーネントは削除できません。ディスク全体の暗号化コンポーネントを削除するには、コンピューターのすべてのハードディスクを復号してください。
- コンピューターに[暗号化されたファイル \(FLE で暗号化\)](#) があるか、ユーザーが[暗号化されたリムーバブルドライブ \(FDE または FLE で暗号化\)](#) を使用している場合、データ暗号化コンポーネントを削除すると、これらのファイルやリムーバブルドライブにアクセスできなくなります。データ暗号化コンポーネントを再インストールすると、これらのファイルやリムーバブルドライブにアクセスできるようになります。

### [管理コンソール \(MMC\) で製品コンポーネントを追加または削除する方法](#)

1. 管理コンソールで、**〔管理サーバー〕** → **〔タスク〕** のフォルダーに移動します。

タスクのリストが表示されます。

2. **〔新規タスク〕** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

**〔Kaspersky Endpoint Security for Windows (11.7.0)〕** → **〔コンポーネントの変更〕** を選択します。

## ステップ 2：製品コンポーネントの変更のタスク設定

ユーザーのコンピューターで使用できる製品コンポーネントを選択します。

**〔共存できないサードパーティ製品の削除〕** をオンにします。競合するアプリケーションのリストは、[配信キット](#)に含まれている incompatible.txt で確認できます。コンピューターに競合するアプリケーションがインストールされていると、Kaspersky Endpoint Security のインストールはエラーで終了します。

必要に応じて、タスクの実行に対して[パスワードによる保護](#)を有効にします：

1. **〔詳細〕** をクリックします。

2. **〔製品コンポーネントの構成の変更に対してパスワードを使用〕** をオンにします。

3. KLABin ユーザーアカウントの認証情報を入力します。

## ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 4：タスク開始スケジュールの設定

たとえば、手動で、またはコンピューターを使用していないときに、タスクを開始するスケジュールを設定します。

## ステップ 5：タスク名の定義

[アプリケーションコントロールコンポーネントの追加] などのタスク名を入力します。

## ステップ 6 : タスク作成の完了

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

その結果、ユーザーのコンピューター上の Kaspersky Endpoint Security コンポーネントのセットはサイレントモードで変更されます。利用可能なコンポーネントの設定は、本製品のローカルインターフェイス上に表示されます。製品に含めなかったコンポーネントは無効になり、これらのコンポーネントの設定も選択できなくなります。

[Web コンソールおよび Cloud コンソールで製品コンポーネントを追加または削除する方法](#) 



1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
2. **[タスク種別]** で、**[コンポーネントの変更]** を選択します。
3. **[タスク名]** に「アプリケーションコントロールコンポーネントの追加」などの簡潔な名前を付けます。
4. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。

## ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。たとえば、別の管理グループを選択するか、選択を作成します。

## ステップ 3：タスク作成の完了

**[タスクの作成が完了したらタスクの詳細を表示する]** をオンにして、ウィザードを終了します。タスクのプロパティで、**[アプリケーション設定]** タブを選択し、使用可能な製品コンポーネントを選択します。

必要に応じて、タスクの実行に対して [パスワードによる保護](#) を有効にします：

1. **[詳細設定]** セクションで、**[製品コンポーネントの構成の変更に対してパスワードを使用]** をオンにします。
2. KLABin ユーザーアカウントの認証情報を入力します。

変更を保存して、タスクを実行します。

その結果、ユーザーのコンピューター上の Kaspersky Endpoint Security コンポーネントのセットはサイレントモードで変更されます。利用可能なコンポーネントの設定は、本製品のローカルインターフェイス上に表示されます。製品に含めなかったコンポーネントは無効になり、これらのコンポーネントの設定も選択できなくなります。

## 旧バージョンの製品からのアップグレード

以前のバージョンの製品から新しいバージョンの製品にアップデートするときは、次の事項に留意してください：

- アップグレードを開始する前に、アクティブなアプリケーションをすべて終了してください。
- コンピューターに [\[ディスク全体の暗号化 \(FDE\)\]](#) を使用して暗号化されたハードドライブがある場合、Kaspersky Endpoint Security のバージョン 10 から 11.0.0 以降のバージョンにアップグレードする際にすべての暗号化されたハードドライブを復号化する必要があります。

アップデートプロセスの最初に、Kaspersky Endpoint Security はディスク全体の暗号化機能が動作しないようにロックします。ディスク全体の暗号化機能をロックできない場合、アップデートのインストールは開始されません。アップデートが完了すると、ディスク全体の暗号化機能を再び使用できるようになります。

Kaspersky Endpoint Security は以下の製品からのアップデートをサポートします：

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (ビルド 10.3.3.275)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (ビルド 10.3.3.304)
- Kaspersky Endpoint Security 11.0.0 for Windows (ビルド 11.0.0.6499)
- Kaspersky Endpoint Security 11.0.1 for Windows (ビルド 11.0.1.90)
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (ビルド 11.0.1.90)
- Kaspersky Endpoint Security 11.1.0 for Windows (ビルド 11.1.0.15919)
- Kaspersky Endpoint Security 11.1.1 for Windows (ビルド 11.1.1.126)
- Kaspersky Endpoint Security 11.2.0 for Windows (ビルド 11.2.0.2254)
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (ビルド 11.2.0.2254)
- Kaspersky Endpoint Security 11.3.0 for Windows (ビルド 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 for Windows (ビルド 11.4.0.233)
- Kaspersky Endpoint Security 11.5.0 for Windows (ビルド 11.5.0.590)
- Kaspersky Endpoint Security 11.6.0 for Windows (ビルド 11.6.0.394)

Kaspersky Endpoint Security 10 Service Pack 2 for Windows を Kaspersky Endpoint Security 11.7.0 for Windows にアップグレードする場合、以前のバージョンの製品で [\[バックアップ\]](#) または [\[隔離\]](#) に置かれていたファイルは、新しいバージョンの製品の [\[バックアップ\]](#) に移動されます。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンの場合、以前のバージョンの製品で [\[バックアップ\]](#) または [\[隔離\]](#) に置かれていたファイルは、新しいバージョンに移行されません。

Kaspersky Endpoint Security のアップデートでは、次の方法を使用できます：

- クライアントデバイスのローカルで、[セットアップウィザード](#)を使用。
- クライアントデバイスのローカルで、[コマンドライン](#)を使用。

- [Kaspersky Security Center](#) を使用してリモートで実行。
- Microsoft Windows のグループポリシー管理エディターを使用してリモートで実行（詳しい手順については、[Microsoft のテクニカルサポートサイト](#) を参照してください）
- [System Center Configuration Manager](#) を使用してリモートで実行

企業のネットワークに配備されたアプリケーションが既定のセット以外の機能を備えている場合、アプリケーションのアップデートは、管理コンソール（MMC）からアップデートする場合と Web コンソールまたは Cloud コンソールからアップデートする場合で異なります。Kaspersky Endpoint Security をアップデートするときには、次の点に留意してください：

- Kaspersky Security Center Web コンソール または Kaspersky Security Center Cloud コンソール  
本製品の新しいバージョンの既定のセットでインストールパッケージを作成した場合は、ユーザーのコンピューターのコンポーネントのセットは変更されません。既定のコンポーネントのセットの Kaspersky Endpoint Security を使用するには、[インストールパッケージのプロパティを開いて](#)、コンポーネントのセットを変更してから元の機能のセットに戻して変更を保存します。
- Kaspersky Security Center の管理コンソール  
アップデート後、アプリケーションコンポーネントのセットはインストールパッケージのコンポーネントのセットと一致します。本製品の新しいバージョンに既定のコンポーネントのセットを含めた場合、既定のセットに含まれない機能（有害 USB 攻撃ブロック機能など）はコンピューターから削除されます。アップデート前と同じコンポーネントのセットの使用を続けるには、[インストールのパッケージの設定](#) で必要なコンポーネントを選択してください。

## 製品の削除

Kaspersky Endpoint Security を削除すると、コンピューターとユーザーデータが脅威から保護されなくなります。

Kaspersky Endpoint Security のアンインストールでは、次の方法を使用できます：

- クライアントデバイスのローカルで、[セットアップウィザード](#) を使用
- クライアントデバイスのローカルで、[コマンドライン](#) を使用
- Kaspersky Security Center を使用してリモートで実行。詳細については、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。
- Microsoft Windows のグループポリシー管理エディターを使用してリモートで実行（詳しい手順については、[Microsoft のテクニカルサポートサイト](#) を参照してください）

本製品のインストール中に Endpoint Agent コンポーネントを選択した場合、次の 2 つのアプリケーションがコンピューターにインストールされます：Kaspersky Endpoint Security および Kaspersky Endpoint Agent。Kaspersky Endpoint Security のアンインストール後、Kaspersky Endpoint Agent も自動的にアンインストールされます。

## Kaspersky Security Center を使用したアンインストール

[アプリケーションのリモートアンインストール] タスクを使用して、リモートで本製品のアンインストールを実行できます。このタスクの実行時に、Kaspersky Endpoint Security は本製品をアンインストールするためのユーティリティをユーザーのコンピューターにダウンロードします。本製品のアンインストールが完了すると、このユーティリティも自動的に削除されます。

#### **管理コンソール (MMC) からアプリケーションを削除する方法**

1. 管理コンソールで、[管理サーバー] → [タスク] のフォルダーに移動します。

タスクのリストが表示されます。

2. [新規タスク] をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

[Kaspersky Security Center 管理サーバー] → [詳細] → [アプリケーションのリモートアンインストール] の順に選択します。

## ステップ 2：削除するアプリケーションの選択

[Kaspersky Security Center に対応するアプリケーションをアンインストールする] を選択します。

## ステップ 3：アプリケーションのアンインストールのタスク設定

Kaspersky Endpoint Security for Windows (11.7.0) プラグインを選択します。

## ステップ 4：アンインストールユーティリティの設定

次の追加のアプリケーション設定を設定します：

- **アンインストールユーティリティの強制ダウンロード**：ユーティリティの配布方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントのツールを使用して Kaspersky Endpoint Security がアンインストールされます。
  - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについては詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。
- **ダウンロード前に OS の種別を確認する** 必要に応じて、このオプションをオフにします。このオプションがオンの場合、コンピューターのオペレーティングシステムが製品のインストール要件を満たさないのにアンインストールユーティリティを誤ってダウンロードしてしまうことを防ぐことができます。コンピューターのオペレーティングシステムが製品のインストール要件を確実に満たしている場合は、この検証をスキップできます。

アプリケーションのアンインストール操作がパスワードで保護されている場合、次の手順を実行します：

1. **「アンインストール用パスワードを使用する」** をオンにします。
2. **「編集」** をクリックします。
3. KLABin アカウントのパスワードを入力します。

## ステップ 5：オペレーティングシステムの再起動設定の選択

アプリケーションをアンインストールした後、再起動が必要です。コンピューターを再起動するために実行するアクションを選択します。

## ステップ 6：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 7：タスクを実行するアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときに利用するユーザーアカウントを選択します。この場合、コンピューターへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をアンインストールする場合は、アカウントを選択する必要はありません。

## ステップ 8：タスク開始スケジュールの設定

たとえば、手動で、またはコンピューターを使用していないときに、タスクを開始するスケジュールを設定します。

## ステップ 9：タスク名の定義

タスクの名前を入力します。たとえば、Kaspersky Endpoint Security 11.7.0 のアンインストールなど。

## ステップ 10：タスク作成の終了

ウィザードを終了します。必要に応じて、**「ウィザードの完了後にタスクを実行」**をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

本製品がサイレントモードでアンインストールされます。

### [Web コンソールと Cloud コンソールからアプリケーションを削除する方法](#)



1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **【アプリケーション】** ドロップダウンリストで、**Kaspersky Security Center** を選択します。
2. **【タスク種別】** で、**【アプリケーションのリモートアンインストール】** を選択します。
3. **【タスク名】** に「サポート部門用のコンピューターからの Kaspersky Endpoint Security のアンインストール」などの簡潔な名前を付けます。
4. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。

## ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。たとえば、別の管理グループを選択するか、選択を作成します。

## ステップ 3：本製品のアンインストール設定の指定

本製品のアンインストール設定を指定します：

1. **【管理対象アプリケーションをアンインストールする】** を選択します。
2. **Kaspersky Endpoint Security for Windows (11.7.0) プラグイン** を選択します。
3. **アンインストールユーティリティの強制ダウンロード**：ユーティリティの配布方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントのツールを使用して Kaspersky Endpoint Security がアンインストールされます。
  - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にはこのオプションを選択できます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビュー

ションポイントについて詳しくは、[Kaspersky Security Centerのオンラインヘルプ](#)を参照してください。

4. **【同時ダウンロード数の上限】**で、管理サーバーに送信されるアンインストールユーティリティのダウンロード要求数の上限を設定します。要求数の上限を設定することで、ネットワークに過剰な負荷を与えずに済みます。
5. **【アンインストール試行回数の上限】**で、製品のアンインストールの試行を繰り返す回数の上限を設定します。Kaspersky Endpoint Security のアンインストールがエラーで終了した場合、タスクは自動的にアンインストールをもう一度開始します。
6. 必要に応じて、**【ダウンロード前に OS の種別を確認する】**をオフにします。このオプションがオンの場合、コンピューターのオペレーティングシステムが製品のインストール要件を満たさないのにアンインストールユーティリティを誤ってダウンロードしてしまうことを防ぐことができます。コンピューターのオペレーティングシステムが製品のインストール要件を確実に満たしている場合は、この検証をスキップできます。

## ステップ 4：タスクを実行するアカウントの選択

ネットワークエージェントをインストールする場合に、オペレーティングシステムの共有フォルダーを使用するときには利用するユーザーアカウントを選択します。この場合、コンピューターへのアクセスには管理者権限が必要です。複数のアカウントを追加できます。指定されたアカウントに十分な権限が付与されていない場合、インストールウィザードでは次に指定されているアカウントが使用されます。既にインストールされているネットワークエージェントを使用して Kaspersky Endpoint Security をアンインストールする場合は、アカウントを選択する必要はありません。

## ステップ 5：タスク作成の完了

**【終了】** をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。

タスクを実行するには、タスクのチェックボックスをオンにし、**【開始】** をクリックします。本製品がサイレントモードでアンインストールされます。アンインストールが完了すると、コンピューターの再起動を要求するメッセージが Kaspersky Endpoint Security によって表示されます。

本製品のアンインストール操作が[パスワードによって保護されている](#)場合、アプリケーションのリモートアンインストールタスクのプロパティで KAdmin アカウントのパスワードを入力してください。このパスワードを指定していないと、タスクは実行されません。

アプリケーションのリモートアンインストールタスクで KAdmin アカウントのパスワードを使用するには：

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Security Center のタスクの中から**アプリケーションのリモートアンインストールタスク**をクリックします。  
タスクのプロパティウィンドウが表示されます。
3. **【アプリケーション設定】** タブを選択します。
4. **【アンインストール用パスワードを使用する】** をオンにします。
5. KAdmin アカウントのパスワードを入力します。

## ウィザードを使用しての製品のアンインストール

Kaspersky Endpoint Security は、Windows オペレーティングシステムでその他のアプリケーションをアンインストールするときと同じように、コントロールパネルを使用してアンインストールされます。セットアップウィザードが起動します。画面に表示される指示に従って操作します。

製品の次回のインストール時（製品の新しいバージョンにアップグレードするときなど）に使用できるように、製品で使用していたデータの中で保存が必要なデータを指定できます。データを指定しない場合、製品が完全に削除されます。

次のデータを保存できます：

- **ライセンスを保存する**：本製品を再度アクティベートしなくてすむようにデータを保存できます。次回のインストール時にライセンスの有効期限が切れていなかった場合、Kaspersky Endpoint Security のライセンスが自動的に追加されます。
- **バックアップファイル**：製品によってスキャンされ、バックアップ保管領域に保管されるファイル。

製品の削除後に保存されたバックアップファイルにアクセスするには、そのファイルを保存するために使用したのと同じバージョンの製品を使用する必要があります。

製品の削除後にバックアップオブジェクトを使用する予定がある場合は、製品の削除前に、これらのオブジェクトを復元する必要があります。ただし、バックアップ保管領域にあるファイルを復元するとコンピューターに損害を与える可能性があるため、カスペルスキーではこれらのファイルの復元を推奨していません。

- **以前の設定を使用する**：製品のセットアップに使用できる製品の設定値を保存できます。
- **暗号鍵のローカル保管領域を保存する**：製品を削除する前に暗号化されたファイルおよびドライブへの直接アクセスを提供するデータを保存できます。暗号化されたファイルおよびドライブへのアクセスを確保するには、Kaspersky Endpoint Security の再インストール時に、暗号化機能のインストールを確実に選択してください。以前に暗号化されたファイルおよびドライブへのアクセスを確保するために、再インストール後に追加で実行する必要がある操作はありません。

# 製品のライセンス

このセクションでは、製品のライセンスに関する一般的な概念に関する情報を提供します。

## 使用許諾契約書について

使用許諾契約書は、お客様と AO Kaspersky Lab を拘束する合意事項であり、お客様が製品を使用する上での条件を規定しています。

製品を使用する前に、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 Endpoint Security を[対話モード](#)でインストールする場合。
- ファイル license.txt を読む：このドキュメントは、[製品配信キット](#)に含まれています。また、製品のインストールフォルダー %Program Files(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\<ロケール>\KES にもあります。

製品のインストール時に使用許諾契約書への同意が確認されると、使用許諾契約書の条件に承諾したものとみなされます。使用許諾契約書の条件を承諾しない場合、インストールを中止する必要があります。

## ライセンスの概要

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。

ライセンスは、使用許諾契約書の条項に従って本製品を使用する、またテクニカルサポートを利用する権利を与えるものです。利用可能な機能と製品の使用に関する条件は、製品のアクティベーションに使用されたライセンスの種類によって異なります。

次の種類のライセンスが提供されています：

- 試用版 - 製品を試用するための無償ライセンス  
通常、試用版ライセンスには短い有効期間が設定されています。試用版ライセンスの有効期間が終了すると、すべての Kaspersky Endpoint Security 機能が無効になります。製品を引き続き使用するには、製品版ライセンスを購入してください。  
試用版ライセンスでアプリケーションをアクティベートできるのは一度だけです。
- 製品版 - Kaspersky Endpoint Security の購入時に提供される有償ライセンス  
製品版ライセンスで使用できる製品の機能は、選択する製品によって異なります。選択した製品は、[ライセンスの証明書](#)に表示されます。利用可能な製品に関する情報については、[カスペルスキーの Web サイト](#)を参照してください。  
製品版のライセンスの有効期間が終了すると、本製品の主要な機能が無効になります。製品を引き続き使用するには、ライセンスを更新してください。ライセンスを更新する予定がない場合は、コンピューターから本製品を削除してください。

## ライセンスの証明書について

ライセンスの証明書とは、ライセンス情報ファイルまたはアクティベーションコードとともに提供される文書です。

ライセンスの証明書に含まれるライセンス情報は次のとおりです：

- ライセンス情報の数値または注文番号
- ライセンスが付与されているユーザーの詳細
- ライセンスでアクティベートできる製品の詳細
- ライセンス単位の数の制限（例：ライセンスを使用してアプリケーションを使用できるデバイスの数）
- ライセンスの有効期間の開始日
- ライセンスの有効期限またはライセンスの有効期間
- 種別：

## 月額制サービスについて

*Kaspersky Endpoint Security* の月額制サービスとは、特定の条件（月額制サービス有効期限や保護対象のデバイス数）で製品を購入することです。サービスプロバイダー（インターネットサービスプロバイダーなど）に *Kaspersky Endpoint Security* の月額制サービスを注文できます。月額制サービスは手動または自動で更新できます。また、キャンセルすることもできます。

月額制サービスは期限付き（たとえば1年間）とすることも、無期限（有効期限なし）とすることもできます。月額制サービスの期限が切れた後も *Kaspersky Endpoint Security* の機能を継続させるには、月額制サービスを更新する必要があります。無期限の月額制サービスは、提供元のサービスが約定日に前払いされていれば、自動的に更新されます。

期限付き月額制サービスの有効期間が終了した後、契約更新の猶予期間がある場合、製品は機能し続けます。猶予期間の有無と長さは、サービスプロバイダーによって規定されます。

月額制サービスで *Kaspersky Endpoint Security* を使用するには、サービスプロバイダーから受け取った [アクティベーションコード](#) を適用する必要があります。アクティベーションコードの適用後、アクティブキーが追加されます。現在のライセンスは、月額制サービスでアプリケーションを使用するためのライセンスを決定します。月額制サービスで予備のライセンスを追加することはできません。

月額制サービスのもとで購入したアクティベーションコードを、*Kaspersky Endpoint Security* の以前のバージョンのアクティベーションに使用することはできません。

## ライセンスについて

ライセンスは、アクティベーションに使用するビットシーケンスで、使用許諾契約書の条件に従ってアプリケーションを使用します。

月額制サービスで追加されるライセンスには、[ライセンス証明書](#)は提供されません。

ライセンス情報ファイルを適用するか、アクティベーションコードを入力することにより、アプリケーションにライセンスを追加できます。

使用許諾契約書の条項に違反すると、カスペルスキーによってライセンスがブロックされる場合があります。ライセンスがブロックされている場合、アプリケーションの使用を継続するには、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、現在と予備の2種類があります。

現在のライセンスは、製品で現在使われているライセンスです。試用版または製品版のライセンスを、現在のライセンスとして追加できます。1つの製品に対して現在のライセンスを2つ以上使用することはできません。

予備のライセンスは、製品を使用する権限をユーザーに付与する、現在使用されていないライセンスです。現在のライセンスの有効期間が終了すると、予備のライセンスが自動的に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ある場合のみ追加できます。

試用版ライセンスは、現在のライセンスとしてのみ追加できます。試用版ライセンスを予備のライセンスとして追加することはできません。現在のライセンスが製品版ライセンスである場合、試用版のライセンスで置き換えることはできません。

ライセンスが禁止されたライセンスのリストに追加された場合、[本製品のアクティベートに使用されたライセンス](#)により定義された本製品の機能は8日間利用可能です。本製品はユーザーに禁止されたライセンスのリストに追加されたことを通知します。8日後、アプリケーションの機能は、ライセンスの有効期限後に使用可能な機能レベルに制限されます。保護および管理コンポーネントを使用して、コンピューターをスキャンすることもできますが、使用できる定義データベースは、ライセンスの有効期間が終了する前にインストールされたものです。また、ライセンスの有効期間が終了する前に変更および暗号化されたファイルも引き続き暗号化されますが、新しいファイルは暗号化されません。Kaspersky Security Network は使用できません。

## About activation code

An *activation code* is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a license key that activates Kaspersky Endpoint Security. You receive an activation code at the email address you specified after purchasing Kaspersky Endpoint Security.

To activate the application with an activation code, Internet access is required to connect to Kaspersky activation servers.

When the application is activated using an activation code, the active key is added. A reserve key can be added only by using an activation code and cannot be added using a key file.

If an activation code is lost after activating the application, you can restore the activation code. You may need an activation code, for example, to register a [Kaspersky Company Account](#). If the activation code was lost after the application activation, contact Kaspersky partner from whom you purchased the license.

## ライセンス情報ファイルについて



ライセンス情報ファイルは、カスペルスキーから受け取った拡張子が .key のファイルです。ライセンス情報ファイルの用途は、製品をアクティベートするライセンスを追加することです。

ライセンス情報ファイルは、Kaspersky Endpoint Security の購入後にカスペルスキーから受け取ります。

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するには、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

誤って削除してしまったライセンス情報ファイルは復元できます。たとえば、カスペルスキーカンパニーアカウントの登録に、ライセンス情報ファイルが必要となる場合があります。

ライセンス情報ファイルを復元するには：

- ご購入元の販売代理店へ問い合わせる
- 既存のアクティベーションコードに基づき、[カスペルスキーの Web サイト](#) でライセンス情報ファイルを取得する

本製品がライセンス情報ファイルを使用してアクティベートされると、現在のライセンスが追加されます。予備のライセンスはライセンス情報ファイルを使用してのみ追加でき、アクティベーションコードを使用して追加することはできません。

## 製品のアクティベーション

アクティベーションは、[ライセンス](#)の有効期間が終了するまで、製品の完全機能版の使用を許可するライセンスをアクティベートするプロセスです。アプリケーションのアクティベーションには、[ライセンス](#)の追加が含まれます。

次のいずれかの方法で製品をアクティベートすることができます：

- [アクティベーションウィザード](#)を使用し、アプリケーションインターフェイスからローカルで実行。現在のライセンスと予備のライセンスの両方を追加できます。
- リモートで [Kaspersky Security Center](#) の機能を使用して、ライセンスの追加タスクを作成してから開始。この方法で、現在のライセンスと予備のライセンスの両方を追加できます。
- リモートで Kaspersky Security Center 管理サーバーの保管領域に保存されているライセンスとアクティベーションコードをクライアントコンピューターに配布。ライセンスの配布については、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。この方法で、現在のライセンスと予備のライセンスの両方を追加できます。

定額制サービスで購入したアクティベーションコードが優先的に配信されます。

- [コマンドライン](#)を使用。

カスペルスキーのアクティベーションサーバー間で負荷が分散されるため、アプリケーションがアクティベーションコードで（リモートインストールまたは非インタラクティブインストール中に）アクティベートされるまでに時間がかかる場合があります。製品をすぐにアクティベートする必要がある場合は、進行中のアクティベーションプロセスを中断して、アクティベーションウィザードを使用したアクティベーションを開始することもできます。



## Kaspersky Security Center を使用した製品のアクティベーション

次の方法で、Kaspersky Security Center からリモートで製品をアクティベートすることができます：

- [ライセンスの追加] タスクを使用  
この方法を使用すると、特定のコンピューターまたは単一の管理グループに属するコンピューターにライセンスを追加できます。
- Kaspersky Security Center 管理サーバーに保存されているライセンスをコンピューターに配信  
この方法を使用すると、Kaspersky Security Center に既に接続されているコンピューターと新しく検出されたコンピューターに自動的にライセンスを追加できます。この方法を使用するには、最初にライセンスを Kaspersky Security Center 管理サーバーに追加する必要があります。Kaspersky Security Center 管理サーバーへのライセンスの追加について詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソールの試用版が提供されています。試用版は、ユーザーが製品の機能を理解できるように設計された Kaspersky Security Center Cloud コンソールの特別なバージョンです。このバージョンでは、30 日間ワークスペースで操作を実行できます。すべての管理対象アプリケーションは、Kaspersky Endpoint Security を含む Kaspersky Security Center Cloud コンソールの試用ライセンスの下で自動的に実行されます。ただし、Kaspersky Security Center Cloud コンソールの試用ライセンスの有効期限が切れると、自身の試用ライセンスを使用して Kaspersky Endpoint Security をアクティベートすることはできません。Kaspersky Security Center のライセンスについて詳しくは、[Kaspersky Security Center Cloud コンソールのオンラインヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソールの試用版では、その後製品版に切り替えることはできません。30日間の期限が切れると、試用ワークスペースはすべてのコンテンツとともに自動的に削除されます。

ライセンスの使用状況を次の方法を使用して監視できます：

- 組織ネットワーク内での [ライセンス使用レポート] を表示する（ [監視とレポート] → [レポート] ）。
- [デバイス] → [管理対象デバイス] タブでコンピューターのステータスを表示する。製品がアクティベートされていない場合、コンピューターには ▲ ステータスと「**アクティベートされていません**」というステータスメッセージが表示されます。
- コンピューターのプロパティでライセンス情報を表示する。
- ライセンスのプロパティを表示する（ [操作] → [ライセンス管理] ）。

### [管理コンソール \(MMC\) で製品をアクティベートする方法](#)

1. 管理コンソールで、**[管理サーバー]** → **[タスク]** のフォルダーに移動します。

タスクのリストが表示されます。

2. **[新規タスク]** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

**[Kaspersky Endpoint Security for Windows (11.7.0)]** → **[ライセンスの追加]** を選択します。

## ステップ 2：ライセンスの追加

[アクティベーションコード](#)を入力するか、ライセンス情報ファイルを選択します。

Kaspersky Security Center のリポジトリへのライセンスの追加について詳しくは、[Kaspersky Security Centerのオンラインヘルプ](#)を参照してください。

## ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 4：タスク開始スケジュールの設定

たとえば、手動で、またはコンピューターを使用していないときに、タスクを開始するスケジュールを設定します。

## ステップ 5：タスク名の定義

Kaspersky Endpoint Security for Windows のアクティベートなど、タスク名を入力します。

## ステップ 6：タスク作成の完了

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。その結果、Kaspersky Endpoint Security は、ユーザーのコンピューターのサイレントモードでアクティベートされます。



1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。

2. **【追加】** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
2. **【タスク種別】** で、**【ライセンスの追加】** を選択します。
3. **【タスク名】** に「マネージャー用の Kaspersky Endpoint Security for Windows のアクティベーション」などの簡潔な名前を付けます。
4. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。**【次へ】** をクリックします。

## ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 3：ライセンスの選択

製品のアクティベーションに使用するライセンスを選択します。**【次へ】** をクリックします。

Web コンソールでライセンスを追加できます（**【操作】** → **【ライセンス管理】**）。

## ステップ 4：タスク作成の完了

**【終了】** をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。タスクを実行するには、タスクのチェックボックスをオンにし、**【開始】** をクリックします。その結果、Kaspersky Endpoint Security は、ユーザーのコンピューターのサイレントモードでアクティベートされます。

ライセンスの追加タスクのプロパティで、コンピューターに予備のライセンスを追加できます。現在のライセンスの有効期限が切れるか削除されると、予備のライセンスがアクティブになります。予備のライセンスを利用できるため、ライセンスの有効期限が切れたときに製品の機能制限を回避できます。

### 管理コンソール (MMC) を使用してコンピューターにライセンスを自動的に追加する方法

1. 管理コンソールで、[管理サーバー] → [カスペルスキーのライセンス] フォルダーに移動します。  
ライセンスのリストが開きます。
2. ライセンスのプロパティを開きます。
3. [全般] セクションで、[自動的に配信されるライセンス] をオンにします。
4. 変更内容を保存します。

これにより、必要に応じてコンピューターにライセンスが自動的に配信されます。ライセンスを現在のライセンスまたは予備のライセンスとして自動配信する際、コンピューター数のライセンス制限（ライセンスのプロパティで設定）が考慮されます。ライセンス数の上限に達すると、コンピューターへのライセンス配信は自動的に停止されます。[デバイス] セクションのライセンスのプロパティで、ライセンスが追加されたコンピューターの台数などのデータを確認できます。

### Web コンソールと Cloud コンソールを使用してコンピューターにライセンスを自動的に追加する方法

1. Web コンソールのメインウィンドウで [操作] → [ライセンス管理] → [カスペルスキーのライセンス] の順に選択します。  
ライセンスのリストが開きます。
2. ライセンスのプロパティを開きます。
3. [全般] で、[ライセンスを自動で配信する] オプションをオンにします。
4. 変更内容を保存します。

これにより、必要に応じてコンピューターにライセンスが自動的に配信されます。ライセンスを現在のライセンスまたは予備のライセンスとして自動配信する際、コンピューター数のライセンス制限（ライセンスのプロパティで設定）が考慮されます。ライセンス数の上限に達すると、コンピューターへのライセンス配信は自動的に停止されます。[デバイス] タブのライセンスのプロパティで、ライセンスが追加されたコンピューターの台数などのデータを確認できます。

## アクティベーションウィザードを使用した製品のアクティベーション

アクティベーションウィザードを使用して *Kaspersky Endpoint Security* をアクティベートするには、次の手順を実行します：

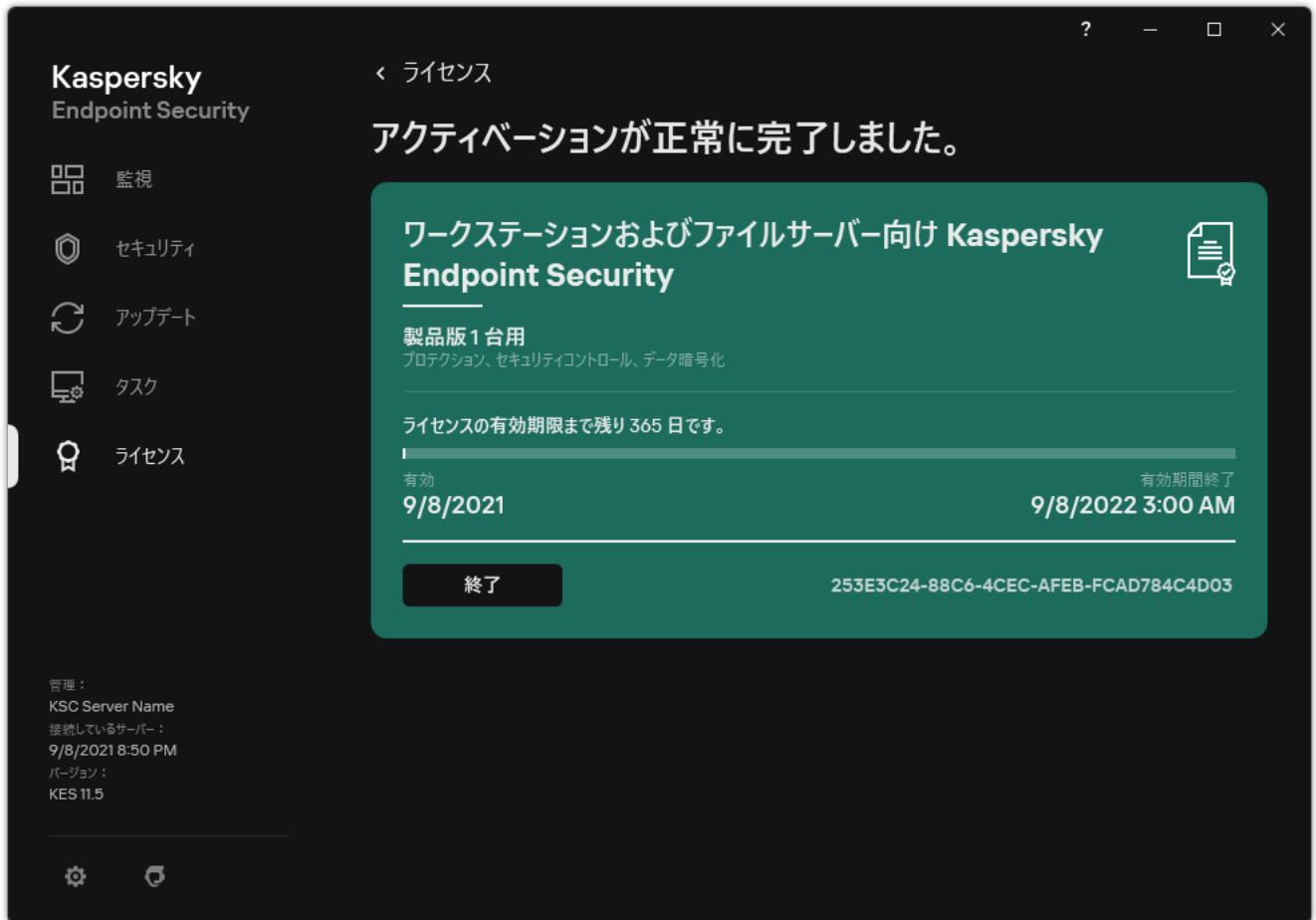
1. メインウィンドウで、[ライセンス] セクションに移動します。
2. [新規ライセンスによる製品のアクティベーション] をクリックします。

アクティベーションウィザードが起動します。アクティベーションウィザードの指示に従います。

## ライセンス情報の表示

ライセンスの情報を確認するには：

メインウィンドウで、**【ライセンス】** セクションに移動します（下の図を参照）。



[ライセンス] ウィンドウ

このセクションには次の内容が表示されます：

- **ライセンスステータス**：1台のコンピューターに複数の[ライセンス](#)を保管できます。ライセンスには、現在と予備の2種類があります。1つの製品に対して現在のライセンスを2つ以上使用することはできません。予備のライセンスは、現在のライセンスが期限切れになったとき、または**【削除】**をクリックして現在のライセンスが削除された後にのみ有効になります。
- **アプリケーション名**：カスペルスキー製品の正式名称。
- **ライセンス**：次の[種別のライセンス](#)を利用できます：試用版と製品版。
- **機能**：ライセンスを使用して利用できる製品機能。機能には、プロテクション、セキュリティコントロール、データ暗号化などがあります。使用可能な機能のリストは、ライセンス証明書にも記載されています。
- **ライセンスに関する追加情報**：ライセンスの有効期間の開始日時および終了日時（現在のライセンスのみ）およびライセンスの有効期間の残り日数です。

ライセンスの有効期間は、オペレーティングシステムで設定されているタイムゾーンでの時間で表示されます。

- **識別 ID**：識別 ID 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から生成される一意の英数字列です。

[ライセンス] ウィンドウで、次の操作も実行できます：

- **ライセンスの購入**または**ライセンスの更新**：ライセンスを購入または更新できる Web サイトが開きます。購入または更新するには、企業の情報を入力して注文に対する支払いを行ってください。
- **新規ライセンスによる製品のアクティベーション**：アクティベーションウィザードが起動します。ウィザードで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ライセンスを追加できます。アクティベーションウィザードでは、現在のライセンスを1つと予備のライセンスを1つのみ追加できます。

## ライセンスの更新または購入

製品をインストールした後でも、ライセンスを購入できます。ライセンスを購入すると、製品をアクティベートするためのアクティベーションコードまたはライセンス情報ファイルを手に入れます。

ライセンスを購入するには、次の手順を実行します：

1. メインウィンドウで、**[ライセンス]** セクションに移動します。
2. 次のいずれかの手順を実行します：
  - ライセンスが追加されていない場合または試用版ライセンスが追加されている場合は、**[ライセンスの購入]** をクリックします。
  - 製品版ライセンスが追加されている場合は、**[ライセンスの更新]** をクリックします。

ライセンス購入用の Web サイトが表示されます。

## 月額制サービスの更新

月額制サービスで本製品を使用している場合、その有効期間が終了するまで、Kaspersky Endpoint Security は一定の間隔でアクティベーションサーバーへの問い合わせを実行します。

無期限の月額制サービスのもとで本製品を使用している場合、Kaspersky Endpoint Security は更新されたライセンスについてバックグラウンドモードでアクティベーションサーバーをチェックします。ライセンスがアクティベーションサーバーで使用可能な場合、前のライセンスを置き換えることにより更新されたライセンスを追加します。このようにして、Kaspersky Endpoint Security の無期限の月額制サービスはユーザー操作を必要とせずに更新されます。

本製品を期限付き月額制サービスで使用している場合、月額制サービスの有効期間（または月額制サービスの更新猶予期間）が終了する日に、Kaspersky Endpoint Security が通知を表示して、月額制サービスの自動更新を停止します。この場合、Kaspersky Endpoint Security は[製品版ライセンスの期限切れ](#)のときと同じ動作をします。つまり、製品はアップデートなしで動作し、Kaspersky Security Network サービスが利用できなくなります。



本製品のインターフェイスからサービスプロバイダーの Web サイトへアクセスするには：

1. メインウィンドウで、**［ライセンス］** セクションに移動します。
2. **［定額制サービスのプロバイダーに問い合わせる］** をクリックします。

定額制サービスの状態を手動で更新できます。これは、猶予期間の後に月額制サービスを更新し、月額制サービスの契約ステータスが自動的に更新されなかった場合に必要になることがあります。

# データ提供

## 使用許諾契約書におけるデータ提供

[アクティベーションコード](#) を適用して Kaspersky Endpoint Security をアクティベートしている場合、本製品が適切に使用されていることを確認するため、以下の情報を定期的にカスペルスキーに自動送信することに同意したことになります：

- Kaspersky Endpoint Security の種別、バージョン、ローカリゼーション
- Kaspersky Endpoint Security のインストールされたアップデートのバージョン
- コンピューターの識別子およびそのコンピューターにインストールされた Kaspersky Endpoint Security の識別子
- シリアル番号と現在のライセンスの識別子
- オペレーティングシステムの種別、バージョンおよびビット数、および仮想環境の名前（Kaspersky Endpoint Security が仮想環境にインストールされている場合）
- 情報の送信時に使用中である Kaspersky Endpoint Security コンポーネントの識別子

カスペルスキーは、この情報を使用して、カスペルスキー製品の使用に関する統計情報を生成する場合があります。

アクティベーションコードを使用することで、上記データの自動送信に同意したことになります。カスペルスキーへの情報の送信に同意しない場合は、[ライセンス情報ファイル](#) を使用して Kaspersky Endpoint Security をアクティベートしてください。

使用許諾契約書の条件に同意することで、次の情報の自動送信に同意したことになります：

- Kaspersky Endpoint Security のアップグレード時：
  - Kaspersky Endpoint Security のバージョン
  - Kaspersky Endpoint Security の識別子
  - 現在のライセンス
  - アップグレードタスクの起動の一意的な識別子
  - Kaspersky Endpoint Security のインストールの一意的な識別子
- Kaspersky Endpoint Security のインターフェイスからのリンクを使用する場合：
  - Kaspersky Endpoint Security のバージョン
  - オペレーティングシステムのバージョン
  - Kaspersky Endpoint Security のアクティベーション日
  - ライセンスの有効期限

- ライセンスの作成日
- Kaspersky Endpoint Security のインストール日
- Kaspersky Endpoint Security の識別子
- オペレーティングシステムで検知された脆弱性の識別子
- 最後にインストールされた Kaspersky Endpoint Security アップデートの識別子
- 検知された脅威を含むファイルのハッシュと、カスペルスキーの分類による脅威の名前
- Kaspersky Endpoint Security のアクティベーションエラーのカテゴリ
- Kaspersky Endpoint Security のアクティベーションエラーコード
- ライセンス有効期限までの日数
- ライセンスが追加されてからの経過日数
- ライセンスの有効期限からの経過日数
- 現在のライセンスが適用されているコンピューターの台数
- 現在のライセンス
- Kaspersky Endpoint Security のライセンス期間
- ライセンスの現在の状態
- 現在のライセンスの種別
- 製品の種別
- アップグレードタスクの起動の一意的識別子
- Kaspersky Endpoint Security のコンピューターへのインストールの一意的識別子
- Kaspersky Endpoint Security のインターフェイス言語

取得した情報は、法令およびカスペルスキーの規定に従って、カスペルスキーにより保護されます。データは暗号化された通信チャネル経由で送信されます。

使用許諾契約書および Kaspersky Security Network に関する声明に同意した後の製品使用状況に関する情報の取得、処理、保存、破棄の詳細な方法については、使用許諾契約書を読み、[カスペルスキーの Web サイト](#)をご参照ください。ファイル license.txt および ksn\_<言語 ID>.txt には、使用許諾契約書および Kaspersky Security Network に関する声明の本文が記載されています。これらは本製品の[配信キット](#)に含まれています。

## Kaspersky Security Network 使用時のデータ提供

Kaspersky Endpoint Security がカスペルスキーに送るデータのセットは、ライセンスの種別と Kaspersky Security Network の使用設定により異なります。

## 4 台以下のコンピューター用のライセンスでの KSN の使用

Kaspersky Security Network に関する声明に同意すると、次の情報の自動送信に同意したことになります：

- KSN 設定のアップデートに関する情報：使用中の設定情報の識別子、受信した設定情報の識別子、設定情報のアップデートのエラーコード。
- スキャンされるファイルと URL アドレスに関する情報：スキャンされたファイルのチェックサム（MD5、SHA2-256、SHA1）およびファイルパターンのチェックサム（MD5）、パターンのサイズ、検知した脅威の種別および権利者の分類に基づく名前、定義データベースの識別子、評価が要求されている URL アドレスおよび参照元の URL アドレス、接続プロトコルの識別子および使用しているポートの番号。
- 脅威を検知したスキャンタスクの識別子。
- 認証を検証するために使用されたデジタル署名に関する情報：スキャンされたオブジェクトの署名に使用された証明書および証明書の公開鍵のチェックサム（SHA256）。
- スキャンを実行している本ソフトウェアのコンポーネントのタスク識別子。
- 定義データベースの識別子および定義データベースのレコードの識別子。
- 端末上の本ソフトウェアのアクティベーションに関する情報：アクティベーションサービスからのチケットの署名済みヘッダー（地域の本ソフトウェアのアクティベーションセンターの識別子、アクティベーションコードのチェックサム、チケットのチェックサム、チケットの作成日、チケットの一意的識別子、チケットのバージョン、ライセンスの状態、チケットの有効期間の開始日時と終了日時、ライセンスの一意的識別子、ライセンスのバージョン）、チケットのヘッダーの署名に使用されている証明書のハッシュ、ライセンス情報ファイルのチェックサム（MD5）。
- 権利者の本ソフトウェアに関する情報：バージョンの詳細、種別、Kaspersky サービスへの接続に使用されるプロトコルのバージョン。

## 5 台以上のコンピューター用のライセンスでの KSN の使用

Kaspersky Security Network に関する声明に同意すると、次の情報の自動送信に同意したことになります：

[Kaspersky Security Network] をオン、[拡張 KSN モード] をオフにすると、次の情報が送信されます：

- KSN 設定のアップデートに関する情報：使用中の設定情報の識別子、受信した設定情報の識別子、設定情報のアップデートのエラーコード。
- スキャンされるファイルと URL アドレスに関する情報：スキャンされたファイルのチェックサム（MD5、SHA2-256、SHA1）およびファイルパターンのチェックサム（MD5）、パターンのサイズ、検知した脅威の種別および権利者の分類に基づく名前、定義データベースの識別子、評価が要求されている URL アドレスおよび参照元の URL アドレス、接続プロトコルの識別子および使用しているポートの番号。
- 脅威を検知したスキャンタスクの識別子。
- 認証を検証するために使用されたデジタル署名に関する情報：スキャンされたオブジェクトの署名に使用された証明書および証明書の公開鍵のチェックサム（SHA256）。
- スキャンを実行している本ソフトウェアのコンポーネントのタスク識別子。
- 定義データベースの識別子および定義データベースのレコードの識別子。

- 端末上の本ソフトウェアのアクティベーションに関する情報：アクティベーションサービスからのチケットの署名済みヘッダー（地域の本ソフトウェアのアクティベーションセンターの識別子、アクティベーションコードのチェックサム、チケットのチェックサム、チケットの作成日、チケットの一意的な識別子、チケットのバージョン、ライセンスの状態、チケットの有効期間の開始日時と終了日時、ライセンスの一意的な識別子、ライセンスのバージョン）、チケットのヘッダーの署名に使用されている証明書ハッシュ、ライセンス情報ファイルのチェックサム（MD5）。
- 権利者の本ソフトウェアに関する情報：バージョンの詳細、種別、Kaspersky サービスへの接続に使用されるプロトコルのバージョン。

[**拡張 KSN モードを有効にする**] と [**Kaspersky Security Network**] を両方オンにすると、前述の情報に加えて次の情報も送信されます：

- 要求された Web リソースの分類結果に関する情報：処理された URL およびホストの IP アドレス、分類を実行した本ソフトウェアのコンポーネントのバージョン、分類方法および Web リソースに定義された一連のカテゴリ。
- 端末にインストールされた本ソフトウェアに関する情報：ソフトウェアおよびその開発元の名前、レジストリキーおよびその値、インストールされたソフトウェアコンポーネントのファイルに関する情報（チェックサム（MD5、SHA2-256、SHA1）、名前、コンピューター上のパス、サイズ、バージョンおよびデジタル署名）。
- コンピューターのウイルス対策の状態に関する情報：使用中の定義データベースのバージョンおよび公開のタイムスタンプ、タスクの識別子およびスキャンを実行したソフトウェアの識別子。
- エンドユーザーによってダウンロードされているファイルに関する情報：ダウンロードファイルおよびダウンロードページの URL および IP アドレス、ダウンロードプロトコルの識別子および接続先ポート番号、URL の状態（悪意があるかどうか）、ファイルの属性、サイズおよびチェックサム（MD5、SHA2-256、SHA1）、ファイルをダウンロードしたプロセスに関する情報（チェックサム（MD5、SHA2-256、SHA1）、作成日時、ビルド日時、自動実行の状態、属性、圧縮プログラムの名前、署名に関する情報、実行ファイルのフラグ、形式の識別子、情報量）、ファイル名および端末上のパス、ファイルのデジタル署名とその生成のタイムスタンプ、検知した URL アドレス、疑わしいまたは悪意があると判明したページのスクリプトの数、生成された HTTP リクエストおよびリクエストへのレスポンスに関する情報。
- 実行中のアプリケーションおよびそれらのモジュールに関する情報：システム上で実行されているプロセスに関するデータ（プロセスの識別子（PID）、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、信頼済みプログラムまたはプロセスの署名、プロセスのファイルとそのチェックサム（MD5、SHA2-256、SHA1）の完全パスおよび起動したコマンドライン、プロセスの整合性レベル、プロセスが属するアプリケーションの説明（アプリケーション名および製造元の情報）、使用されるデジタル署名の信頼性を検証するための情報、またはファイルのデジタル署名が存在しない場合は存在しないことを示す情報）、プロセスに読み込まれたモジュールに関する情報（名前、サイズ、種別、作成日時、属性、チェックサム（MD5、SHA2-256、SHA1）、コンピューター上のパス）、PE ファイルヘッダー情報、圧縮プログラムの名前（ファイルが圧縮されている場合）。
- 悪意のある可能性のあるオブジェクトおよび活動に関する情報：検知したオブジェクトの名前およびコンピューター上の完全パス、処理されたファイルのチェックサム（MD5、SHA2-256、SHA1）、検知した日時、感染したファイルの名前およびサイズおよびそのパス、パステンプレートコード、実行ファイルのフラグ、オブジェクトがコンテナであるかどうかを示すフラグ、圧縮プログラムの名前（ファイルが圧縮されている場合）、ファイル種別コード、ファイル形式の識別子、マルウェアが実行した処理のリストおよびそれに対応したソフトウェアとユーザーの判定、判定に使用された定義データベースの識別子および定義データベースのレコードの識別子、悪意のある可能性があるオブジェクトであることを示すフラグ、権利者の分類による検知された脅威の名前、危険度レベル、検知ステータスおよび検知方法、解析されたコンテキストに含めた理由およびコンテキスト内のファイルのシーケンス番号、チェックサム（MD5、SHA2-256、SHA1）、感染したメッセージまたはリンクの送信に使用されたアプリケーションの実行ファイルの名前と属性、ブロックされたオブジェクトのホストの匿名化した IP アドレス（IPv4 および IPv6）、ファイルの情報量、ファイルの自動実行のフラグ、システム内でファイルが最初に検知された時刻、前回統計情報が送信されてからファイルが実行された回数、悪意のあるオブジェクトを受信したメールクライアントの名前とチェックサム（MD5、SHA2-256、SHA1）およびサイズに関する情報、スキャンを実行したソフトウェアのタスクの識別子、ファイルの評価または署名がチェックされたかどうかのフラグ、ファイル

の処理結果、当該オブジェクトに対して収集されたパターンのチェックサム（MD5）、サイズおよびパターン（バイト）、適用された検知技術の技術仕様。

- スキャンしたオブジェクトに関する情報：ファイルの移動先の信頼グループおよび移動元の信頼グループ、当該カテゴリに分類された理由、カテゴリの識別子、元のカテゴリおよびカテゴリデータベースのバージョンに関する情報、ファイルの信頼済み証明書のフラグ、ファイルの製造元、ファイルのバージョン、ファイルが含まれているアプリケーションの名前およびバージョン。
- 検知された脆弱性に関する情報：脆弱性データベース内の脆弱性の識別子、脆弱性の危険度。
- 実行ファイルのエミュレーションに関する情報：ファイルのサイズおよびチェックサム（MD5、SHA2-256、SHA1）、エミュレーションコンポーネントのバージョン、エミュレーション深度、エミュレーション中に取得された論理ブロックのプロパティの配列および論理ブロック内の関数の配列、実行ファイルのPEヘッダーのデータ。
- 攻撃元コンピューターのIPアドレス（IPv4 および IPv6）、攻撃の標的となったコンピューターのポート番号、攻撃に使用されたIPパケットのプロトコルの識別子、攻撃対象（組織名、Webサイト）、攻撃への対処のフラグ、攻撃の重み、信頼度。
- ネットワークリソースの偽装に関連した攻撃に関する情報：閲覧したWebサイトのDNSおよびIPアドレス（IPv4 および IPv6）。
- 要求されたWebリソースのDNSアドレスおよびIPアドレス（IPv4 または IPv6）、WebリソースにアクセスしているファイルおよびWebクライアントに関する情報、ファイルの名前とサイズおよびチェックサム（MD5、SHA2-256、SHA1）、ファイルの完全パスとパステンプレートコード、デジタル署名の確認結果、KSNのステータス。
- マルウェアの処理のロールバックに関する情報：動作がロールバックされたファイルのデータ（ファイル名、ファイルの完全パス、サイズおよびチェックサム（MD5、SHA2-256、SHA1））、成功または失敗した削除処理に関するデータ、ファイルの名前変更とコピーおよびレジストリ内の値の復元（レジストリキーの名前およびその値）、マルウェアによって変更されたシステムファイルに関するロールバック実施前後の情報。
- アダプティブアノマリコントロールコンポーネントの実行セットに関する情報：トリガーされたルールの識別子とステータス、ルールがトリガーされたときに本ソフトウェアにより実行された処理、プロセスまたはスレッドが疑わしい動作を実行しているユーザーアカウントの種別および疑わしい動作の影響を受けたプロセスに関する情報（スクリプト識別子またはプロセスファイル名、プロセスファイルへの完全パス、パステンプレートコード、プロセスファイルのチェックサム（MD5、SHA2-256、SHA1））。疑わしい動作を実行したオブジェクトおよび疑わしい動作の影響を受けたオブジェクトに関する情報（レジストリキー名またはファイル名、ファイルへの完全パス、パステンプレートコード、およびファイルのチェックサム（MD5、SHA2-256、SHA1））。
- 読み込まれたソフトウェアの機能に関する情報。モジュールファイルの名前、サイズおよびチェックサム（MD5、SHA2-256、SHA1）、完全パスおよびパステンプレートコード、モジュールファイルのデジタル署名設定、署名の作成日時、モジュールファイルに署名した発行先および組織名、モジュールが読み込まれたプロセスの識別子、モジュールの供給元の名前、読み込み列内のモジュールのシーケンス番号。
- 本ソフトウェアとKSNサービスとの通信品質に関する情報：統計が生成された期間の開始日時と終了日時、リクエストの品質および使用されている各KSNサービスの接続に関する情報、（KSNサービス識別子、成功したリクエストの数、キャッシュからの応答があったリクエストの数、失敗したリクエストの数（ネットワークの問題、KSNが本ソフトウェアの設定で無効、誤ったルーティング）、成功したリクエストの時間範囲、キャンセルされたリクエストの時間範囲、制限時間を超えたリクエストの時間範囲、キャッシュから取得されたKSNへの接続の数、成功したKSNへの接続の数、失敗したKSNへの接続の数、成功したトランザクションの数、失敗したトランザクションの数、成功したKSNへの接続の時間範囲、失敗したKSNへの接続の時間範囲、成功したトランザクションの時間範囲、失敗したトランザクションの時間範囲）。

- 悪意のある可能性のあるオブジェクトが検知された場合に、プロセスのメモリ内のデータに関して提供される情報：システムのオブジェクト階層（ObjectManager）の要素、UEFI BIOS メモリのデータ、レジストリキーの名前とその値。
- システムログのイベントに関する情報。イベントのタイムスタンプ、イベントが見つかったログの名前、イベントの種別およびカテゴリ、イベントの発生元の名前およびイベントの説明。
- ネットワーク接続に関する情報。ポートを開いたプロセスを開始したファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、プロセスファイルのパスおよびデジタル署名、ローカルおよびリモートのIPアドレス、ローカルおよびリモートの接続ポート番号、接続状態、ポートが開かれたときのタイムスタンプ
- コンピューター上の本ソフトウェアのインストールおよびアクティベーションの日付に関する情報：ライセンスを購入した代理店の識別子、ライセンスのシリアル番号、アクティベーションサービスからのチケットの署名済みヘッダー（地域の本ソフトウェアのアクティベーションセンターの識別子、アクティベーションコードのチェックサム、チケットのチェックサム、チケットの作成日、チケットの一意な識別子、チケットのバージョン、ライセンスの状態、チケットの有効期間の開始日時と終了日時、ライセンスの一意な識別子、ライセンスのバージョン）、チケットのヘッダーの署名に使用されている証明書のハッシュ、ライセンス情報ファイルのチェックサム（MD5）、コンピューターにインストールされたソフトウェアの一意な識別子、アップデートされるアプリケーションの種別および識別子、アップデートタスクの識別子。
- インストールされているすべてのアップデート一式に関する情報、および最後にインストールまたは削除されたアップデート一式に関する情報、アップデート情報の送信を発生させたイベントの種別、最後にアップデートをインストールしてからの経過時間、現在インストールされている定義データベースに関する情報。
- コンピューター上のソフトウェアの処理に関する情報：CPUの使用に関するデータ、メモリの使用（プライベートバイト、非ページプール、ページプール）に関するデータ、ソフトウェアのプロセス中のアクティブなスレッド数および保留中のプロセス数、エラーが発生する前のソフトウェアの処理時間。
- 本ソフトウェアインストール後および前回のアップデート適用後に発生したソフトウェアダンプおよびシステムダンプ（BSOD）の数、クラッシュしたソフトウェアモジュールの識別子とバージョン、ソフトウェアプロセスのメモリスタック、およびクラッシュ時の定義データベースに関する情報。
- システムダンプ（BSOD）のデータ：コンピューターでBSODが発生したことを示すフラグ、BSODの原因となったドライバーの名前、ドライバーのアドレスおよびメモリスタック、BSODが発生するまでのセッションの時間を示すフラグ、クラッシュしたドライバーのメモリスタック、保管されたメモリダンプの種別、BSODが10分以上継続する前のOSセッションのフラグ、ダンプの一意な識別子、BSODのタイムスタンプ。
- 本ソフトウェアのコンポーネントの操作中に発生したエラーまたはパフォーマンスの問題に関する情報：本ソフトウェアのステータスの識別子、エラー種別、エラーが発生したときのコードと原因および時刻、コンポーネントの識別子、エラーが発生した製品のモジュールおよびプロセス、エラー発生中のタスクまたはアップデートカテゴリの識別子、本ソフトウェアが使用するドライバーのログ（エラーコード、モジュール名、ソースファイル名およびエラーが発生した行）
- 定義データベースおよび本ソフトウェアのコンポーネントのアップデートに関する情報：最後のアップデート中および現在のアップデート中にダウンロードされたインデックスファイルの名前と日時。
- 本ソフトウェアの操作の異常終了に関する情報：ダンプファイルの生成日時、種別、本ソフトウェアの操作の異常終了の起因となったイベントの種別（予期しない電源の切断、サードパーティ製アプリケーションのクラッシュ）、予期しない電源の切断が発生した日時。
- ソフトウェアドライバーとハードウェアおよびソフトウェアとの互換性に関する情報：ソフトウェアコンポーネントの機能を制限するOSのプロパティに関する情報（セキュアブート、KPTI、WHQL エンフォース、BitLocker、大文字と小文字の区別）、インストールされたダウンロードソフトウェアの種別（UEFI、BIOS）、Trusted Platform Module（TPM）の識別子、TPM仕様のバージョン、コンピューターに組み込ま



れている CPU に関する情報、Code Integrity と Device Guard の操作モードとパラメータ、ドライバの操作モードおよび現在のモードの使用理由、ソフトウェアドライバのバージョン、コンピューターにおけるソフトウェアとハードウェアの仮想化サポート状況。

- エラーの発生原因となったサードパーティ製アプリケーションに関する情報：名前、バージョンおよび言語、エラーコードおよびアプリケーションのシステムログに含まれるエラーに関する情報、該当するサードパーティ製アプリケーションのエラーのアドレスおよびメモリストック、ソフトウェアのコンポーネント内でエラーが発生したことを示すフラグ、エラーが発生するまでサードパーティ製アプリケーションが動作していた時間、エラーが起きたアプリケーションプロセスイメージのチェックサム (MD5、SHA2-256、SHA1)、アプリケーションプロセスイメージのパスおよびパスのテンプレートコード、アプリケーションに関連付けられたエラー記述を含むシステムログからの情報、エラーが起きたアプリケーションモジュールに関する情報 (例外の識別子、アプリケーションモジュールのオフセットとしてのクラッシュメモリアドレス、モジュールの名前とバージョン、権利者のプラグインで発生したアプリケーションクラッシュの識別子およびクラッシュのメモリストック、クラッシュ発生までのアプリケーションセッションの時間)。
- 本ソフトウェアのアップデータコンポーネントのバージョン、コンポーネントが動作中のアップデートタスク実行中にアップデータコンポーネントがクラッシュした回数、アップデートタスク種別の識別子、アップデータコンポーネントがアップデートタスクを完了させようとして失敗した回数。
- 本ソフトウェアのシステム監視コンポーネントの動作に関する情報：コンポーネントの詳細バージョン、イベントキューをオーバーフローさせたイベントのコードおよび該当するイベントの数、キューがオーバーフローしたイベントの総数、イベントを開始したプロセスのファイルに関する情報 (ファイル名およびコンピューター上のパス、ファイルパスのテンプレートコード、ファイルに関連付けられたプロセスのチェックサム (MD5、SHA2-256、SHA1))、発生したイベント遮断の識別子、遮断フィルターのバージョン、遮断されたイベントの種別の識別子、キュー内の最初のイベントと現在のイベント間におけるイベントキューのサイズとイベントの数、キュー内の期限切れイベントの数、現在のイベントを開始したプロセスのファイルに関する情報 (ファイル名およびコンピューター上のパス、ファイルパスのテンプレートコード、ファイルに関連付けられたプロセスのチェックサム (MD5、SHA2-256、SHA1))、イベントの処理時間、イベントの処理時間の上限、統計を送信する確率、処理時間制限を超えた OS イベントに関する情報 (イベントの日時、定義データベースの初期化繰り返しの回数、定義データベースのアップデート後に最後の初期化繰り返しが実行された日時、各システム監視コンポーネントのイベント処理遅延時間、キューにあるイベントの数、処理されたイベントの数、現在の種別の遅延イベントの数、現在の種別のイベントの合計遅延時間、すべてのイベントの合計遅延時間)。
- ソフトウェアパフォーマンスの問題が発生した場合に SysConfig / SysConfigEx / WinSATAssessment イベントが出力される Microsoft の Windows イベントトレースツール (ETW : Event Tracing for Windows) からの情報：コンピューターに関する情報 (機種、製造元、筐体のフォームファクター、バージョン)、Windows パフォーマンスメトリクスに関する情報 (WinSAT 評価、Windows パフォーマンスインデックス)、ドメイン名、物理プロセッサおよび論理プロセッサに関する情報 (物理プロセッサおよび論理プロセッサの数、製造元、モデル、ステッピングレベル、コア数、クロック周波数、CUID、キャッシュ特性、論理プロセッサ特性、サポートされるモードと命令を示すフラグ)、RAM モジュールに関する情報 (種別、フォームファクター、製造元、モデル、容量、メモリ割り当ての細分性)、ネットワークインターフェイスに関する情報 (IP アドレスおよび MAC アドレス、名前、説明、ネットワークインターフェイスの設定、種別ごとのネットワークパッケージの数とサイズの内訳、ネットワーク通信速度、種別ごとのネットワークエラー数の内訳)、IDE コントローラーの設定、DNS サーバーの IP アドレス、ビデオカードに関する情報 (モデル、説明、製造元、互換性、ビデオメモリ容量、画面許可、ピクセルあたりのビット数、BIOS バージョン)、プラグアンドプレイのデバイスに関する情報 (名前、説明、デバイス識別子 [PnP、ACPI])、ディスクおよびストレージデバイスに関する情報 (ディスクまたはフラッシュデバイスの数、製造元、モデル、ディスク容量、シリンダー数、シリンダーあたりのトラック数、トラックあたりのセクター数、セクター容量、キャッシュ特性、シーケンシャル番号、パーティション数、SCSI コントローラーの設定)、論理ディスクに関する情報 (シーケンシャル番号、パーティション容量、ボリューム容量、ボリューム文字、パーティション種別、ファイルシステム種別、クラスター数、クラスターのサイズ、クラスターあたりのセクター数、空のクラスターと占有されているクラスターの数、起動可能ボリュームの文字、ディスクの先頭に関するパーティションのオフセットアドレス)、BIOS マザーボードに関する情報 (製造元、発売日、バージョン)、マザーボードに関する情報 (製造元、モデル、タイプ) 物理メモリに関する情報 (共有されている容量およびフリーの容量)、オペレーティングシステムのサービスに関する情報 (名前、説明、ステータス、タグ、プロセスに関する情報 [名前および PID])、コンピューターの電力消費のパラメータ、割り込みコントローラーの設定、Windows システムフォルダーのパス (Windows お

よび System32)、OS に関する情報 (バージョン、ビルド、発売日、名前、種別、インストール日)、ページファイルのサイズ、モニターに関する情報 (番号、製造元、画面許可、解像度の容量、種別) ビデオカードドライバに関する情報 (製造元、発売日、バージョン)。

- EventTrace / EventMetadata イベントが出力される Microsoft の ETW からの情報 : システムイベントのシーケンスに関する情報 (種別、時間、日付、タイムゾーン)、トレース結果を含むファイルに関するメタデータ (名前、構造、トレースパラメータ、種別ごとのトレース操作数の内訳)、OS に関する情報 (名前、種別、バージョン、ビルド、リリース日、開始時刻)。
- Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power イベントが出力される Microsoft の ETW からの情報 : 開始および完了したプロセスに関する情報 (名前、PID、開始パラメータ、コマンドライン、リターンコード、電力管理パラメータ、開始および完了した時刻、アクセストークン種別、SID、セッション識別子、インストールされている記述子の数)、スレッドの優先順位の変更に関する情報 (TID、優先順位、時間)、プロセスのディスク操作に関する情報 (種別、時刻、容量、数)、使用可能なメモリプロセスの構造と容量に対する変更履歴。
- StackWalk / Perfinfo イベントが出力される Microsoft の ETW からの情報 : パフォーマンスカウンターに関する情報 (個々のコードセクションのパフォーマンス、関数呼び出しのシーケンス、PID、TID、ISR および DPC のアドレスと属性)。
- KernelTraceControl-ImageID イベントが出力される Microsoft の ETW からの情報 : 実行可能ファイルおよび動的ライブラリの情報 (名前、画像サイズ、完全パス)、PDB ファイルの情報 (名前、識別子)、実行可能ファイルの VERSIONINFO リソースデータ (名前、説明、作成者、場所、アプリケーションのバージョンと識別子、ファイルのバージョンと識別子)。
- FileIo / DiskIo / Image / Windows Kernel Disk イベントが出力される Microsoft の ETW からの情報 : ファイルおよびディスク操作に関する情報 (種別、容量、開始時刻、完了時刻、継続時間、完了ステータス、PID、TID、ドライバーの関数呼び出しアドレス、I/O 要求パケット (IRP)、Windows ファイルオブジェクト属性)、ファイルおよびディスク操作に関連するファイルに関する情報 (名前、バージョン、サイズ、完全パス、属性、オフセット、イメージのチェックサム、オープンおよびアクセスのオプション)。
- PageFault イベントが出力される Microsoft の ETW からの情報 : メモリページのアクセスエラーに関する情報 (アドレス、時間、容量、PID、TID、Windows ファイルオブジェクトの属性、メモリ割り当てパラメータ)。
- Thread イベントが出力される Microsoft の ETW からの情報 : スレッドの作成または完了に関する情報、開始されたスレッドに関する情報 (PID、TID、スタックのサイズ、CPU リソースの優先順位と割り当て、I/O リソース、スレッド間のメモリページ、スタックアドレス、init 関数のアドレス、スレッド環境ブロック (TEB : Thread Environment Block) のアドレス、Windows サービスタグ)。
- Microsoft Windows Kernel Memory イベントが出力される Microsoft の ETW からの情報 : メモリ管理操作に関する情報 (完了ステータス、時刻、数量、PID)、メモリ割り当て構造 (種別、容量、セッション識別子、PID)。
- パフォーマンスの問題が発生した場合のソフトウェア操作に関する情報 : ソフトウェアのインストール識別子、パフォーマンス低下の種別と値、ソフトウェア内のイベントの順序に関する情報 (時間、タイムゾーン、種別、完了状況、ソフトウェアコンポーネント識別子、ソフトウェアの操作シナリオの識別子、TID、PID、関数呼び出しアドレス)、チェックするネットワーク接続に関する情報 (URL、接続方向、ネットワークパッケージのサイズ)、PDB ファイルに関する情報 (名前、識別子、実行可能ファイルのイメージサイズ)、チェックするファイルに関する情報 (名前、完全パス、チェックサム)、ソフトウェアパフォーマンス監視パラメータ。
- 最新の OS の再起動の失敗に関する情報 : OS をインストールしてから再起動に失敗した回数、システムダンプに関する情報 (エラーのコードおよびパラメータ、OS の動作エラーの原因となったモジュールの名前、バージョンおよびチェックサム (CRC32)、モジュールのオフセットとしてのエラーのアドレス、システムダンプのチェックサム (MD5、SHA2-256、SHA1) )。

- ファイルの署名に使用されるデジタル署名の信頼性を検証するための情報：証明書のフィンガープリント、チェックサムのアゴリズム、証明書の公開鍵およびシリアル番号、証明書の発行者名、証明書の検証結果および証明書のデータベース識別子。
- 本ソフトウェアのセルフディフェンス機能への攻撃を実行したプロセスに関する情報：プロセスファイルの名前およびサイズ、チェックサム（MD5、SHA2-256、SHA1）、プロセスファイルへの完全パスおよびファイルパスのテンプレートコード、作成またはビルド時のタイムスタンプ、実行ファイルのフラグ、プロセスファイルの属性、プロセスファイルの署名に使用された証明書に関する情報、プロセスを実行したアカウントのコード、プロセスにアクセスするために実行した操作の識別子、操作の実行時に使用したリソースの種別（プロセス、ファイル、レジストリオブジェクト、FindWindow 検索関数）、操作の実行時に使用したリソースの名前、操作の成功を示すフラグ、プロセスのファイルのステータスおよび KSN に準拠した署名。
- 本ソフトウェアに関する情報：詳細バージョン、種別、ソフトウェアの言語および動作状況、インストールされた本ソフトウェア機能のバージョンおよびその動作状況、インストールされた本ソフトウェアのアップデートに関する情報、TARGET フィルターの値、権利者のサービスに接続するために使用されたプロトコルのバージョン。
- コンピューターにインストールされたハードウェアに関する情報：種別、名前、機種、ファームウェアのバージョン、搭載または接続されたデバイスのパラメータ、本ソフトウェアをインストールしたコンピューターの一意的識別子。
- オペレーティングシステムのバージョンおよびインストールされているアップデートに関する情報：ビットサイズ、エディションおよび OS 実行方法のパラメータ、OS カーネルファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、OS の起動日時。
- 実行ファイルおよび非実行ファイルの全体および一部。
- コンピューターの RAM の一部。
- OS 起動時に採用されるセクター。
- ネットワーク通信のデータパケット。
- 疑わしい、および悪意のあるオブジェクトを含む Web ページまたはメール。
- WMI リポジトリ上のクラスおよびそれらのインスタンスの記述。
- アプリケーション活動に関するレポート：
  - 送信されるファイルの名前、サイズおよびバージョン、説明およびチェックサム（MD5、SHA2-256、SHA1）、ファイル形式の識別子、ファイルの製造元の名前、ファイルが属するアプリケーションの名前、コンピューター上の完全パス、ファイルのパステンプレートコード、ファイルの作成日時および更新日時
  - 証明書の有効期間の開始日時と終了日時（ファイルにデジタル署名がある場合）、署名適用の日時、証明書の発行者名、証明書の所有者に関する情報、証明書のフィンガープリント、公開鍵およびそれぞれの生成アルゴリズム、証明書のシリアル番号
  - 実行中のプロセスを開始したアカウント名
  - プロセスが実行されている端末名のチェックサム（MD5、SHA2-256、SHA1）
  - プロセスウィンドウのタイトル
  - 定義データベースの識別子、カスペルスキーの分類による検知された脅威の名前

- 使用中のライセンスに関するデータ、識別子、種別および有効期限
- 情報提供時点の端末のローカル時間
- プロセスがアクセスしたファイルの名前とパス
- プロセスがアクセスしたレジストリキーの名前および値
- プロセスがアクセスした URL および IP アドレス
- 実行ファイルのダウンロード元 URL および IP アドレス

## 欧州連合の規則（GDPR）の順守

Kaspersky Endpoint Security は次の方法でデータをカスペルスキーに送信することがあります：

- Kaspersky Security Network を使用する。
- アクティベーションコードで本製品をアクティベートする。
- 製品モジュールと定義データベースをアップデートする。
- 製品インターフェイス内のリンクを使用する。
- ダンプの書き込み。

データの分類およびどこからデータを受け取ったかにかかわらず、カスペルスキーは高い水準のデータセキュリティ対策を遵守し、お客様のデータを保護するためにさまざまな法的、組織的および技術的な手法を取り入れてデータのセキュリティおよび機密性を保証し、適用法によりお客様の権利を確保します。プライバシーポリシーの本文は[製品の配信キット](#)に含まれており、[カスペルスキーの Web サイト](#)でも参照いただけます。

Kaspersky Endpoint Security を使用する前に、[使用許諾契約書](#)および[Kaspersky Security Network に関する声明](#)の転送されるデータの説明をよく読み、ご確認ください。説明されている方法で Kaspersky Endpoint Security から転送される特定のデータが、お客様の地域の法律または基準により個人データと分類される場合は、これらのデータは合法的に処理され、このようなデータの転送および收拾についてはお客様の同意のもと行われるものであることをお客様自身が保証する必要があります。

使用許諾契約書および Kaspersky Security Network に関する声明に同意した後の製品使用状況に関する情報の取得、処理、保存、破棄の詳細な方法については、使用許諾契約書を読み、[カスペルスキーの Web サイト](#)をご参照ください。ファイル license.txt および ksn\_<言語 ID>.txt には、使用許諾契約書および Kaspersky Security Network に関する声明の本文が記載されています。これらは本製品の[配信キット](#)に含まれています。

カスペルスキーにデータを送信したくない場合は、データの提供を無効にすることができます。

## Kaspersky Security Network の使用

Kaspersky Security Network を使用することで、お客様は自動的に [Kaspersky Security Network に関する声明](#)で説明されるデータを提供することに合意したものとします。カスペルスキーへのこのようなデータの提供に同意しない場合は、プライベート KSN を使用するか、[KSN の使用を無効](#)にしてください。プライベート KSN について詳しくは、管理者向けに提供されている *Kaspersky Private Security Network* のガイドを参照してください。

## アクティベーションコードで本製品をアクティベートする

アクティベーションコードを使用することで、お客様は[使用許諾契約書](#)に記載されているデータを自動的に提供することに同意するものとします。カスペルスキーへのデータの提供に同意しない場合は、[ライセンス情報ファイルを使用して Kaspersky Endpoint Security をアクティベート](#)してください。

## 製品モジュールと定義データベースをアップデートする

カスペルスキーのサーバーを使用することで、お客様は[使用許諾契約書](#)に記載されているデータを自動的に提供することに同意するものとします。カスペルスキーは、この情報を Kaspersky Endpoint Security が合法的に使用されていることを検証するために使用します。このような情報をカスペルスキーに提供したくない場合、[Kaspersky Security Centerを使用してデータベースをアップデートするか、カスペルスキーのアップデートユーティリティ](#)を使用してください。

## 製品インターフェイス内のリンクを使用する

製品インターフェイスのリンクを使用することで、お客様は[使用許諾契約書](#)に記載されているデータを自動的に提供することに同意するものとします。特定のリンクがどのようなデータを提供するかについては、製品インターフェイスのどこにあるリンクか、またどのような問題を解決しようとしているかによって異なります。カスペルスキーへのデータの送信に同意しない場合は、[簡易的な製品インターフェイス](#)を使用するか、[製品インターフェイスを非表示](#)にしてください。

## ダンプ書き込み

[ダンプへの書き込みを有効](#)にすると、Kaspersky Endpoint Security はファイルが作成された時点でのアプリケーションプロセスからのすべてのメモリーデータを含むダンプファイルを作成します。

## 使用開始時に行う設定

Kaspersky Endpoint Security のインストール後、次のインターフェイスを使用して本製品を管理できます。

- [ローカルアプリケーションインターフェイス](#)
- Kaspersky Security Center の管理コンソール
- Kaspersky Security Center Web コンソール
- Kaspersky Security Center Cloud コンソール

### Kaspersky Security Center の管理コンソール

Kaspersky Security Center では、Kaspersky Endpoint Security のインストールとアンインストール、製品の設定、使用できる製品コンポーネントセットの変更、ライセンスの追加、アップデートおよびスキャンタスクの開始と停止を、リモートで実行できます。

Kaspersky Security Center から Kaspersky Endpoint Security 管理プラグインを使用して、製品を管理できます。

Kaspersky Security Center を使用した本製品の管理について詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

### Kaspersky Security Center Web コンソール および Kaspersky Security Center Cloud コンソール

Kaspersky Security Center Web コンソール（以下、「Web コンソール」とも表記）は、組織ネットワークのセキュリティシステムの管理と維持のための主要タスクを一元的に実行できる Web アプリケーションです。Web コンソールは、Kaspersky Security Center のユーザーインターフェイスコンポーネントとして提供されています。Kaspersky Security Center Web コンソールについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソール（以下、「Cloud コンソール」）は、組織ネットワークの管理と保護のためのクラウドベースのソリューションです。Kaspersky Security Center Cloud コンソールについて詳しくは、[Kaspersky Security Center Cloud コンソールのオンラインヘルプ](#) を参照してください。

Web コンソールと Cloud コンソールでは次の操作を実行できます：

- 組織のセキュリティシステムのステータスの監視
- ネットワーク内のデバイスへのカスペルスキー製品のインストール
- インストール済み製品の管理
- セキュリティシステムのステータスに関するレポートの表示

Web コンソール、Cloud コンソール、Kaspersky Security Center 管理コンソールを使用した Kaspersky Endpoint Security の管理では、それぞれ異なる管理機能が提供されます。コンソールが異なると、[管理可能な Kaspersky Endpoint Security のコンポーネントとタスク](#)も異なります。



# Kaspersky Endpoint Security for Windows の管理プラグインについて

Kaspersky Endpoint Security for Windows の管理プラグインは Kaspersky Endpoint Security と Kaspersky Security Center の連携を有効にします。管理プラグインでは、[ポリシー](#)、[タスク](#)、[個別のローカル環境用の製品設定](#)を使用して、Kaspersky Security を管理できます。Kaspersky Security Center Web コンソールとの連携は Web プラグインによって提供されます。

管理プラグインのバージョンが、クライアントコンピューターにインストールされた Kaspersky Endpoint Security のバージョンと異なることがあります。インストールされているバージョンの管理プラグインの機能が、インストールされているバージョンの Kaspersky Endpoint Security の機能よりも少ない場合、足りない機能の設定は、管理プラグインでは管理されません。その設定は、Kaspersky Endpoint Security のローカルインターフェイスでユーザーが変更できます。

Web プラグインは、Kaspersky Security Center Web コンソールに既定でインストールはされません。Kaspersky Security Center 管理コンソールの管理プラグインは管理者用のワークステーションにインストールされますが、Web プラグインは Kaspersky Security Center Web コンソールがインストールされているコンピューターにインストールする必要があります。ブラウザから Web コンソールにアクセスできる管理者は全員、Web プラグインの機能を利用できます。Web コンソールのインターフェイスで、インストールされている Web プラグインを確認できます：[[コンソールの設定](#)] → [[プラグイン](#)]。Web プラグインのバージョンと Web コンソールとの互換性について詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。

## Web プラグインのインストール

Web プラグインをインストールするには、次の操作を実行します：

- Kaspersky Security Center Web コンソールのクイックスタートウィザードを使用して Web プラグインをインストールする。

初めて Web コンソールから管理サーバーに接続すると、Web コンソールで自動的にクイックスタートウィザードが表示されます。Web コンソールのインターフェイスからクイックスタートウィザードを実行することもできます（ [[検出と製品の導入](#)] → [[導入と割り当て](#)] → [[クイックスタートウィザード](#)]）。クイックスタートウィザードでは、インストールされている Web プラグインが最新バージョンか確認したり、必要なアップデートをダウンロードできます。Kaspersky Security Center Web コンソールのクイックスタートウィザードについて詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。

- Web コンソールで利用可能な配布パッケージのリストを使用して Web プラグインをインストールする。

Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージを選択して Web プラグインをインストールします： [[コンソールの設定](#)] → [[プラグイン](#)]。利用可能な配布パッケージのリストは、Kaspersky アプリケーションの新しいバージョンがリリースされた後に自動的に更新されます。

- その他のアップデート元から Web コンソールの配布パッケージをダウンロードする。

Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージの ZIP アーカイブファイルを追加して Web プラグインをインストールします： [[コンソールの設定](#)] → [[プラグイン](#)]。Web プラグインの配布パッケージは、たとえば Kaspersky Web サイトからダウンロードできます。

## 管理プラグインのアップデート

Kaspersky Endpoint Security for Windows 管理プラグインをアップデートするには、最新版のプラグイン（[配信キット](#)に含まれます）をダウンロードし、プラグインインストールウィザードを実行します。



新しいバージョンの Web プラグインが利用できるようになると、使用中の Web プラグインでアップデートが利用できるようになったことを示す通知が Web コンソール上に表示されます。この Web コンソール上の通知から、Web プラグインのバージョンのアップデート操作を行う画面に移動することができます。Web コンソールのインターフェイスで、新しい Web プラグインのアップデートがないかを手動で確認することもできます（**[コンソールの設定]** → **[プラグイン]**）。アップデート中に、以前のバージョンの Web プラグインは自動的にアンインストールされます。

Web プラグインをアップデートすると、既存の項目（ポリシーやタスクなど）が保存されます。Kaspersky Endpoint Security の新機能に関わる設定項目が既存の項目に追加されるとともに、これらの設定項目には既定値が適用されます。

Web プラグインをアップデートするには、次の操作を実行します：

- Web プラグインのリストを使用して Web プラグインをアップデート（オンラインモードの場合）  
Web プラグインをアップデートするには、Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージを選択します（**[コンソールの設定]** → **[プラグイン]**）。Web コンソールは、Kaspersky サーバーで利用可能なアップデートを確認し、関連するアップデートをダウンロードします。
- ファイルから Web プラグインをアップデート  
Web プラグインをアップデートするには、Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージの ZIP アーカイブファイルを選択する必要があります：**[コンソールの設定]** → **[プラグイン]**。Web プラグインの配布パッケージは、たとえば Kaspersky Web サイトからダウンロードできます。Kaspersky Endpoint Security の Web プラグインは、より新しいバージョンの Web プラグインにのみアップデートできます。Web プラグインをバージョンの古い Web プラグインにアップデートすることはできません。

（ポリシーやタスクなどの項目が開かれると、Web プラグインが互換性情報を確認します。Web プラグインのバージョンが、互換性情報で示されているバージョン以上である場合、その項目の設定を変更できます。そうでない場合、Web プラグインを使用して項目の設定を変更することはできません。Web プラグインをアップデートしてください。

## 異なるバージョンの管理プラグインを使用する場合の留意点

Kaspersky Endpoint Security の管理プラグインとの互換性に関する情報で、指定されたバージョン以上のバージョンの管理プラグインがある場合にのみ、Kaspersky Security Center 経由で Kaspersky Endpoint Security を管理できます。[配信キット](#)に含まれている installer.ini ファイルで、管理プラグインの最低限必要なバージョンを表示できます。

（ポリシーやタスクなどの）項目が開かれると、管理プラグインが互換性情報を確認します。管理プラグインのバージョンが、互換性情報で示されているバージョン以上である場合、その項目の設定を変更できます。そうでない場合、管理プラグインを使用して項目の設定を変更することはできません。管理プラグインをアップデートしてください。

## Kaspersky Endpoint Security 10 for Windows の管理プラグインのアップデート

管理コンソールに Kaspersky Endpoint Security 10 for Windows の管理プラグインがインストールされている場合、Kaspersky Endpoint Security 11 for Windows の管理プラグインのインストール時には次の事項に留意してください：


- Kaspersky Endpoint Security 10 for Windows の管理プラグインはアンインストールされず、利用可能な状態で管理コンソールに残ります。そのため、バージョン 10 と 11 の製品で作業する場合は 2 つの管理プラグインにアクセスすることになります。
- Kaspersky Endpoint Security 11 for Windows の管理プラグインでは、ユーザーのコンピューターにインストールされている Kaspersky Endpoint Security 10 for Windows の管理はサポートされません。
- また、Kaspersky Endpoint Security 11 for Windows の管理プラグインでは、Kaspersky Endpoint Security 10 for Windows の管理プラグインを使用して作成された項目（例：ポリシー、タスク）はサポートされません。

ポリシーとタスクのバージョン 10 からバージョン 11 への変換には、ポリシーとタスクのバッチ変換ウィザードを使用できます。ポリシーとタスクの変換について詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。



## Kaspersky Endpoint Security 11 for Windows の管理プラグインのアップデート

管理コンソールに Kaspersky Endpoint Security 11 for Windows の管理プラグインがインストールされている場合、より新しいバージョンの Kaspersky Endpoint Security 11 for Windows の管理プラグインのインストール時には次の事項に留意してください：

- 古いバージョンの Kaspersky Endpoint Security 11 for Windows の管理プラグインはアンインストールされません。
- より新しいバージョンの Kaspersky Endpoint Security 11 for Windows の管理プラグインで、ユーザーのコンピューターにインストールされている古いバージョンの Kaspersky Endpoint Security 11 for Windows の管理がサポートされます。
- 古いバージョンの管理プラグインで作成されたポリシーやタスクなどの項目の設定を、新しいバージョンの管理プラグインを使用して変更できます。
- アップデートが完了してからポリシー、ポリシーのプロファイル、タスクが最初に保存されるときに、新しいバージョンの管理プラグインは、アップデートで新たに追加された設定項目に対しては既定値を割り当てます。

そのため、管理プラグインのアップデートが完了したら、アップデートで新たに追加された設定項目について、ポリシーとポリシープロファイルを確認し、必要に応じて適切な値を保存しなおすことを推奨します。この操作を実行しなかった場合、ユーザーのコンピューターにインストールされている Kaspersky Endpoint Security では、アップデートで新たに追加された設定項目について既定値が適用されるとともにこれらの設定がローカルで編集可能な状態になります（設定のロック状態が「」になります）。設定の確認は、階層の最上位のポリシーとポリシープロファイルから開始することを推奨します。また、使用するユーザーアカウントとしては、Kaspersky Security Center のすべての機能領域へのアクセス権が付与されているユーザーアカウントの使用を推奨します。

本製品の.new機能について詳しくは、リリースノートまたは[ヘルプ内のページ](#)を参照してください。

- 新しいバージョンの管理プラグインで既存の設定項目に新しく設定できるパラメータが追加された場合は、この設定項目でこれまでに指定されていた設定のロックの状態（ / ）は変更されません。
- 管理プラグインをバージョン 11.2.0 にアップグレードする場合は、自動的に変換するためポリシーを開く必要があります。その際、Kaspersky Endpoint Security は KSN への参加について確認するよう要求します。

組織内のコンピューター上ですでにバージョン 11.20 にアップグレードしている場合は、KSN への参加に関する声明に同意するまで、KSN への参加は無効になります。

## 外部サービスと相互作用する暗号化プロトコルを使用する場合の留意点

Kaspersky Endpoint Security および Kaspersky Security Center は暗号化された TLS 通信チャネル (Transport Layer Security) を使用してカスペルスキーの外部のサービスと動作します。Kaspersky Endpoint Security は次の機能で外部サービスを使用します：

- 定義データベースとソフトウェアモジュールのアップデート
- アクティベーションコードで本製品をアクティベートする (アクティベーション 2.0)
- Kaspersky Security Network を使用する

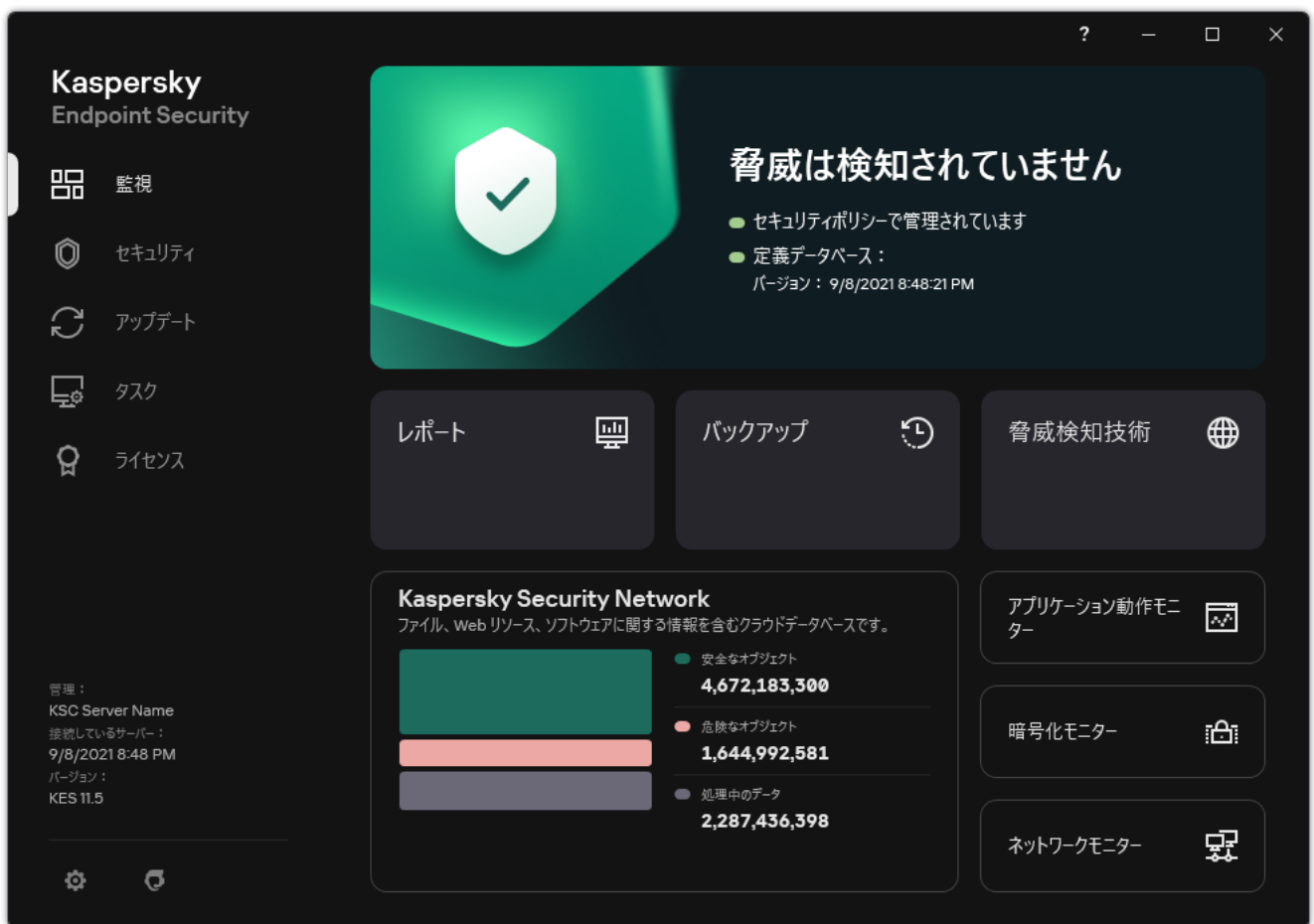
TLS の使用は次の機能を提供することで本製品を保護します：

- 暗号化。メッセージの内容は機密扱いで、サードパーティのユーザーに開示されることはありません。
- 整合性。メッセージの受信者は、送信者がメッセージを送ってから内容が変更されていないことに確信を持てます。
- 認証。受信者は通信が信頼済みのカスペルスキーのサーバーとの間にのみ確立されていることに確信を持てます。

Kaspersky Endpoint Security はサーバー認証に公開鍵証明書を使用します。証明書で作業するには公開鍵基盤 (PKI) が必要です。認証局は PKI の一部です。カスペルスキーのサービスは非常に専門的で公開されていないため、カスペルスキーは独自の認証局を使用します。thawte、verisign、globaltrust またはその他のルート証明書が失効した場合、カスペルスキー PKI は問題なく動作します。

MITM (HTTP プロトコルのパースをサポートするソフトウェアおよびハードウェアツール) を持つ環境は、Kaspersky Endpoint Security により安全でないと認識されます。カスペルスキーサービスと動作する際にエラーが発生する可能性があります。例えば、自己署名された証明書の使用に関してエラーが発生する可能性があります。これらのエラーは、お客さまの環境の HTTPS 検出ツールが Kaspersky PKI を認識しないために発生する可能性があります。これらの問題を修正するには、[外部サービスと相互作用するための除外リスト](#)を設定する必要があります。





## 製品のインターフェイス



メインウィンドウ

## 監視

- レポート**：本製品の動作中、個別の機能およびタスク中に発生したイベントを表示します。
- バックアップ**：本製品が削除した感染ファイルのコピーのリストを表示します。
- 脅威検知技術**：脅威の検知技術およびこの技術により検知された脅威の数に関する情報を表示します。
- Kaspersky Security Network**：Kaspersky Endpoint Security と Kaspersky Security Network との接続ステータスとグローバル KSN 統計です。KSN (*Kaspersky Security Network*) はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。
- アプリケーション動作モニター**：インストールされたアプリケーションの動作に関する情報を表示します。システムウォッチャーは、アプリケーションと関連するファイル、レジストリ、オペレーティングシステムのイベントを追跡します。
- ネットワークモニター**：リアルタイムで コンピューターのネットワークの動作に関する情報を表示 します。
- 暗号化モニター**：リアルタイムでディスクの暗号化または復号化プロセスを確認します。暗号化モニターは、Kaspersky Disk Encryption または BitLocker Drive Encryption がインストールされている場合のみ利用可能です。

<b>セキュリティ</b>	インストールされた機能の動作ステータスです。機能の設定やレポートを表示することもできます。
<b>アップデート</b>	Kaspersky Endpoint Security のアップデートタスクを管理します。 <a href="#">定義データベースと製品モジュールのアップデート</a> および <a href="#">最新のアップデートのロールバック</a> ができます。管理者は <a href="#">セクションをユーザーに対して非表示</a> にしたり、 <a href="#">タスク管理を制限</a> したりできます。
<b>タスク</b>	Kaspersky Endpoint Security のスキャンタスクを管理します。 <a href="#">ウイルススキャン</a> および <a href="#">アプリケーション整合性チェック</a> を実行できます。管理者は <a href="#">ユーザーに対してタスクを非表示</a> にしたり、 <a href="#">タスクの管理を制限</a> したりできます。
<b>ライセンス</b>	製品のライセンス <a href="#">ライセンスの購入</a> 、 <a href="#">本製品のアクティベート</a> 、または <a href="#">定額制サービスの更新</a> ができます。 <a href="#">現在のライセンスに関する情報を表示</a> することもできます。
	本製品の設定：管理者は <a href="#">Kaspersky Security Center の設定の変更を禁止</a> することができます。
	本製品に関する情報：Kaspersky Endpoint Security の現在のバージョン、定義データベースの公開日、ライセンスおよびその他の情報です。製品の購入、インストール、製品の使用方法などについて役立つ情報、推奨事項、よくある質問に対する回答を提供するカスペルスキーの情報源を表示することも可能です。
 / 	利用可能なアップデートや暗号化されたファイルやデバイスへのアクセスの要求に関する情報を含むメッセージです。





## タスクバーの通知領域の製品アイコン

Kaspersky Endpoint Security をインストールするとすぐに、Microsoft Windows タスクバーの通知領域に製品アイコンが表示されます。


このアイコンは、次の目的で表示されます：

- 製品の動作を表示する
- 製品のコンテキストメニューおよびメインウィンドウへのショートカットを提供する

製品の動作に関する情報をユーザーが確認できるように、製品ステータスに応じて次のアイコンが表示されます：

-  アイコンは、製品の非常に重要な保護機能が有効であることを示しています。本製品のアップデート後に再起動が必要な場合など、ユーザーが操作を実行する必要がある場合は警告アイコン () が表示されます。
-  アイコンは、製品の非常に重要な保護機能が無効になっているか、不具合があることを示しています。例えば、ライセンスの有効期間が終了していたり、アプリケーションエラーの結果として保護機能の不具合となることがあります。コンピューターの保護の問題についての説明とともに警告アイコン () が表示されます。

製品アイコンのコンテキストメニューには、次の項目があります：

- **Kaspersky Endpoint Security for Windows**：メインウィンドウを開きます。このウィンドウで、コンポーネントとタスクの動作を調整したり、処理されたファイルと検知された脅威の統計を表示したりすることができます。
- **保護機能の一時停止 / 保護機能の再開**ポリシーでロック () が設定されていないすべての保護機能および管理コンポーネントの動作を一時的に停止します。この操作を実行する前に、Kaspersky Security Center の



ポリシーを無効にしておくことを推奨します。

保護機能と管理コンポーネントの動作を停止する前に、[Kaspersky Endpoint Security へのアクセス用のパスワード](#)（アカウントパスワードまたは一時パスワード）の入力が製品で要求されます。続いて、一時停止する期間を、「指定した時間だけ一時停止する」「再起動まで一時停止する」「ユーザーが要求したら再開する」のいずれかの方式で指定できます。

コンテキストメニューのこの項目は、[パスワードによる保護が有効](#)な場合に選択できます。保護機能と管理コンポーネントの動作を再開するには、製品アイコンのコンテキストメニューで「**保護機能の再開**」をクリックします。

保護機能と管理コンポーネントの動作を一時停止しても、アップデートタスクとスキャンタスクには影響ありません。また、本製品による Kaspersky Security Network の使用も継続されます。


- **ポリシーを無効にする / ポリシーを有効にする**：Kaspersky Security Center で設定したポリシーをコンピューター上で無効にします。ポリシーでロックされている設定（ 状態）も含めて、Kaspersky Endpoint Security のすべての設定を編集できるようになります。ポリシーが無効になっている場合、アプリケーションから [Kaspersky Endpoint Security へのアクセス用のパスワード](#)（アカウントパスワードまたは一時パスワード）の入力が要求されます。コンテキストメニューのこの項目は、[パスワードによる保護が有効](#)な場合に選択できます。ポリシーを有効にするには、製品アイコンのコンテキストメニューで「**ポリシーを有効にする**」を選択します。
- **設定**：本製品の設定ウィンドウが表示されます。
- **サポート**：カスペルスキーのテクニカルサポートへの問い合わせに必要な情報を確認できるウィンドウが表示されます。
- **製品情報**：この項目を指定すると、製品の詳細を確認できる情報ウィンドウが表示されます。
- **終了**：この項目を指定すると、Kaspersky Endpoint Security が終了します。コンテキストメニューでこの項目をクリックすると、コンピューターの RAM が解放されます。



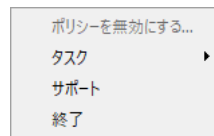
製品アイコンのコンテキストメニュー

## 簡略化したアプリケーションインターフェイス

Kaspersky Endpoint Security がインストールされたクライアントコンピューターに対し、[簡略化したアプリケーションインターフェイスを表示](#)するよう設定された Kaspersky Security Center ポリシーが適用されている場合、そのクライアントコンピューターでは製品のメインウィンドウが使用できません。Kaspersky Endpoint Security のアイコン（以下の図を参照）を右クリックすると、次の項目を含むコンテキストメニューが表示されます：

- **ポリシーを無効にする / ポリシーを有効にする**：Kaspersky Security Center で設定したポリシーをコンピューター上で無効にします。ポリシーでロックされている設定（ 状態）も含めて、Kaspersky Endpoint Security のすべての設定を編集できるようになります。ポリシーが無効になっている場合、アプリケーションから [Kaspersky Endpoint Security へのアクセス用のパスワード](#)（アカウントパスワードまたは一時パスワード）の入力が要求されます。コンテキストメニューのこの項目は、[パスワードによる保護が有効](#)な場合に選択できます。ポリシーを有効にするには、製品アイコンのコンテキストメニューで「**ポリシーを有効にする**」を選択します。

- **タスク** : ドロップダウンリストの内容は次のとおりです :
  - **整合性チェック** :
  - **以前の定義データベースのバージョンにロールバック** :
  - **完全スキャン** :
  - **オブジェクトスキャン** :
  - **簡易スキャン** :
  - **アップデート** :
- **サポート** : カスペルスキーのテクニカルサポートへの問い合わせに必要な情報を確認できるウィンドウが表示されます。
- **終了** : この項目を指定すると、Kaspersky Endpoint Security が終了します。コンテキストメニューでこの項目をクリックすると、コンピューターの RAM が解放されます。



簡略化したインターフェイスが表示されている場合の、製品アイコンのコンテキストメニュー

## 製品インターフェイスの表示の設定

ユーザー向けに製品インターフェイスの表示を設定することができます。ユーザーは次の方法で製品を操作することができます :

- **簡略化して表示** : クライアントコンピューター上で、本製品のメインウィンドウにアクセスできなくなり、[Windows の通知領域のアイコン](#)だけが利用できます。アイコンのコンテキストメニューから [Kaspersky Endpoint Security の一定範囲に限定された操作を実行](#)できます。製品アイコンの上の通知も表示されません。
- **通常が表示** : クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウと [Windows の通知領域のアイコン](#)が利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。
- **表示しない** : クライアントコンピューター上で、Kaspersky Endpoint Security の動作に関するメニューなどが表示されません。 [Windows の通知領域のアイコン](#)と通知も表示されません。

### [管理コンソール \(MMC\) で製品インターフェイスの表示モードを設定する方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔全般設定〕** → **〔インターフェイス〕** の順に選択します。
6. **〔ユーザーインターフェイス〕** セクションで、次のいずれかを実行します：
  - 以下のインターフェイス要素をクライアントコンピューターに表示するには、 **〔アプリケーションインターフェイスを表示する〕** をオンにします。
    - **〔スタート〕** メニュー内の製品名を含むフォルダー
    - Microsoft Windows タスクバーの通知領域にある [Kaspersky Endpoint Security のアイコン](#)
    - ポップアップ通知

このチェックボックスをオンにすると、ユーザーはアプリケーションインターフェイスで製品の設定を表示でき、権限によって設定を変更できます。

  - すべての Kaspersky Endpoint Security のインターフェイスをクライアントコンピューターで非表示にするには、 **〔アプリケーションインターフェイスを表示する〕** をオフにします。
7. Kaspersky Endpoint Security がインストールされたクライアントコンピューターで [簡略化したアプリケーションインターフェイス](#) を表示する場合は、 **〔ユーザーインターフェイス〕** セクションで **〔簡略化したアプリケーションインターフェイス〕** をオンにします。

## Web コンソールと Cloud コンソールで製品インターフェイスの表示モードを設定する方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ポータブルモードのサポートを有効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[全般設定]** → **[インターフェイス]** を選択します。
5. **[ユーザーインターフェイス]** セクションで、表示される製品のインターフェイスを設定します。
  - **簡略化して表示** : クライアントコンピューター上で、本製品のメインウィンドウにアクセスできなくなり、[Windows の通知領域のアイコン](#)だけが利用できます。アイコンのコンテキストメニューから [Kaspersky Endpoint Security の一定範囲に限定された操作を実行](#) できます。製品アイコンの上の通知も表示されます。
  - **通常の表示** : クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウと [Windows の通知領域のアイコン](#) が利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。
  - **表示しない** : クライアントコンピューター上で、Kaspersky Endpoint Security の動作に関するメニューなどが表示されません。[Windows の通知領域のアイコン](#) と通知も表示されません。
6. 変更内容を保存します。

## 使用開始時に行う設定

クライアントコンピューターへの製品の導入が完了したら、Kaspersky Security Center Web コンソールから Kaspersky Endpoint Security を管理するために次の操作を実行する必要があります :

- ポリシーを作成して設定する。

ポリシーを使用して、同じ Kaspersky Endpoint Security 設定を管理グループ内のすべてのクライアントコンピューターに適用できます。Kaspersky Security Center のクイックスタートウィザードでは、Kaspersky Endpoint Security のポリシーが自動的に作成されます。

- **[アップデート]** タスクと **[スキャン]** タスクを作成する。

**[アップデート]** タスクは、コンピューターのセキュリティを最新の状態に保つために必要です。このタスクを実行すると、Kaspersky Endpoint Security の [定義データベースとソフトウェアモジュール](#) がアップデートされます。アップデートタスクは、Kaspersky Security Center のクイックスタートウィザードで自動的に作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows の Web プラグインをインストールすることを選択します。

**[スキャン]** タスクは、ウイルスなどのマルウェアをすみやかに検知するために必要です。スキャンタスクは、手動で作成する必要があります。

### [管理コンソール \(MMC\) でウイルススキャンタスクを作成する方法](#)

1. 管理コンソールで、[管理サーバー] → [タスク] のフォルダーに移動します。  
タスクのリストが表示されます。

2. [新規タスク] をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

[Kaspersky Endpoint Security for Windows (11.7.0)] → [ウイルススキャン] を選択します。

## ステップ 2：スキャン範囲

スキャンタスクの実行時に、Kaspersky Endpoint Security によってスキャンされるオブジェクトのリストを作成します。

## ステップ 3：Kaspersky Endpoint Security の処理

脅威の検知時の処理を選択します：

- **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。
- **駆除する。駆除できない場合は通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除ができない場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
- **通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
- **すぐに特別な駆除を実行する**：チェックボックスがオンの場合、Kaspersky Endpoint Security は特別な駆除を使用してスキャン中にアクティブな脅威を処理します。

この特別な駆除技術の目的は、RAM 内部でそのプロセスを既に開始している悪意のあるプログラムをオペレーティングシステムから除去して Kaspersky Endpoint Security が他の方法でそれらのアプリケーションを除去しないようにすることです。その結果、脅威が駆除されます。特別な駆除を実行している間は、新しいプロセスの起動やオペレーティングシステムレジストリの修正を行わないように指示されます。特別な駆除には大量のオペレーティングシステムリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。特別な駆除の完了後、Kaspersky Endpoint Security はユーザーに確認することなくコンピューターを再起動します。

[コンピューターを使用していないときにのみ実行する] を使用してタスク実行モードを設定します。このチェックボックスでは、コンピューターリソースが限られているときにウイルススキャンタスクを中断する機能を有効にするか無効にするかを切り替えます。スクリーンセーバーがオフの状態でかつコンピューターのロックが解除されている場合、ウイルススキャンタスクは一時停止します。

## ステップ 4：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 5：タスクを実行するアカウントの選択

ウイルススキャンタスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。スキャン範囲にアクセスが制限されたネットワークドライブまたはその他のオブジェクトが含まれる場合は、適切なアクセス権を持つユーザーアカウントを選択します。

## ステップ 6：タスク開始スケジュールの設定

タスクを開始するスケジュールを設定します。例えば、手動、または定義データベースがリポジトリにダウンロードされた後に開始するなどです。

## ステップ 7：タスク名の定義

タスクの名前を入力します。たとえば、「毎日の完全スキャン」など。

## ステップ 8：タスク作成の完了

ウィザードを終了します。必要に応じて、**「ウィザードの完了後にタスクを実行」** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。設定が完了すると、指定したスケジュールに従ってユーザーのコンピューターでスキャンタスクが実行されるようになります。

### [Web コンソールでウイルススキャンタスクを作成する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
  2. **[追加]** をクリックします。  
タスクウィザードが起動します。
  3. タスクの設定を指定します：
    - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
    - b. **[タスク種別]** で、**[ウイルススキャン]** を選択します。
    - c. **[タスク名]** に「週次のスキャン」などの短く分かりやすい名前を付けます。
    - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。
  4. タスク範囲の指定方法に応じて、対象デバイスを選択します。**[次へ]** をクリックします。
  5. **[終了]** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
  6. タスクのスケジュールを設定するには、タスクのプロパティを開きます。  
週に1回以上の頻度でタスクが実行されるようにスケジュール設定することを推奨します。
  7. タスクの横にあるチェックボックスをオンにします。
  8. **[開始]** をクリックします。  
タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。
- 設定が完了すると、指定したスケジュールに従ってユーザーのコンピューターでスキャンタスクが実行されるようになります。

## ポリシーの管理

ポリシーとは、1つの管理グループを対象に製品設定をまとめて指定したものです。1つの製品に対して、異なる設定値をもつ複数のポリシーを設定できます。管理グループが異なる場合、1つの製品を異なる設定で動作させることができます。各管理グループに、独自のポリシーを設定できます。

ポリシー設定は同期中にネットワークエージェントを経由してクライアントコンピューターに送信されます。既定では、ポリシー設定が変更されると、管理サーバーがただちに同期を実行します。クライアントコンピューターのUDPポート15000が同期に使用されます。管理サーバーは、既定では15分ごとに同期を実行します。ポリシー設定後の同期が失敗した場合、次の同期は設定されたスケジュールに従って実行されます。

### アクティブなポリシーと非アクティブポリシー

ポリシーは管理対象コンピューターのグループを対象に作成され、アクティブまたは非アクティブにできます。アクティブなポリシーの設定は、同期中にクライアントコンピューターに保存されます。1台のコンピューターに複数のポリシーを同時に適用することはできません。各管理グループでアクティブにできるポリシーは1つの製品につき1つのみです。

非アクティブポリシーは個数の制限なく作成できます。非アクティブポリシーは、ネットワーク内のコンピューターの製品設定に影響を及ぼしません。非アクティブポリシーは、ウイルス攻撃などの非常時に設定を切り替える準備を行う目的で使用されます。たとえば、フラッシュドライブを使用した攻撃が発生した場合、フラッシュドライブへのアクセスをブロックするポリシーをアクティブにできます。この場合、それまでアクティブだったポリシーは自動的に非アクティブになります。

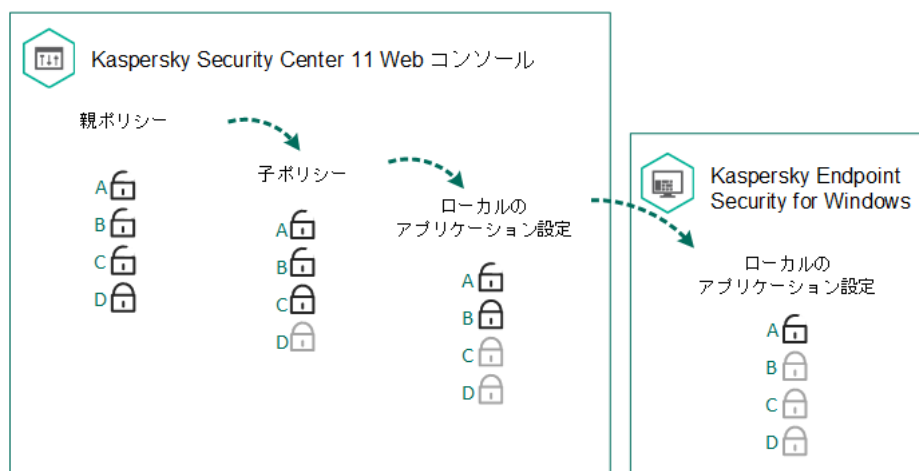
## モバイルユーザーポリシー

モバイルユーザーポリシーは、コンピューターが組織ネットワーク外に出た場合に有効になります。

## 設定の継承

管理者グループのようなポリシーは、階層構造になっています。既定では、子ポリシーは親ポリシーの設定を継承します。子ポリシーは、階層レベルで下位のポリシーで、下位の管理グループまたはセカンダリ管理サーバーに割り当てられているポリシーです。親ポリシーからの設定の継承を無効にすることができます。

各ポリシー設定には、子ポリシーまたは[ローカルアプリケーション設定](#)で設定を変更できるかどうかを示す属性 $\triangle$ があります。 $\triangle$ 属性は、子ポリシーで親ポリシーの設定の継承がオンになっている場合にのみ適用されます。モバイルユーザーポリシーは、管理グループの階層でその他のポリシーに影響を及ぼしません。



設定の継承

ポリシー設定にアクセスする権限（読み取り、書き込み、実行）は、Kaspersky Security Center 管理サーバーへのアクセス権を持つ各ユーザーに対して指定され、さらに Kaspersky Endpoint Security の各機能の範囲に対して個別に指定されます。ポリシー設定にアクセスする権限を指定するには、Kaspersky Security Center 管理サーバーのプロパティウィンドウの【セキュリティ】セクションに移動します。

## ポリシーの作成

### [管理コンソール（MMC）でポリシーを作成する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを選択します。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. **〔新規ポリシー〕** をクリックします。  
ポリシーウィザードが起動します。
5. ポリシーウィザードの指示に従います。

### [Web コンソールと Cloud コンソールでポリシーを作成する方法](#)



1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. [追加] をクリックします。  
ポリシーウィザードが起動します。
3. Kaspersky Endpoint Security for Windows を選択し、[次へ] をクリックします。
4. Kaspersky Security Network (KSN) に関する声明の内容を確認し、同意するかどうかを選択して [次へ] をクリックします。
5. [全般] タブで次の操作を実行できます：
  - ポリシー名の変更
  - ポリシーのステータスの選択：
    - **アクティブ**：次の同期の実行後、このポリシーがクライアントコンピューター上でアクティブなポリシーとして使用されます。
    - **非アクティブ**：バックアップ用のポリシーです。必要に応じて、非アクティブなポリシーのステータスをアクティブに変更できます。
    - **モバイルユーザー**：このポリシーは、コンピューターが組織ネットワーク外に出た場合に有効になります。
  - 設定の継承設定：
    - **親ポリシーから設定を継承する**：このスイッチをオンにすると、上位のポリシーからポリシーの設定値が継承されます。親ポリシーで  が指定されている設定は子ポリシーで変更できません。
    - **設定を子ポリシーへ強制的に継承させる**：このオプションがオンの場合、ポリシー設定の値が子ポリシーに反映されます。子ポリシーのプロパティで、[親ポリシーから設定を継承する] は自動的にオンになり、オフにすることはできません。設定のステータスが  以外の設定は親ポリシーから子ポリシーに設定が継承されます。親ポリシーで  ステータスが設定された子ポリシーは編集できません。
6. [アプリケーション設定] タブで、[Kaspersky Endpoint Security のポリシー設定](#)を編集できます。
7. 変更内容を保存します。

次の同期時に、クライアントコンピューターで Kaspersky Endpoint Security の設定が適用されます。メイン画面の [サポート] ボタン (ポリシー名など) をクリックすると、Kaspersky Endpoint Security インターフェイスでコンピューターに適用されているポリシーに関する情報を表示できます。そのためには、ネットワークエージェントのポリシーの設定で、拡張ポリシーデータの受信を有効にする必要があります。ネットワークエージェントのポリシーについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

## セキュリティレベルインジケータ

セキュリティレベルインジケータは、ポリシーのプロパティウィンドウの上部に表示されます。このインジケータの値は以下のいずれかです：

- **保護レベル：高**：以下のカテゴリのすべての保護機能が有効になっている場合、インジケータがこの値で緑色になります。
  - **緊急**：このカテゴリには以下のコンポーネントが含まれます：
    - ファイル脅威対策
    - ふるまい検知
    - 脆弱性攻撃ブロック
    - 修復エンジン
  - **重要**：このカテゴリには以下のコンポーネントが含まれます：
    - Kaspersky Security Network
    - ウェブ脅威対策
    - メール脅威対策
    - ホスト侵入防止
- **保護レベル：中**：「重要」コンポーネントのいずれかが無効になっている場合、インジケータがこの値で黄色になります。
- **保護レベル：低**：以下のいずれかの場合、インジケータがこの値で赤になります：
  - 「緊急」コンポーネントのいずれかが無効になっている場合
  - 2つ以上の「重要」コンポーネントが無効になっている場合

インジケータの値が **保護レベル：中** または **保護レベル：低** の場合、インジケータの右に **推奨される保護機能** ウィンドウを表示するリンクが表示されます。このウィンドウで、推奨される保護機能を有効にできます。

## タスクの管理

次の種類のタスクを作成することで、Kaspersky Security Center を通して Kaspersky Endpoint Security を管理することができます：

- 個別のクライアントコンピューター向けに設定するローカルタスク
- 管理グループ内のクライアントコンピューター向けに設定するグループタスク
- コンピューターの抽出を対象としたタスク

グループタスク、コンピューターの抽出を対象とするタスク、ローカルタスクは、個数の制限なく作成することができます。管理グループとコンピューターの抽出を対象とした操作については、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

Kaspersky Endpoint Security は、以下のタスクをサポートします：

- **ウイルススキャン**：タスク設定で指定したコンピューターの領域でウイルスやその他の脅威をスキャンします。Kaspersky Endpoint Security による保護が適切に機能するには、[スキャン] タスクが必要となります。

す。このタスクはクイックスタートウィザードで作成されます。週に1回以上の頻度で[タスクが実行されるようにスケジュール設定](#)することを推奨します。

- **ライセンスの追加**：このタスクの実行時に、製品をアクティベートするライセンス（予備のライセンスを含む）が追加されます。タスクを実行する前に、タスクの実行対象となるコンピューターの台数がライセンスで利用が許可されるコンピューターの台数を超過しないことを確認してください。
- **コンポーネントの変更**：タスクの設定で指定されたコンポーネントのリストに従って、コンポーネントをインストールまたは削除します。ファイル脅威対策は削除できません。Kaspersky Endpoint Security のコンポーネントの最適な組み合わせを使用することで、コンピューターのリソース消費量を抑制できます。
- **インベントリ**：コンピューターに保管されているすべてのアプリケーションの実行ファイルに関する情報が取得されます。[インベントリ] タスクは、アプリケーションコントロール機能によって実行されます。アプリケーションコントロール機能がインストールされていない場合、このタスクはエラーにより失敗します。
- **アップデート**：定義データベースおよびソフトウェアモジュールをアップデートします。Kaspersky Endpoint Security による保護が適切に機能するには、[アップデート] タスクが必要となります。このタスクはクイックスタートウィザードで作成されます。1日に1回以上の頻度でタスクが実行されるようにスケジュール設定することを推奨します。
- **データの消去**：Kaspersky Endpoint Security は、指定した設定に応じて、即座にまたは Kaspersky Security Center への接続が長期間行われなかったときにユーザーのコンピューターのファイルとフォルダーを削除します。
- **アップデートのロールバック**：前回アップデートした定義データベースとソフトウェアモジュールを元に戻します。このタスクは、新しい定義データベースに、安全なアプリケーションのブロックにつながる可能性のある不正なデータが含まれてしまっていた場合などに必要です。
- **整合性チェック**：Kaspersky Endpoint Security が、アプリケーションファイルを分析し、ファイルに破損や変更がないかと、アプリケーションファイルのデジタル署名を検証します。
- **認証エージェントアカウントの管理**：Kaspersky Endpoint Security は、認証エージェントのアカウントを設定します。暗号化されたドライブを操作するには、認証エージェントが必要です。オペレーティングシステムを読み込む前に、ユーザーはエージェントで認証を完了する必要があります。

タスクは、コンピューター上で [Kaspersky Endpoint Security が起動され動作中の場合にのみ](#)実行されません。

## 新しいタスクを追加する

### [管理コンソール \(MMC\) でタスクを作成する方法](#)


1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで **[タスク]** フォルダーを選択します。
3. **[新規タスク]** をクリックします。  
タスクウィザードが起動します。
4. タスクウィザードの指示に従います。

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **[タスク種別]** ドロップダウンリストで、クライアントコンピューター上で実行するタスクを選択します。
  - c. **[タスク名]** に「**経理部門で使用中の製品のアップデート**」などの簡潔な名前を付けます。
  - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。 **[次へ]** をクリックします。
5. **[終了]** をクリックして、ウィザードを終了します。

タスクのリストに新しいタスクが表示されます。タスクには既定の設定が適用されます。タスクの設定を編集するには、タスクのプロパティを開きます。タスクを実行するには、タスクのチェックボックスをオンにし、**[開始]** をクリックする必要があります。タスクの開始後にタスクを停止して、あとで再開することもできます。

タスクのリストで、それぞれのタスクのステータスやコンピューター上でのタスクの実行結果に関する統計情報など、タスクの実行結果を監視することができます。タスクの実行を監視するためにイベントの抽出を作成することもできます（**[監視とレポート]** - **[イベントの抽出]**）。イベントの抽出について詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)  を参照してください。タスクの実行結果は、ローカル環境の Windows イベントログと [Kaspersky Endpoint Security のレポート](#) にも記録されます。

## タスクのアクセスコントロール

Kaspersky Endpoint Security のタスクにアクセスする権限（読み取り、書き込み、実行）は、Kaspersky Endpoint Security の機能範囲へのアクセスの設定により、Kaspersky Security Center 管理サーバーへのアクセス権を持つ各ユーザーに対して定義されます。Kaspersky Endpoint Security の機能範囲に対するアクセス権を設定するには、Kaspersky Security Center 管理サーバーのプロパティウィンドウの **[セキュリティ]** セクションに移動します。Kaspersky Security Center を使用したタスクの管理について詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)  を参照してください。

ポリシーを使用してユーザーのタスクへのアクセス権を設定できます（タスク管理モード）。例えば、Kaspersky Endpoint Security のインターフェイスからグループタスクを非表示にすることができます。

## [管理コンソール \(MMC\) から Kaspersky Endpoint Security インターフェイスでタスク管理モードを設定する方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [ローカルタスク] → [タスク管理] の順に選択します。
6. タスク管理モードを設定します（下記の表を参照）。
7. 変更内容を保存します。

### Web コンソールから Kaspersky Endpoint Security インターフェイスでタスク管理モードを設定する方法


1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. ポータブルモードのサポートを有効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [ローカルタスク] → [タスク管理] に移動します。
5. タスク管理モードを設定します（下記の表を参照）。
6. 変更内容を保存します。

#### タスク管理の設定

パラメータ	説明
ローカルタスクの使用を許可する	<p>このチェックボックスをオンにすると、ローカルタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。その他のポリシー制限がない場合、ユーザーはタスクの設定と実行ができます。ただし、ユーザーはタスク実行スケジュールを設定することはできません。ユーザーはタスクを手動でのみ実行できます。</p> <p>チェックボックスをオフにすると、ローカルタスクの使用を停止します。このモードでは、スケジュールにのっとったローカルタスクの実行は行われません。Kaspersky Endpoint Security のローカルインターフェイスでタスクの開始や設定ができなくなります。また、コマンドラインの使用時にもタスクの開始や設定ができなくなります。</p> <p>ファイルまたはフォルダーのウイルススキャンについては、スキャンするファイルまたはフォルダーのコンテキストメニューから [スキャン] を選択すれば開始できます。オブジェクトスキャンタスクの既定の設定値で、スキャンタスクが開始します。</p>
グループタスクの	<p>このチェックボックスをオンにすると、グループタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。ユーザーはアプリケーションインターフェイスでタスクのリストを表示できます。</p>

表示を許可する	このチェックボックスをオフにすると、空白のタスクリストを表示します。
グループタスクの管理を許可する	<p>このチェックボックスをオンにすると、Kaspersky Security Center 内で指定されたグループタスクを開始および停止できます。ユーザーはアプリケーションインターフェイスまたは簡略化したアプリケーションインターフェイスでタスクを開始および停止できます。</p> <p>このチェックボックスをオフにすると、Kaspersky Endpoint Security がスケジュールされたタスクを自動的に開始するか、管理者が Kaspersky Security Center で手動でタスクを開始します。</p>

## 個別のローカル環境用の製品設定

Kaspersky Security Center で、特定のコンピューターにインストールされている Kaspersky Endpoint Security の設定を編集できます。これが、ローカルアプリケーション設定です。一部の設定は編集できない可能性があります。その場合、これらの設定には [ポリシーのプロパティ](#) で  属性が割り当てられており、設定の編集がロックされています。

[管理コンソール \(MMC\) で個別のローカル環境用の製品設定を設定する方法](#) 



1. Kaspersky Security Center の管理コンソールを開きます。
  2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、対象のクライアントコンピューターが属する管理グループの名前のフォルダーを開きます。
  3. 作業領域で、 **〔デバイス〕** タブを選択します。
  4. Kaspersky Endpoint Security の設定を行うコンピューターを選択します。
  5. クライアントコンピューターのコンテキストメニューから **〔プロパティ〕** を選択します。  
クライアントコンピューターのプロパティウィンドウが開きます。
  6. クライアントコンピューターのプロパティウィンドウで、 **〔アプリケーション〕** セクションを選択します。  
クライアントコンピューターのプロパティウィンドウの右側に、クライアントコンピューターにインストールされているカスペルスキー製品のリストが表示されます。
  7. Kaspersky Endpoint Security を選択します。
  8. カスペルスキー製品のリストの下にある **〔プロパティ〕** をクリックします。  
**Kaspersky Endpoint Security for Windows の設定**ウィンドウが表示されます。
  9. **〔全般設定〕** セクションで、Kaspersky Endpoint Security の設定値およびレポートや保管領域の設定値を指定します。  
**Kaspersky Endpoint Security for Windows** の設定ウィンドウの残りのセクションは、Kaspersky Security Center の標準的なセクションと同じです。これらのセクションの説明については、Kaspersky Security Center のオンラインヘルプを参照してください。
- 特定の設定に対する変更をブロックするポリシーがアプリケーションに適用される場合、それらの設定は、 **〔全般設定〕** セクションでのアプリケーション設定時には編集できません。
10. 変更内容を保存するには、Kaspersky Endpoint Security for Windows のプロパティウィンドウで **〔OK〕** をクリックします。

## [Web コンソールおよび Cloud コンソールで個別のローカル環境用の製品設定を設定する方法](#)



1. Web コンソールのメインウィンドウで、**【デバイス】** → **【管理対象デバイス】** の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。  
コンピューターのプロパティが表示されます。
3. **【アプリケーション】** タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。  
ローカルアプリケーション設定が表示されます。
5. **【アプリケーション設定】** タブを選択します。
6. ローカルアプリケーション設定を編集します。
7. ローカルアプリケーション設定の項目は暗号化の設定を除いて**ポリシー設定**と同一です。

## Kaspersky Endpoint Security の起動と終了

Kaspersky Endpoint Security をユーザーのコンピューターにインストールすると、製品が自動的に起動されます。既定では、Kaspersky Endpoint Security はオペレーティングシステムが起動してから起動します。オペレーティングシステムの設定でアプリケーションの自動起動を構成することはできません。

オペレーティングシステムの起動後 Kaspersky Endpoint Security の定義データベースをダウンロードするには、コンピューターの性能によって最大 2 分かかることがあります。その間、コンピューターの保護レベルが低下します。既に起動したオペレーティングシステム上で Kaspersky Endpoint Security を起動したときの定義データベースのダウンロードでは、コンピューターの保護レベルは低下しません。


### 管理コンソール (MMC) で Kaspersky Endpoint Security の起動を設定するには

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **【管理対象デバイス】** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、**【ポリシー】** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**【全般設定】** → **【タスク管理】** の順に選択します。
6. 製品の自動起動を設定するには、**【コンピューターの開始時に Kaspersky Endpoint Security for Windows を開始する】** をオンにします。
7. 変更内容を保存します。

### Web コンソールで Kaspersky Endpoint Security の起動を設定するには

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 製品の起動を設定するコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[全般設定]** を選択します。
5. **[アプリケーション設定]** をクリックします。
6. 製品の自動起動を設定するには、**[コンピューターの開始時に Kaspersky Endpoint Security for Windows を開始する]** をオンにします。
7. 変更内容を保存します。



### 製品のインターフェイスで Kaspersky Endpoint Security の起動を設定するには

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[アプリケーション設定]** の順に選択します。
3. 製品の自動起動を設定するには、**[コンピューターの開始時に Kaspersky Endpoint Security for Windows を開始する]** をオンにします。
4. 変更内容を保存します。

Kaspersky Endpoint Security を手動で終了すると、お使いのコンピューターと個人情報が脅威にさらされるため、手動での終了は推奨されません。必要に応じて、製品を終了せずに必要な時間だけ プロテクションを一時停止 することができます。

**[保護ステータス]** ウィジェットを使用して製品のステータスを監視できます。

### 管理コンソール (MMC) で Kaspersky Endpoint Security を起動または停止するには

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、対象のクライアントコンピューターが属する管理グループの名前のフォルダーを開きます。
3. 作業領域で、 [デバイス] タブを選択します。
4. 本製品を起動または停止するコンピューターを選択します。
5. クライアントコンピューターを右クリックしてコンテキストメニューを表示し、 [プロパティ] を選択します。
6. クライアントコンピューターのプロパティウィンドウで、 [アプリケーション] セクションを選択します。  
クライアントコンピューターのプロパティウィンドウの右側に、クライアントコンピューターにインストールされているカスペルスキー製品のリストが表示されます。
7. Kaspersky Endpoint Security を選択します。
8. 次の手順に従います：
  - 本製品を起動するには、カスペルスキー製品リストの右側にある  ボタンをクリックします。
  - 本製品を停止するには、カスペルスキー製品リストの右側にある  ボタンをクリックします。

### Web コンソールで Kaspersky Endpoint Security を起動または停止するには

1. Web コンソールのメインウィンドウで、 [デバイス] → [管理対象デバイス] の順に選択します。
2. 本製品を起動または停止するコンピューターを選択します。  
コンピューターのプロパティウィンドウが開きます。
3. [アプリケーション] タブを選択します。
4. Kaspersky Endpoint Security for Windows のチェックボックスを選択します。
5. [開始] または [停止] をクリックします。

### コマンドラインを使用して Kaspersky Endpoint Security を起動または停止するには

コマンドラインを使用して本製品を停止させるには、[システムサービスの外部からの管理を有効にします](#)。



コマンドラインから製品を起動または停止する際には、Kaspersky Endpoint Security の配信キットに含まれている klpsm.exe ファイルが使用されます。

1. 管理者としてコマンドラインインタープリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. コマンドラインから製品を起動するには、「klpsm.exe start\_avp\_service」と入力します。
4. コマンドラインから製品を停止するには、「klpsm.exe stop\_avp\_service」と入力します。

## プロテクションとコントロールの一時停止と再開

プロテクションとコントロールを一時停止すると、Kaspersky Endpoint Security の保護および管理コンポーネントが一時的にすべて無効になります。

製品のステータスは、[タスクバーの通知領域の製品アイコン](#)によって示されます。

-  アイコンは、コンピュータープロテクションとコントロールが一時停止されていることを表します。
-  アイコンは、コンピュータープロテクションとコントロールが有効になっていることを表します。

プロテクションとコントロールを一時停止または再開しても、スキャンまたはアップデートタスクには影響ありません。

プロテクションとコントロールを一時停止または再開するときにネットワーク接続が既に確立されている場合、ネットワーク接続の中断に関する通知が表示されます。

プロテクションとコントロールを一時停止するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューから **[保護機能の一時停止]** を選択します (下の図を参照)。  
コンテキストメニューのこの項目は、[パスワードによる保護が有効](#)な場合に選択できます。

3. 次のいずれかのオプションを選択します：

- **指定時間経過後に再開** - プロテクションとコントロールは、下部のドロップダウンリストで指定した時間が経過すると再開されます。
- **本製品の再起動後に再開** - プロテクションとコントロールは、製品を終了して再開したとき、またはオペレーティングシステムを再起動したときに再開されます。このオプションを使用するには、自動起動を有効にする必要があります。
- **一時停止** - プロテクションとコントロールは、再び有効にしたときに再開されます。

4. **【保護機能の一時停止】** をクリックします。

Kaspersky Endpoint Security はポリシーでロック (🔒) が設定されていないすべての保護機能および管理コンポーネントの動作を一時的に停止します。この操作を実行する前に、Kaspersky Security Center のポリシーを無効にしておくことを推奨します。



製品アイコンのコンテキストメニュー

プロテクションとコントロールを再開するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューから **【保護機能の再開】** を選択します。

プロテクションとコントロールは、選択したプロテクションとコントロールの一時停止オプションに関係なく、いつでも再開できます。

# コンピューターのウイルススキャン

スキャンは、コンピューターのセキュリティに必要不可欠です。スキャンを定期的に行うことで、セキュリティレベルの設定が低いなどの理由により、保護機能で検知されない悪意のあるソフトウェアが拡散する可能性を排除できます。

Kaspersky Endpoint Security は、コンテンツが OneDrive クラウドストレージにあるファイルをスキャンせず、これらのファイルがスキャンされていないことを示すログエントリを作成します。

## 完全スキャン

コンピューター全体の徹底的なスキャン。Kaspersky Endpoint Security が、次のオブジェクトをスキャンします：

- カーネルメモリ
- オペレーティングシステムの起動時に読み込まれるオブジェクト
- ディスクブートセクター
- システムバックアップ
- すべてのハードディスクドライブとリムーバブルドライブ

カスペルスキーのエキスパートは、完全スキャンタスクのスキャン範囲を変更しないことを推奨します。

コンピューターのリソース消費量を抑えるために、完全スキャンタスクではなくバックグラウンドスキャンタスクを使用することを推奨します。これは、コンピューターのセキュリティレベルには影響しません。

## 簡易スキャン

既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。

カスペルスキーのエキスパートは、簡易スキャンタスクのスキャン範囲を変更しないことを推奨します。

## オブジェクトスキャン

Kaspersky Endpoint Security はユーザーが選択したオブジェクトをスキャンします。次のリストから任意のオブジェクトをスキャンできます：

- システムメモリ
- オペレーティングシステムの起動時に読み込まれるオブジェクト

- システムバックアップ
- Microsoft Outlook のメールボックス
- ハードディスク、リムーバブルドライブ、およびネットワークドライブ
- 選択した任意のファイル

## バックグラウンドスキャン

バックグラウンドスキャンモードでは、Kaspersky Endpoint Security はユーザー向けの通知を表示せずにスキャンを実行します。バックグラウンドスキャンは、その他のスキャン種別（完全スキャンなど）よりも、リソース消費量が少なくなります。このモードでは、Kaspersky Endpoint Security はスタートアップオブジェクト、ブートセクター、システムメモリ、システムパーティションをスキャンします。

## 整合性チェック

ソフトウェアモジュールに破損や変更がないかチェックします。

## コンピューターのスキャン

スキャンは、コンピューターのセキュリティに必要不可欠です。スキャンを定期的に行うことで、セキュリティレベルの設定が低いなどの理由により、保護機能で検知されない悪意のあるソフトウェアが拡散する可能性を排除できます。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

Kaspersky Endpoint Security には、事前定義された完全スキャン、簡易スキャン、カスタムスキャンといった標準タスクがあります。組織に Kaspersky Security Center 管理システムが配備されている場合、[ウイルススキャンタスクを作成](#)してスキャンを設定することができます。Kaspersky Security Center では、[バックグラウンドスキャンタスク](#)も利用可能です。バックグラウンドスキャンを設定することはできません。

### [管理コンソール \(MMC\) でウイルススキャンを実行する方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [タスク] タブを選択します。
4. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。  
必要に応じて、 [ウイルススキャン](#) タスクを作成します。
5. コンピューターのプロパティウィンドウで、 [設定] セクションを選択します。
6. スキャンタスクを設定します（下の表を参照）。  
必要に応じて、 [スキャンタスクのスケジュールを設定します](#)。
7. 変更内容を保存します。
8. スキャンタスクを実行します。

コンピューターのスキャンが開始されます。タスクの実行をコンピューターの電源をオフにするなどで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。

### [Web コンソールと Cloud コンソールでウイルススキャンを実行する方法](#)

1. Web コンソールのメインウィンドウで、 [デバイス] → [タスク] の順に選択します。  
タスクのリストが表示されます。
2. スキャンタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. スキャンタスクを設定します（下の表を参照）。  
必要に応じて、 [スキャンタスクのスケジュールを設定します](#)。
5. 変更内容を保存します。
6. スキャンタスクを実行します。

コンピューターのスキャンが開始されます。タスクの実行をコンピューターの電源をオフにするなどで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。

### [製品インターフェイスでウイルススキャンを実行する方法](#)

1. メインウィンドウで、**[タスク]** セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙) をクリックします。
3. スキャンタスクを設定します (下の表を参照)。  
必要に応じて、[スキャンタスクのスケジュールを設定します](#)。
4. 変更内容を保存します。
5. スキャンタスクを実行します。

コンピューターのスキャンが開始されます。スキャンされたファイルの数、スキャンの残り時間など、スキャンの進捗が表示されます。**[停止]** ボタンを押すことでいつでもタスクを停止することができます。スキャンタスクが表示されない場合は、管理者により[ポリシー内でローカルタスクの使用が禁止](#)されていることを意味します。

#### スキャン設定

パラメータ	説明
セキュリティレベル	<p>Kaspersky Endpoint Security はスキャンを実行するために異なる設定のグループを使用します。本製品に保存されているこれらの設定のグループはセキュリティレベルと呼ばれます：</p> <ul style="list-style-type: none"> <li>• <b>高</b>：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルのスキャン時には、メール形式のファイルもスキャンします。</li> <li>• <b>推奨</b>：Kaspersky Endpoint Security は、コンピューターに接続しているすべてのハードディスク、ネットワークドライブ、リムーバブルドライブに格納されているファイルのうち、特定の形式のファイル、さらに OLE 埋め込みオブジェクトをスキャンします。アーカイブやインストールパッケージはスキャンしません。</li> <li>• <b>低</b>：Kaspersky Endpoint Security は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の拡張子を持つ新しいファイルまたは変更されたファイルをスキャンします。複合ファイルはスキャンしません。</li> </ul> <p>セキュリティレベルは、事前に設定されているものから選択することも、手動で設定することもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。</p>
脅威の検知時の処理	<p><b>駆除する。駆除できない場合は削除する</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。</p> <p><b>駆除する。駆除できない場合は通知する</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除ができない場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。</p> <p><b>通知する</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>感染したファイルを駆除または削除する前に、Kaspersky Endpoint Security は<a href="#">ファイルを復元またはあとで駆除できた場合</a>に必要な場合に備えてバックアップファイルを作成します。</p> </div>

	Windows ストアアプリの一部であるファイルで感染が検知された場合、そのファイルが削除されます。
<b>すぐに特別な駆除を実行する</b>  (Kaspersky Security Center コンソール内でのみ利用可能)	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>コンピューターに適用されているポリシーのプロパティで<b>特別な駆除が有効</b>になっている場合のみ、コンピューター上のウイルススキャンタスク中に特別な駆除が実行されます。</p> </div> <p>チェックボックスがオンの場合、Kaspersky Endpoint Security はウイルススキャンタスクの実行中にアクティブな感染を検知すると、すぐに駆除します。アクティブな感染の駆除後、Kaspersky Endpoint Security はユーザーに通知せずにコンピューターを再起動します。</p> <p>チェックボックスがオフの場合、Kaspersky Endpoint Security はウイルススキャンタスクの実行中にアクティブな感染を検知してもすぐには駆除しません。Kaspersky Endpoint Security はローカルの製品レポートおよび Kaspersky Security Center でアクティブな感染イベントを作成します。アクティブな感染は、特別な駆除機能がオンになっているときにウイルススキャンタスクが再度実行されたときに駆除することができます。このように、システム管理者は特別な駆除を実行し、コンピューターを自動的に再起動するために適切なタイミングを選択することができます。</p>
<b>スキャン範囲</b>	スキャンタスクの実行時に、Kaspersky Endpoint Security によってスキャンされるオブジェクトのリスト。スキャン範囲に指定できるオブジェクトは次のとおりです：カーネルメモリ、実行中の処理、ブートセクター、システムのバックアップ保管領域、メールデータベース、ハードディスク、リムーバブルドライブまたはネットワークドライブ、フォルダーまたはファイル。
<b>スキャンのスケジュール</b>	<b>手動開始</b> ：都合の良いときに手動でスキャンを開始できる実行方法です。 <b>スケジュールで指定</b> ：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。
<b>製品起動後 N 分後に開始</b>	本製品の開始後、遅れてスキャンタスクを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。
<b>未実行のタスクを実行する</b>	このチェックボックスをオンにすると、スキップされたスキャンタスクは実行可能になると同時に開始されます。スキャンタスクの開始時間にコンピューターの電源がオフになっていた場合などに、スキャンタスクがスキップされることがあります。このチェックボックスをオフにすると、スキップされたスキャンタスクは開始されません。代わりに、現在のスケジュールに従って、次のスキャンタスクが実行されます。
<b>コンピューターを使用していないときにのみ実行する</b>	コンピューターのリソースの負荷が高い場合にスキャンタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。
<b>&lt;ユーザー名&gt;として実行</b>	既定では、スキャンタスクはオペレーティングシステムに登録されたユーザー名で実行されます。保護範囲には、ネットワークドライブやその他特定のアクセス権限を必要とするオブジェクトが含まれることがあります。Kaspersky Endpoint Security の設定に適した権限を持っているユーザーを指定して、このユーザーアカウントでスキャンタスクを実行できます。
<b>ファイル種別</b>	<div style="border: 1px solid black; padding: 5px;"> <p>Kaspersky Endpoint Security では、拡張子のないファイルは実行ファイルとみなされます。Kaspersky Endpoint Security では、スキャン対象としたファイルの種類にかか</p> </div>

ならず、必ず実行ファイルをスキャンします。

**すべてのファイル。**この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。

**ファイル形式でファイルをスキャン。**この設定を有効にした場合、Kaspersky Endpoint Security は感染する可能性のあるファイルのみをスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。

**拡張子でファイルをスキャン。**この設定を有効にした場合、Kaspersky Endpoint Security は感染する可能性のあるファイルのみをスキャンします。ファイル形式はファイルの拡張子に基づいて識別されます。

既定では、ファイルはその形式でスキャンされます。悪意のあるファイルには、「.123」など、感染ファイルの可能性のある拡張子のリストにはない拡張子が指定されていることがあるため、拡張子を指定するスキャンはあまり安全であるとは言えません。

**新規作成または更新されたファイルのみスキャン**

新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。

**スキャン時間が次を超えたファイルをスキップ**

単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。

**アーカイブをスキャン**

次の形式のアーカイブのファイルをスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR および ICE。

**配布パッケージをスキャン**

このチェックボックスでは、サードパーティの配布パッケージのスキャンを有効または無効にします。

**Microsoft Office 形式のファイルのスキャン**

Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。

**メール形式を解析してスキャン**

このチェックボックスでは、メール形式およびメールデータベースのファイルをスキャンする際の Kaspersky Endpoint Security のオプションを有効または無効にします。

本製品は、コンピューターに Microsoft Outlook x86 メールクライアントを持つ場合のみ MS Outlook、Windows Mail、Outlook Express および EML メールファイル形式のみを完全スキャンします。

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はコンポーネント（ヘッダー、本文、添付ファイル）に分割され、それぞれで脅威がスキャンされます。

チェックボックスをオフにすると、Kaspersky Endpoint Security はメール形式のファイルを1つのファイルとしてスキャンします。

**パスワードで保護されているアーカイブをスキャン**

このチェックボックスをオンにすると、Kaspersky Endpoint Security はパスワードで保護されたアーカイブをスキャンします。アーカイブのファイルをスキャンする前に、パスワードの入力が求められます。

このチェックボックスをオフにすると、Kaspersky Endpoint Security はパスワードで保護されたアーカイブのスキャンをスキップします。

**大きな複合**

<p><b>ファイルのスキャンしない</b></p>	<p>このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。</p> <p>このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。</p> <p>圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。</p>
<p><b>機械学習とシグネチャ分析</b></p>	<p>機械学習とシグネチャ分析では、既知の脅威の説明と脅威を無効化する方法が登録された Kaspersky Endpoint Security の定義データベースを使用します。この方法を使用する保護では、許容できる最低限のセキュリティレベルが提供されます。</p> <p>カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。</p>
<p><b>ヒューリスティック分析</b></p>	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
<p><b>iSwift</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>特定のファイルのスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。</p>
<p><b>iChecker</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>特定のファイルのスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル (EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR) にのみ適用する点です。</p>

Scanning removable drives when they are connected to the computer



Kaspersky Endpoint Security scans all files that you run or copy, even if the file is located on a removable drive (File Threat Protection component). To prevent the spread of viruses and other malware, you can configure automatic scans of removable drives when they are connected to the computer. Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files. The component keeps a computer secure by running scans that implement machine learning, heuristic analysis (high level) and signature analysis. Kaspersky Endpoint Security also uses iSwift and iChecker scan optimization technologies. The technologies are always on and cannot be disabled.


### [How to configure running the Removable drives scan in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Local Tasks** → **Removable drives scan**.
6. In the **Action when a removable drive is connected** drop-down list, select **Detailed Scan** or **Quick Scan**.
7. Configure advanced options for Removable drives scan (see table below).
8. Save your changes.

### [How to configure running the Removable drives scan in the Web Console and Cloud Console](#)

1. In the main window of Web Console, select **Devices** → **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.  
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local Tasks** → **Removable drives scan**.
5. In the **Action when a removable drive is connected** drop-down list, select **Detailed Scan** or **Quick Scan**.
6. Configure advanced options for Removable drives scan (see table below).
7. Save your changes.

### [How to configure running the Removable drives scan in the application interface](#)

1. In the main application window, go to the **Tasks** section.
2. In the task list, select the scan task and click .
3. Use the **Removable drives scan** toggle to enable or disable scans of removable drives upon connection to the computer.
4. Configure advanced options for Removable drives scan (see table below).
5. Save your changes.

As a result, Kaspersky Endpoint Security runs a Removable drives scan for removable drives that are not larger than the specified maximum size. If the *Removable drives scan* task is not displayed, it means the administrator [has prohibited using local tasks in the policy](#).

Removable drives scan task settings

Parameter	Description
<b>Action when a removable drive is connected</b>	<p><b>Detailed Scan</b> If this item is selected, when a removable drive is connected, Kaspersky Endpoint Security scans all files on the removable drive, including files nested in compound objects, archives, distribution packages, and files in office formats. Kaspersky Endpoint Security does not scan files in mail formats or password-protected archives.</p> <p><b>Quick Scan</b> If this option is selected, after a removable drive is connected Kaspersky Endpoint Security scans only <a href="#">files of specific formats</a> that are most vulnerable to infection, and does not unpack compound objects.</p>
<b>Maximum removable drive size</b>	<p>If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the <b>Action when a removable drive is connected</b> drop-down list on removable drives with a size not more than the specified maximum drive size.</p> <p>If the check box is cleared, Kaspersky Endpoint Security performs the action that is selected in the <b>Action when a removable drive is connected</b> drop-down list on removable drives of any size.</p>
<b>Show scan progress</b>	<p>If the check box is selected, Kaspersky Endpoint Security displays the progress of removable drives scan in a separate window and in the <b>Tasks</b> window.</p> <p>If the check box is cleared, Kaspersky Endpoint Security performs removable drives scan in the background.</p>
<b>Block the stopping of the scan task</b>	<p>If the check box is selected, the <b>Stop</b> button in the <b>Tasks</b> window and the <b>Stop</b> button in the <b>Virus Scan</b> window are not available in the local interface of Kaspersky Endpoint Security.</p>

## バックグラウンドスキャン

バックグラウンドスキャンモードでは、Kaspersky Endpoint Security はユーザー向けの通知を表示せずにスキャンを実行します。バックグラウンドスキャンは、その他のスキャン種別（完全スキャンなど）よりも、リソース消費量が少なくなります。このモードでは、Kaspersky Endpoint Security はスタートアップオブジェクト、ブートセクター、システムメモリ、システムパーティションをスキャンします。次のケースでは、バックグラウンドスキャンが開始されます。

- 定義データベースがアップデートされた。



- Kaspersky Endpoint Security が起動してから 30 分が経過した。
- 前回のタスクから 6 時間が経過した。
- コンピューターが 5 分以上アイドル状態になっている（コンピューターがロックされているまたはスクリーンセーバーが実行されている）。

コンピューターが 5 分以上アイドル状態になっていてバックグラウンドスキャンが開始された場合、次のいずれかの条件が満たされるとスキャンが中断されます。

- コンピューターが再びアクティブな状態になった。

ただし、バックグラウンドスキャンが実行されていない期間が 10 日を超えている場合、スキャンは中断されません。

- コンピューターがバッテリーモードに切り替わった（ノートパソコンなど）

バックグラウンドスキャンの実行時に、Kaspersky Endpoint Security では、OneDrive クラウドストレージ上にコンテンツがあるファイルはスキャンされません。

### 管理コンソール (MMC) でバックグラウンドスキャンを有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[ローカルタスク] → [バックグラウンドスキャン] の順に選択します。
6. [バックグラウンドスキャン] を使用して機能を有効または無効にします。
7. 変更内容を保存します。

### Web コンソールと Cloud コンソールでバックグラウンドスキャンを有効にする方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [ローカルタスク] → [バックグラウンドスキャン] に移動します。
5. [バックグラウンドスキャン] を使用して機能を有効または無効にします。
6. 変更内容を保存します。

### 製品インターフェイスでバックグラウンドスキャンを有効にする方法

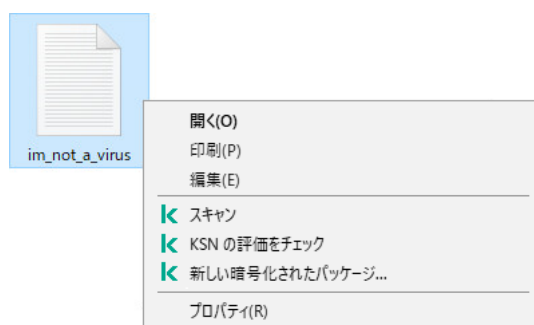
1. メインウィンドウで、[タスク] セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙️) をクリックします。
3. [バックグラウンドスキャン] を使用して機能を有効または無効にします。
4. 変更内容を保存します。

バックグラウンドスキャンが表示されない場合は、管理者により ポリシー内でローカルタスクの使用が禁止 されていることを意味します。

## コンテキストメニューからのスキャン

Kaspersky Endpoint Security では、個別のファイルに対してウイルスなどのマルウェアを対象とするスキャンをコンテキストメニューから実行できます (以下の図を参照)。

コンテキストメニューからスキャンを実行した時に、Kaspersky Endpoint Security では、OneDrive クラウドストレージ上にコンテンツがあるファイルはスキャンされません。



コンテキストメニューからのスキャン

## 管理コンソール (MMC) でコンテキストメニューからのスキャンを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[ローカルタスク] → [コンテキストメニューからのスキャン] の順に選択します。
6. コンテキストメニューからのスキャンを設定します (下の表を参照)。
7. 変更内容を保存します。

## Web コンソールおよび Cloud コンソールでコンテキストメニューからのスキャンを設定する方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [ローカルタスク] → [コンテキストメニューからのスキャン] の順に選択します。
5. コンテキストメニューからのスキャンを設定します (下の表を参照)。
6. 変更内容を保存します。

## 製品インターフェイスでコンテキストメニューからのスキャンを設定する方法

1. メインウィンドウで、[タスク] セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙) をクリックします。
3. コンテキストメニューからのスキャンを設定します (下の表を参照)。
4. 変更内容を保存します。

コンテキストメニューからのスキャンタスクが表示されない場合は、管理者により ポリシー内でローカルタスクの使用が禁止 されていることを意味します。

コンテキストメニューからのスキャンタスクの設定

パラメー

説明

タ	
セキュリティレベル	<p>Kaspersky Endpoint Security はスキャンを実行するために異なる設定のグループを使用します。本製品に保存されているこれらの設定のグループはセキュリティレベルと呼ばれます：</p> <ul style="list-style-type: none"> <li>• <b>高</b>：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルのスキャン時には、メール形式のファイルもスキャンします。</li> <li>• <b>推奨</b>：Kaspersky Endpoint Security は、コンピューターに接続しているすべてのハードディスク、ネットワークドライブ、リムーバブルドライブに格納されているファイルのうち、特定の形式のファイル、さらに OLE 埋め込みオブジェクトをスキャンします。アーカイブやインストールパッケージはスキャンしません。</li> <li>• <b>低</b>：Kaspersky Endpoint Security は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の拡張子を持つ新しいファイルまたは変更されたファイルをスキャンします。複合ファイルはスキャンしません。</li> </ul>
脅威の検知時の処理	<p><b>駆除する。駆除できない場合は削除する</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。</p> <p><b>駆除する。駆除できない場合はブロックする</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除ができない場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。</p> <p><b>通知する</b>：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。</p>
ファイル種別	<div style="border: 1px solid gray; padding: 10px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security では、拡張子のないファイルは実行ファイルとみなされません。Kaspersky Endpoint Security では、スキャン対象としたファイルの種類にかかわらず、必ず実行ファイルをスキャンします。</p> </div> <p><b>すべてのファイル</b>。この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。</p> <p><b>ファイル形式でファイルをスキャン</b>。この設定を有効にした場合、Kaspersky Endpoint Security は<u>感染する可能性のあるファイルのみ</u>をスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。</p> <p><b>拡張子でファイルをスキャン</b>。この設定を有効にした場合、Kaspersky Endpoint Security は<u>感染する可能性のあるファイルのみ</u>をスキャンします。ファイル形式はファイルの拡張子に基づいて識別されます。</p> <p>既定では、ファイルはその形式でスキャンされます。悪意のあるファイルには、「.123」など、感染ファイルの可能性のある拡張子のリストにはない拡張子が指定されていることがあるため、拡張子を指定するスキャンはあまり安全であるとは言えません。</p>
新規作成または更新されたファイルのみスキャン	<p>新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。</p>
スキャン時間が次を超えた	<p>単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。</p>

<b>ファイルをスキップ</b>	
<b>アーカイブをスキャン</b>	<p>次の形式のアーカイブのファイルをスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR およびICE。</p>
<b>配布パッケージをスキャン</b>	<p>このチェックボックスでは、配布パッケージのスキャンを有効または無効にします。</p>
<b>Microsoft Office 形式のファイルのスキャン</b>	<p>Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。</p>
<b>メール形式を解析してスキャン</b>	<p>このチェックボックスでは、メール形式およびメールデータベースのファイルをスキャンする際の Kaspersky Endpoint Security のオプションを有効または無効にします。</p> <p>本製品は、コンピューターに Microsoft Outlook x86 メールクライアントを持つ場合のみ MS Outlook、Windows Mail、Outlook Express および EML メールファイル形式のみを完全スキャンします。</p> <p>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はコンポーネント（ヘッダー、本文、添付ファイル）に分割され、それぞれで脅威がスキャンされます。</p> <p>チェックボックスをオフにすると、Kaspersky Endpoint Security はメール形式のファイルを1つのファイルとしてスキャンします。</p>
<b>パスワードで保護されているアーカイブのスキャン</b>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security はパスワードで保護されたアーカイブをスキャンします。アーカイブのファイルをスキャンする前に、パスワードの入力が求められます。</p> <p>このチェックボックスをオフにすると、Kaspersky Endpoint Security はパスワードで保護されたアーカイブのスキャンをスキップします。</p>
<b>大きな複合ファイルのスキャンしない</b>	<p>このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。</p> <p>このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。</p> <p>圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。</p>
<b>機械学習とシグネチャ分析</b>	<p>機械学習とシグネチャ分析では、既知の脅威の説明と脅威を無効化する方法が登録された Kaspersky Endpoint Security の定義データベースを使用します。この方法を使用する保護では、許容できる最低限のセキュリティレベルが提供されます。</p> <p>カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。</p>
<b>ヒューリスティック分析</b>	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
<b>iSwift</b>	<p>特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。</p>

	ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル (EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR) にのみ適用する点です。

## 本製品の整合性の確認

ソフトウェアモジュールに破損や変更がないかチェックします。たとえば、アプリケーションライブラリのデジタル署名が正しくない場合、そのライブラリは破損していると考えられます。整合性チェックタスクは、アプリケーションファイルをスキャンするためのタスクです。Kaspersky Endpoint Security で悪意のあるオブジェクトが検知され、そのオブジェクトを無害化できなかった場合、整合性チェックタスクを実行してください。

整合性チェックタスクは Kaspersky Security Center Web コンソールおよび管理コンソールの両方で作成できます。Kaspersky Security Center Cloud コンソールではこのタスクを作成できません。

アプリケーションの整合性が侵害されている状況として、次のケースがあります：

- 悪意のあるオブジェクトによって Kaspersky Endpoint Security のファイルが変更された。この場合、オペレーティングシステムのツールを使用して Kaspersky Endpoint Security を復元します。復元が完了したら、コンピューターの完全スキャンを実行し、それから整合性チェックを再び実行してください。
- デジタル署名の有効期限が切れている。この場合、Kaspersky Endpoint Security をアップデートします。

### [管理コンソール \(MMC\) を使用してアプリケーションの整合性チェックを実行する方法](#)



1. 管理コンソールで、**[管理サーバー]** → **[タスク]** のフォルダーに移動します。

タスクのリストが表示されます。

2. **[新規タスク]** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

**[Kaspersky Endpoint Security for Windows (11.7.0)]** → **[整合性チェック]** を選択します。

## ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 3：タスク開始スケジュールの設定

たとえば、手動で、またはウイルス発生が検知されたときに、タスクを開始するスケジュールを設定します。

## ステップ 4：タスク名の定義

コンピューターの感染後の整合性チェックなど、タスクの名前を入力します。

## ステップ 5：タスク作成の完了

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。本製品の整合性がチェックされます。整合性チェックタスクのプロパティで、タスクのスケジュールを設定することもできます（下の表を参照）。

[Web コンソールを使用してアプリケーションの整合性チェックを実行する方法](#)



1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **【タスク種別】** で、**【整合性チェック】** を選択します。
  - c. **【タスク名】** に「コンピューターへの感染を検知後のアプリケーションの整合性のチェック」などの短く分かりやすい名前を付けます。
  - d. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。**【次へ】** をクリックします。
5. **【終了】** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
6. タスクの横にあるチェックボックスをオンにします。

本製品の整合性がチェックされます。整合性チェックタスクのプロパティで、タスクのスケジュールを設定することもできます（下の表を参照）。

### 製品インターフェイスで整合性チェックを実行する方法

1. メインウィンドウで、**【タスク】** セクションに移動します。
2. タスクのリストが表示されます。整合性チェックタスクを選択して **【スキャン】** をクリックします。

本製品の整合性がチェックされます。整合性チェックタスクのプロパティで、タスクのスケジュールを設定することもできます（下の表を参照）。整合性チェックが表示されない場合は、管理者により **ポリシー内でローカルタスクの使用が禁止** されていることを意味します。

整合性チェックタスク

パラメータ	説明
スキャンのスケジュール	<p><b>手動開始</b>：都合の良いときに手動でスキャンを開始できる実行方法です。</p> <p><b>スケジュールで指定</b>：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。</p>
スキップしたタスクを後で実行する	<p>このチェックボックスをオンにすると、スキップされたスキャンタスクは実行可能になると同時に開始されます。スキャンタスクの開始時間にコンピューターの電源がオフになっていた場合などに、スキャンタスクがスキップされることがあります。このチェックボックスをオフにすると、スキップされたスキャンタスクは開始されません。代わりに、現在のスケジュールに従って、次のスキャンタスクが実行されます。</p>

<b>コンピューターを使用していないときにのみ実行する</b>	コンピューターのリソースの負荷が高い場合にスキャンタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。
<b>&lt;ユーザー名&gt;として実行</b> (Kaspersky Security Center コンソール内でのみ利用可能)	既定では、スキャンタスクはオペレーティングシステムに登録されたユーザー名で実行されます。アプリケーションのインストールフォルダーにアクセスするには特別な権限が必要になることがあります。Kaspersky Endpoint Security の設定に適した権限を持っているユーザーを指定して、このユーザーアカウントでスキャンタスクを実行できます。

## スキャン範囲の編集

スキャン範囲は、フォルダーのパスおよびタスクの実行時に Kaspersky Endpoint Security がスキャンするパスのリストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。

スキャン範囲を編集するには、カスタムスキャンタスクの使用を推奨します。カスペルスキーのエキスパートは、完全スキャンおよび簡易スキャンタスクのスキャン範囲の変更は推奨しません。

Kaspersky Endpoint Security には、スキャン範囲の一部に次の事前定義されたオブジェクトがあります。

- **メール**  
データファイル (PST) 、オフラインデータファイル (OST) など、Outlook メールクライアントに関連するファイル。
- **カーネルメモリ**
- **実行中のプロセスおよびスタートアップオブジェクト**  
システムの起動時に実行されるプロセスやアプリケーション実行ファイルによって使用されているメモリ。
- **ディスクブートセクター**  
ハードディスクおよびリムーバブルディスクのブートセクター。
- **システムバックアップ**  
System Volume Information フォルダーの内容。
- **すべてのリムーバブルドライブ**
- **すべてのハードディスク**
- **すべてのネットワークドライブ**

スキャン範囲からフォルダーやファイルを除外するには、[フォルダーまたはファイルを信頼ゾーンに追加](#)します。

### [管理コンソール \(MMC\) でスキャン範囲を編集する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[タスク] タブを選択します。
4. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。  
必要に応じて、[ウイルススキャン](#)タスクを作成します。
5. コンピューターのプロパティウィンドウで、[設定] セクションを選択します。
6. [スキャン範囲] で、[設定] をクリックします。
7. 表示されたウィンドウで、スキャン範囲に含めるまたは除外するオブジェクトを選択します。
8. スキャン範囲に新しいオブジェクトを追加するには：
  - a. [追加] をクリックします。
  - b. [オブジェクト] フィールドにフォルダーまたはファイルのパスを入力して [追加] をクリックします。

マスクを使用する

- 「\*」 (アスタリスク) 文字。「\」 および 「/」 (ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字) を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
- 2つの連続した「\*」 (アスタリスク) 文字。ファイル名またはフォルダー名内の、「\」 および 「/」 (ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字) を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。
- 「?」 (クエスションマーク)。「\」 および 「/」 (ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字) を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。

スキャン範囲のオブジェクトのリストからオブジェクトを削除しなくてもオブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

9. 変更内容を保存します。

## [Web コンソールと Cloud コンソールでスキャン範囲を編集する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
  2. スキャンタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。必要に応じて、**ウイルススキャン**タスクを作成します。
  3. **[アプリケーション設定]** タブを選択します。
  4. **[スキャン範囲]** で、スキャン範囲に含めるまたは除外するオブジェクトを選択します。
  5. スキャン範囲に新しいオブジェクトを追加するには：
    - a. **[追加]** をクリックします。
    - b. **[パス]** フィールドにフォルダーまたはファイルのパスを入力して **[OK]** をクリックします。  
マスクを使用する
      - 「\*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
      - 2つの連続した「\*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。
      - 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。
  6. 変更内容を保存します。
- スキャン範囲のオブジェクトのリストからオブジェクトを削除しなくてもオブジェクトをスキャンから除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。

## **製品インターフェイスでスキャン範囲を編集する方法**

1. メインウィンドウで、**[タスク]** セクションに移動します。
2. タスクのリストで、**[カスタムスキャン]** タスクを選択して **[選択]** をクリックします。  
その他のタスクのスキャン範囲も編集することができます。カスペルスキーのエキスパートは、完全スキャンおよび簡易スキャンタスクのスキャン範囲の変更は推奨しません。
3. 表示されたウィンドウで、スキャン範囲に含めるオブジェクトを選択します。
4. 変更内容を保存します。

スキャンタスクが表示されない場合は、管理者により ポリシー内でローカルタスクの使用が禁止 されていることを意味します。

## スケジュールされたスキャンの実行

コンピューターの完全スキャンには時間がかかり、コンピューターのリソースも必要となります。その他のソフトウェアのパフォーマンスに影響を与えないよう、コンピューターのスキャンを実行するのに最適な時間を選択する必要があります。Kaspersky Endpoint Security を使用して、コンピューターのスキャンの標準スケジュールを設定できます。組織に業務スケジュールがある場合、この機能が便利です。夜間や週末にコンピューターのスキャンを実行するよう設定できます。何らかの理由（コンピューターの電源が入っていないなど）でスキャンタスクを実行できない場合、スキップされたタスクが実行可能になると同時に自動的に実行されるように設定することができます。

最適な時間のスキャンスケジュールの設定が難しい場合は、次の特定の条件を満たす場合 Kaspersky Endpoint Security を使用してコンピューターのスキャンを実行できます：

- データベースのアップデート後：  
Kaspersky Endpoint Security はアップデートシグネチャがあるデータベースでコンピューターのスキャンを実行します。
- 本製品の起動後：  
製品の開始から指定した時間が経過した際、Kaspersky Endpoint Security はスキャンを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。
- Wake-on-LAN：  
コンピューターの電源がオフの場合でも、Kaspersky Endpoint Security はスケジュールに従ってコンピューターのスキャンを実行します。そのため、本製品はオペレーティングシステムの Wake-on-LAN 機能を使用します。Wake-on-LAN 機能とは、ローカルネットワークを介して特殊な信号を送信することで遠隔からコンピューターの電源をオンにします。この機能を使用するには、BIOS 設定で Wake-on-LAN 機能を有効にする必要があります。  
Wake-on-LAN を使用したスキャンの実行を設定できるのは、Kaspersky Security Center のウイルススキャンタスクのみです。製品インターフェイスではコンピューターのスキャンの Wake-on-LAN を有効にすることはできません。
- コンピューターを使用していないとき：  
Kaspersky Endpoint Security は、スクリーンセーバーが起動しているまたは画面がロックされているときにスケジュールに従ってコンピューターのスキャンを実行します。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はスキャンを一時停止します。そのため、本製品がコンピューターの完全スキャンを実行するのに数日かかることがあります。

## 管理コンソール (MMC) でスキャンのスケジュールを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[タスク] タブを選択します。
4. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。  
必要に応じて、ウイルススキャンタスクを作成します。
5. コンピューターのプロパティウィンドウで、[スケジュール] セクションを選択します。
6. スキャンタスクのスケジュールを設定します。
7. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。
8. 変更内容を保存します。

## Web コンソールと Cloud コンソールでスキャンのスケジュールを設定する方法

1. Web コンソールのメインウィンドウで、[デバイス] → [タスク] の順に選択します。  
タスクのリストが表示されます。
2. スキャンタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
3. [スケジュール] タブを選択します。
4. スキャンタスクのスケジュールを設定します。
5. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。
6. 変更内容を保存します。

## 製品インターフェイスでスキャンのスケジュールを設定する方法



コンピューターにポリシーが適用されていない場合にのみスキャンスケジュールを設定することができます。ポリシーが適用されているコンピューターは、Kaspersky Security Center でウイルススキャンタスクのスケジュールを設定してください。

1. メインウィンドウで、**[タスク]** セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙) をクリックします。  
完全スキャン、簡易スキャンまたは整合性チェックの実行スケジュールを設定できます。カスタムスキャンは手動でのみ実行できます。
3. **[スキャンスケジュール]** をクリックします。
4. 表示されたウィンドウで、スキャンタスクの実行のスケジュールを設定します。
5. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します (下の表を参照してください)。
6. 変更内容を保存します。

#### スキャンスケジュールの設定

パラメータ	説明
スキャンのスケジュール	<p><b>手動開始</b> : 都合の良いときに手動でスキャンを開始できる実行方法です。</p> <p><b>スケジュールで指定</b> : このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。</p>
製品起動後 N 分後に開始	本製品の開始後、遅れてスキャンタスクを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。
スキップしたタスクを後で実行する	このチェックボックスをオンにすると、スキップされたスキャンタスクは実行可能になると同時に開始されます。スキャンタスクの開始時間にコンピューターの電源がオフになっていた場合などに、スキャンタスクがスキップされることがあります。このチェックボックスをオフにすると、スキップされたスキャンタスクは開始されません。代わりに、現在のスケジュールに従って、次のスキャンタスクが実行されます。
コンピューターを使用していないときにのみ実行する	コンピューターのリソースの負荷が高い場合にスキャンタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。
タスクの開始を自動的にランダムに遅延させる (Kaspersky Security Center コンソール内でのみ利用可能)	<p>このチェックボックスがオンの場合、タスクはスケジュールに厳密に従わず、特定の間隔でランダムに、つまりタスクの開始時刻は分散して実行されます。ランダムに開始することで、タスクがスケジュール通りに実行されることにより、多数のコンピューターから同時に管理サーバーにアクセスが集中することを避けられます。</p> <p>ランダムに開始されるタスクの開始時刻の範囲は、タスクが作成された際、そのタスクが割り当てられたコンピューターの数に基づいて自動的に計算されます。それ以降、タスクは算出された開始時刻に実行されます。しかし、タスクの設定が変更されたり手動で実行された場合は、計算される開始時刻は変更されます。</p> <p>チェックボックスがオフの場合、タスクはスケジュールされた時刻に実行されます。</p>



**Wake on LANの機能を使用してタスク開始前にデバイスを起動する (分)**

(Kaspersky Security Center コンソール内でのみ利用可能)

このチェックボックスがオンの場合、コンピューターのオペレーティングシステムの起動が完了するまで指定した時間をおいてからタスクが実行されます。既定の時間は5分です。

電源がオフのコンピューターも含めてすべてのコンピューターでタスクを実行する場合はこのチェックボックスをオンにしてください。

## 異なるユーザーとしてスキャンを実行する

既定では、スキャンタスクはオペレーティングシステムに登録されたユーザー名で実行されます。保護範囲には、ネットワークドライブやその他特定のアクセス権限を必要とするオブジェクトが含まれることがあります。Kaspersky Endpoint Security の設定に適した権限を持っているユーザーを指定して、このユーザーアカウントでスキャンタスクを実行できます。

異なるユーザーを指定して実行できるのは次のスキャンです：

- 簡易スキャン
- 完全スキャン
- オブジェクトスキャン
- [コンテキストメニューからのスキャン](#)

[リムーバブルドライブのスキャン](#)、[バックグラウンドスキャン](#)、または[整合性チェック](#)を実行するユーザー権限を指定することはできません。

### [管理コンソール \(MMC\) で異なるユーザーとしてスキャンを実行する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[タスク] タブを選択します。
4. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
5. タスクのプロパティウィンドウで、[アカウント] セクションを選択します。
6. スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。
7. 変更内容を保存します。

### [Web コンソールまたはクラウドコンソールで異なるユーザーとしてスキャンを実行する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. スキャンタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
3. **[設定]** タブを選択します。
4. **[アカウント]** で **[設定]** をクリックします。
5. スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。
6. 変更内容を保存します。

### **製品インターフェイスで異なるユーザーとしてスキャンを実行する方法**

1. メインウィンドウで、**[タスク]** セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙) をクリックします。
3. **[詳細設定]** → **[次のユーザーで実行]** をクリックします。
4. 表示されるウィンドウで、スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。
5. 変更内容を保存します。

スキャンタスクが表示されない場合は、管理者により[ポリシー内でローカルタスクの使用が禁止](#)されていることを意味します。

## スキャンの最適化

ファイルスキャンを最適化することができます。最適化することで、スキャン時間を短縮したり、Kaspersky Endpoint Security の処理速度を向上させたりすることができます。スキャンを最適化するには、新しいファイルと前回のスキャン以降に変更されたファイルのみをスキャンします。このモードは、簡易ファイルと複合ファイルの両方に適用されます。また、単一のファイルのスキャンする際の制限を設定することもできます。特定の期間が経過すると、ファイルは現在のスキャンから除外されます（アーカイブ、および複数のファイルを含むオブジェクトは除く）。

ウイルスやその他のマルウェアの隠蔽には、アーカイブやデータベースなどの複合ファイルに埋め込む技術が一般的に使用されています。このような方法で隠されているウイルスやその他のマルウェアを検知するためには、複合ファイルを解凍する必要がありますが、スキャンの速度が低下する場合があります。スキャンする複合ファイル種別を限定することで、スキャンを高速化できます。

また、iChecker テクノロジーと iSwift テクノロジーを有効にすることもできます。iChecker テクノロジーと iSwift テクノロジーを使用すると、前回スキャンを実行してから変更されていないファイルがスキャンから除外されるため、ファイルのスキャン速度を最適化することができます。

### **管理コンソール (MMC) でスキャンを最適化する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [タスク] タブを選択します。
4. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。  
必要に応じて、 [ウイルススキャン](#) タスクを作成します。
5. コンピューターのプロパティウィンドウで、 [設定] セクションを選択します。
6. [セキュリティレベル] セクションの [設定] 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。
7. [スキャンの最適化] ブロックで、スキャンを設定します：
  - **新規作成または更新されたファイルのみスキャン**：新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。  
新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。
  - **スキャン時間が次を超えたファイルをスキップ**：単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。
8. [詳細] をクリックします。  
複合ファイルのスキャンの設定ウィンドウが表示されます。
9. [サイズ制限] で、 [大きな複合ファイルのスキャンしない] をオンにします。単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。

アーカイブから展開されるサイズの大きいファイルは、 [大きな複合ファイルのスキャンしない] がオンにされているかどうかに関係なくスキャンされます。

10. [OK] をクリックします。
11. [詳細] タブを選択します。
12. [スキャン技術] ブロックで、スキャンで使用する方法の名前の横にあるチェックボックスをオンにします。
  - **iSwift** 特定のファイルのスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

- iChecker特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル (EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR) にのみ適用する点です。

13. 変更内容を保存します。

## Web コンソールと Cloud コンソールでスキャンを最適化する方法

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. スキャンタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。必要に応じて、**ウイルススキャン**タスクを作成します。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威の検知時の処理]**、**[新規作成または更新されたファイルのみスキャン]** をオンにします。新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。  
新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。
5. **[大きな複合ファイルのスキャンしない]** をオンにします。単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。

アーカイブから展開されるサイズの大きいファイルは、**[大きな複合ファイルのスキャンしない]** がオンにされているかどうかに関係なくスキャンされます。

6. **[詳細設定]** で、**[スキャン時間が次を超えたファイルをスキップ]** をオンにします。単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。
7. 変更内容を保存します。

## 製品インターフェイスでスキャンを最適化する方法

1. メインウィンドウで、**[タスク]** セクションに移動します。
2. タスクのリストで、スキャンタスクを選択してボタン (⚙) をクリックします。
3. **[詳細設定]** をクリックします。
4. **[スキャンの最適化]** ブロックで、スキャンを設定します：
  - **新規作成または更新されたファイルのみスキャン**：新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。  
新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。
  - **スキャン時間が次を超えたファイルをスキップ**：単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。
5. **[サイズ制限]** で、**[大きな複合ファイルのスキャンしない]** をオンにします。単一のオブジェクトのスキャン時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のファイルスキャン処理が停止します。このオプションをオンにすると、スキャン時間を短縮できます。

アーカイブから展開されるサイズの大きいファイルは、**[大きな複合ファイルのスキャンしない]** がオンにされているかどうかに関係なくスキャンされます。

6. **[スキャン技術]** ブロックで、スキャンで使用する方法の名前の横にあるチェックボックスをオンにします。
  - **iSwift** 特定のファイルのスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
  - **iChecker** 特定のファイルのスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル (EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR) にのみ適用する点です。

7. 変更内容を保存します。

スキャンタスクが表示されない場合は、管理者により ポリシー内でローカルタスクの使用が禁止 されていることを意味します。



## 定義データベースとソフトウェアモジュールのアップデート

Kaspersky Endpoint Security の定義データベースとソフトウェアモジュールをアップデートすることにより、コンピューターを最新の方法で保護することができます。世界では、毎日、新しいウイルスと他の種類のマルウェアが出現しています。Kaspersky Endpoint Security データベースには、脅威に関する情報と脅威を無効化する方法が格納されています。脅威をすばやく検知するため、定義データベースとソフトウェアモジュールを定期的にアップデートしてください。

定期的なアップデートには、現在のライセンスが必要です。現在のライセンスがない場合、アップデートは一度だけ実行することができます。

Kaspersky Endpoint Security の主なアップデート元は、カスペルスキーのアップデートサーバーです。

カスペルスキーのアップデートサーバーからアップデートパッケージを正常にダウンロードするには、コンピューターをインターネットに接続する必要があります。既定では、インターネットの接続設定は自動的に行われます。プロキシサーバーを使用する場合は、設定を調整する必要があります。

アップデートは HTTPS プロトコルを経由してダウンロードされます。HTTPS プロトコル経由でダウンロードできない場合は、HTTP プロトコル経由でダウンロードすることもできます。

アップデートの実行中、次のオブジェクトがコンピューターにダウンロードされインストールされます：

- Kaspersky Endpoint Security の定義データベース：コンピューターの保護は、ウイルスおよびその他の脅威のシグネチャとそれらを無効化する方法についての情報を含む定義データベースを使用して実現されます。保護機能はこの情報を使用して、コンピューター上で感染したファイルを検索して無効化します。定義データベースには、定期的に、新しい脅威とそれに対処する方法のレコードが追加されます。このため、定義データベースを定期的にアップデートしてください。

Kaspersky Endpoint Security の定義データベースに加えて、アプリケーションのコンポーネントでネットワークトラフィックのインターセプトを可能にするネットワークドライバーがアップデートされます。

- ソフトウェアモジュール：Kaspersky Endpoint Security の定義データベースに加えて、ソフトウェアモジュールもアップデートできます。ソフトウェアモジュールをアップデートすることにより、Kaspersky Endpoint Security の脆弱性が修正されるとともに新しい機能が追加され、さらに既存の機能が強化されます。

アップデート中、コンピューター上のソフトウェアモジュールと定義データベースがアップデート元にある最新のバージョンと比較されます。現在の定義データベースとソフトウェアモジュールがそれぞれの最新バージョンと異なる場合、アップデート内の不足している部分がコンピューターにインストールされます。

コンテキストヘルプファイルは、ソフトウェアモジュールのアップデートとともにアップデートできます。

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、アップデートパッケージのサイズが大きくなり、インターネットトラフィックが最大で数十 MB まで増加することがあります。

Kaspersky Endpoint Security の定義データベースに関する情報は、メインウィンドウまたは通知領域の本製品のアイコンの上にカーソルを置いた際に表示されるツールチップに表示されます。

アップデート結果、およびアップデートタスクの実行中に発生するイベントに関する情報が [Kaspersky Endpoint Security のレポートに記録されます](#)。

## データベースと製品モジュールのアップデートシナリオ

Kaspersky Endpoint Security の定義データベースとソフトウェアモジュールをアップデートすることにより、コンピューターを最新の方法で保護することができます。世界では、毎日、新しいウイルスと他の種類のマルウェアが出現しています。Kaspersky Endpoint Security データベースには、脅威に関する情報と脅威を無効化する方法が格納されています。脅威をすばやく検知するため、定義データベースとソフトウェアモジュールを定期的にアップデートしてください。

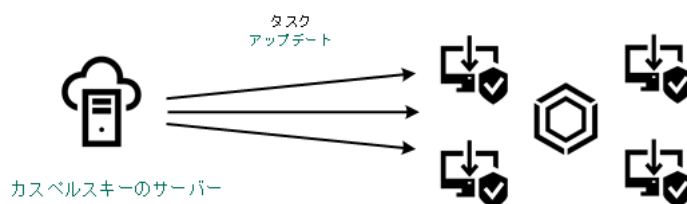
ユーザーのコンピューター上で次のオブジェクトがアップデートされます。

- 定義データベース：定義データベースには、マルウェアを識別するシグネチャのデータベース、ネットワーク攻撃の説明、悪意のある Web サイトおよびフィッシングサイトの URL のデータベースと、バナーのデータベース、スパムのデータベースなどのデータが含まれています。
- ソフトウェアモジュール：ソフトウェアモジュールのアップデートは、製品に含まれる脆弱性の解決とコンピューターの保護技術の強化のために実施されます。モジュールのアップデートにより、製品機能の動作が変更されたり、新機能が追加される場合があります。

Kaspersky Endpoint Security では、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方法として、次の方法をサポートしています：

- カスペルスキーのサーバーからアップデートを実行

カスペルスキーのアップデートサーバーは世界中のさまざまな国に設置されています。これにより、アップデート処理を高い信頼度で実行できます。あるサーバーからアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を次のサーバーに切り替えます。



カスペルスキーのサーバーからアップデートを実行

- 一元的なアップデート

一元的なアップデートを使用すると、ネットワーク外部とのインターネットトラフィック量を減らすことができ、なおかつアップデートの監視が容易になります。

一元的なアップデートでは次の手順を実行します。

1. 組織ネットワーク内のリポジトリにアップデートパッケージをダウンロードします。

アップデートパッケージは、管理サーバーの「管理サーバーのリポジトリへのアップデートのダウンロード」タスクを使用してリポジトリにダウンロードされます。

2. アップデートパッケージを共有フォルダーにダウンロードします（必要ない場合は省略可能な手順）。

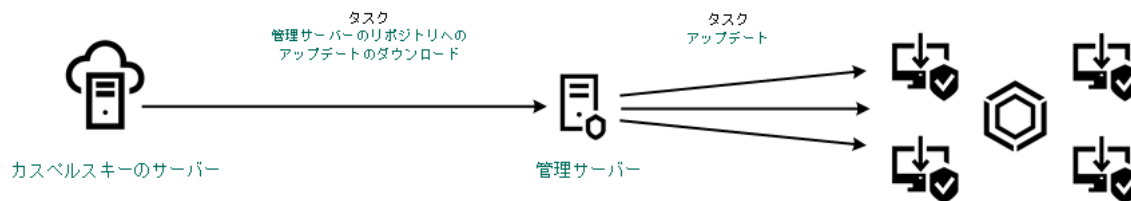
次の方法を使用して共有フォルダーにアップデートパッケージをダウンロードできます。

- Kaspersky Endpoint Security の [アップデート] タスクを使用する。このタスクは、企業のローカルネットワーク内のコンピューター 1 台を対象とします。
- Kaspersky Update Utility を使用する。Kaspersky Update Utility の使用について詳しくは、[カスペルスキーのナレッジベース](#)を参照してください。

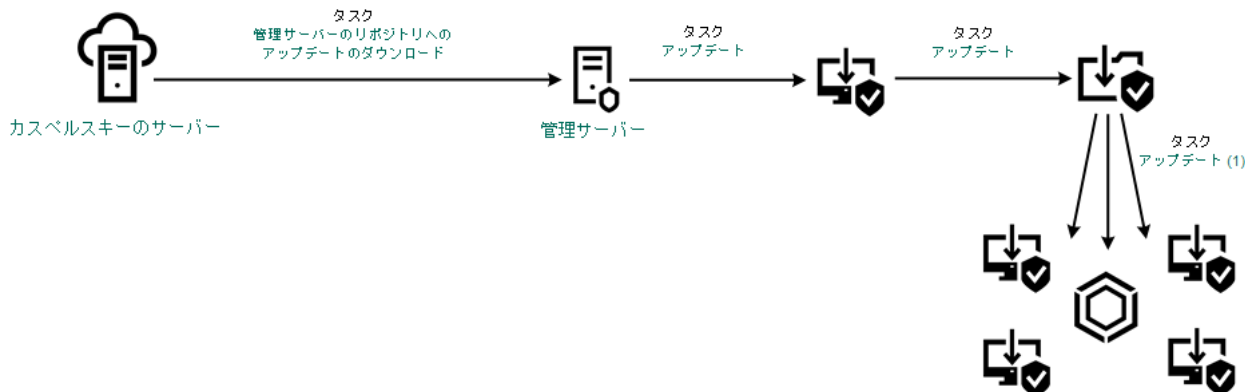
3. クライアントコンピューターにアップデートパッケージを配布します。



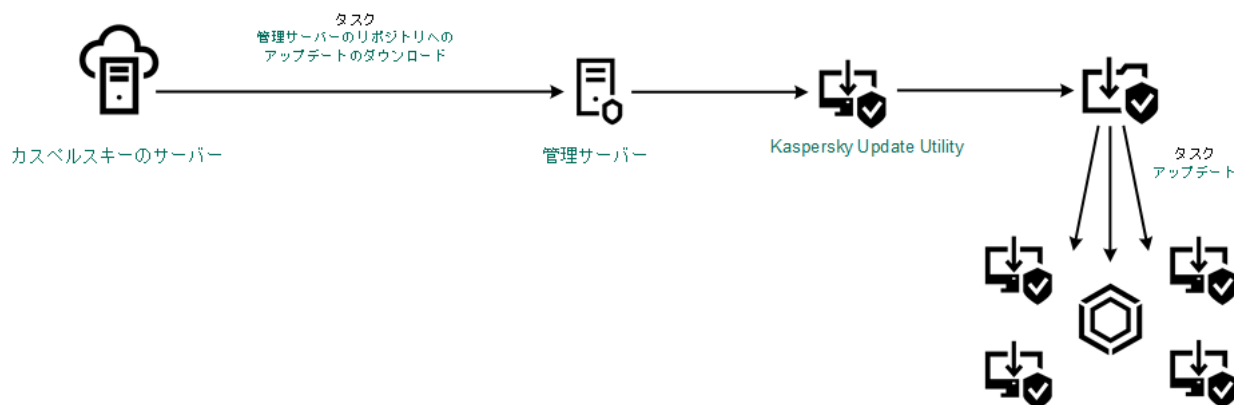
アップデートパッケージは、Kaspersky Endpoint Security の [アップデート] タスクを使用して配布されます。管理グループごとに、個数の制限なくアップデートタスクを作成できます。



サーバーリポジトリからアップデート



共有フォルダーからアップデート



Kaspersky Update Utility を使用してのアップデート

Web コンソールの場合、アップデート元の既定のリストには Kaspersky Security Center 管理サーバーとカスペルスキーのアップデートサーバーが含まれています。Kaspersky Security Center Cloud コンソールの場合、アップデート元の既定のリストにはディストリビューションポイントとカスペルスキーのアップデートサーバーが含まれています。ディストリビューションポイントについて詳しくは、*Kaspersky Security Center Cloud* コンソールのヘルプを参照してください。リストに他のアップデート元を追加できます。アップデート元には、HTTP/FTP サーバーと共有フォルダーを指定できます。あるアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を次のアップデート元に切り替えます。

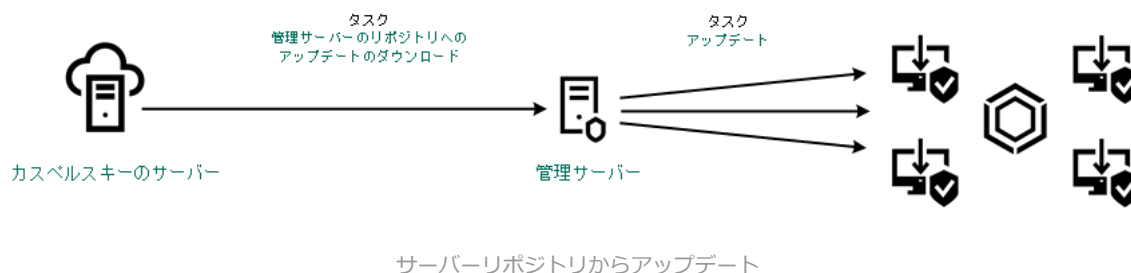
アップデートは通常のネットワークプロトコルを使用してカスペルスキーのアップデートサーバーまたはその他の FTP サーバーか HTTP サーバーからダウンロードされます。アップデート元へのアクセスにプロキシサーバーへの接続が必要になった場合、[Kaspersky Endpoint Security のポリシー設定でプロキシサーバー設定を指定します](#)。

## サーバーリポジトリからアップデート

インターネットトラフィックの増加を抑えるために、ローカルエリアネットワーク上のコンピューターがサーバーリポジトリからアップデートを受け取るように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設定できます。これを行うには、Kaspersky Security Center がカスペルスキーのアップデートサーバーからリポジトリ（FTP サーバー、HTTP サーバー、ネットワークフォルダー、ローカルフォルダーのいずれか）にアップデートパッケージをダウンロードする必要があります。ローカルエリアネットワーク上のコンピューターは、アップデートパッケージを該当するサーバーリポジトリから取得できるようになります。

サーバーリポジトリから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取得するように設定するには、次の手順を実行します：

1. 管理サーバーのリポジトリにアップデートをダウンロードするタスクを設定します（「管理サーバーのリポジトリへのアップデートのダウンロード」タスク）。
2. 指定したサーバーリポジトリからローカルエリアネットワーク上のコンピューターに定義データベースとソフトウェアモジュールのアップデートを実行するための設定（「アップデート」タスク）を行います。



サーバーリポジトリへのアップデートパッケージのダウンロードを設定するには：

1. Web コンソールのメインウィンドウで、**「デバイス」** → **「タスク」** の順に選択します。  
タスクのリストが表示されます。
2. **「管理サーバーのリポジトリへのアップデートのダウンロード」** タスクを選択します。  
タスクのプロパティウィンドウが表示されます。  
「管理サーバーのリポジトリへのアップデートのダウンロード」タスクは、Kaspersky Security Center Web コンソールのクイックスタートウィザードで自動的に作成されます。また、このタスクは1つしか作成できません。
3. **「アプリケーション設定」** タブを選択します。
4. **「その他の設定」** セクションで **「設定」** をクリックします。
5. **「アップデート保存先フォルダー」** で、Kaspersky Security Center がカスペルスキーのアップデートサーバーから取得したアップデートパッケージをコピーする保存先として FTP サーバー、HTTP サーバー、ネットワークフォルダー、ローカルフォルダーのいずれかのアドレスを指定します。

アップデート元について次のパス形式が使用されます：

- FTP サーバーまたは HTTP サーバーの場合は、その Web アドレスまたは IP アドレスを入力します。  
例：http://dn1-01.geo.kaspersky.com/ または 93.191.13.103  
FTP サーバーの場合は、認証設定をアドレスに含めるかたちで次の形式で指定できます：ftp://<ユーザー名>:<パスワード>@<ホスト>:<ポート>
- ネットワークフォルダーの場合は、UNC パスを入力します。  
例：\\ Server\Share\Update distribution
- ローカルフォルダーの場合は、フォルダーへの完全パスを入力します。

例 : C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\

6. 変更内容を保存します。

指定したサーバー保管領域からの *Kaspersky Endpoint Security* のアップデートを設定するには :

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. *Kaspersky Endpoint Security* の**アップデート**タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。  
アップデートタスクは、*Kaspersky Security Center* のクイックスタートウィザードで自動的に作成されます。アップデートタスクを作成するには、ウィザードの実行中に、*Kaspersky Endpoint Security for Windows* の Web プラグインをインストールすることを選択します。
3. **[アプリケーション設定]** タブ - **[ローカルモード]** を選択します。
4. アップデート元のリストで、**[追加]** をクリックします。
5. **[ソース]** で、*Kaspersky Security Center* がカスペルスキーのアップデートサーバーから取得したアップデートパッケージをコピーする保存先となっている FTP サーバー、HTTP サーバー、ネットワークフォルダー、またはローカルフォルダーのアドレスを指定します。

アップデート元のアドレスは、アップデートのダウンロード先となるサーバー保管領域を指定するときに **[アップデート保存先フォルダー]** に入力したアドレス（先述した手順を参照）と一致する必要があります。

6. **[ステータス]** セクションで **[有効]** をオンにします。
  7. **[OK]** をクリックします。
  8. 必要に応じて、**[上へ]** と **[下へ]** でアップデート元の優先順位を編集します。
  9. 変更内容を保存します。
- 1番上で指定したアップデート元からアップデートを実行できない場合、*Kaspersky Endpoint Security* はアップデート元を自動的に次のアップデート元に切り替えます。

## 共有フォルダーからアップデート

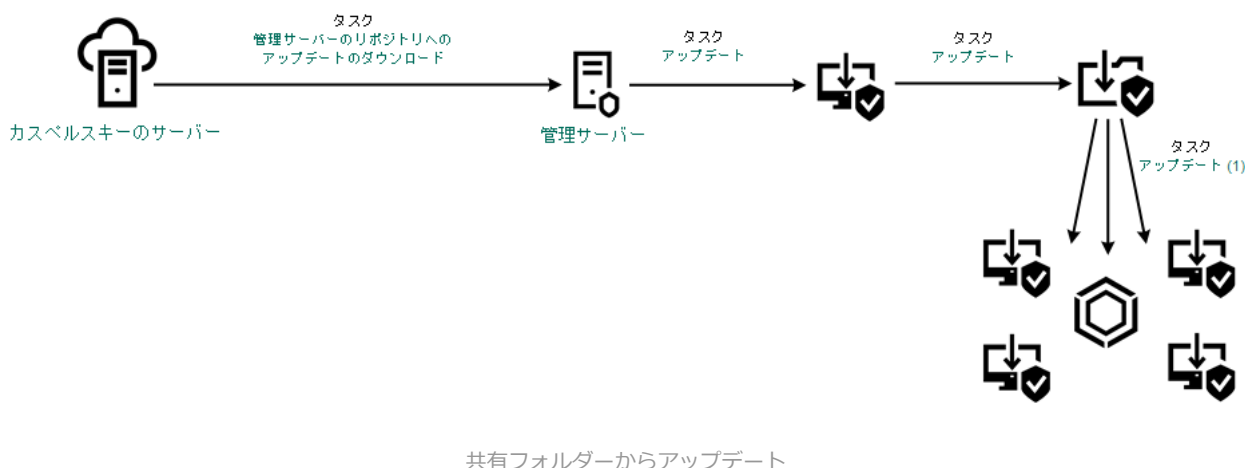
インターネットトラフィックの増加を抑えるために、ローカルエリアネットワーク上のコンピューターが共有フォルダーからアップデートを受け取るように定義データベースとソフトウェアモジュールのアップデートを設定できます。これを行うには、ローカルエリアネットワーク上のいずれかのコンピューターが *Kaspersky Security Center* の管理サーバーまたはカスペルスキーのアップデートサーバーからアップデートパッケージを取得し、取得したアップデートパッケージを共有フォルダーにコピーする必要があります。ローカルエリアネットワーク上のその他のコンピューターは、アップデートパッケージを共有フォルダーから取得できるようになります。

共有フォルダーから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取得するように設定するには、次の手順を実行します :

1. [サーバーリポジトリからの定義データベースと製品モジュールのアップデートを設定します。](#)

2. 企業 LAN 上のいずれかのコンピューターで、アップデートパッケージの共有フォルダーへのコピーを有効にします（下の手順を参照）。
3. 指定した共有フォルダーから企業 LAN 上の残りのコンピューターに定義データベースとソフトウェアモジュールのアップデートを実行するための設定を行います（下の手順を参照）。

共有フォルダーにアップデートパッケージをコピーする Kaspersky Endpoint Security アプリケーションのバージョンおよび言語は、共有フォルダーからデータベースをアップデートするアプリケーションのバージョンと言語と一致している必要があります。アプリケーションのバージョンが一致しない場合、データベースのアップデートはエラーで終了する可能性があります。



アップデートパッケージの共有フォルダーへのコピーを有効にするには：

1. Web コンソールのメインウィンドウで、[デバイス] → [タスク] の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Endpoint Security の**アップデート**タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。  
アップデートタスクは、Kaspersky Security Center のクイックスタートウィザードで自動的に作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows の Web プラグインをインストールすることを選択します。
3. [アプリケーション設定] タブ - [ローカルモード] を選択します。
4. アップデート元を設定します。  
アップデート元は、カスペルスキーのアップデートサーバー、Kaspersky Security Center の管理サーバー、その他の FTP サーバーまたは HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。
5. [アップデートをフォルダーにコピー] をオンにします。
6. [パス] フィールドに、共有フォルダーへの UNC パスを入力します（例：\\Server\Share\Update distribution）。  
フィールドが空白の場合、Kaspersky Endpoint Security はアップデートパッケージをフォルダー C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\ にコピーします。
7. 変更内容を保存します。

このアップデートタスクは、その他のコンピューターのアップデート元として動作するコンピューターに割り当てる必要があります。

共有フォルダーからのアップデートを設定するには：

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **[タスク種別]** で、**[アップデート]** を選択します。
  - c. **[タスク名]** に「共有フォルダーからのアップデート」などの簡潔な名前を付けます。
  - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。

このアップデートタスクは、アップデート元として動作するコンピューター以外の、ローカルエリアネットワーク内のコンピューターに割り当てる必要があります。

4. タスク範囲の指定方法に応じて、対象デバイスを選択し、**[次へ]** をクリックします。
5. **[終了]** をクリックして、ウィザードを終了します。  
タスクのテーブルに新しいタスクが表示されます。
6. 新しく作成した **[アップデート]** タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
7. **[アプリケーション設定]** セクションを選択します。
8. **[ローカルモード]** タブを選択します。
9. **[アップデート元]** セクションで、**[追加]** をクリックします。
10. **[ソース]** に共有フォルダーのパスを入力します。

ソースアドレスは、アップデートパッケージのコピー先となる共有フォルダーを指定するときに **[パス]** に入力したアドレス（先述した手順を参照）と一致する必要があります。

11. **[OK]** をクリックします。
12. 必要に応じて、**[上へ]** と **[下へ]** でアップデート元の優先順位を編集します。
13. 変更内容を保存します。

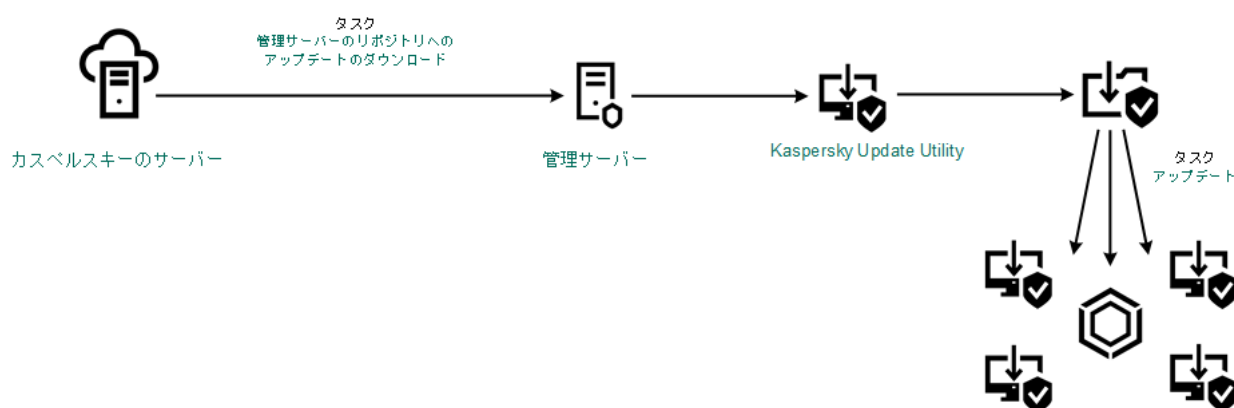
## Kaspersky Update Utility を使用してのアップデート

インターネットトラフィックの増加を抑えるために、Kaspersky Update Utility を使用して共有フォルダーにアップデートを配置し、ローカルエリアネットワーク上のコンピューターが共有フォルダーからアップデートを受け取るように、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設定できます。これを行うには、ローカルエリアネットワーク上のいずれかのコンピューターが Kaspersky Security Center の管理サーバーまたはカスペルスキーのアップデートサーバーからアップデートパッケージを取得し、取得したアップデートパッケージを Kaspersky Update Utility を使用して共有フォルダーにコピーする必要があります。ローカルエリアネットワーク上のその他のコンピューターは、アップデートパッケージを共有フォルダーから取得できるようになります。

共有フォルダーから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取得するように設定するには、次の手順を実行します：

1. [サーバーリポジトリからの定義データベースと製品モジュールのアップデートを設定します。](#)
2. ローカルエリアネットワーク内のいずれか1台のコンピューターに Kaspersky Update Utility をインストールします。
3. アップデートパッケージの共有フォルダーへのコピーを、Kaspersky Update Utility の設定で指定します。
4. 指定した共有フォルダーからローカルエリアネットワーク上の残りのコンピューターに定義データベースとソフトウェアモジュールのアップデートを実行するための設定を行います。

共有フォルダーにアップデートパッケージをコピーする Kaspersky Endpoint Security アプリケーションのバージョンおよび言語は、共有フォルダーからデータベースをアップデートするアプリケーションのバージョンと言語と一致している必要があります。アプリケーションのバージョンが一致しない場合、データベースのアップデートはエラーで終了する可能性があります。



Kaspersky Update Utility を使用してのアップデート

Kaspersky Update Utility の配布パッケージは、[カスペルスキーのテクニカルサポートサイト](#) からダウンロードできます。Kaspersky Update Utility のインストールが完了したら、アップデート元（たとえば、管理サーバーのリポジトリなど）と、アップデートパッケージのコピー先となる共有フォルダーをそれぞれ選択します。Kaspersky Update Utility の使用について詳しくは、[カスペルスキーのナレッジベース](#) を参照してください。

共有フォルダーからのアップデートを設定するには：

1. Web コンソールのメインウィンドウで、[デバイス] → [タスク] の順に選択します。  
タスクのリストが表示されます。



2. Kaspersky Endpoint Security の**アップデート**タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。  
アップデートタスクは、Kaspersky Security Center のクイックスタートウィザードで自動的に作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows の Web プラグインをインストールすることを選択します。
3. [**アプリケーション設定**] タブ - [**ローカルモード**] を選択します。
4. アップデート元のリストで、**[追加]** をクリックします。
5. [**ソース**] フィールドに、共有フォルダーへの UNC パスを入力します（例：\\Server\Share\Update distribution）。

ソースアドレスは、Kaspersky Update Utility の設定で指定したアドレスと一致する必要があります。

6. [**OK**] をクリックします。
7. 必要に応じて、**[上へ]** と **[下へ]** でアップデート元の優先順位を編集します。
8. 変更内容を保存します。

## モバイルモードでのアップデート

モバイルモードとは、コンピューターを組織ネットワーク外で使用しているとき（オフラインのコンピューター）の Kaspersky Endpoint Security の操作モードです。オフラインのコンピューターとモバイルユーザーについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。

組織ネットワーク外のオフラインコンピューターは、管理サーバーに接続して定義データベースとソフトウェアモジュールのアップデートを行うことができません。既定では、カスペルスキーのアップデートサーバーのみが、モバイルモードで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アップデート元として使用されます。インターネット接続でプロキシサーバーを使用するかどうかは[モバイルユーザーポリシー](#)で指定されます。モバイルユーザーポリシーは別途作成する必要があります。Kaspersky Endpoint Security がモバイルモードに切り替わると、アップデートタスクが2時間ごとに起動されます。

モバイルモードでのアップデート設定を編集するには：

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Endpoint Security の**アップデート**タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。  
アップデートタスクは、Kaspersky Security Center のクイックスタートウィザードで自動的に作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows の Web プラグインをインストールすることを選択します。  
**[アプリケーション設定]** タブ - **[モバイルモード]** を選択します。
3. アップデート元を設定します。アップデート元は、カスペルスキーのアップデートサーバー、その他の FTP サーバーおよび HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。
4. 変更内容を保存します。

指定した設定に応じて、クライアントコンピューターがモバイルモードに切り替わったときも定義データベースとソフトウェアモジュールがアップデートされます。

## アップデートタスクの開始と停止

Kaspersky Endpoint Security アップデートタスクは、選択したアップデートタスクの実行方法にかかわらず、いつでも開始または停止することができます。

アップデートタスクを開始または停止するには、次の手順を実行します：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. **[定義データベースと機能のアップデート]** ブロックで、アップデートを開始する場合は **[アップデート]** をクリックします。

Kaspersky Endpoint Security は製品モジュールおよび定義データベースのアップデートを開始します。タスクの進捗、ダウンロードされたファイルおよびアップデート元が表示されます。**[アップデートの停止]** ボタンを押すことでいつでもタスクを停止することができます。

[簡略化したアプリケーションインターフェイス](#)が表示されている場合にアップデートタスクを開始または停止するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューの **[タスク]** で、以下のいずれかを実行します：
  - 実行されていないアップデートタスクを選択して開始する
  - 実行中のアップデートタスクを選択して停止する
  - 一時停止中のアップデートタスクを選択して再開する

## 別のユーザーアカウントの権限でのアップデートタスクの開始

既定では、Kaspersky Endpoint Security のアップデートタスクは、オペレーティングシステムへのログインに使用したアカウントを持つユーザーの代わりに開始されます。ただし、Kaspersky Endpoint Security は、必要な権利がないことが原因でユーザーがアクセスできないアップデート元（アップデートパッケージを含む共有フォルダーからアップデートを実行する場合など）やプロキシサーバーの認証が設定されていないアップデート元からアップデートされる場合があります。Kaspersky Endpoint Security の設定でアップデートの権限を持つユーザーを指定して、そのユーザーアカウントで Kaspersky Endpoint Security のアップデートタスクを開始できます。

別のユーザーアカウントでアップデートタスクを開始するには：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. タスクのリストが表示されます。アップデートタスクを選択してボタン (⚙) をクリックします。
3. **[定義データベースをアップデートするユーザー]** をクリックします。
4. 表示されるウィンドウで、**[他のユーザー]** を選択します。

5. アップデート元にアクセスするために必要な権限をもつユーザーのアカウント認証情報を入力します。
6. 変更内容を保存します。

## アップデートタスクの実行方法の選択

何らかの理由（コンピューターの電源が入っていないなど）でアップデートタスクを実行できない場合、スキップされたタスクが実行可能になると同時に自動的に開始されるように設定することができます。

アップデートタスクの実行方法に **「スケジュールで指定」** を選択した場合、および Kaspersky Endpoint Security の開始時間とアップデートタスクの開始スケジュールが一致する場合は、製品が開始されるまでアップデートタスクの実行を延期することができます。アップデートタスクは、Kaspersky Endpoint Security の開始後、指定した期間が経過した後にのみ実行できます。

アップデートタスクの実行方法を選択するには：

1. メインウィンドウで、 **「アップデート」** をクリックします。
2. タスクのリストが表示されます。アップデートタスクを選択してボタン (⚙️) をクリックします。
3. **「定義データベースのアップデートのスケジュール」** をクリックします。
4. 表示されたウィンドウで、アップデートタスクの実行モードを選択します。
  - Kaspersky Endpoint Security で、アップデートパッケージがアップデート元から使用できるかどうかに応じてアップデートタスクを実行するには、 **「自動開始」** を選択します。Kaspersky Endpoint Security によるアップデートパッケージの確認の頻度は、ウイルスの発生中には高くなり、そうでないときには低くなります。
  - アップデートタスクを手動で開始するには、 **「手動開始」** を選択します。
  - アップデートタスクの実行スケジュールを設定するには、別のオプションを選択します。アップデートタスクを開始する詳細について設定します：
    - **「本製品の起動からタスク開始までの時間」** に、Kaspersky Endpoint Security 開始後、アップデートタスクを開始するまでの期間を指定します。
    - 実行されなかったタスクを機会のあり次第実行するには、 **「コンピューターがオフの場合、スケジュールされたスキャンを翌日に実行する」** をオンにします。
5. 変更内容を保存します。

## Adding an update source

An *update source* is a resource that contains updates for databases and application modules of Kaspersky Endpoint Security.


Update sources include the Kaspersky Security Center server, Kaspersky update servers, and network or local folders.

The default list of update sources includes Kaspersky Security Center and Kaspersky update servers. You can add other update sources to the list. You can specify HTTP/FTP servers and shared folders as update sources.

Kaspersky Endpoint Security does not support updates from HTTPS servers unless they are Kaspersky's update servers.

If several resources are selected as update sources, Kaspersky Endpoint Security tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source.

*To add an update source:*

1. In the main application window, go to the **Update** section.
2. This opens the task list; select the update task and click .
3. Click the **Select update sources** button.
4. In the window, click the **Add** button.
5. In the window that opens, specify the address of the FTP or HTTP server, network folder or local folder that contains the update package.

The following path format is used for update source:

- For an FTP or HTTP server, enter its web address or IP address.  
For example, `http://dn1-01.geo.kaspersky.com/` or `93.191.13.103`.  
For an FTP server, you can specify the authentication settings within the address in the following format:  
`ftp://<user name>:<password>@<node>:<port>`.
- For a network folder, enter the UNC path.  
For example, `\\ Server\Share\Update distribution`.
- For a local folder, enter the full path to that folder.  
For example, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Click the **Select** button.
7. Configure the priorities of update sources by using the **Up** and **Down** buttons.
8. Save your changes.

## 共有フォルダーからのアップデートの設定

インターネットトラフィックの増加を抑えるために、ローカルエリアネットワーク上のコンピューターが共有フォルダーからアップデートを受け取るように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設定できます。これを行うには、ローカルエリアネットワーク上のいずれかのコンピューターが Kaspersky Security Center の管理サーバーまたはカスペルスキーのアップデートサーバーからアップデートパッケージを取得し、取得したアップデートパッケージを共有フォルダーにコピーする必要があります。ローカルエリアネットワーク上のその他のコンピューターは、アップデートパッケージを共有フォルダーから取得できるようになります。

共有フォルダーから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取得するように設定するには、次の手順を実行します：

1. ローカルエリアネットワーク上のいずれかのコンピューターで、アップデートパッケージの共有フォルダーへのコピーを有効にします。
2. 指定した共有フォルダーからローカルエリアネットワーク上の残りのコンピューターに定義データベースとソフトウェアモジュールのアップデートを実行するための設定を行います。

アップデートパッケージの共有フォルダーへのコピーを有効にするには：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. タスクのリストが表示されます。アップデートタスクを選択してボタン (⚙) をクリックします。
3. **[アップデートの配信]** ブロックで、**[アップデートをフォルダーにコピー]** をオンにします。
4. 共有フォルダーへの UNC パスを入力します (例： \\Server\Share\Update distribution)。
5. 変更内容を保存します。

共有フォルダーからのアップデートを設定するには：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. タスクのリストが表示されます。アップデートタスクを選択してボタン (⚙) をクリックします。
3. **[アップデート元の選択]** を選択します。
4. **[追加]** をクリックします。
5. 表示されたウィンドウで、共有フォルダーへのパスを入力します。

ソースアドレスは、アップデートパッケージのコピー先となる共有フォルダーを指定するときに入力したアドレス (先述した手順を参照) と一致する必要があります。

6. **[選択]** をクリックします。
7. 必要に応じて、**[上へ]** と **[下へ]** でアップデート元の優先順位を編集します。
8. 変更内容を保存します。

## 製品モジュールのアップデート

製品モジュールのアップデートには、エラーの修正、パフォーマンスの向上、新機能の追加が含まれます。新しい製品モジュールのアップデートが利用可能になると、これらのアップデートのインストールを確認する必要があります。製品のインターフェイスまたは Kaspersky Security Center のどちらからでも製品モジュールのアップデートのインストールの確認ができます。アップデートが利用可能になると、Kaspersky Endpoint Security のメインウィンドウの次の通知が表示されます：重要なアップデート (📢) または緊急アップデート (🔔) ソフトウェアモジュールのアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。製品モジュールのアップデートおよび Kaspersky Security Center のアップデートの確認に関する記録については、[Kaspersky Security Center のヘルプ](#) を参照してください。

製品のアップデートのインストール後、コンピューターの再起動が必要になることがあります。

ソフトウェアモジュールのアップデートを設定するには：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. タスクのリストが表示されます。アップデートタスクを選択してボタン (⚙️) をクリックします。
3. **[製品機能のダウンロードおよびアップデートのインストール]** ブロックで、**[製品機能のアップデートをダウンロード]** を選択します。
4. インストールする製品機能のアップデートを選択します。
  - **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、ソフトウェアモジュールのアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべてのソフトウェアモジュールは、インストールがアプリケーションインターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。
  - **承認済みのアップデートのみをインストール**：このオプションをオンにすると、ソフトウェアモジュールのアップデートが利用できるようになると、インストールがアプリケーションインターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。
5. 変更内容を保存します。

## プロキシサーバーを使用する際のアップデート

定義データベースおよびソフトウェアモジュールのアップデートのアップデート元からのダウンロード用に、必要に応じてプロキシサーバー設定を指定できます。アップデート元が複数ある場合、すべてのアップデート元にプロキシサーバー設定が適用されます。一部のアップデート元ではプロキシサーバーを使用する必要がない場合、ポリシーのプロパティでプロキシサーバーの使用を無効化できます。Kaspersky Endpoint Security は、プロキシサーバーを使用して、Kaspersky Security Network およびアクティブセッションサーバーにアクセスします。

アップデート元へのプロキシサーバー経由の接続を設定するには：

1. Web コンソールのメインウィンドウで、⚙️ をクリックします。  
管理サーバーのプロパティウィンドウが表示されます。
2. **[インターネットアクセスの設定]** に移動します。
3. **[プロキシサーバーを使用する]** をオンにします。




4. プロキシサーバーのアドレスと認証設定（ユーザー名とパスワード）を入力してプロキシサーバーの接続設定を指定します。

5. 変更内容を保存します。

特定の管理グループでプロキシサーバーの使用を無効にするには：

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. プロキシサーバーの使用を無効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [全般設定] - [ネットワークの設定] を選択します。
5. [プロキシサーバーの設定] で、[ローカルアドレスにはプロキシサーバーを使用しない] を選択します。
6. 変更内容を保存します。

製品インターフェイスでプロキシサーバーを設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[詳細設定] → [ネットワーク設定] の順に選択します。
3. [プロキシサーバー] で、[プロキシサーバーの設定] をクリックします。
4. 表示されたウィンドウで、プロキシサーバーのアドレスを特定する方法を選択します：
  - **プロキシサーバー設定を自動的に検出する**  
既定ではこのオプションが選択されます。Kaspersky Endpoint Security はオペレーティングシステムの設定で定義されているプロキシサーバーを使用します
  - **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した場合は、プロキシサーバーへの接続の設定（プロキシサーバーのアドレスおよびポート）を指定する必要があります。
5. プロキシサーバーの認証を有効にする場合は、[プロキシサーバー認証を使用する] を選択し、ユーザーアカウントの認証情報を入力してください。
6. 共有フォルダーから [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](#) ときにプロキシサーバーの使用を無効にする場合は、**ローカルアドレスにはプロキシサーバーを使用しない** チェックボックスをオンにします。
7. 変更内容を保存します。

Kaspersky Endpoint Security はアプリケーションモジュールおよび定義データベースのアップデートのダウンロードにプロキシサーバーを使用します。Kaspersky Endpoint Security は、プロキシサーバーを使用して、KSN サーバーおよびカスペルスキーのアクティベーションサーバーにアクセスします。プロキシサーバーで認証情報が必要で、ユーザーアカウントの認証情報が提供されていないか正しくなかった場合、Kaspersky Endpoint Security はユーザー名とパスワードを入力するよう促します。

## 前回のアップデートのロールバック

定義データベースとソフトウェアモジュールが初めてアップデートされてから、定義データベースとソフトウェアモジュールを以前のバージョンにロールバックする機能が有効になります。

ユーザーがアップデートプロセスを開始するごとに、Kaspersky Endpoint Security によって現在の定義データベースとソフトウェアモジュールのバックアップコピーが作成されます。これにより、必要に応じて、定義データベースとソフトウェアモジュールを前のバージョンにロールバックすることができます。前回のアップデートへのロールバックは、新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。

前回のアップデートにロールバックするには：

1. メインウィンドウで、**[アップデート]** をクリックします。
2. **[以前の定義データベースのバージョンにロールバック]** ブロックで、**[ロールバック]** をクリックします。

Kaspersky Endpoint Security は定義データベースをアップデート前の状態に戻します。ロールバックの進捗、ダウンロードされたファイルおよびアップデート元が表示されます。**[アップデートの停止]** ボタンを押すことでいつでもタスクを停止することができます。

[簡略化したアプリケーションインターフェイス](#)が表示されている場合にロールバックタスクを開始または停止するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューの**[タスク]** で、以下のいずれかを実行します：
  - 実行されていないロールバックタスクを選択して開始します。
  - 実行中のロールバックタスクを選択して停止します。
  - 一時停止中のロールバックタスクを選択して再開します。

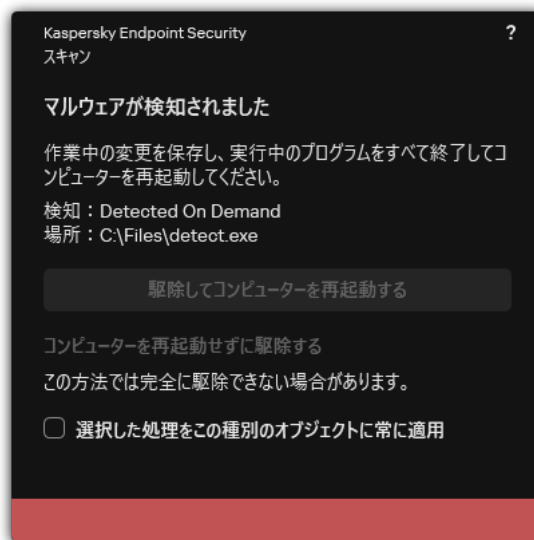
## アクティブな脅威に対する操作

Kaspersky Endpoint Security は、何らかの理由で処理されていないファイルに関する情報を記録します。この情報は、アクティブな脅威のリストにイベントの形式で記録されます。Kaspersky Endpoint Security は、特別な駆除技術を使用してアクティブな脅威を処理します。特別な駆除はワークステーションとサーバーに対して異なる動作をします。特別な駆除技術は、[ウイルススキャン](#)タスクの設定および[製品設定](#)で設定できます。

### ワークステーションにおけるアクティブな脅威の駆除

ワークステーションでアクティブな脅威を処理するには、製品設定で[特別な駆除技術を有効](#)にしてください。次に、[ウイルススキャン](#)タスクのプロパティで設定します。タスクのプロパティには **[すぐに特別な駆除を実行する]** チェックボックスがあります。オンにすると、Kaspersky Endpoint Security はユーザーに通知せずに駆除を実行します。駆除が完了すると、コンピューターは再起動されます。オフの場合、Kaspersky Endpoint Security はアクティブな脅威に関する通知を表示します（下の図を参照してください）。ファイルを処理せずにこの通知を閉じることはできません。

コンピューターに適用されているポリシーのプロパティで[特別な駆除が有効](#)になっている場合のみ、コンピューター上のウイルススキャンタスク中に特別な駆除が実行されます。



アクティブな脅威についての通知

### サーバーにおけるアクティブな脅威の駆除

サーバーでアクティブな脅威を処理するには、次の操作を行います：

- 製品設定で[特別な駆除技術を有効](#)にします。
- ウィルススキャンタスクのプロパティで **[すぐに特別な駆除を実行する]** を有効にします。

サーバー向けの Windows を実行しているコンピューターに Kaspersky Endpoint Security がインストールされている場合、Kaspersky Endpoint Security は通知を表示しません。そのため、ユーザーはアクティブな脅威を駆除する操作を選択することができません。脅威を駆除するには、製品設定で[特別な駆除技術を有効](#)にして、ウイルススキャンタスクのプロパティで **[すぐに特別な駆除を実行する]** を有効にする必要があります。その後ウイルススキャンタスクを開始します。

## アクティブな脅威の処理

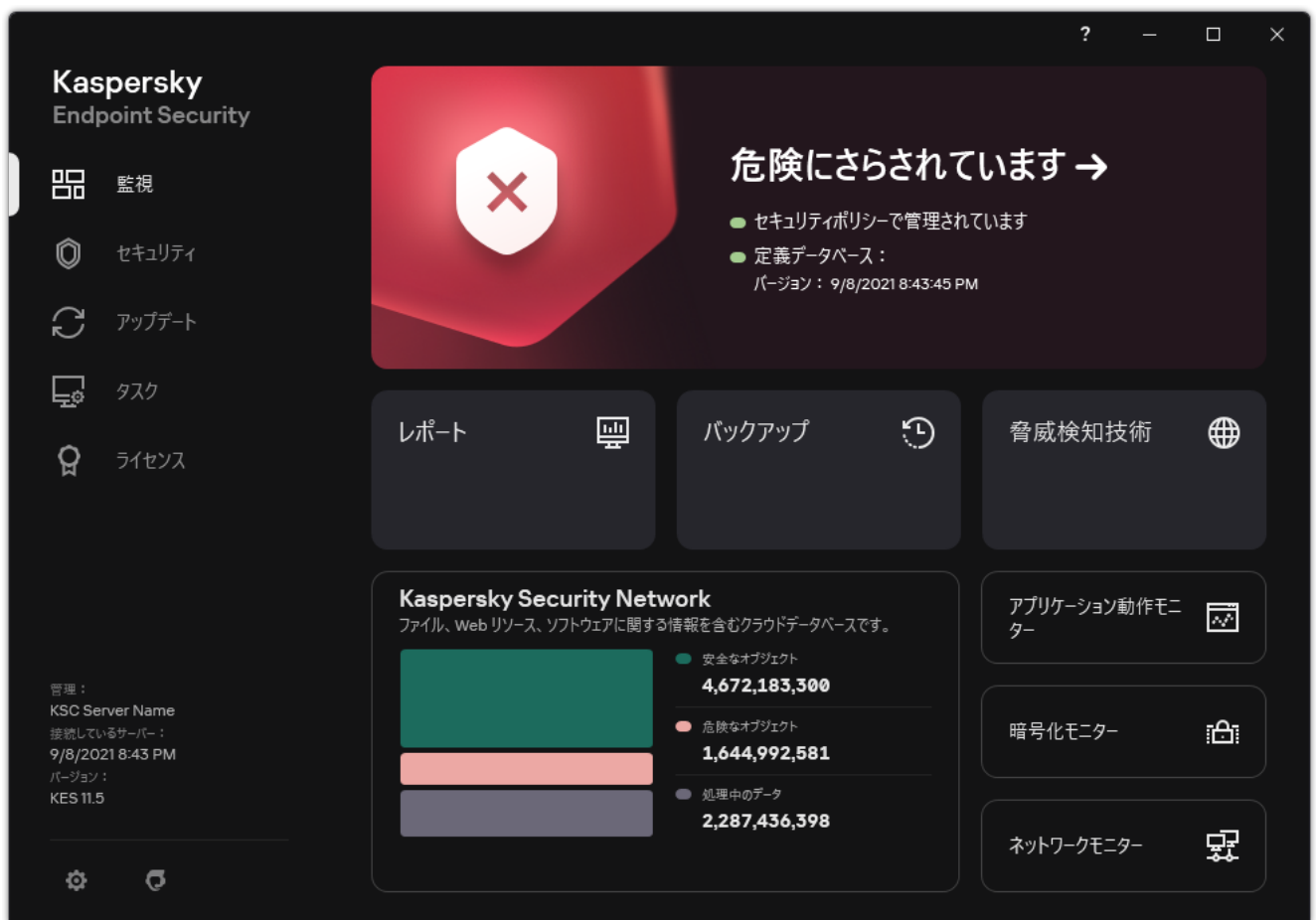
ウイルスなどの脅威の検知のためのコンピュートースキャンの際に、Kaspersky Endpoint Security が指定された製品設定に基づいてこのファイルに次のいずれかの処理を実行すると、感染したファイルは「処理済み」とみなされます：

- 駆除する
- 削除する
- 駆除できない場合は削除する

ウイルスなどの脅威の検知のためのコンピュートースキャンの際に、Kaspersky Endpoint Security が指定された製品設定に基づいて感染したファイルにいずれかの処理を試み、何らかの理由で失敗した場合、そのファイルがアクティブな脅威のリストに移動されます。

このようなケースは、次のような場合に発生します：

- スキャンされたファイルを使用できない場合。たとえば、スキャンされたファイルが、書き込み権限のないネットワークドライブやリムーバブルドライブに配置されているような場合です。
- スキャンタスクの【脅威の検知時の処理】セクションで【通知する】が選択されていて、感染したファイルに関する通知が表示された際に、ユーザーが【スキップ】を選択した場合。



脅威が検知された際のメインウィンドウ

アクティブな脅威を処理するには：

1. メインウィンドウで、【詳細】をクリックします。  
アクティブな脅威のリストが表示されます。

2. 処理するオブジェクトを選択します。

3. 脅威をどのように処理するか選択します：

- **解決**。このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。
- **スキップ**。このオプションを選択すると、Kaspersky Endpoint Security はアクティブな脅威のリストからこの項目を削除します。ほかにアクティブな脅威がない場合は、コンピューターのステータスは OK に変わります。オブジェクトが次に検知された場合は、Kaspersky Endpoint Security はアクティブな脅威のリストに新しい項目を追加します。
- **ファイルの場所を開く**。このオプションを選択すると、Kaspersky Endpoint Security はファイルマネージャーでオブジェクトのあるフォルダーを開きます。オブジェクトを手動で削除する、または保護範囲に含まれないフォルダーに移動することができます。
- **詳細**。このオプションを選択すると、Kaspersky Endpoint Security は[カスペルスキーのウイルス百科事典の Web サイト](#)を開きます。

# コンピューターの保護

## ファイル脅威対策

ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターのRAMに常駐します。このコンポーネントは、コンピューターのすべてのドライブと接続されたドライブのファイルをスキャンします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。


コンポーネントは、ユーザーまたはアプリケーションがアクセスしたファイルをスキャンします。悪意のあるファイルが検知された場合、Kaspersky Endpoint Security はファイル操作をブロックします。その後、ファイル脅威対策の設定に応じて、悪意のあるファイルを駆除または削除します。

コンテンツが OneDrive クラウドに保存されているファイルにアクセスしようとする時、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードしてスキャンします。

## ファイル脅威対策の有効化と無効化

既定では、ファイル脅威対策は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。ファイル脅威対策では、異なる設定の組み合わせを適用できます。アプリケーションに保存されるこれらの設定の組み合わせ（**高**、**推奨**、**低**）は、「セキュリティレベル」と呼ばれます。カスペルスキーのエキスパートが推奨する設定グループは、**[推奨]** セキュリティレベルです（下の表を参照）。セキュリティレベルは、事前に設定されているものから選択することも、手動で設定することもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

ファイル脅威対策を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイル脅威対策]** の順に選択します。
3. **[ファイル脅威対策]** トグルスイッチを使用して機能を有効または無効にします。
4. この機能を有効にした場合は **[セキュリティレベル]** セクションで次の操作を実行してください。
  - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：
  - **高**：このファイルセキュリティレベルを選択すると、ファイル脅威対策は開いたファイル、保存したファイル、実行されたファイルのすべてに対して最も厳しいコントロールを適用します。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているすべてのファイルの種類をスキャンします。また、アーカイブ、インストールパッケージ、OLE 埋め込みオブジェクトもスキャンします。
  - **推奨**：このセキュリティレベルはカスペルスキーが推奨するセキュリティレベルです。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の形式のファイル、OLE 埋め込みオブジェクトをスキャンします。アーカイブまたはインストールパッケージはスキャンしません。推奨されるセキュリティレベルの設定値は次の表を参照してください。



- **低**：このファイルセキュリティレベル設定では、スキャンの速度が最大になります。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されている、指定した拡張子のファイルのみをスキャンします。複合ファイルはスキャンしません。
- カスタムのセキュリティレベルを設定する場合は、**[詳細設定]** をクリックして、機能の設定を定義します。

ウィンドウ上部にある**[推奨のセキュリティレベルに戻す]** をクリックすると、事前設定されたセキュリティレベルを復元することができます。

## 5. 変更内容を保存します。

カスペルスキーが推奨するファイル脅威対策の設定値（推奨されるセキュリティレベル）

パラメータ	値	説明
ファイル種別	ファイル形式でファイルをスキャン	この設定を有効にした場合、Kaspersky Endpoint Security は <b>感染する可能性のあるファイルのみ</b> をスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。
ヒューリスティック分析	低	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。  悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
新規作成または更新されたファイルのみスキャン	有効	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
iSwift	有効	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker	有効	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。
Microsoft Office 形式のファイルのスキャン	有効	Microsoft Office 形式のファイルのスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。


スキャンモード	スマートモードでスキャン	オブジェクトに対する処理の分析に基づいて、オブジェクトをスキャンします。たとえば、Microsoft Office ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。
脅威の検知時の処理	駆除する。駆除できない場合は削除する	このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。

## ファイル脅威対策の自動的な一時停止

指定した時間、または指定したアプリケーションの使用中に、ファイル脅威対策が自動的に一時停止するよう設定できます。

ファイル脅威対策が他のアプリケーションと競合した場合、ファイル脅威対策が最も優先されます。機能の実行中に競合が発生した場合は、[カスペルスキーのテクニカルサポート](#)にお問い合わせください。サポート担当者が、ファイル脅威対策と他のアプリケーションが同時に作動できるように設定するお手伝いをします。


ファイル脅威対策の自動一時停止を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【ファイル脅威対策の一時停止】** ブロックで、**【ファイル脅威対策の一時停止】** をクリックします。
5. 表示されたウィンドウで、ファイル脅威対策の一時停止の設定を指定します：
  - a. ファイル脅威対策が自動で一時停止するスケジュールを設定します。
  - b. ファイル脅威対策が動作を一時停止するアプリケーションのリストを作成します。
6. 変更内容を保存します。

## 感染したファイルに対してファイル脅威対策が行う処理の変更

既定では、ファイル脅威対策は、検知した感染したファイルすべての駆除を自動的に試みます。駆除に失敗した場合は、ファイルを削除します。

感染したファイルに対してファイル脅威対策が行う処理を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイル脅威対策]** の順に選択します。
3. **[脅威の検知時の処理]** セクションで、必要なオプションを選択します。
  - **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。
  - **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除ができない場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
  - **ブロック**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。

感染したファイルを駆除または削除する前に、Kaspersky Endpoint Security は [ファイルを復元またはあとで駆除できた場合](#) に必要な場合によってバックアップファイルを作成します。

4. 変更内容を保存します。

## ファイル脅威対策の保護範囲の設定



保護範囲とは、このコンポーネントが有効な場合にスキャンされるオブジェクトを意味します。各コンポーネントの保護範囲には、それぞれ異なる特性があります。ファイル脅威対策の保護範囲のプロパティは、スキャン対象ファイルの場所と種別です。既定では、ファイル脅威対策のスキャン対象は、ハードディスク、リムーバブルドライブ、およびネットワークドライブから実行された [感染する可能性があるファイル](#) のみです。

スキャンするファイル種別を選択するときには、次の点に留意してください：

1. 特定の形式（TXT 形式など）の場合、その形式のファイルに悪意のあるコードが侵入し、その後有効化されるというケースはあまり発生しません。一方で、実行コードを含んでいる形式のファイル（exe、dll など）があります。実行コードは、この目的を意図していないファイル形式（DOC 形式など）にも含まれている場合があります。このようなファイルについては、悪意のあるコードの侵入と有効化のリスクが高くなります。
2. 侵入者はウイルスやその他の悪意のあるアプリケーションの拡張子を txt に変え、実行ファイルの形式でコンピューターに送信する可能性があります。拡張子でのファイルのスキャンを選択すると、このようなファイルのスキャンはスキップされます。ファイル形式でのスキャンが選択されている場合、Kaspersky Endpoint Security は拡張子に関係なくファイルのヘッダーを分析します。この分析により、ファイルが実行ファイル形式（例：EXE）であることが判明した場合、スキャンが実行されます。

保護範囲を作成するには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイル脅威対策]** の順に選択します。
3. **[詳細設定]** をクリックします。
4. **[ファイル種別]** セクションで、ファイル脅威対策がスキャンするファイルの種別を指定します。
  - **すべてのファイル**。この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。
  - **ファイル形式でファイルをスキャン**。この設定を有効にした場合、Kaspersky Endpoint Security は**感染する可能性のあるファイルのみ**  をスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。
  - **拡張子でファイルをスキャン**。この設定を有効にした場合、Kaspersky Endpoint Security は**感染する可能性のあるファイルのみ**  をスキャンします。ファイル形式はファイルの拡張子に基づいて識別されます。
5. **[保護範囲の編集]** をクリックします。
6. 表示されたウィンドウで、保護範囲に含めるまたは除外するオブジェクトを選択します。

既定で保護範囲に含まれているオブジェクトの削除または編集はできません。

7. 保護範囲に新しいオブジェクトを追加するには：
  - a. **[追加]** をクリックします。  
フォルダーのツリーが開きます。
  - b. オブジェクトを選択して **[選択]** をクリックします。

スキャン範囲のオブジェクトのリストからオブジェクトを削除しなくてもオブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。


8. 変更内容を保存します。

## スキャン方法の使用

Kaspersky Endpoint Security は、機械学習とシグネチャ分析と呼ばれるスキャン技術を使用します。Kaspersky Endpoint Security のシグネチャ分析では、検知されたオブジェクトと定義データベース内のレコードが照合されます。カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。


保護の有効性を高めるには、ヒューリスティック分析を使用します。悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。

ファイル脅威対策でのヒューリスティック分析の使用を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. 脅威に対してヒューリスティック分析を使用する場合は、**【スキャン方法】** ブロックの **【ヒューリスティック分析】** を選択します。次に、スライダーを使用して、ヒューリスティック分析レベル（低、中、高のいずれか）を設定します。
5. 変更内容を保存します。

## ファイル脅威対策で使用するスキャン技術の設定

ファイル脅威対策で使用するスキャン技術を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【スキャン技術】** ブロックで、ファイル脅威対策で使用する方法の名前の横にあるチェックボックスをオンにします。
  - **iSwift** 特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
  - **iChecker** 特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。
5. 変更内容を保存します。


## スキャンの最適化

ファイル脅威対策が行うファイルのスキャンを最適化し、スキャン時間を短縮したり、Kaspersky Endpoint Security の処理速度を向上させたりすることができます。スキャンを最適化するには、新しいファイルと前回のスキャン以降に変更されたファイルのみをスキャンします。このモードは、簡易ファイルと複合ファイルの両方に適用されます。

[iChecker テクノロジーおよび iSwift テクノロジーの使用を有効化](#)することもできます。これらのテクノロジーを使用すると、前回スキャンを実行してから変更されていないファイルがスキャンから除外されるため、ファイルのスキャン速度を最適化することができます。

ファイルスキャンを最適化するには、次の手順を実行します：



1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【スキャンの最適化】** セクションで、**【新規作成または更新されたファイルのみスキャン】** をオンにします。
5. 変更内容を保存します。


## 複合ファイルのスキャン

ウイルスやその他のマルウェアの隠蔽には、アーカイブやデータベースなどの複合ファイルに埋め込む技術が一般的に使用されています。このような方法で隠されているウイルスやその他のマルウェアを検知するためには、複合ファイルを解凍する必要がありますが、スキャンの速度が低下する場合があります。スキャンする複合ファイル種別を限定することで、スキャンを高速化できます。

感染している複合ファイルの処理方法（駆除または削除）は、ファイルの種別により異なります。

ファイル脅威保護では、RAR、ARJ、ZIP、CAB、LHA 形式の複合ファイルが駆除されます。それ以外の形式のファイルはすべて削除されます（メールデータベースを除く）。

複合ファイルのスキャンを設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【複合ファイルのスキャン】** セクションで、スキャンする複合ファイルの種別として、圧縮ファイル、インストールパッケージ、Office 形式のファイルのいずれかを指定します。
5. 新しいファイルおよび更新されたファイルのみのスキャンが無効になっている場合は、複合ファイルの種別ごとにスキャンの設定（特定の種別のファイルをすべてスキャンまたは新しいファイルのみスキャン）を指定してください。

新しいファイルまたは更新されたファイルのみのスキャンが有効になっている場合は、Kaspersky Endpoint Security はすべての種別の複合ファイルで新しいまたは更新されたもののみをスキャンします。

6. 複合ファイルのスキャンを詳細に設定します。

- **大きな複合ファイルのスキャンしない**

このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。

このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。



アーカイブから展開されるサイズの大きいファイルは、**【大きな複合ファイルをスキャンしない】**がオンにされているかどうかに関係なくスキャンされます。

#### ● 複合ファイルをバックグラウンドで展開する

このチェックボックスをオンにすると、指定された値よりも大きいサイズの複合ファイルには、これらのファイルをスキャンする前にアクセスできます。この場合、複合ファイルの解凍とスキャンはバックグラウンドで実行されます。

指定された値より小さいサイズの複合ファイルには、これらのファイルを解凍してスキャンした後にのみアクセスできます。


この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を解凍してスキャンした後にのみ複合ファイルにアクセスできます。

7. 変更内容を保存します。

## スキャン方法の変更

【スキャンモード】では、ファイル脅威対策によるファイルスキャンを実行する条件が設定されています。既定では、ファイルはスマートモードでスキャンされます。このモードでは、ファイルがスキャンされるかどうかの判断は、ユーザー、ユーザーに代わるアプリケーション（ログインに使用されたアカウントまたは異なるユーザーアカウントで実行）、またはオペレーティングシステムによるファイルの操作が分析された後に決定されます。たとえば、Microsoft Office Word ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。

ファイルスキャン方法を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイル脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【スキャンモード】** セクションで目的のモードを選択します。
  - **スマートモードでスキャン**：オブジェクトに対する処理の分析に基づいて、オブジェクトをスキャンします。たとえば、Microsoft Office ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。
  - **ファイルのアクセス時と更新時にスキャン**：オブジェクトを開こうとするときまたは修正しようとするときにオブジェクトをスキャンします。
  - **ファイルのアクセス時にスキャン**：オブジェクトを開こうとする際にのみオブジェクトをスキャンします。
  - **ファイルの実行時にスキャン**：オブジェクトを実行しようとする際にのみオブジェクトをスキャンします。

5. 変更内容を保存します。

## ウェブ脅威対策

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ウェブ脅威対策は、インターネットからの悪意のあるファイルのダウンロードを防ぎ、悪意のある Web サイトやフィッシングサイトをブロックします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

Kaspersky Endpoint Security では、HTTP、HTTPS、FTP のトラフィック、URL、IP アドレスがスキャンされます。[Kaspersky Endpoint Security で監視するポートを指定する](#)か、すべてのポートを監視対象として選択できます。

HTTPS トラフィックをスキャンするには、[暗号化された接続のスキャンを有効にする](#)必要があります。

ユーザーが、悪意のある Web サイトやフィッシングサイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックし、警告を表示します（下の図を参照）。



Web サイトへのアクセスが拒否されたことを示すメッセージ

## ウェブ脅威対策の有効化と無効化

既定では、ウェブ脅威対策は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。ウェブ脅威対策では、異なる設定の組み合わせを適用できます。アプリケーションに保存されるこれらの設定の組み合わせ（**高**、**推奨**、**低**）は、「セキュリティレベル」と呼ばれます。カスペルスキーのエキスパートが推奨する設定グループは、**[推奨]** セキュリティレベルです（下の表を参照）。HTTP および GTP プロトコルを介して受け取りまたは転送された Web トラフィックに対して、Web トラフィックのセキュリティレベルを事前インストールされたセキュリティレベルから選択することも、カスタマイズすることもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

ウェブ脅威対策を有効または無効にするには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ウェブ脅威対策]** の順に選択します。

3. **[ウェブ脅威対策]** トグルスイッチを使用して機能を有効または無効にします。

4. この機能を有効にした場合は **[セキュリティレベル]** セクションで次の操作を実行してください。

- 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：
  - **高**：HTTP や FTP 経由でコンピューターが受信する Web トラフィックをウェブ脅威対策が最大限にスキャンするときのセキュリティレベル。ウェブ脅威対策は、あらゆる定義データベースを使用してすべての Web トラフィックオブジェクトを詳細にスキャンし、最も徹底的な [ヒューリスティック分析](#) を実行します。
  - **推奨**：Kaspersky Endpoint Security のパフォーマンスと Web トラフィックのセキュリティの間で最適なバランスが取れたセキュリティレベル。ウェブ脅威対策は **中** スキャンレベルでヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、この Web トラフィックセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。
  - **低**：この Web トラフィックセキュリティレベルの設定により、Web トラフィックのスキャンの速度が最大になります。ウェブ脅威対策は **低** スキャンレベルでヒューリスティック分析を実行します。
- カスタムのセキュリティレベルを設定する場合は、**[詳細設定]** をクリックして、機能の設定を定義します。

ウィンドウ上部にある **[推奨のセキュリティレベルに戻す]** をクリックすると、事前設定されたセキュリティレベルを復元することができます。

5. 変更内容を保存します。

カスペルスキーが推奨するウェブ脅威対策の設定値（推奨されるセキュリティレベル）


パラメータ	値	説明
悪意のある Web アドレスのデータベースで Web アドレスをチェックする	有効	Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
フィッシングサイトのデータベースで Web アドレスをチェックする	有効	フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
ヒュー	スキ	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用し

<b>リスティック分析を使用する</b> (ウェブ脅威対策)	<b>ヤン</b> (レベル中)	<p>ても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>ウイルスやその他の脅威を持つアプリケーションがないかWebトラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
<b>ヒューリスティック分析を使用する</b> (フィッシング対策)	<b>有効</b>	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p>
<b>脅威の検知時の処理</b>	<b>ダウンロードをブロックする</b>	<p>このオプションがオンの場合、Webトラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザ上に表示します。</p>

## 悪意のある Web トラフィックオブジェクトに対する処理の変更

既定では、ウェブ脅威対策は Web トラフィック内に感染したオブジェクトを検知すると、このオブジェクトへのアクセスをブロックし、処理に関する通知を表示します。

悪意のある Web トラフィックオブジェクトに対する処理を変更するには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ウェブ脅威対策]** の順に選択します。
3. **[脅威の検知時の処理]** セクションで、悪意のある Web トラフィックオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。
  - **ダウンロードのブロック**：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザ上に表示します。
  - **通知する**：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。
4. 変更内容を保存します。

## フィッシングサイトまたは悪意のある Web サイトのデータベースで URL をチェックする

リンクをスキャンして、そのリンクがフィッシングサイトの URL のリストに含まれているかどうかを確認することにより、フィッシング攻撃を回避することができます。フィッシング攻撃は偽装して行われることがあります。たとえば、メールが銀行から来たもので、その銀行のオフィシャル Web サイトへのリンクが含まれているように見せかけます。リンクをクリックすると、その銀行の偽装サイトに移動します。偽装サイトにアクセスしているにもかかわらず、ブラウザにはその銀行の実際の Web アドレスが表示されているように見ることがあります。それ以降、偽装サイトでの処理がすべて追跡され、現金が盗まれることがあります。

フィッシングサイトへのリンクは、メールからだけでなく、ICQ メッセージなどの他のソースから受け取ることもあります。このため、ウェブ脅威対策は、Web トラフィックのレベルでフィッシングサイトへのアクセスを試行し、その Web サイトへのアクセスをブロックします。フィッシングサイトの URL のリストは、Kaspersky Endpoint Security の配信キットに含まれています。

フィッシングサイトおよび悪意のある Web サイトのデータベースと照合して URL を確認するには、以下の設定を行います：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ウェブ脅威対策]** の順に選択します。
3. **[詳細設定]** をクリックします。
4. 次の手順に従います：
  - 悪意のある Web サイトのデータベースと照合してリンクを確認する場合は、**[スキャン方法]** セクションで **[悪意のある Web アドレスのデータベースで Web アドレスをチェックする]** をオンにします。Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。

悪意のある Web アドレスのデータベース内に登録があるかどうかを判断するためにすべてのリンクをスキャンします。アプリケーションのスキャン設定はリンクのスキャン機能に影響しません。**暗号化された接続のスキャンが無効**になっている場合、Kaspersky Endpoint Security は、ネットワークトラフィックが暗号化された接続を経由して転送されていても悪意のある Web サイトのデータベースでリンクをチェックします。

- ウェブ脅威対策機能でフィッシングサイトのデータベースを使用してリンクをチェックする場合は **[フィッシング対策]** ブロックで **[フィッシングサイトのデータベースで Web アドレスをチェックする]** を選択します。フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。

また、リンクを [Kaspersky Security Network](#) の評価データベースと照合して確認することもできます。




5. 変更内容を保存します。

## ウェブ脅威対策でのヒューリスティック分析の使用

保護の有効性を高めるには、ヒューリスティック分析を使用します。Kaspersky Endpoint Security のヒューリスティック分析では、オペレーティングシステムにおけるアプリケーションの動作が分析されます。ヒューリスティック分析を使用することで、Kaspersky Endpoint Security の定義データベースに現在登録されていない脅威を検知できます。

ヒューリスティック分析の使用を設定するには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ウェブ脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. ウィルスやその他のマルウェアを見つけるためにヒューリスティック分析を使用して Web トラフィックをスキャンする場合は、**【スキャン方法】** ブロックで、**【ヒューリスティック分析を使用する】** を選択します。次に、スライダーを使用して、ヒューリスティック分析レベル（**低**、**中**、**高**のいずれか）を設定します。
5. フィッシングリンクを含む Web ページを見つけるためにヒューリスティック分析を使用してスキャンする場合は、**【フィッシング対策】** ブロックで、**【ヒューリスティック分析を使用する】** を選択します。
6. 変更内容を保存します。

## 信頼する URL のリストの作成

コンテンツが信頼できる Web サイトのリストを作成できます。ウェブ脅威対策は、信頼できる Web サイトからのデータでは、ウィルスおよびその他の脅威が含まれるかどうかを分析しません。既知の Web サイトからのファイルのダウンロードが、ウェブ脅威対策によって妨げられる場合などに、このオプションを使用してください。

URL は特定の Web ページのアドレスまたは Web サイトのアドレスです。

信頼する URL のリストを作成するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ウェブ脅威対策】** の順に選択します。
3. **【詳細設定】** をクリックします。
4. **【信頼する URL の Web トラフィックをスキャンしない】** をオンにします。

このチェックボックスをオンにすると、ウェブ脅威対策は、信頼する Web サイトにアドレスが含まれている Web ページ / Web サイトのコンテンツをスキャンしません。信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。



5. 信頼するコンテンツを含む URL / Web サイトのリストを作成します。
6. 変更内容を保存します。

## 信頼する URL のリストのエクスポート / インポート

信頼する URL のリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の Web アドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、Web アドレスのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

[管理コンソール \(MMC\) で信頼する URL のリストをエクスポートおよびインポートする方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔脅威対策〕** → **〔ウェブ脅威対策〕** の順に選択します。
6. **〔設定〕** をクリックします。
7. 表示されたウィンドウで、 **〔信頼する URL〕** タブを選択します。
8. 信頼する URL のリストをエクスポートするには：
  - a. 編集対象の信頼する URL を選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。  
信頼する URL が何も選択されていない場合、すべての URL がエクスポートされます。
  - b. **〔エクスポート〕** をクリックします。
  - c. 表示されたウィンドウで、信頼する URL のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **〔保存〕** をクリックします。  
Kaspersky Endpoint Security は、信頼する URL のリスト全体を XML ファイルにエクスポートします。
9. 信頼する URL のリストをインポートするには：
  - a. **〔インポート〕** をクリックします。  
表示されたウィンドウで、信頼するアドレスのリストをインポートする XML ファイルを選択します。
  - b. **〔開く〕** をクリックします。  
コンピューターに信頼するアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
10. 変更内容を保存します。

[Web コンソールおよび Cloud コンソールで信頼する URL のリストをエクスポートおよびインポートする方法](#) 

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Web アドレスのリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[ウェブ脅威対策]** を選択します。
5. **[信頼する URL]** ブロックで除外リストをエクスポートするには：
  - a. 編集対象の信頼する URL を選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 表示されたウィンドウで、信頼する URL のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、信頼する URL のリスト全体を XML ファイルにエクスポートします。
6. **[信頼する URL]** ブロックで除外リストをインポートするには：
  - a. **[インポート]** をクリックします。  
表示されたウィンドウで、信頼するアドレスのリストをインポートする XML ファイルを選択します。
  - b. **[開く]** をクリックします。  
コンピューターに信頼するアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
7. 変更内容を保存します。

## メール脅威対策

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、悪意のあるリンクやフィッシングリンクのメッセージもスキャンします。既定では、メール脅威対策はコンピューターの RAM に常駐し、POP3、SMTP、IMAP、NNTP プロトコル、または Microsoft Office Outlook メールクライアント (MAPI) を使用して送受信されるすべてのメッセージをスキャンします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

メールクライアントがブラウザで開いている場合、メール脅威対策はメッセージをスキャンしません。


添付ファイルで悪意のあるファイルが検知されると、Kaspersky Endpoint Security はメッセージの件名を「[Message infected] <メッセージの元の件名>」または「[Infected object deleted] <メッセージの元の件名>」に変更します。

このコンポーネントは、コンピューターにインストールされているメールクライアントと連携します。Microsoft Office Outlook メールクライアントの場合、[追加のパラメータを持つ拡張機能](#)が提供されます。メール脅威対策の機能拡張は、Kaspersky Endpoint Security のインストール中に Microsoft Office Outlook メールクライアントに組み込まれます。

## メール脅威対策の有効化と無効化

既定では、メール脅威対策は有効になっており、カスペルスキーのエキスペートが推奨するモードで実行されています。メール脅威対策では、異なる設定の組み合わせを適用します。アプリケーションに保存されるこれらの設定の組み合わせ（**高**、**推奨**、**低**）は、「セキュリティレベル」と呼ばれます。カスペルスキーのエキスペートが推奨する設定グループは、**[推奨]** のメールセキュリティレベルです（下の表を参照）。事前インストールされたメールセキュリティレベルから選択するか、セキュリティレベルをカスタマイズすることもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

メール脅威対策を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[メール脅威対策]** の順に選択します。
3. **[メール脅威対策]** トグルスイッチを使用して機能を有効または無効にします。
4. この機能を有効にした場合は **[セキュリティレベル]** セクションで次の操作を実行してください。
  - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：
    - **高**：このメールセキュリティレベルを選択すると、メール脅威対策は最も厳格にメールをスキャンします。メール脅威対策は送受信されたメールメッセージをスキャンし、徹底的なヒューリスティック分析を実行します。リスクの高い環境で作業している場合には **[高]** メールセキュリティレベルが推奨されます。このような環境の例としては、一元化されたメールアンチウイルスで守られていない家庭用ネットワークからのフリーメールサービスへの接続などがあります。
    - **推奨**：Kaspersky Endpoint Security のパフォーマンスとメールのセキュリティの間で最適なバランスが取れたメールセキュリティレベル。メール脅威対策は送受信メールをスキャンし、中レベルのヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、このメールセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。
    - **低**：このメールセキュリティレベルを選択すると、メール脅威対策は受信メールのみをスキャンし、簡易ヒューリスティック分析を実行します。メールに添付されている圧縮ファイルはスキャンしません。このメールセキュリティレベルでは、オペレーティングシステムのリソースの使用を最小限に抑えながら、メールのスキャン速度が最大化します。「**低**」メールセキュリティレベルは、十分に保護された環境で作業している場合に推奨されます。このような環境の例としては、一元化されたメールセキュリティが適用された企業 LAN などがあります。
  - カスタムのセキュリティレベルを設定する場合は、**[詳細設定]** をクリックして、機能の設定を定義します。

ウィンドウ上部にある **[推奨のセキュリティレベルに戻す]** をクリックすると、事前設定されたセキュリティレベルを復元することができます。

## 5. 変更内容を保存します。

カスペルスキーが推奨するメール脅威対策の設定値（推奨されるセキュリティレベル）


パラメータ	値	説明
保護範囲	送受信メッセージ	<p>保護範囲には、機能の実行中にチェックするオブジェクトが含まれます：<b>送受信メッセージ</b>または<b>受信メッセージ</b>。</p> <p>お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。</p>
Microsoft Outlook アドインに接続	有効	<p>このチェックボックスをオンにすると、POP3、SMTP、NNTP、IMAP プロトコルで送信されるメールのスキャンは、Microsoft Outlook に組み込まれた拡張機能側で有効になります。</p> <p>メールのスキャンに Microsoft Outlook 用機能拡張を使用している場合は、Exchange キャッシュモードを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、<a href="#">マイクロソフトサポート技術情報</a>を参照してください。</p>
添付のアーカイブのスキャン	有効	<p>次の形式のアーカイブのファイルのスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR および ICE。</p>
添付の Office 形式ファイルのスキャン	有効	<p>Microsoft Office 形式のファイルのスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。</p>
添付ファイルのフィルター	選択した種別の添付ファイルの名前を変更する：	<p>このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。</p>
ヒューリスティック分析	スキャン (レベル中)	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
脅威の検知時の処	駆除す	<p>感染したオブジェクトが送受信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。ユーザーはメ</p>

理	る。 駆除 でき ない 場合 は削 除す る	ッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security は感染したオブジェクトを削除します。Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「[Infected object was deleted] <メッセージの元の件名>」に変更します。
---	---	---

## 感染したメールに対する処理の変更

既定では、メール脅威対策は、検知した感染ファイルすべての駆除を自動的に試みます。駆除に失敗した場合は、感染したメールを削除します。

感染したメールに対する処理を変更するには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[メール脅威対策]** の順に選択します。
3. **[脅威の検知時の処理]** セクションで、Kaspersky Endpoint Security が感染したメールを検知したときに実行する処理を選択します。
  - **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が送受信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security は感染したオブジェクトを削除します。Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「[Infected object was deleted] <メッセージの元の件名>」に変更します。
  - **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security はメッセージの件名に警告を追加して、件名を「[Message infected] <メッセージの元の件名>」に変更します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。
  - **ブロック**：感染したオブジェクトが受信メッセージで検知された場合、Kaspersky Endpoint Security はメッセージの件名に警告を追加して、件名を「[Message infected] <メッセージの元の件名>」に変更します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、Kaspersky Endpoint Security はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。
4. 変更内容を保存します。

## メール脅威対策の保護範囲の設定



保護範囲とは、あるコンポーネントが有効な場合にスキャンされるオブジェクトを意味します。各コンポーネントの保護範囲には、それぞれ異なる特性があります。メール脅威対策の保護範囲には、本コンポーネントをメールクライアントに拡張する設定、および本機能でトラフィックをスキャンするメールメッセージの種類とメールプロトコルが含まれます。既定では、Kaspersky Endpoint Security は送受信メールと POP3、SMTP、NNTP、IMAP プロトコル経由のトラフィックをスキャンし、Microsoft Office Outlook メールクライアントに統合されます。

メール脅威対策の保護範囲を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[メール脅威対策]** の順に選択します。
3. **[詳細設定]** をクリックします。
4. **[保護範囲]** ブロックで、スキャンするメッセージを選択します。

- **送受信メッセージ**

- **受信のみ**

お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。

受信メッセージのみのスキャンを選択した場合は、メールで拡散するメールワームがコンピューター上に存在する可能性があるため、すべての送信メールを一度スキャンしてください。これにより、感染したメッセージが監視されずにコンピューターから大量送信されるという問題を避けることができます。

5. **[接続]** セクションで、次を実行します：

- POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメッセージがコンピューターで受信される前にスキャンする場合は、**[POP3、SMTP、NNTP、IMAP トラフィックのスキャン]** をオンにします。

POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメッセージがコンピューターで受信される前にスキャンしない場合は、**[POP3、SMTP、NNTP、IMAP トラフィックのスキャン]** をオフにします。この場合、**[Microsoft Outlook アドインに接続]** がオンになっていれば、メッセージはコンピューターが受信した後 Microsoft Office Outlook に組み込まれたメール脅威対策機能拡張によってスキャンされます。

**[POP3、SMTP、NNTP、IMAP トラフィックのスキャン]** がオフになっていると、Microsoft Office Outlook 以外のメールクライアントを使用している場合にメール脅威対策は POP3、SMTP、NNTP、IMAP プロトコル経由で送信されたメッセージをスキャンしません。

- Microsoft Office Outlook からメールアンチウイルスを設定できるようにし、POP3、SMTP、NNTP、IMAP、MAPI プロトコル経由で送信されたメールをコンピューターで受信した後 Microsoft Office Outlook に組み込まれた機能拡張でスキャンする場合は、**[Microsoft Outlook アドインに接続]** をオンにします。

Microsoft Office Outlook からメールアンチウイルス設定へのアクセスをブロックし、POP3、SMTP、NNTP、IMAP、MAPI プロトコル経由で送信されたメールをコンピューターで受信した後 Microsoft Office Outlook に組み込まれたプラグインでスキャンしない場合は、**[Microsoft Outlook アドインに接続]** をオフにします。


メール脅威対策の機能拡張は、Kaspersky Endpoint Security のインストール中に Microsoft Office Outlook メールクライアントに組み込まれます。

6. 変更内容を保存します。

## メールに添付されている複合ファイルのスキャン

メッセージの添付ファイルのスキャンを有効化または無効化することができます。また、スキャン対象となる添付ファイルの最大サイズとスキャンの最長時間を制限することもできます。

メールに添付されている複合ファイルのスキャンを設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[メール脅威対策]** の順に選択します。
3. **[詳細設定]** をクリックします。
4. **[複合ファイルのスキャン]** セクションで、スキャンを設定します：
  - **添付の Office 形式ファイルのスキャン**：Microsoft Office 形式のファイルのスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。
  - **添付のアーカイブのスキャン**：次の形式のアーカイブのファイルのスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR および ICE。

スキャン中に Kaspersky Endpoint Security がメッセージ本文に圧縮ファイルのパスワードを検出した場合は、このパスワードを使用して圧縮ファイルの内容に対して悪意のあるアプリケーションのスキャンを実行します。この場合、パスワードは保存されません。圧縮ファイルはスキャン中に解凍されます。圧縮ファイルの解凍中にアプリケーションでエラーが発生した場合、次のパスに保存されたファイルを手動で削除できます：`%systemroot%\temp`。このファイルには接頭辞 PR が付いています。

- **次のサイズを超えるアーカイブをスキャンしない**：このチェックボックスをオンにすると、メール脅威対策が指定したサイズを超える、メールメッセージに添付されたアーカイブをスキャンしません。このチェックボックスをオフにすると、添付オブジェクトのサイズに関係なく、メール脅威対策がメール添付のアーカイブをスキャンします。
- **アーカイブのスキャンの時間を制限する**：このチェックボックスを選択すると、メールメッセージに添付されたアーカイブのスキャンに割り当てられる時間が指定の時間に制限されます。


5. 変更内容を保存します。

## メール添付ファイルのフィルター

添付ファイルのフィルター機能は、送信されるメールには適用されません。

悪意のあるアプリケーションは、メールの添付ファイルという形式で配信されることがあります。メールの添付ファイル種別によるフィルタリングを設定し、特定の種類のファイルを自動的に名前変更したり削除したりできます。特定の種類の添付ファイルの名前を変更することにより、悪意のあるアプリケーションの自動実行を防ぐことができます。

添付ファイルのフィルター処理を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[メール脅威対策]** の順に選択します。
3. **[詳細設定]** をクリックします。
4. **[添付ファイルのフィルター]** セクションで、次のいずれかを実行します：
  - **フィルタリングを無効にする**：このオプションをオンにした場合、メール脅威対策は、メールに添付されているファイルをフィルター処理しません。
  - **選択した種別の添付ファイルの名前を変更する**：このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc\_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。
  - **選択した種別の添付ファイルを削除する**：このオプションをオンにした場合、メール脅威対策は特定の種類の添付ファイルをメールから削除します。
5. 前の手順で **[選択した種別の添付ファイルの名前を変更する]** または **[選択した種別の添付ファイルを削除する]** をオンにした場合、必要なファイル種別の横にあるチェックボックスをオンにします。
6. 変更内容を保存します。

## 添付ファイルのフィルターの拡張子のエクスポートおよびインポート

添付ファイルのフィルターの拡張子を XML ファイルにエクスポートすることができます。また、エクスポートまたはインポート機能を使用して、拡張子のバックアップをとったり、別のサーバーにリストを移行することができます。

[管理コンソール \(MMC\) で添付ファイルのフィルターの拡張子のリストをエクスポートおよびインポートする方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [脅威対策] → [メール脅威対策] の順に選択します。
6. [セキュリティレベル] セクションの [設定] をクリックします。
7. 表示されたウィンドウで、 [添付ファイルのフィルター] タブを選択します。
8. 拡張子のリストをエクスポートするには：
  - a. エクスポートする拡張子を選択します。複数のポートを選択するには、CTRL または SHIFT キーを使用します。
  - b. [エクスポート] をクリックします。
  - c. 表示されたウィンドウで、拡張子のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. [保存] をクリックします。

Kaspersky Endpoint Security は、拡張子のリスト全体を XML ファイルにエクスポートします。
9. 拡張子のリストをインポートするには：
  - a. [インポート] をクリックします。
  - b. 表示されたウィンドウで、拡張子のリストをインポートする XML ファイルを選択します。
  - c. [開く] をクリックします。

コンピューターに拡張子のリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
10. 変更内容を保存します。

[Web コンソールおよび Cloud コンソールで添付ファイルのフィルターの拡張子のリストをエクスポートおよびインポートする方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 除外リストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[メール脅威対策]** を選択します。
5. **[添付ファイルのフィルター]** ブロックで拡張子のリストをエクスポートするには：
  - a. エクスポートする拡張子を選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 表示されたウィンドウで、拡張子のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、拡張子のリスト全体を XML ファイルにエクスポートします。
6. **[添付ファイルのフィルター]** ブロックで拡張子のリストをインポートするには：
  - a. **[インポート]** をクリックします。
  - b. 表示されたウィンドウで、拡張子のリストをインポートする XML ファイルを選択します。
  - c. **[開く]** をクリックします。  
コンピューターに拡張子のリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
7. 変更内容を保存します。

## Microsoft Office Outlook におけるメールのスキャン

Kaspersky Endpoint Security のインストール中に、メール脅威対策の機能拡張が Microsoft Office Outlook（以降、「Outlook」）に組み込まれます。この機能拡張を使用して、Outlook 内からメール脅威対策の設定を開いたり、メールでウイルスなどの脅威をスキャンするタイミングを指定したりすることができます。メール脅威対策の Outlook 用機能拡張では、POP3、SMTP、NNTP、IMAP、および MAPI の各プロトコル経由で送受信されたメッセージをスキャンできます。Kaspersky Endpoint Security は、他のメールクライアント（Microsoft Outlook Express®、Windows Mail、Mozilla™Thunderbird™ など）との連携もサポートしています。

メール脅威対策の機能拡張は Outlook 2010、2013、2016 および 2019 の操作をサポートします。

Mozilla Thunderbird メールクライアントを使用する場合、フィルターを使用してメールを [受信トレイ] フォルダーから移動すると、メール脅威対策は IMAP プロトコルで送信されるメールのウイルスなどの脅威をスキャンしません。

Outlook では、受信メッセージはまずメール脅威対策によってスキャンされ (Kaspersky Endpoint Security のインターフェイスで [\[POP3、SMTP、NNTP、IMAP トラフィックをスキャンする\]](#) がオンになっている場合)、次にメール脅威対策の Outlook 用機能拡張によってスキャンされます。メール脅威対策がメッセージ内で悪意のあるオブジェクトを検知すると、通知が表示されます。

Kaspersky Endpoint Security のインターフェイスで [\[Microsoft Outlook アドインに接続\]](#) がオンになっている場合、メール脅威対策の設定を Outlook で直接指定できます。

送信メッセージは、まずメール脅威対策の Outlook 用機能拡張によってスキャンされ、次にメール脅威対策によってスキャンされます。

メールのスキャンにメール脅威対策の Outlook 用機能拡張を使用している場合は、Exchange キャッシュモードを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、[マイクロソフトサポート技術情報](#) を参照してください。

Kaspersky Security Center を使用してメール脅威対策の Outlook 用機能拡張の操作モードを設定するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[脅威対策] → [メール脅威対策] の順に選択します。
6. [セキュリティレベル] セクションの [設定] をクリックします。
7. [接続] セクションで、[設定] をクリックします。
8. [メール保護] ウィンドウで以下の操作を実行してください：
  - 受信メッセージがメールボックスに届いたときにメッセージをスキャンする場合は、[メール受信時にスキャンする] を選択します。
  - 受信したメッセージをユーザーが開いたときにメッセージをスキャンする場合は、[メール閲覧時にスキャンする] を選択します。
  - 送信時にメッセージをスキャンする場合は、[メール送信時にスキャンする] を選択します。
9. 変更内容を保存します。

## ネットワーク脅威対策




ネットワーク脅威対策は、受信ネットワークトラフィックをスキャンし、典型的なネットワーク攻撃の活動をチェックします。Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、Kaspersky Endpoint Security データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、[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](#)時にアップデートされます。

## ネットワーク脅威対策の有効化と無効化

既定では、ネットワーク脅威対策は有効になっており、最適モードで実行されています。必要に応じて、ネットワーク脅威対策を無効にすることができます。


ネットワーク脅威対策を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ネットワーク脅威対策]** の順に選択します。
3. **[ネットワーク脅威対策]** トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

ネットワーク脅威対策を有効にすると、受信ネットワークトラフィックをスキャンし、典型的なネットワーク攻撃の活動をチェックします。Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。

## 攻撃元コンピューターのブロック

攻撃元コンピューターをブロックするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ネットワーク脅威対策]** の順に選択します。
3. **[攻撃元コンピューターをブロックする時間]** をオンにします。

このチェックボックスをオンにすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。

ブロックのリストは[ネットワークモニターツール](#)ウィンドウで表示できます。

Kaspersky Endpoint Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。


4. **[攻撃元コンピューターをブロックする時間]** の右側のフィールドで、別に攻撃元のコンピューターをブロックする時間を設定します。
5. 変更内容を保存します。

Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の開始を検知すると、攻撃しているコンピューターとのすべてのネットワーク接続をブロックします。

## ブロックから除外するアドレスの設定

Kaspersky Endpoint Security はネットワーク攻撃を認識し、パケット数の大きな保護されていないネットワーク接続（監視カメラなど）をブロックすることができます。信頼するデバイスについては、除外リストにデバイスの IP アドレスを追加できます。

ブロックから除外するアドレスを設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ネットワーク脅威対策]** の順に選択します。
3. **[除外リストの管理]** をクリックします。
4. **[追加]** をクリックします。
5. ネットワーク攻撃防御の対象にしないコンピューターの IP アドレスを入力します。
6. 変更内容を保存します。

除外リストに登録されたデバイスの活動はトラックされません。

## ブロックの除外対象のリストのエクスポート / インポート

除外リストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーにリストを移行することができます。

[管理コンソール \(MMC\) で除外リストをエクスポートおよびインポートする方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔脅威対策〕** → **〔ネットワーク脅威対策〕** の順に選択します。
6. **〔ネットワーク脅威対策の設定〕** ブロックで、 **〔除外リスト〕** をクリックします。
7. ルールのリストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。  
除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。
  - b. **〔エクスポート〕** をクリックします。
  - c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **〔保存〕** をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
8. 除外リストをインポートするには：
  - a. **〔インポート〕** をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. **〔開く〕** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
9. 変更内容を保存します。

## [Web コンソールおよび Cloud コンソールで除外リストをエクスポートおよびインポートする方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 除外リストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[ネットワーク脅威対策]** を選択します。
5. **[ネットワーク脅威対策の設定]** ブロックで、**[除外リスト]** をクリックします。  
除外リストが表示されます。
6. ルールのリストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。
  - d. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - e. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
7. 除外リストをインポートするには：
  - a. **[インポート]** をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. **[開く]** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

## ネットワーク攻撃の種別に対応した保護を設定する

Kaspersky Endpoint Security を使用して、次の種別のネットワーク攻撃に対する保護を管理できます。


- ネットワークフラディングとは、Web サーバーなど、企業のネットワークリソースに対する攻撃を意味します。これは、大量のリクエストを送信し、ネットワークリソースの帯域幅をオーバーロードさせる攻撃です。攻撃されると、ユーザーは企業のネットワークリソースにアクセスできなくなります。

- ポートのスキャンとは、コンピューターのUDPポート、TCPポート、ネットワークサービスをスキャンする攻撃を意味します。これにより、攻撃者がコンピューターの脆弱性を把握して、より悪質な攻撃を仕掛けることができるようになります。また、コンピューターのオペレーティングシステムを識別し、そのオペレーティングシステムに適したネットワーク攻撃を行うためにポートがスキャンされることもあります。
- MACスプーフィング攻撃では、ネットワークデバイス（ネットワークカード）のMACアドレスを変更します。その結果、攻撃者はデバイスに送信されたデータを別のデバイスにリダイレクトし、このデータにアクセスすることができます。Kaspersky Endpoint SecurityでMACスプーフィング攻撃をブロックし、攻撃に関する通知を管理者に送信できます。

一部の許可されるアプリケーションがこのような攻撃と似た動作を行う場合は、これらの検知機能を無効にすることができます。これにより誤検知を減らすことができます。

既定では、Kaspersky Endpoint Securityはネットワークフラッディングおよびポートのスキャン、MACスプーフィング攻撃を監視しません。

ネットワーク攻撃の種別に対応した保護を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ネットワーク脅威対策]** の順に選択します。
3. これらの攻撃の検知を有効または無効にするには、**[ポートのスキャンおよびネットワークフラッディングを攻撃として扱う]** トグルスイッチを使用します。
4. **[MACスプーフィング対策]** トグルスイッチを使用します。
5. **[MACスプーフィング攻撃を検知したとき]** ブロックで、次のオプションを選択します：
  - 通知のみ
  - 通知してブロック
6. 変更内容を保存します。

## ファイアウォール

ファイアウォールは、インターネットまたはローカルネットワークでの作業中に、コンピューターへの不正な接続をブロックします。ファイアウォールは、コンピューター上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業LANを保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義されたネットワークルールを使用してコンピューターを保護します。

ネットワークエージェントはKaspersky Security Centerとの連携に使用されます。ファイアウォールは本製品とネットワークエージェントが正常に動作するために、自動でネットワークルールを作成します。その結果、ファイアウォールはコンピューターのいくつかのポートを開きます。どのポートが開かれるかは、ディストリビューションポイントなど、コンピューターの役割により異なります。コンピューターで開かれるポートについて詳しくは、[Kaspersky Security Centerのヘルプ](#)を参照してください。

## ネットワークルール

次の情報に基づいてネットワークルールを構成できます：

- ネットワークパケットルール：ネットワークパケットルールでは、アプリケーションに関係なく、ネットワークパケットに制限が適用されます。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。Kaspersky Endpoint Security には、カスペルスキーのエキスパートが推奨する権限を持つネットワークパケットルールが事前に定義されています。
- アプリケーションネットワークルール：アプリケーションネットワークルールでは、特定のアプリケーションのネットワークアクティビティに制限が適用されます。このルールでは、ネットワークパケットの特徴だけでなく、このネットワークパケットの宛先またはネットワークパケットを発行する特定のアプリケーションも考慮されます。

オペレーティングシステムのリソース、プロセス、および個人データへのアプリケーションの制御されたアクセスは、アプリケーション権限を使用することにより、[ホスト侵入防止](#)によって提供されます。

アプリケーションの最初の起動時に、ファイアウォールは次の動作を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティの確認。  
ファイアウォールがより効果的に機能するように、[Kaspersky Security Network に参加](#)することを推奨します。
3. 信頼グループのいずれかにアプリケーションを配置します：信頼、弱い制限付き、強い制限付き、ブロック。

[許可グループ](#)は、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は [ホスト侵入防止の設定](#)に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じて、アプリケーションのネットワーク動作をブロックします。たとえば、強い制限付きの信頼グループのアプリケーションは、ネットワーク接続を使用できません。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のネットワークルールをそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

## ネットワークルールの優先度

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ネットワーク動作が複数のルールに追加された場合、ファイアウォールは最も優先度の高いルールに従ってネットワーク動作を制限します。



ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。同じ種類のネットワークアクティビティに、ネットワークパケットルールとアプリケーションのネットワークルールの両方が指定されている場合、そのネットワークアクティビティはネットワークパケットルールに従って処理されます。

アプリケーションのネットワークルールは次のように動作します：アプリケーションのネットワークルールには、パブリック、ローカル、または許可するなど、ネットワークのステータスに基づいたアクセスルールが含まれます。例えば、強い制限付きの信頼グループのアプリケーションは、既定ではすべてのステータスのネットワーク内でネットワークアクティビティが許可されません。個別のアプリケーション（親アプリケーション）にネットワークルールが指定されている場合、他のアプリケーションの子プロセスは、親アプリケーションのネットワークルールに基づいて実行されます。アプリケーションにネットワークルールが指定されていない場合は、子プロセスはアプリケーションの信頼グループのネットワークアクセスルールに基づいて実行されます。

例えば、ブラウザ X 以外のすべてのアプリケーションのすべてのステータスのネットワークアクティビティを禁止したとします。その後ブラウザ X（親アプリケーション）からブラウザ Y（子プロセス）のインストールを開始した場合、ブラウザ Y のインストーラはネットワークにアクセスし、必要なファイルをダウンロードします。インストール後、ブラウザ Y はファイアウォールの設定により、すべてのネットワーク接続を拒否します。子プロセスとしてのブラウザ Y のネットワークアクティビティを禁止するには、ブラウザ Y のインストーラに対してネットワークルールを設定する必要があります。

## ネットワーク接続のステータス

ファイアウォールを使用すると、ネットワーク接続の状態に応じてネットワーク動作を制御できます。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムからネットワーク接続のステータスを受け取ります。オペレーティングシステムでのネットワーク接続のステータスは、接続のセットアップ時にユーザーが設定します。[Kaspersky Endpoint Security の設定でネットワーク接続のステータスを変更](#)できます。ファイアウォールは、オペレーティングシステムではなく、Kaspersky Endpoint Security の設定のネットワークステータスに応じてネットワーク動作を監視します。

ネットワーク接続種別は、次のいずれかの種類になります：

- **パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。


既定では、ファイアウォールは、[パブリックネットワーク] ステータスをインターネットに割り当てます。インターネットのステータスは変更できません。

- **プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。
- **許可するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。

## ファイアウォールの有効化または無効化

既定では、ファイアウォールは有効化され、最適なモードで機能します。


ファイアウォールを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【ファイアウォール】** トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

## ネットワーク接続種別の変更

既定では、ファイアウォールは、**【パブリックネットワーク】** ステータスをインターネットに割り当てます。インターネットのステータスは変更できません。

ネットワーク接続種別を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【使用可能なネットワーク】** をクリックします。
4. ステータスを変更するネットワーク接続を選択します。
5. **【ネットワーク種別】** 列で、ネットワーク接続のステータスを選択します。
  - **パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。
  - **プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。
  - **許可するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。
6. 変更内容を保存します。

## ネットワークパケットルールの管理

ネットワークパケットルールの管理では、次の操作を実行できます：

- 新しいネットワークパケットルールを作成する。  
新しいネットワークパケットルールを作成するには、ネットワークパケットとデータストリームに適用する一連の条件と処理を作成します。
- ネットワークパケットルールを有効化または無効化する。

既定では、ファイアウォールによって作成されるすべてのネットワークパケットルールのステータスが「有効」になります。ネットワークパケットルールが有効な場合、ファイアウォールはこのルールを適用します。

ネットワークパケットルールのリストで選択した任意のネットワークパケットルールを無効にすることができます。ネットワークパケットルールが無効な場合、ファイアウォールはこのルールを一時的に適用しません。

既定では、新しいカスタムネットワークパケットルールは、「有効」ステータスでネットワークパケットルールのリストに追加されます。

- 既存のネットワークパケットルールの設定を編集する。

新しいネットワークパケットルールの作成後、必要時にはいつでもそのルールに戻って設定を編集したり、変更を加えたりすることができます。

- ネットワークパケットルールに適用するファイアウォールの処理を変更する。

ネットワークパケットルールのリストで、特定のネットワークパケットルールに一致するネットワークの動作の検知時にファイアウォールが実行する処理を編集することができます。

- ネットワークパケットルールの優先度を変更する。

リストから選択したネットワークパケットルールの優先度を変更することができます。

- ネットワークパケットルールを削除する。

ネットワークパケットルールを削除して、ファイアウォールがネットワークの動作の検知時にこのルールを適用しないようにしたり、ネットワークパケットルールのリストにこのルールが「無効」ステータスで表示されないようにしたりすることができます。

## ネットワークパケットルールの作成

次の方法でネットワークパケットルールを作成できます：

- [ネットワークモニター](#)ツールを使用する。

ネットワークモニターは、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。ルールを設定する必要がないため便利です。一部のファイアウォールの設定はネットワークモニターのデータから自動的に挿入されます。ネットワークモニターは製品のインターフェイスのみで使用できます。

- ファイアウォールを設定する。


ファイアウォールの設定を詳細に調整できます。その時点でネットワークの操作がない場合にも、ネットワークの動作に関してルールを作成できます。

ネットワークパケットルールを作成するときには、アプリケーションのネットワークルールに優先するという点に留意する必要があります。

### [製品のインターフェイスでネットワークモニターツールを使用してネットワークパケットルールを作成する方法](#)

1. 製品のメインウィンドウの **【監視】** で、 **【ネットワークモニター】** をクリックします。
2. **【ネットワークの動作】** タブを選択します。  
**【ネットワークの動作】** タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。
3. ネットワーク接続のコンテキストメニューで、 **【ネットワークパケットルールを作成する】** を選択します。  
ネットワークルールのプロパティが開きます。
4. パケットルールに **【有効】** を設定します。
5. **【名前】** フィールドに、ネットワークサービスの名前を手動で入力します。
6. ネットワークルールを設定します（下記の表を参照）。  
**【ネットワークルールテンプレート】** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
7. ネットワークルールの処理を **レポート** に反映する場合は、 **【イベントを記録】** をオンにします。
8. **【保存】** をクリックします。  
新しいネットワークルールがリストに追加されます。
9. **【上へ】** と **【下へ】** を使用してネットワークルールの優先度を設定します。
10. 変更内容を保存します。

## **製品のインターフェイスでファイアウォールの設定を使用してネットワークパケットルールを作成する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイアウォール]** の順に選択します。
3. **[パケットルール]** をクリックします。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
4. **[追加]** をクリックします。  
ネットワークルールのプロパティが開きます。
5. パケットルールに **[有効]** を設定します。
6. **[名前]** フィールドに、ネットワークサービスの名前を手動で入力します。
7. ネットワークルールを設定します（下記の表を参照）。  
**[ネットワークルールテンプレート]** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
8. ネットワークルールの処理を レポート に反映する場合は、**[イベントを記録]** をオンにします。
9. **[保存]** をクリックします。  
新しいネットワークルールがリストに追加されます。
10. **[上へ]** と **[下へ]** を使用してネットワークルールの優先度を設定します。
11. 変更内容を保存します。

## 管理コンソール (MMC) でネットワークパケットルールを作成する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [脅威対策] → [ファイアウォール] の順に選択します。
6. [ファイアウォールの設定] ブロックで、 [設定] をクリックします。  
ネットワークパケットルールおよびアプリケーションネットワークルールのリストが表示されます。
7. [ネットワークパケットルール] タブを選択します。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
8. [追加] をクリックします。  
パケットルールのプロパティが開きます。
9. [名前] フィールドに、ネットワークサービスの名前を手動で入力します。
10. ネットワークルールを設定します（下記の表を参照）。  
ボタン (🔍) をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
11. ネットワークルールの処理を [レポート](#) に反映する場合は、 [イベントを記録] をオンにします。
12. [保存] をクリックします。  
新しいネットワークルールがリストに追加されます。
13. [上へ] と [下へ] を使用してネットワークルールの優先度を設定します。
14. 変更内容を保存します。

ファイアウォールはルールに従ってネットワークパケットを制御します。パケットルールをリストから削除しなくても、ファイアウォールの操作からパケットルールを無効にすることができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

## [Web コンソールと Cloud コンソールでネットワークパケットルールを作成する方法](#)



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[ファイアウォール]** の順に選択します。
5. **[ファイアウォールの設定]** ブロックで、**[ネットワークパケットルール]** をクリックします。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
6. **[追加]** をクリックします。  
パケットルールのプロパティが開きます。
7. **[名前]** フィールドに、ネットワークサービスの名前を手動で入力します。
8. ネットワークルールを設定します（下記の表を参照）。  
**[テンプレートを選択]** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
9. ネットワークルールの処理を **レポート** に反映する場合は、**[イベントを記録]** をオンにします。
10. **[保存]** をクリックします。  
新しいネットワークルールがリストに追加されます。
11. **[上へ]** と **[下へ]** を使用してネットワークルールの優先度を設定します。
12. 変更内容を保存します。

ファイアウォールはルールに従ってネットワークパケットを制御します。パケットルールをリストから削除しなくても、ファイアウォールの操作からパケットルールを無効にすることができます。**[ステータス]** 列のトグルスイッチを使用してパケットルールを有効または無効にします。


#### ネットワークパケットルールの設定

パラメータ	説明
処理	<b>許可：</b> <b>ブロック：</b> <b>アプリケーションルールに準拠</b> このオプションを選択すると、ファイアウォールはネットワーク接続に <b>アプリケーションネットワークルール</b> を適用します。
プロトコル	選択したプロトコル（TCP、UDP、ICMP、ICMPv6、IGMP および GRE）に対してネットワークの動作を制御します。 ICMP または ICMPv6 プロトコルを選択すると、ICMP パケットの種類とコードを定義できます。 TCP または UDP をプロトコルの種類として選択すると、接続が監視されるローカルコンピューターとリモートコンピューターのポートをカンマ区切りで指定できます。

通信方向	<p><b>受信（パケット）</b> ファイアウォールはすべての受信ネットワークパケットにネットワークルールを適用します。</p> <p><b>受信</b> リモートコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。</p> <p><b>受信 / 送信</b> ネットワーク接続を開始したのがユーザーのコンピューターかリモートコンピューターが関係なく、送受信ネットワークパケットにネットワークルールが適用されます。</p> <p><b>送信（パケット）</b> ファイアウォールはすべての送信ネットワークパケットにネットワークルールを適用します。</p> <p><b>送信</b> ユーザーのコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。</p>
	<p>TCP プロトコルが接続を確立します。TCP に <b>受信</b>、<b>送信</b> および <b>受信 / 送信</b> を使用します。その他すべてのプロトコルは接続を確立しませんが、パケットを送信します。その他すべてのプロトコルには、<b>受信（パケット）</b>、<b>送信（パケット）</b> または <b>受信 / 送信</b> を使用します。</p>
ネットワークアダプター	<p>ネットワークパケットを送信または受信することができるネットワークアダプターです。ネットワークアダプターの設定を行うことで、同じ IP アドレスのネットワークアダプターによって送受信されるネットワークパケットを区別できます。</p>
最大生存時間 (TTL)	<p>最大生存時間 (TTL) に基づいてネットワークパケットの制御を制限します。</p>
リモートアドレス	<p>ネットワークパケットを送信または受信するリモートコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のリモートネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めることも、IP アドレスの範囲を指定することも、IP アドレスごとに別のリストを作成することも、または許可するネットワーク、ローカルネットワーク、パブリックネットワークなどのサブネットを選択することもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。</p>
ローカルアドレス	<p>ネットワークパケットを送信または受信するコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のローカルネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めたり、IP アドレスごとに別のリストを作成したり、IP アドレスの範囲を指定したりすることもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。</p>
	<p>アプリケーションのローカルアドレスが取得できない場合があります。この場合、このパラメータは無視されます。</p>


## ネットワークパケットルールの有効化または無効化

ネットワークパケットルールを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【パケットルール】** をクリックします。  
ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。
4. リストから、目的のネットワークパケットルールを選択します。
5. **【ステータス】** 列のトグルスイッチを使用してルールを有効または無効にします。
6. 変更内容を保存します。

## ネットワークパケットルールに対するファイアウォール処理の変更

ネットワークパケットルールに適用するファイアウォールの処理を変更するには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【パケットルール】** をクリックします。  
ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。
4. ネットワークパケットルールのリストからルールを選択し、**【編集】** をクリックします。
5. **【処理】** で、この種類のネットワークの動作が検知されたときにファイアウォールによって実行される次のいずれかの処理を選択します：
  - **許可：**
  - **ブロック：**
  - **アプリケーションルールに準拠**
6. 変更内容を保存します。


## ネットワークパケットルールの優先順位の変更

ネットワークパケットルールの優先順位は、ネットワークパケットルールのリスト内の位置で決定されます。ネットワークパケットルールリストの最上位にあるルールの優先順位が最も高くなります。

手動で作成したネットワークパケットルールは、ネットワークパケットルールリストの末尾に追加され、その優先順位は最も低くなります。

ファイアウォールでは、ネットワークパケットルールはネットワークパケットルールリストの上から順に実行されます。ファイアウォールでは、特定のネットワーク接続に適用される処理済みの各ネットワークパケットルールに従って、そのネットワーク接続の設定で指定されているアドレスおよびポートへのネットワークアクセスが許可またはブロックされます。

ネットワークパケットルールの優先順位を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【パケットルール】** をクリックします。  
ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。
4. リストで、優先順位を変更するネットワークパケットルールを選択します。
5. **【上へ】** と **【下へ】** を使用してネットワークルールの優先度を設定します。
6. 変更内容を保存します。

## ネットワークパケットルールのエクスポートおよびインポート

ネットワークパケットルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のルールをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ネットワークパケットルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

[管理コンソール \(MMC\) でネットワークパケットルールのリストをエクスポートおよびインポートする方法](#) 

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔脅威対策〕** → **〔ファイアウォール〕** の順に選択します。
6. ネットワークパケットルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。  
ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
  - b. **〔エクスポート〕** をクリックします。
  - c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **〔保存〕** をクリックします。  
Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
7. ネットワークパケットルールのリストをインポートするには：
  - a. **〔インポート〕** をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. **〔開く〕** をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

## Web コンソールおよび Cloud コンソールでネットワークパケットルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ルールのリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[ファイアウォール]** の順に選択します。
5. **[ネットワークパケットルール]** をクリックします。
6. ネットワークパケットルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択したルールのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。
  - d. **[エクスポート]** をクリックします。  
Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを XML ファイルでエクスポートします。
7. ネットワークパケットルールのリストをインポートするには：
  - a. **[インポート]** をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. **[開く]** をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

## アプリケーションネットワークルールの管理

既定では、Kaspersky Endpoint Security はファイルまたはネットワークの動作が監視対象となっているソフトウェアの開発元名別に、コンピューターにインストールされているすべてのアプリケーションをグループ化します。アプリケーショングループは許可グループに分類されます。すべてのアプリケーションとアプリケーショングループは、アプリケーションコントロールルールプロパティ、アプリケーションネットワークルールプロパティ、実行優先順プロパティを親グループから継承します。

**[ホスト侵入防止]** と同様に、ファイアウォールは、グループ内にあるすべてのアプリケーションのネットワークの動作をフィルターする際に、アプリケーショングループに対してネットワークルールを適用するように既定で設定されています。アプリケーションネットワークルールでは、グループ内のアプリケーションによる異なるネットワーク接続へのアクセス権限が定義されます。



既定では、ファイアウォールは、Kaspersky Endpoint Security がコンピューター上で検知した各アプリケーショングループに対してネットワークルールを作成します。既定で作成されたアプリケーショングループのネットワークルールに適用されるファイアウォールの処理は変更できます。既定で作成されているアプリケーショングループのネットワークルールの優先度を編集、削除、無効化、変更することはできません。

個別のアプリケーションに対するネットワークルールも作成できます。そのルールは、アプリケーションが属するグループに対するネットワークルールよりも優先度が高くなります。

## アプリケーションネットワークルールの作成

既定では、アプリケーションの動作は、ネットワークルールによってコントロールされます。このルールは、Kaspersky Endpoint Security が初めて起動したときにアプリケーションを割り当てた許可グループに定義されます。必要に応じて、許可グループ全体、個別のアプリケーション、あるいは許可グループ内に定義されているアプリケーショングループのネットワークルールを作成できます。

手動で定義されたネットワークルールは、許可グループに定義されたネットワークルールより優先されます。言い換えると、手動で定義されたアプリケーションルールが許可グループに定義されたアプリケーションルールと異なる場合、ファイアウォールはそのアプリケーションに対して手動で定義されたルールに従って操作を制御します。

既定では、ファイアウォールは各アプリケーションに対して次のネットワークルールを作成します：

- 許可するネットワーク内のネットワークの動作。
- ローカルネットワーク内のネットワークの動作。
- パブリックネットワーク内のネットワークの動作。

Kaspersky Endpoint Security は以下のように事前定義されたネットワークに従ってアプリケーションのネットワークの動作を制御します：

- 信頼および弱い制限付き：すべてのネットワーク動作が許可されます。
- 強い制限付きおよびブロック：すべてのネットワーク動作がブロックされます。

事前定義されたアプリケーションルールは編集または削除することはできません。

次の方法でアプリケーションネットワークルールを作成できます：


- ネットワークモニターツールを使用する。  
ネットワークモニターは、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。ルールを設定する必要がないため便利です。一部のファイアウォールの設定はネットワークモニターのデータから自動的に挿入されます。ネットワークモニターは製品のインターフェイスのみで使用できます。
- ファイアウォールを設定する。  
ファイアウォールの設定を詳細に調整できます。その時点でネットワークの操作がない場合にも、ネットワークの動作に関してルールを作成できます。

アプリケーションネットワークルールを作成する際、ネットワークパケットルールはアプリケーションネットワークルールより優先されることに注意してください。

## 製品のインターフェイスでネットワークモニターツールを使用してアプリケーションネットワークルールを作成する方法

1. 製品のメインウィンドウの **[監視]** で、 **[ネットワークモニター]** をクリックします。
2. **[ネットワークの動作]** または **[開いているポート]** タブを選択します。  
 **[ネットワークの動作]** タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。  
 **[開いているポート]** タブには、コンピューターで開いているネットワークポートがすべて表示されます。
3. ネットワーク接続のコンテキストメニューで、 **[アプリケーションルールを作成]** を選択します。  
 アプリケーションルールおよびプロパティのウィンドウが開きます。
4. **[ネットワークルール]** タブを選択します。  
 ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
5. **[追加]** をクリックします。  
 ネットワークルールのプロパティが開きます。
6. **[名前]** フィールドに、ネットワークサービスの名前を手動で入力します。
7. ネットワークルールを設定します（下記の表を参照）。  
 **[ネットワークルールテンプレート]** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
 ネットワークルール設定は自動で入力されます。
8. ネットワークルールの処理を **レポート** に反映する場合は、 **[イベントを記録]** をオンにします。
9. **[保存]** をクリックします。  
 新しいネットワークルールがリストに追加されます。
10. **[上へ]** と **[下へ]** を使用してネットワークルールの優先度を設定します。
11. 変更内容を保存します。

## 製品のインターフェイスでファイアウォールの設定を使用してアプリケーションネットワークルールを作成する方法

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【アプリケーションルール】** をクリックします。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
4. アプリケーションのリストで、ネットワークルールを作成するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、**【詳細とルール】** を選択します。  
アプリケーションルールおよびプロパティのウィンドウが開きます。
6. **【ネットワークルール】** タブを選択します。
7. **【追加】** をクリックします。  
ネットワークルールのプロパティが開きます。
8. **【名前】** フィールドに、ネットワークサービスの名前を手動で入力します。
9. ネットワークルールを設定します（下記の表を参照）。  
**【ネットワークルールテンプレート】** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
10. ネットワークルールの処理を[レポート](#)に反映する場合は、**【イベントを記録】** をオンにします。
11. **【保存】** をクリックします。  
新しいネットワークルールがリストに追加されます。
12. **【上へ】** と **【下へ】** を使用してネットワークルールの優先度を設定します。
13. 変更内容を保存します。

## **管理コンソール (MMC) でアプリケーションネットワークルールを作成する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔脅威対策〕** → **〔ファイアウォール〕** の順に選択します。
6. **〔ファイアウォールの設定〕** ブロックで、 **〔設定〕** をクリックします。  
ネットワークパケットルールおよびアプリケーションネットワークルールのリストが表示されます。
7. **〔アプリケーションネットワークルール〕** タブを選択します。
8. **〔追加〕** をクリックします。
9. 表示されたウィンドウで、ネットワークルールを作成するアプリケーションを検索する条件を入力します。  
アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
10. **〔更新〕** をクリックします。  
Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。
11. 必要なアプリケーションを選択します。
12. **〔選択したアプリケーションを信頼グループに追加する〕** で、 **〔既定のグループ〕** を選択し、 **〔OK〕** をクリックします。  
アプリケーションが既定のグループに追加されます。
13. 対象のアプリケーションを選択して、アプリケーションのコンテキストメニューから **〔アプリケーション権限〕** を選択します。  
アプリケーションルールおよびプロパティのウィンドウが開きます。
14. **〔ネットワークルール〕** タブを選択します。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
15. **〔追加〕** をクリックします。  
ネットワークルールのプロパティが開きます。
16. **〔名前〕** フィールドに、ネットワークサービスの名前を手動で入力します。
17. ネットワークルールを設定します（下記の表を参照）。  
ボタン (🔍) をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
18. ネットワークルールの処理を [レポート](#) に反映する場合は、 **〔イベントを記録〕** をオンにします。

19. **【保存】** をクリックします。

新しいネットワークルールがリストに追加されます。

20. **【上へ】** と **【下へ】** を使用してネットワークルールの優先度を設定します。

21. 変更内容を保存します。

[Web コンソールと Cloud コンソールでアプリケーションネットワークルールを作成する方法](#) 

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[脅威対策]** → **[ファイアウォール]** の順に選択します。
5. **[ファイアウォールの設定]** ブロックで、**[アプリケーションネットワークルール]** をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
6. **[アプリケーション権限]** タブを選択します。  
ウィンドウの左側に許可グループのリスト、右側にそのプロパティが表示されます。
7. **[追加]** をクリックします。  
ウィザードがアプリケーションを許可グループに追加します。
8. アプリケーションに対して適切な許可グループを選択します。
9. **アプリケーション**の種別を選択します。 **[次へ]** をクリックします。  
複数のアプリケーションのネットワークルールを作成する場合は、**[グループ]** を選択してアプリケーショングループの名前を定義します。
10. アプリケーションのリストで、ネットワークルールを作成するアプリケーションを選択します。  
フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
11. **[OK]** をクリックしてウィザードを完了します。  
アプリケーションが許可グループに追加されます。
12. ウィンドウの左側で、アプリケーションを選択します。
13. ウィンドウの右側で、ドロップダウンリストから **[ネットワークルール]** を選択します。  
ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
14. **[追加]** をクリックします。  
アプリケーションルールのプロパティが開きます。
15. **[名前]** フィールドに、ネットワークサービスの名前を手動で入力します。
16. ネットワークルールを設定します（下記の表を参照）。  
**[テンプレートを選択]** をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。  
ネットワークルール設定は自動で入力されます。
17. ネットワークルールの処理を **レポート** に反映する場合は、**[イベントを記録]** をオンにします。
18. **[保存]** をクリックします。



新しいネットワークルールがリストに追加されます。

19. [上へ] と [下へ] を使用してネットワークルールの優先度を設定します。

20. 変更内容を保存します。

#### アプリケーションネットワークルールの設定

パラメータ	説明
処理	許可： ブロック：
プロトコル	選択したプロトコル（TCP、UDP、ICMP、ICMPv6、IGMP および GRE）に対してネットワークの動作を制御します。 ICMP または ICMPv6 プロトコルを選択すると、ICMP パケットの種類とコードを定義できます。 TCP または UDP をプロトコルの種類として選択すると、接続が監視されるローカルコンピューターとリモートコンピューターのポートをカンマ区切りで指定できます。
通信方向	受信 受信 / 送信 送信
リモートアドレス	ネットワークパケットを送信または受信するリモートコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のリモートネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めることも、IP アドレスの範囲を指定することも、IP アドレスごとに別のリストを作成することも、または許可するネットワーク、ローカルネットワーク、パブリックネットワークなどのサブネットを選択することもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。
ローカルアドレス	ネットワークパケットを送信または受信するコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のローカルネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めたり、IP アドレスごとに別のリストを作成したり、IP アドレスの範囲を指定したりすることもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">アプリケーションのローカルアドレスが取得できない場合があります。この場合、このパラメータは無視されます。</div>

## アプリケーションネットワークルールの有効化と無効化

アプリケーションネットワークルールを有効または無効にするには、次の手順を実行します：


1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【アプリケーションルール】** をクリックします。  
アプリケーションルールのリストのテーブルが開きます。
4. アプリケーションのリストで、ネットワークルールを作成または編集するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、**【詳細とルール】** を選択します。  
アプリケーションルールおよびプロパティのウィンドウが開きます。
6. **【ネットワークルール】** タブを選択します。
7. アプリケーショングループのネットワークルールのリストで、目的のネットワークルールを選択します。  
**【ネットワークルールのプロパティ】** ウィンドウが表示されます。
8. ネットワークルールに **【有効】** または **【無効】** を設定します。  
ファイアウォールによって既定で作成されたアプリケーショングループのネットワークルールは、無効にできません。
9. 変更内容を保存します。


## アプリケーションネットワークルールのファイアウォール処理の変更

アプリケーションまたはアプリケーショングループに対して既定で作成されたすべてのネットワークルールに適用されているファイアウォール処理を変更したり、アプリケーションまたはアプリケーショングループに対するカスタムネットワークルールのファイアウォール処理を変更したりできます。

アプリケーションまたはアプリケーショングループに対するすべてのネットワークルールに適用するファイアウォールの処理を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【ファイアウォール】** の順に選択します。
3. **【アプリケーションルール】** をクリックします。  
アプリケーションルールのリストのテーブルが開きます。
4. 既定で作成されるすべてのネットワークルールに適用するファイアウォールの処理を変更するには、リストでアプリケーションまたはアプリケーショングループを選択します。手動で作成されたネットワークルールは変更されません。
5. 右クリックでコンテキストメニューを開き、**【ネットワークルール】** を選択し、割り当てる操作を選択します：
  - **継承**
  - **許可：**
  - **ブロック：**
6. 変更内容を保存します。

アプリケーションまたはアプリケーショングループに対する単一のネットワークルールに適用するファイアウォールの処理を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイアウォール]** の順に選択します。
3. **[アプリケーションルール]** をクリックします。  
アプリケーションルールのリストのテーブルが開きます。
4. リストで、単一のネットワークルールに対する処理を変更するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、**[詳細とルール]** を選択します。  
アプリケーションルールおよびプロパティのウィンドウが開きます。
6. **[ネットワークルール]** タブを選択します。
7. ファイアウォールの処理を変更するネットワークルールを選択します。
8. **[権限]** 列で右クリックして、コンテキストメニューを表示し、割り当てる処理を次のいずれかから選択します：
  - **継承**
  - **許可**：
  - **ブロック**：
  - **イベントの記録**
9. 変更内容を保存します。


## アプリケーションネットワークルールの優先度の変更

ネットワークルールの優先度は、ネットワークルールのリスト内の位置によって決まります。ファイアウォールでは、アプリケーションネットワークルールはネットワークルールリストの上から順に実行されます。ファイアウォールでは、特定のネットワーク接続に適用される処理済みネットワークルールに従って、そのネットワーク接続の設定で示されているアドレスおよびポートへのネットワークアクセスが許可またはブロックされます。

手動で作成されたネットワークルールの優先度は、既定のネットワークルールよりも高くなります。

既定で作成されているアプリケーショングループのネットワークルールの優先度を変更することはできません。

ネットワークルールの優先度を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[ファイアウォール]** の順に選択します。

3. **「アプリケーションルール」** をクリックします。  
アプリケーションルールのリストのテーブルが開きます。
4. アプリケーションのリストで、ネットワークルールの優先度を変更するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、**「詳細とルール」** を選択します。  
アプリケーションルールおよびプロパティのウィンドウが開きます。
6. **「ネットワークルール」** タブを選択します。
7. 優先度を変更するネットワークルールを選択します。
8. **「上へ」** および **「下へ」** を使用して、ネットワークルールをリストの適切な場所に移動します。
9. 変更内容を保存します。

## ネットワークモニター

ネットワークモニターは、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。

ネットワークモニターを開始するには：

製品のメインウィンドウの **「監視」** で、**「ネットワークモニター」** をクリックします。

**「ネットワークモニター」** ウィンドウが表示されます。このウィンドウの次の4つのタブに、コンピューターのネットワークの動作に関する情報が表示されます：

- **「ネットワークの動作」** タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。このタブでは、ファイアウォールの操作のための [ネットワークパケットルールを作成](#) することができます。
- **「開いているポート」** タブには、コンピューターで開いているネットワークポートがすべて表示されます。このタブでは、ファイアウォールの操作のための [ネットワークパケットルール](#) および [アプリケーションルール](#) を作成することができます。
- **「ネットワークトラフィック」** タブには、ユーザーが現在接続しているネットワークにおける、クライアントコンピューターと他のコンピューターの間を送受信ネットワークトラフィックの量が表示されます。
- **「ブロック中のコンピューター」** タブには、ネットワーク攻撃の試行元として検知された後にネットワーク脅威対策によってネットワークの動作がブロックされたリモートコンピューターのIPアドレスが表示されます。

## 有害 USB 攻撃ブロック

ウイルスの中には、オペレーティングシステムでUSBデバイスがキーボードとして検知されるように、USBデバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します（下の図を参照）。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID および PID、キーボードが接続されたポート番号）が、認証されたキーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターの USB ポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、新しいコードが生成されます。[数値コードの入力試行回数は指定](#)できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合（下の図を参照）、本製品はキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックは、既定ではインストールされません。有害 USB 攻撃ブロックが必要な場合は、製品のインストール前に[インストールパッケージ](#)のプロパティにコンポーネントを追加するか、製品のインストール後に[利用可能なコンポーネントを変更](#)できます。




キーボード承認

## 有害 USB 攻撃ブロックの有効化と無効化

有害 USB 攻撃ブロックのインストール前にオペレーティングシステムによってキーボードとして識別され、コンピューターに接続された USB デバイスは、コンポーネントのインストール後は、認証済みとみなされます。

有害 USB 攻撃ブロックを有効または無効にするには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[有害 USB 攻撃ブロック]** の順に選択します。
3. **[有害 USB 攻撃ブロック]** トグルスイッチを使用して機能を有効または無効にします。
4. **[USB デバイスの認証]** で、認証コードの入力に関するセキュリティ設定を調整します：
  - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は1～10 です。たとえば、認証コードを5回まで許可する設定にすると、認証コードの入力を5回目に失敗したあとに USB デバイスがブロックされます。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを5回まで入力できます。
  - **最大試行回数を超えた場合のタイムアウト（分）**：認証コードの入力の失敗回数が指定した回数を超えた後に USB デバイスをブロックする時間です。有効な値は1～180（分）です。
5. 変更内容を保存します。

有害 USB 攻撃ブロックが有効になると、Kaspersky Endpoint Security はオペレーティングシステムによってキーボードとして認識された接続済みの USB デバイスの認証を要求します。認証されていないキーボードは、認証されるまでユーザーは使用できません。

## USB デバイスの認証時のセキュリティキーボードの使用

セキュリティキーボードは、任意の文字の入力をサポートしない USB デバイス（バーコードスキャナーなど）の認証時にのみ使用してください。未知の USB デバイスの認証時に、セキュリティキーボードを使用しないでください。

セキュリティキーボードを使用した認証を許可またはブロックするには：

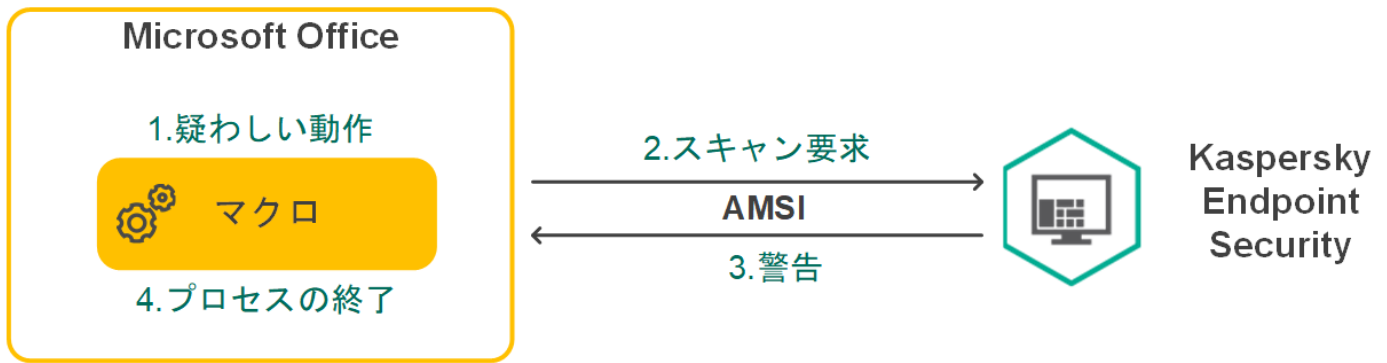
1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[脅威対策]** → **[有害 USB 攻撃ブロック]** の順に選択します。
3. **[USB デバイスの認証時にセキュリティキーボードの使用を禁止する]** を使用して認証時のセキュリティキーボードの使用をブロックまたは許可します。
4. 変更内容を保存します。

## AMSI 保護

AMSI 保護機能は Microsoft 社の AMSI (Antimalware Scan Interface) をサポートすることを目的とした機能です。AMSI (Antimalware Scan Interface) により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト（たとえば、PowerShell スクリプトなど）のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。対象となるサードパーティ製品としては、たとえば Microsoft Office 製品があります。AMSI について詳しくは、[Microsoft 社の資料](#) を参照してください。

AMSI 保護機能では、脅威の検知とサードパーティ製品への検知された脅威に関する通知のみを実行できます。脅威に関する通知を受信したサードパーティ製品側では、脅威による悪意のあるふるまいを許可しません（たとえば、プロセスを終了します）。





AMSI の動作例

また、一定間隔の間に特定のサードパーティ製品から上限を超えてスキャン要求を受信した場合などにも、AMSI 保護機能でそのサードパーティ製品からのスキャン要求を拒否する場合があります。Kaspersky Endpoint Security は、拒否したサードパーティ製品のスキャン要求に関する情報を管理サーバーに送信します。[\[AMSI 保護機能との相互作用をブロックしない\]](#) がオンになっているサードパーティ製品からのスキャン要求は拒否されません。


AMSI 保護機能は、ワークステーションおよびサーバー用の次のオペレーティングシステムで使用できます：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2022

## AMSI 保護の有効化と無効化

既定では、AMSI 保護は有効です。


AMSI 保護を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[\[脅威対策\]](#) → [\[AMSI 保護\]](#) の順に選択します。
3. [\[AMSI 保護\]](#) を使用して機能を有効または無効にします。
4. 変更内容を保存します。

## AMSI 保護機能を使用した複合ファイルのスキャン

ウイルスやその他のマルウェアの隠蔽には、アーカイブなどの複合ファイルに埋め込む技術が一般的に使用されています。このような方法で隠されているウイルスやその他のマルウェアを検知するためには、複合ファイルを解凍する必要がありますが、スキャンの速度が低下する場合があります。スキャンする複合ファイル種別を限定することで、スキャンを高速化できます。

AMSI保護機能を使用した複合ファイルのスキャンを設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【脅威対策】** → **【AMSI 保護】** の順に選択します。
3. **【複合ファイルのスキャン】** セクションで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。
4. **【サイズ制限】** セクションで、次のいずれかを実行します：
  - AMSI 保護を使用して大きな複合ファイルを解凍しない場合は、**【大きな複合ファイルのスキャンしない】** をオンにし、**【ファイルの最大サイズ】** に任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
  - AMSI 保護を使用して大きな複合ファイルを解凍する場合は、**【大きな複合ファイルのスキャンしない】** をオフにします。

アーカイブから展開されるサイズの大きいファイルは、**【大きな複合ファイルのスキャンしない】** がオンにされているかどうかに関係なくスキャンされます。

5. 変更内容を保存します。


## 脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとする、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。

## 脆弱性攻撃ブロックの有効化と無効化

既定では、脆弱性攻撃ブロックは有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。必要に応じて、脆弱性攻撃ブロックを停止できます。

脆弱性攻撃ブロックを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【先進の脅威対策】** → **【脆弱性攻撃ブロック】** の順に選択します。
3. **【脆弱性攻撃ブロック】** を使用して機能を有効または無効にします。


4. 変更内容を保存します。

脆弱性攻撃ブロックを有効にすると、Kaspersky Endpoint Security は脆弱性があるアプリケーションによって実行されるファイルを監視します。脆弱性があるアプリケーションのファイルが、そのユーザー以外によって使用されていることを検知した場合、本製品は操作をブロックするなど、選択されている処理を行います。

## 攻撃を検知した場合に行う処理の選択

既定では、脆弱性を利用した攻撃が検知されると、攻撃によって試行された処理をブロックします。


攻撃を検知した場合に行う処理を選択するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[脆弱性攻撃ブロック]** の順に選択します。
3. 必要な処理を **[攻撃を検知したとき]** ドロップダウンリストから選択します：
  - **操作をブロックする**：この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。
  - **通知する**：この項目を選択した場合、攻撃が検知されると、攻撃に関する情報がログに記録され、攻撃に関する情報がアクティブな脅威のリストに追加されます。
4. 変更内容を保存します。

## システムプロセスのメモリ保護

既定では、システムプロセスのメモリ保護は有効です。

システムプロセスのメモリ保護を有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[脆弱性攻撃ブロック]** の順に選択します。
3. **[システムプロセスのメモリ保護を有効にする]** トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

Kaspersky Endpoint Security はシステムプロセスへアクセスしようとする外部プロセスをブロックします。

## ふるまい検知


ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures (BSS) を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

## ふるまい検知の有効化と無効化

既定では、ふるまい検知は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。必要に応じて、ふるまい検知を停止できます。

ふるまい検知を無効にすると、保護機能のパフォーマンスが低下するため、絶対に必要な場合を除いて無効にしないでください。脅威を検知するために、保護機能がふるまい検知によって収集されたデータを要求する場合があります。


ふるまい検知を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【先進の脅威対策】** → **【ふるまい検知】** の順に選択します。
3. **【ふるまい検知】** を使用して機能を有効または無効にします。
4. 変更内容を保存します。

ふるまい検知が有効になっていると、Kaspersky Endpoint Security はオペレーティングシステム内で行われるアプリケーションの動作を、Behavior Stream Signatures を使用して分析します。

## マルウェアの動作を検知したときに実行する処理の選択

悪意のある動作を行うアプリケーションがあった場合の対応を選択するには、次の手順を行ってください：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【先進の脅威対策】** → **【ふるまい検知】** の順に選択します。
3. **【マルウェアの動作を検知したとき】** ブロックで、必要な処理を選択します：
  - **ファイルを削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
  - **アプリケーションを終了する**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。
  - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。
4. 変更内容を保存します。

## 外部からの暗号化に対する共有フォルダーの保護

このコンポーネントは、NTFS ファイルシステムを使用しており EFS で暗号化されていない大容量ストレージデバイスに保存されたファイルに対する操作のみを監視します。

外部からの暗号化に対する共有フォルダーの保護は、共有フォルダー内の操作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。


既定では、外部からの暗号化に対する共有フォルダーの保護は無効になっています。

Kaspersky Endpoint Security のインストール後、コンピューターを再起動するまでは、外部からの暗号化に対する共有フォルダーの保護は制限されます。

## 外部からの暗号化に対する共有フォルダーの保護の有効化または無効化


Kaspersky Endpoint Security のインストール後、コンピューターを再起動するまでは、外部からの暗号化に対する共有フォルダーの保護は制限されます。

外部からの暗号化に対する共有フォルダーの保護を有効化または無効化するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ふるまい検知]** の順に選択します。
3. **[外部からの暗号化に対する共有フォルダーの保護を有効にする]** を使用して、外部からの暗号化を示唆する操作の検知を有効または無効にします。
4. 変更内容を保存します。

## 外部からの共有フォルダーの暗号化を検知した場合に行う処理の選択

外部からの共有フォルダーの暗号化を検知した場合に行う処理を選択するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ふるまい検知]** の順に選択します。
3. **[外部からの暗号化に対する共有フォルダーの保護]** ブロックで関連する操作を選択します。
  - **接続をブロックする時間**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、次の操作が実行されます：
    - 変更を試行しているコンピューターによるネットワーク動作をブロックします。
    - 変更されようとしているファイルのバックアップコピーを作成します。
    - [ローカルアプリケーションインターフェイスのレポート](#) にレコードが追加されます。

- 検知された悪意のある活動に関する情報を Kaspersky Security Center に送信します。

また、修復エンジンがオンの場合、変更されたファイルがバックアップコピーから復元されます。

- **通知する**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、次の操作が実行されます：

- [ローカルアプリケーションインターフェイスのレポート](#)にレコードが追加されます。
- 項目をアクティブな脅威のリストに追加します。
- 検知された悪意のある活動に関する情報を Kaspersky Security Center に送信します。


4. 変更内容を保存します。

## 外部からの暗号化に対する共有フォルダーの保護から除外するアドレスの設定

外部からの暗号化に対する共有フォルダーの保護から除外するアドレスを設定するには、ログオンの監査サービスを有効にしておく必要があります。既定では、ログオンの監査サービスは無効です（ログオンの監査サービスの有効化に関する詳細な情報については、Microsoft の Web サイトを参照してください）。

共有フォルダーの保護からアドレスを除外する機能は、Kaspersky Endpoint Security が開始する前から動作しているリモートコンピューターに対しては適用されません。Kaspersky Endpoint Security が開始した後でリモートコンピューターを再起動することで、そのリモートコンピューターに対して共有フォルダーの保護からアドレスを除外する機能が有効になります。

共有フォルダーに対して外部からの暗号化を実行するリモートコンピューターを除外するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ふるまい検知]** の順に選択します。
3. **[除外リスト]** ブロックで、**[除外リストの設定]** をクリックします。
4. 除外リストに IP アドレスまたはコンピューター名を追加するには、**[追加]** をクリックします。
5. 外部からの暗号化に対する処理を実行しない IP アドレスまたはコンピューター名を入力します。
6. 変更内容を保存します。

## 外部からの暗号化に対する共有フォルダーの保護の除外リストのエクスポートおよびインポート

除外リストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーにリストを移行することができます。



## 管理コンソール (MMC) で除外リストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ふるまい検知] の順に選択します。
6. [外部からの暗号化に対する共有フォルダーの保護] セクションで、 [除外リスト] をクリックします。
7. ルールのリストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。複数のポートを選択するには、CTRL または SHIFT キーを使用します。  
除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。
  - b. [エクスポート] をクリックします。
  - c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. [保存] をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
8. 除外リストをインポートするには：
  - a. [インポート] をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. [開く] をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
9. 変更内容を保存します。

## Web コンソールおよび Cloud コンソールで除外リストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 除外リストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[ふるまい検知]** を選択します。
5. **[除外リスト]** ブロックで除外リストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。
  - d. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - e. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
6. **[除外リスト]** ブロックで除外リストをインポートするには：
  - a. **[インポート]** をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. **[開く]** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
7. 変更内容を保存します。

## ホスト侵入防止

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。

コンポーネントは、アプリケーション権限を使用してアプリケーションの動作を制御します。アプリケーション権限には、次のアクセスパラメータが含まれます：

- オペレーティングシステムリソースへのアクセス（自動起動オプション、レジストリキーなど）
- 個人データ（ファイルやアプリケーションなど）へのアクセス

アプリケーションのネットワーク動作は、ネットワークルールを使用して[ファイアウォール](#)によって制御されます。

アプリケーションの最初の起動時に、ホスト侵入防止は次の処理を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティの確認。

ホスト侵入防止がより効果的に機能するように、[Kaspersky Security Network に参加](#)することを推奨します。

3. 信頼グループのいずれかにアプリケーションを配置します：信頼、弱い制限付き、強い制限付き、ブロック。

[許可グループ](#)は、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は [ホスト侵入防止の設定](#) に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じてアプリケーション動作をブロックします。たとえば、高い制限付きの信頼グループのアプリケーションは、オペレーティングシステムモジュールへのアクセスを拒否されます。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のアプリケーション権限をそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

## ホスト侵入防止の有効化と無効化

既定では、ホスト侵入防止は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。


[管理コンソール \(MMC\) でホスト侵入防止を有効または無効にする方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [ホスト侵入防止] を使用して機能を有効または無効にします。
7. 変更内容を保存します。

### Web コンソールおよび Cloud コンソールでホスト侵入防止を有効または無効にする方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [先進の脅威対策] → [ホスト侵入防止] を選択します。
5. [ホスト侵入防止] トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

### 製品インターフェイスでホスト侵入防止を有効または無効にする方法

1. メインウィンドウで、  をクリックします。
2. 本製品の設定ウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
3. [ホスト侵入防止] トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

ホスト侵入防止機能が有効になっている場合、Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを [信頼グループ](#) に配置します。Kaspersky Endpoint Security は許可グループに基づいてアプリケーションの操作をブロックします。

## アプリケーション許可グループの管理

アプリケーションを初めて起動するたびに、ホスト侵入防止がアプリケーションのセキュリティをチェックし、[許可グループ](#)の1つに割り当てます。

アプリケーションスキャンでは、Kaspersky Endpoint Security はまず既知のアプリケーションの定義データベースを検索して一致するエントリを探し、同時に Kaspersky Security Network データベースに要求を送信します（インターネット接続が利用できる場合）。定義データベースと Kaspersky Security Network データベースの検索結果に基づいて、アプリケーションがいずれかの許可グループに配置されます。次回以降、アプリケーションが起動するたびに、Kaspersky Endpoint Security は KSN にアプリケーションの評価を問い合わせ、KSN データベースでのアプリケーションの評価が変更された場合には、アプリケーションを別の許可グループに移動します。

Kaspersky Endpoint Security が [すべての不明なアプリケーションを自動的に割り当てる](#) 許可グループを指定することもできます。Kaspersky Endpoint Security の前に起動したアプリケーションは、[\[ホスト侵入防止の設定\] ウィンドウで指定された](#) 許可グループに自動的に移動します。

Kaspersky Endpoint Security より前に起動したアプリケーションについては、ネットワーク動作のみ管理されます。管理は、[ファイアウォールで指定](#)されたネットワークルールに従って実行されます。

## アプリケーションの許可グループを変更する

アプリケーションを初めて起動するたびに、ホスト侵入防止がアプリケーションのセキュリティをチェックし、[許可グループ](#)の1つに割り当てます。

アプリケーションを自動的に割り当てられた許可グループから別の許可グループに移動することは推奨されません。代わりに、必要に応じて、[個別のアプリケーションの権限を編集](#)できます。

### [管理コンソール \(MMC\) でアプリケーションの許可グループを変更する方法](#)


1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **「管理対象デバイス」** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **「ポリシー」** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **「先進の脅威対策」** → **「ホスト侵入防止」** の順に選択します。
6. **「アプリケーションコントロールルールと保護対象のリソース」** で、 **「設定」** をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
7. **「アプリケーション権限」** タブを選択します。
8. **「追加」** をクリックします。
9. 表示されたウィンドウで、許可グループを変更するアプリケーションを検索する条件を入力します。  
アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字 **「\*」** および **「？」** をサポートします。
10. **「更新」** をクリックします。  
Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。
11. 必要なアプリケーションを選択します。
12. **「選択したアプリケーションを信頼グループに追加する」** で、アプリケーションの許可グループを選択します。
13. 変更内容を保存します。


## [Web コンソールおよび Cloud コンソールで製品の許可グループを変更する方法](#)



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[ホスト侵入防止]** を選択します。
5. **[アプリケーション権限と保護対象のリソース]** で、**[アプリケーション権限と保護対象のリソース]** をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
6. **[アプリケーション権限]** タブを選択します。  
ウィンドウの左側に許可グループのリスト、右側にそのプロパティが表示されます。
7. **[追加]** をクリックします。  
ウィザードがアプリケーションを許可グループに追加します。
8. アプリケーションに対して適切な許可グループを選択します。
9. **アプリケーション**の種別を選択します。 **[次へ]** をクリックします。  
複数のアプリケーションの許可グループを変更する場合は、**[グループ]** を選択してアプリケーショングループの名前を定義します。
10. アプリケーションのリストで、変更するアプリケーショングループを選択します。  
フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
11. **[OK]** をクリックしてウィザードを完了します。  
アプリケーションが許可グループに追加されます。
12. 変更内容を保存します。

## **製品のインターフェイスでアプリケーションの許可グループを変更する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの管理]** 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が開きます。
4. 必要なアプリケーションを選択します。
5. アプリケーションのコンテキストメニューから **[制限]** → **<許可グループ>** をクリックします。
6. 変更内容を保存します。

アプリケーションは別の許可グループに追加されます。Kaspersky Endpoint Security は許可グループに基づいてアプリケーションの操作をブロックします。 (ユーザー定義)ステータスがアプリケーションに割り当てられます。Kaspersky Security Network でアプリケーションの評価が変更された場合、ホスト侵入防止機能はアプリケーションの許可グループを変更しません。

## 許可グループの権限の設定

既定では、許可グループごとに[最適なアプリケーション権限](#)が作成されます。許可グループに含まれるアプリケーショングループの権限の設定は、許可グループの権限の設定を継承します。

[管理コンソール \(MMC\) で許可グループの権限を変更する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーションコントロールルールと保護対象のリソース] で、 [設定] をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
7. [アプリケーション権限] タブを選択します。
8. 必要な許可グループを選択します。
9. 許可グループのコンテキストメニューから [グループ権限] を選択します。  
許可グループのプロパティが開きます。
10. 次のいずれかの手順を実行します：
  - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、 [ファイルとシステムレジストリ] タブを選択します。
  - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、 [権限] タブを選択します。


アプリケーションのネットワーク動作は、ネットワークルールを使用して [ファイアウォール](#) によって制御されます。

11. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します： **継承**、 **許可** (✓) または **禁止** (⊗)。
12. コンピューターのリソース使用を監視する場合は、 [イベントを記録] (✓ / ⊗) を選択します。  
Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます (許可または禁止)。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。
13. 変更内容を保存します。

## [Web コンソールと Cloud コンソールで許可グループの権限を変更する方法](#)

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
  2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
  3. [アプリケーション設定] タブを選択します。
  4. [先進の脅威対策] → [ホスト侵入防止] を選択します。
  5. [アプリケーション権限と保護対象のリソース] で、[アプリケーション権限と保護対象のリソース] をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
  6. [アプリケーション権限] タブを選択します。  
ウィンドウの左側に許可グループのリスト、右側にそのプロパティが表示されます。
  7. ウィンドウの左側で、対応する許可グループを選択します。
  8. ウィンドウの右側で、ドロップダウンリストから次のいずれかを実行します：
    - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、[ファイルとシステムレジストリ] を選択します。
    - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、[権限] を選択します。
- アプリケーションのネットワーク動作は、ネットワークルールを使用して[ファイアウォール](#)によって制御されます。
9. 関連するリソースに関しては、対応する操作の列で必要な次のオプションを選択します：継承、許可 (✓) または 禁止 (✗)。
  10. コンピューターのリソース使用を監視する場合は、[イベントを記録] (✓/✗) を選択します。  
Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます (許可または禁止)。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。
  11. 変更内容を保存します。

## 製品インターフェイスで許可グループの権限を変更する方法

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの管理]** 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が開きます。
4. 必要な許可グループを選択します。
5. 許可グループのコンテキストメニューから **[詳細とルール]** を選択します。  
許可グループのプロパティが開きます。
6. 次のいずれかの手順を実行します：
  - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、**[ファイルとシステムレジストリ]** タブを選択します。
  - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、**[権限]** タブを選択します。

アプリケーションのネットワーク動作は、ネットワークルールを使用して [ファイアウォール](#) によって制御されます。

7. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可** (🟢) または **禁止** (🔴)。
8. コンピューターのリソース使用を監視する場合は、**[イベントを記録]** (📄) を選択します。  
Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます (許可または禁止)。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。
9. 変更内容を保存します。

許可グループの権限が変更されます。Kaspersky Endpoint Security は許可グループに基づいてアプリケーションの操作をブロックします。■の状態 (ユーザー設定) が許可グループに割り当てられます。

## Kaspersky Endpoint Security の前に起動したアプリケーションの許可グループを選択する

Kaspersky Endpoint Security より前に起動したアプリケーションについては、ネットワーク動作のみ管理されます。管理は、ファイアウォールで指定された [ネットワークルール](#) に従って実行されます。アプリケーションのネットワーク活動を監視するときに適用するネットワークルールを指定するには、許可グループを選択します。


[管理コンソール \(MMC\) で Kaspersky Endpoint Security の前に起動したアプリケーションの許可グループを選択する方法](#) 

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーション権限] ブロックで、 [編集] をクリックします。
7. [本製品より前に起動したアプリケーションの信頼グループ] には、適切な 信頼グループ を選択します。
8. 変更内容を保存します。

#### Web コンソールおよび Cloud コンソールで Kaspersky Endpoint Security の前に起動したアプリケーションの許可グループを選択する方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [先進の脅威対策] → [ホスト侵入防止] を選択します。
5. [本製品より前に起動したアプリケーションの信頼グループ] には、適切な 信頼グループ を選択します。
6. 変更内容を保存します。

#### 製品インターフェイスで Kaspersky Endpoint Security の前に起動したアプリケーションの許可グループを選択する方法

1. メインウィンドウで、  をクリックします。
2. 本製品の設定ウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
3. [本製品より前に起動したアプリケーションの信頼グループ] で、適切な 信頼グループ を選択します。
4. 変更内容を保存します。



Kaspersky Endpoint Security より前に起動したアプリケーションはその他の許可グループに追加されます。Kaspersky Endpoint Security は許可グループに基づいてアプリケーションの操作をブロックします。

## 不明なアプリケーションに許可グループを選択する

アプリケーションの初回起動時に、ホスト侵入防止機能はアプリケーションの許可グループを決定します。インターネット接続がないか、Kaspersky Security Network にこのアプリケーションに関する情報がない場合、Kaspersky Endpoint Security は既定でこのアプリケーションを「弱い制限付き」グループに配置します。KSN でこの不明だったアプリケーションに関する情報が検知されると、Kaspersky Endpoint Security はこのアプリケーションの権限を更新します。その後、[アプリケーションの権限を手動で編集](#)できます。


### [管理コンソール \(MMC\) で不明なアプリケーションに許可グループを選択する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーションの処理ルール] ブロックで、[既存のグループに追加できないアプリケーションの信頼グループ] ドロップダウンリストから必要な許可グループを選択します。  
[Kaspersky Security Network への参加が有効](#)な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の許可グループに振り分けられることがあります。
7. [未知のアプリケーションの権限を KSN データベースからアップデートする] を使用して、不明なアプリケーションの権限の自動更新を設定します。
8. 変更内容を保存します。

### [Web コンソールおよび Cloud コンソールで不明なアプリケーションに許可グループを選択する方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[ホスト侵入防止]** を選択します。
5. **[アプリケーションの処理ルール]** ブロックで、**[既存のグループに追加できないアプリケーションの信頼グループ]** ドロップダウンリストから必要な許可グループを選択します。  
[Kaspersky Security Network への参加が有効](#)な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の許可グループに振り分けられることがあります。
6. **[未知のアプリケーションの権限を KSN データベースからアップデートする]** を使用して、不明なアプリケーションの権限の自動更新を設定します。
7. 変更内容を保存します。

#### **製品インターフェイスで不明なアプリケーションに許可グループを選択する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの処理ルール]** で、必要な信頼グループを選択します。  
[Kaspersky Security Network への参加が有効](#)な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の許可グループに振り分けられることがあります。
4. **[不明だったアプリケーションのルールを KSN から更新する]** を使用して、不明なアプリケーションの権限の自動更新を設定します。
5. 変更内容を保存します。

## デジタル署名されたアプリケーションに許可グループを選択する

Kaspersky Endpoint Security は、Microsoft の証明書およびカスペルスキーの証明書で署名されたアプリケーションを常に「許可」グループに配置します。


#### **管理コンソール (MMC) でデジタル署名されたアプリケーションに許可グループを選択する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーションの処理ルール] ブロックで、 [デジタル署名があるアプリケーションを信頼する] を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する許可グループの自動割り当てを有効または無効にします。  
信頼済みの製造元とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。 [手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加](#)することも可能です。  
このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して [許可グループ](#) を決定します。
7. 変更内容を保存します。

#### Web コンソールおよび Cloud コンソールでデジタル署名されたアプリケーションに許可グループを選択する方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [先進の脅威対策] → [ホスト侵入防止] を選択します。
5. [アプリケーションの処理ルール] ブロックで、 [デジタル署名があるアプリケーションを信頼する] を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する許可グループの自動割り当てを有効または無効にします。  
信頼済みの製造元とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。 [手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加](#)することも可能です。  
このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して [許可グループ](#) を決定します。
6. 変更内容を保存します。

#### 製品インターフェイスでデジタル署名されたアプリケーションに許可グループを選択する方法

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの処理ルール]** ブロックで、**[デジタル署名があるアプリケーションを信頼する]** を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する許可グループの自動割り当てを有効または無効にします。  
信頼済みの製造元とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。[手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加](#)することも可能です。  
このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して[許可グループ](#)を決定します。
4. 変更内容を保存します。

## アプリケーション権限の管理

既定では、アプリケーションの動作は、アプリケーションの権限によってコントロールされます。このルールは、Kaspersky Endpoint Security が初めて起動したときにアプリケーションを割り当てた[許可グループ](#)に定義されます。必要に応じて、許可グループ全体、個別のアプリケーション、あるいは許可グループ内に定義されているアプリケーショングループの[アプリケーションの権限を編集](#)できます。

手動で定義されたアプリケーションの権限は、許可グループに定義されたアプリケーションの権限より優先されます。言い換えると、手動で定義されたアプリケーションの権限が許可グループに定義されたアプリケーションの権限と異なる場合、ホスト侵入防止はそのアプリケーションに対して手動で定義された権限に従って操作を制御します。

アプリケーションに対して作成したルールは、子アプリケーションに継承されます。例えば、cmd.exe のすべてのネットワーク操作をブロックした場合、cmd.exe により開始された notepad.exe ではすべてのネットワーク操作がブロックされます。アプリケーションが、アプリケーションの子アプリケーションでない別のアプリケーションから開始された場合、ルールは継承されません。

### [管理コンソール \(MMC\) でアプリケーションの権限を変更する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーションコントロールルールと保護対象のリソース] で、 [設定] をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
7. [アプリケーション権限] タブを選択します。
8. [追加] をクリックします。
9. 表示されたウィンドウで、アプリケーションの権限を変更するアプリケーションを検索する条件を入力します。  
アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
10. [更新] をクリックします。  
Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。
11. 必要なアプリケーションを選択します。
12. [選択したアプリケーションを次の信頼グループに追加] で、 [既定のグループ] を選択し、 [OK] をクリックします。  
アプリケーションが既定のグループに追加されます。
13. 対象のアプリケーションを選択して、アプリケーションのコンテキストメニューから [アプリケーション権限] を選択します。  
アプリケーションのプロパティが表示されます。
14. 次のいずれかの手順を実行します：
  - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、 [ファイルとシステムレジストリ] タブを選択します。
  - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、 [権限] タブを選択します。

アプリケーションのネットワーク動作は、ネットワークルールを使用して[ファイアウォール](#)によって制御されます。

15. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可** (✓) または **禁止** (⊗)。





16. コンピューターのリソース使用を監視する場合は、**「イベントを記録」** (  /  ) を選択します。

Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

17. 変更内容を保存します。

## [Web コンソールと Cloud コンソールでアプリケーションの権限を変更する方法](#)







1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
  2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
  3. [アプリケーション設定] タブを選択します。
  4. [先進の脅威対策] → [ホスト侵入防止] を選択します。
  5. [アプリケーション権限と保護対象のリソース] で、[アプリケーション権限と保護対象のリソース] をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
  6. [アプリケーション権限] タブを選択します。  
ウィンドウの左側に許可グループのリスト、右側にそのプロパティが表示されます。
  7. [追加] をクリックします。  
ウィザードがアプリケーションを許可グループに追加します。
  8. アプリケーションに対して適切な許可グループを選択します。
  9. アプリケーションの種別を選択します。 [次へ] をクリックします。  
複数のアプリケーションの許可グループを変更する場合は、[グループ] を選択してアプリケーショングループの名前を定義します。
  10. アプリケーションのリストで、変更するアプリケーションの権限を選択します。  
フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
  11. [OK] をクリックしてウィザードを完了します。  
アプリケーションが許可グループに追加されます。
  12. ウィンドウの左側で、アプリケーションを選択します。
  13. ウィンドウの右側で、ドロップダウンリストから次のいずれかを実行します：
    - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、[ファイルとシステムレジストリ] を選択します。
    - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、[権限] を選択します。
- アプリケーションのネットワーク動作は、ネットワークルールを使用して[ファイアウォール](#)によって制御されます。
14. 関連するリソースに関しては、対応する操作の列で必要な次のオプションを選択します：継承、許可 (  ) または 禁止 (  ) 。
  15. コンピューターのリソース使用を監視する場合は、[イベントを記録] (  /  ) を選択します。

Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

16. 変更内容を保存します。

## [製品インターフェイスでアプリケーションの権限を変更する方法](#)

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの管理]** 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が開きます。
4. 必要なアプリケーションを選択します。
5. アプリケーションのコンテキストメニューから **[詳細とルール]** を選択します。  
アプリケーションのプロパティが表示されます。
6. 次のいずれかの手順を実行します：
  - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への許可グループの権限を編集するには、**[ファイルとシステムレジストリ]** タブを選択します。
  - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する許可グループの権限を編集する場合は、**[権限]** タブを選択します。
7. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可** () または **禁止** ()。
8. コンピューターのリソース使用を監視する場合は、**[イベントを記録]** () を選択します。  
Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。
9. **[除外リスト]** タブを選択して、アプリケーションの詳細を設定します（下記の表を参照）。
10. 変更内容を保存します。

アプリケーションの詳細設定

パラメータ	説明
開いたファイルをスキャンしない	アプリケーションが開いたファイルはすべて Kaspersky Endpoint Security のスキャンの対象外になります。例えば、信頼するアプリケーションを使用してファイルのバックアップをしていた場合など、この機能により Kaspersky Endpoint Security のリソースの消費量を減少させることができます。
アプリケーションの動作を監視しない	Kaspersky Endpoint Security はアプリケーションのファイルとオペレーティングシステム内のネットワークアクティビティを監視しません。アプリケーションの動作は、 <a href="#">ふるまい検知</a> 、 <a href="#">脆弱性攻撃ブロック</a> 、 <a href="#">ホスト侵入防止</a> 、 <a href="#">修復エンジン</a> および <a href="#">ファイアウォール</a> により監視されています。
親プロセス (親アプリケーション) の制限を継承しない	親プロセスで設定された制限は子プロセスには適用されません。親プロセスは、 <a href="#">アプリケーション権限</a> (ホスト侵入防止) および <a href="#">アプリケーションネットワークルール</a> (ファイアウォール) が設定されたアプリケーションによって開始されます。
子アプリケーションの動作を監視しない	Kaspersky Endpoint Security はファイルまたはこのアプリケーションによって開始されたアプリケーションのネットワークの動作を監視しません。
アプリケーションインターフェイス	<a href="#">Kaspersky Endpoint Security のセルフディフェンス</a> は、リモートコンピューターからのアプリケーションサービスを管理しようとする試みをすべて

との相互作用を許可する	ブロックします。このチェックボックスをオンにすると、リモートアクセスアプリケーションで Kaspersky Endpoint Security インターフェイスを経由して Kaspersky Endpoint Security 設定を管理できます。
暗号化されたネットワークトラフィックをスキャンしない / すべてのトラフィックをスキャンしない	アプリケーションにより開始されたネットワークトラフィックは Kaspersky Endpoint Security のスキャンから除外されます。すべてのトラフィックまたは暗号化されたトラフィックをスキャンから除外することも可能です。個別の IP アドレスおよびポート番号をスキャンから除外することも可能です。

## オペレーティングシステムのリソースと個人データの保護

ホスト侵入防止は、さまざまなカテゴリのオペレーティングシステムリソースおよび個人情報の処理を可能にするアプリケーションの権限を管理します。カスペルスキーのエキスパートは、保護対象のリソースの事前設定カテゴリを確立しています。たとえば、[オペレーティングシステム] カテゴリには、アプリケーションの自動実行に関連付けられたすべてのレジストリキーを一覧にする [スタートアップ設定] サブカテゴリがあります。これらのカテゴリ内の保護対象のリソースまたは保護対象のリソースの事前設定カテゴリを編集したり、削除したりすることはできません。



### [管理コンソール \(MMC\) で保護対象のリソースを追加する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [ホスト侵入防止] の順に選択します。
6. [アプリケーションコントロールルールと保護対象のリソース] で、 [設定] をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
7. [保護対象のリソース] タブを選択します。  
ウィンドウの左側に保護対象のリソースのリストと、対応する許可グループに基づいたこれらのリソースにアクセスするための権限が表示されます。
8. 新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。  
サブカテゴリを追加する場合は、 [追加] → [カテゴリ] の順に選択します。
9. [追加] をクリックします。ドロップダウンリストで、追加したいリソースの種別を選択します：  
[ファイルまたはフォルダー]、または [レジストリキー]。
10. 表示されたウィンドウで、ファイル、フォルダーまたはレジストリキーを選択します。  
追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security が各許可グループのアクセス権を表示します。新しいリソースの横にあるチェックボックスを使用して、リソースに対するアプリケーションの操作のコントロールを無効にすることも可能です。
11. 変更内容を保存します。

## Web コンソールと Cloud コンソールで保護対象のリソースを追加する方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[ホスト侵入防止]** を選択します。
5. **[アプリケーション権限と保護対象のリソース]** で、**[アプリケーション権限と保護対象のリソース]** をクリックします。  
アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
6. **[保護対象のリソース]** タブを選択します。  
ウィンドウの左側に保護対象のリソースのリストと、対応する許可グループに基づいたこれらのリソースにアクセスするための権限が表示されます。
7. **[追加]** をクリックします。  
新規リソースウィザードが表示されます。
8. **[グループ名]** をクリックして新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。  
サブカテゴリを追加する場合は、**[保護対象のリソースのカテゴリ]** を選択します。
9. 追加したいリソースの種別を選択します：**[ファイルまたはフォルダー]**、または**[レジストリキー]**。
10. ファイル、フォルダー、またはレジストリキーを選択します。
11. **[OK]** をクリックしてウィザードを完了します。  
追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security が各許可グループのアクセス権を表示します。**[状態]** 列のチェックボックスを使用して、アプリケーションのリソースに対する操作のコントロールを無効にできます。
12. 変更内容を保存します。

## **製品インターフェイスで保護対象のリソースを追加する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[リソースの管理]** をクリックします。  
保護対象のリソースのリストが表示されます。
4. 新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。  
サブカテゴリを追加する場合は、**[追加]** → **[カテゴリ]** の順に選択します。
5. **[追加]** をクリックします。ドロップダウンリストで、追加したいリソースの種別を選択します：  
**[ファイルまたはフォルダー]**、または **[レジストリキー]**。
6. 表示されたウィンドウで、ファイル、フォルダーまたはレジストリキーを選択します。  
追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security がアプリケーションのリストおよび各アプリケーションのアクセス権を表示します。**[状態]** 列の **[コントロールを無効にする]** () を使用して、リソースに対するアプリケーションの操作のコントロールを無効にすることができます。
7. 変更内容を保存します。

Kaspersky Endpoint Security は追加されたオペレーティングシステムのリソースや個人データへのアクセスを管理します。Kaspersky Endpoint Security はアプリケーションに割り当てられた許可グループに基づいてアプリケーションのリソースへのアクセスをコントロールします。[アプリケーションの信頼グループは手動で変更](#)できます。

## 未使用のアプリケーションに関する情報の削除

Kaspersky Endpoint Security は、アプリケーションの権限を使用して、アプリケーションの活動を制御します。アプリケーションの権限は、信頼グループによって決定されます。Kaspersky Endpoint Security はアプリケーションの初回起動時にアプリケーションを許可グループに追加します。[アプリケーションの信頼グループは手動で変更](#)できます。[個々のアプリケーションの権限を手動で構成](#)することもできます。Kaspersky Endpoint Security は、アプリケーションに関する次の情報を保存します：アプリケーションの信頼グループ、およびアプリケーション権限。

Kaspersky Endpoint Security は、未使用のアプリケーションに関する情報を自動的に削除して、コンピューターのリソースを節約します。Kaspersky Endpoint Security は、次のルールに従ってアプリケーションの情報を削除します：

- アプリケーションの許可グループと権限が自動的に決定された場合は、Kaspersky Endpoint Security は 30 日後にこのアプリケーションに関する情報を削除します。アプリケーション情報の保管期間を変更したり、自動削除をオフにしたりすることはできません。
- アプリケーションを手動で信頼グループに入れるか、アクセス権を設定した場合、Kaspersky Endpoint Security は 60 日（既定の保存期間）後にこのアプリケーションに関する情報を削除します。アプリケーションの情報の保存期間を変更するか、自動削除をオフにすることができます（以下の手順を参照）。

情報が削除されたアプリケーションを起動すると、Kaspersky Endpoint Security はそのアプリケーションを初めて起動したかのように分析します。

### [管理コンソール \(MMC\) で未使用のアプリケーションに関する情報の自動削除を設定する方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔先進の脅威対策〕** → **〔ホスト侵入防止〕** の順に選択します。
6. **〔アプリケーションの処理ルール〕** ブロックで、次のいずれかを実行します：
  - 自動削除を設定する場合は、 **〔次の期間以上使用されなかったアプリケーションのルールを削除する〕** をオンにして、日数を指定します。


手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30日後に Kaspersky Endpoint Security によって削除されます。
  - 自動削除をオフにする場合は、 **〔次の期間以上使用されなかったアプリケーションのルールを削除する〕** オフにします。

手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。
7. 変更内容を保存します。

## Web コンソールおよび Cloud コンソールで未使用のアプリケーションに関する情報の自動削除を設定する方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[ホスト侵入防止]** を選択します。
5. **[アプリケーションの処理ルール]** ブロックで、次のいずれかを実行します：
  - 自動削除を設定する場合は、**[次の期間以上使用されなかったアプリケーションのルールを削除する]** をオンにして、日数を指定します。  
手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30日後に Kaspersky Endpoint Security によって削除されます。
  - 自動削除をオフにする場合は、**[次の期間以上使用されなかったアプリケーションのルールを削除する]** オフにします。  
手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。
6. 変更内容を保存します。

### **製品インターフェイスで未使用のアプリケーションに関する情報の自動削除を設定する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[ホスト侵入防止]** の順に選択します。
3. **[アプリケーションの処理ルール]** ブロックで、次のいずれかを実行します：
  - 自動削除を設定する場合は、**[次の期間以上使用されなかったアプリケーションのルールを削除する]** をオンにして、日数を指定します。  
手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30日後に Kaspersky Endpoint Security によって削除されます。
  - 自動削除をオフにする場合は、**[次の期間以上使用されなかったアプリケーションのルールを削除する]** オフにします。  
手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。
4. 変更内容を保存します。

## ホスト侵入防止の監視

ホスト侵入防止機能の操作に関するレポートを受け取ることができます。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

ホスト侵入防止の操作を監視するには、レポートの書き込みを有効にする必要があります。例えば、[ホスト侵入防止機能の設定で個別のアプリケーションのレポートの転送を有効にすることができます](#)。

ホスト侵入防止の監視を設定する際には、Kaspersky Security Center へのイベント転送時のネットワーク負荷を考慮に入れてください。レポートは Kaspersky Endpoint Security のローカルログ内にものみレポートを保存することも可能です。

## 音声、映像へのアクセスの保護

犯罪者はマイクや Web カメラなどの音声や映像を記録する端末にアクセスするために特別なプログラムを使用することがあります。Kaspersky Endpoint Security はアプリケーションがいつ音声または映像ストリームを受け取るかを制御し、認証されないデータの傍受からデータを保護します。

既定では、Kaspersky Endpoint Security はアプリケーションの音声または映像ストリームへのアクセスを次のように制御します：

- 信頼、および弱い制限付きのアプリケーションは、既定で端末からの音声または映像ストリームの受信を許可されます。
- 強い制限付き、またはブロック対象のアプリケーションは、既定で端末からの音声または映像ストリームの受信を許可されません。

[手動でアプリケーションの音声または映像ストリームの受信を許可することができます](#)。

### 音声ストリームの保護の特性

音声ストリームの保護には、次の特性があります：

- [ホスト侵入防止が有効になっている場合にのみ](#)、この機能が動作します。
- ホスト侵入防止が開始するより前にアプリケーションが音声ストリームの受信を始めた場合、そのアプリケーションの音声ストリームの受信は許可され、通知は表示されません。
- アプリケーションが音声ストリームの受信を始めたあと、そのアプリケーションを [ブロック] または [強い制限付き] グループに移動した場合、そのアプリケーションの音声ストリームの受信は許可され、通知は表示されません。
- 音声録音デバイスへのアプリケーションのアクセス設定を変更したのち（たとえば、[アプリケーションの音声ストリーム受信をブロックしたのち](#)）、そのアプリケーションの音声ストリームの受信を停止するには、アプリケーションを再起動する必要があります。

- 音声録音デバイスからの音声ストリームのアクセスの管理は、アプリケーションの Web カメラアクセス設定に依存しません。
- Kaspersky Endpoint Security は、内蔵マイクおよび外付けマイクへのアクセスのみを保護します。その他の音声ストリーミングデバイスはサポートされません。
- デジタル一眼レフカメラ、ポータブルビデオカメラ、アクションカメラなどのデバイスからの音声ストリームの保護は保証されません。
- Kaspersky Endpoint Security をインストールしたのち、音声および映像を記録または再生するアプリケーションを最初に起動すると、音声および映像の再生または記録が中断することがあります。これは、音声録音デバイスへのアプリケーションのアクセスを管理する機能を有効にするために必要です。Kaspersky Endpoint Security が最初に起動するときに、音声ハードウェアを管理するシステムサービスが再起動します。

## アプリケーションの Web カメラへのアクセスの保護機能の特性

Web カメラへのアクセスの保護機能には、次の考慮事項と制限があります：

- 本製品は、Web カメラのデータの処理で得られた映像および静止画を管理します。
- 本製品は、Web カメラから受信した映像ストリームの一部である音声ストリームを管理します。
- 本製品は、USB または IEEE1394 で接続され、Windows のデバイスマネージャーで **【イメージング デバイス】** として表示される Web カメラのみを管理します。
- Kaspersky Endpoint Security は、以下の Web カメラをサポートします：
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

このリストにない Web カメラのサポートは保証されません。

## 修復エンジン

修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックするとき、次の種別のマルウェアの動作に対して処理を実行します：

#### • ファイルの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
- マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
- マルウェアによって変更または削除されたファイルを復元します。

ファイルの修復機能には[いくつかの制限事項](#)があります。

#### • レジストリの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成されたレジストリキーを削除します。
- マルウェアによって変更または削除されたレジストリキーは復元されません。

#### • システムの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって開始されたプロセスを終了します。
- 悪意のあるアプリケーションによって侵入されたプロセスを終了します。
- マルウェアによって停止されたプロセスは再開しません。

#### • ネットワークの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによるネットワーク動作をブロックします。
- マルウェアが侵入したプロセスによるネットワーク動作をブロックします。

マルウェアの動作のロールバックは、[ファイル脅威対策](#)または[ふるまい検知](#)から開始するか、[ウイルススキャン](#)中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピューターデータの整合性に悪影響を与えません。


[管理コンソール \(MMC\) で修復エンジンを有効または無効にする方法](#) 

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [先進の脅威対策] → [修復エンジン] の順に選択します。
6. [修復エンジン] を使用して機能を有効または無効にします。
7. 変更内容を保存します。

### Web コンソールおよび Cloud コンソールで修復エンジンを有効または無効にする方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [先進の脅威対策] → [修復エンジン] を選択します。
5. [修復エンジン] を使用して機能を有効または無効にします。
6. 変更内容を保存します。

### 製品インターフェイスで修復エンジンを有効または無効にする方法

1. メインウィンドウで、  をクリックします。
2. 本製品の設定ウィンドウで、 [先進の脅威対策] → [修復エンジン] の順に選択します。
3. [修復エンジン] を使用して機能を有効または無効にします。
4. 変更内容を保存します。

修復エンジンを有効にすると、悪意のあるアプリケーションが検知された場合、そのアプリケーションによるオペレーティングシステム内での動作がロールバックされます。



コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

KSN (Kaspersky Security Network) はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。

Kaspersky Security Network の使用は任意です。本製品の初期設定中に、KSN を使用するかどうか尋ねられます。KSN への参加はいつでも開始または中止できます。

KSN に参加している間に生成されたカスペルスキー統計情報の送信や、そのような情報の保存と破棄について詳しくは、KSN 声明および[カスペルスキーの Web サイト](#)を参照してください。Kaspersky Security Network 声明のテキストが含まれたファイル ksn\_<言語 ID>.txt は製品[配信キット](#)に含まれています。

KSN サーバーの負荷を低減するため、Kaspersky Security Network に対するリクエストを一時的に無効にした部分的に制限したりする定義データベースのアップデートを、カスペルスキーのエキスパートが公開することがあります。この場合、製品のローカルインターフェイスでの KSN への接続ステータスは「制限付きで有効」になります。

## KSN インフラストラクチャの種別

Kaspersky Endpoint Security では、次の種別の KSN インフラストラクチャの使用をサポートしています：

- ほとんどのカスペルスキー製品で使用されるのがグローバル KSN です。KSN の参加者は、Kaspersky Security Network から情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、Kaspersky Security Network の評価データベースと統計情報のデータベースに追加されます。
- プライベート KSN は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターから KSN にデータを送信せずに Kaspersky Security Network の評価データベースや統計情報のデータにアクセスできるようにするソリューションです。プライベート KSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：
  - コンピューターがインターネットに接続されていない。
  - 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

既定では、Kaspersky Security Center はグローバル KSN を使用します。管理コンソール (MMC)、Kaspersky Security Center Web コンソール、および[コマンドライン](#)からプライベート KSN の使用を設定できます。Kaspersky Security Center Cloud コンソールでは、プライベート KSN の使用を設定できません。

プライベート KSN について詳しくは、管理者向けに提供されている *Kaspersky Private Security Network* のガイドを参照してください。

## KSN プロキシ



Kaspersky Security Center 管理サーバーによって管理されるクライアントコンピューターは、KSN プロキシサービス経由で KSN と連携できます。


KSN プロキシサービスは次の機能を提供します：

- クライアントコンピューターはインターネットに直接アクセスしなくても、KSN にクエリを実行し、情報を送信できます。
- KSN プロキシは処理データをキャッシュすることにより、外部ネットワークとの通信チャネルの負荷を軽減し、クライアントコンピューターによって要求される情報の受信を高速化します。

KSN プロキシサービスについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

## Kaspersky Security Network の使用の有効化と無効化

*Kaspersky Security Network* の使用を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[Kaspersky Security Network]** の順に選択します。
3. **[Kaspersky Security Network]** を使用して機能を有効または無効にします。

KSN の使用を有効にすると、Kaspersky Endpoint Security に、Kaspersky Security Network に関する声明が表示されます。Kaspersky Security Network (KSN) に関する声明の条項に同意する場合は、内容を確認した上で同意してください。

既定では、拡張 KSN モードが使用されます。拡張 KSN モードは、カスペルスキーに[詳細なデータ](#)を送信するモードです。

4. 必要に応じて、**[拡張 KSN モードを有効にする]** をオフにしてください。
5. 変更内容を保存します。

KSN の使用を有効にすると、Kaspersky Endpoint Security は Kaspersky Security Network から受け取ったファイル、Web リソース、アプリケーションの評価に関する情報を使用します。

## プライベート KSN の制限事項

プライベート KSN (以下「KSPN」とも表記) は、オブジェクト (ファイルまたは Web アドレス) の評価をチェックするためのローカルの評価データベースです。ローカルの評価データベースに追加されたオブジェクトの評価は KSN または KPSN に追加されたものより優先度は高くなります。たとえば、Kaspersky Endpoint Security がコンピューターをスキャン中に KSN または KPSN に評価を要求したとします。あるファイルに対して、ローカルの評価データベースに「信頼済みでない」という評価があり、KSN または KPSN に「信頼済み」という評価があった場合、Kaspersky Endpoint Security はファイルを「信頼済みでない」と判断して検出し、検知された脅威に対して定義された操作を実行します。

しかし、Kaspersky Endpoint Security が KSN または KPSN にオブジェクトの評価を要求しないこともあります。この場合、Kaspersky Endpoint Security KPSN のローカル評価データベースからデータを受け取りません。Kaspersky Endpoint Security は次の理由で KSN または KPSN にオブジェクトの評価を要求しないことがあります：


- カスペルスキー製品がオフラインの評価データベースを使用している。オフラインの評価データベースは、カスペルスキー製品の動作中にリソースの最適化をするため、またコンピューター上の特に重要なオブジェクトを保護するために設計されています。オフライン評価データベースは、Kaspersky Security Network のデータに基づいてカスペルスキーによって作成されています。カスペルスキー製品は特定のアプリケーションの定義データベースがアップデートされる際にあわせてオフラインの評価データベースをアップデートします。オフラインの評価データベースにスキャンされるオブジェクトに関する情報が存在する場合、製品はKSN または KPSN にこのオブジェクトの評価を要求しません。
- スキャンの除外リスト (信頼ゾーン) は製品の設定で指定されます。該当する場合、製品はローカルの評価データベースのオブジェクトの評価を判断に使用しません。
- 製品が iSwift または iChecker などのスキャンの最適化技術を使用している、または KSN / KPSN への評価の要求をキャッシュしている場合。この場合は製品が以前にスキャンしたオブジェクトの評価を要求しません。
- 負荷を最適化するため、本製品は特定の形式またはサイズのファイルのみスキャンします。対応する形式およびサイズの制限はカスペルスキーによって定義されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。たとえば、ファイル脅威対策機能など、スキャンの最適化の設定を製品インターフェイスから設定することも可能です。

## 保護機能のクラウドモードの有効化と無効化

クラウドモードで動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用している本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。

Kaspersky Private Security Network を使用する場合、クラウドモードは Kaspersky Private Security Network 3.0 以降で使用できます。

保護機能のクラウドモードを有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[先進の脅威対策]** → **[Kaspersky Security Network]** の順に選択します。
3. **[クラウドモードを有効にする]** トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

次のアップデートから、Kaspersky Endpoint Security は軽量なバージョンの定義データベースをダウンロードします。

軽量なバージョンの定義データベースが使用できない場合、通常のバージョンの定義データベースに自動的に切り替えられます。

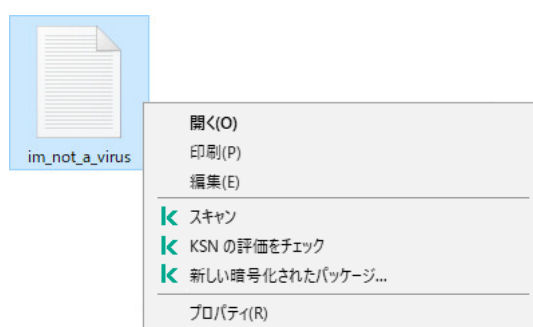
## Kaspersky Security Network でのファイルの評価の確認

ファイルのセキュリティに疑問がある場合は、Kaspersky Security Network でその評判を確認できます。

[Kaspersky Security Network に関する声明](#)の条件に同意した場合、ファイルの評価を確認できます。

Kaspersky Security Network でのファイルの評価を確認するには：

ファイルコンテキストメニューを開き、**KSN の評価をチェック**オプションを選択します（下の図を参照）。



ファイルコンテキストメニュー

Kaspersky Endpoint Security は、ファイルの評価を表示します：

**許可**：Kaspersky Security Network のほとんどのユーザーは、ファイルが信頼できることを確認しています。

**警告** **ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア**：悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアについて詳しくは、カスペルスキーの[ウイルス百科事典](#)を参照してください。[これらのアプリケーションを信頼するリストに追加](#)できます。

**ブロック**：[脅威をもたらす](#)ウイルスまたはその他のアプリケーション。

**不明**：Kaspersky Security Network には、ファイルに関する情報はありません。定義データベースを使用して、ファイルをスキャンできます（コンテキストメニューの**スキャン**オプション）。

Kaspersky Endpoint Security は、ファイルの評価を決定するために使用された KSN ソリューションを表示します：[グローバル KSN](#)または[プライベート KSN](#)。

Kaspersky Endpoint Security は、ファイルに関する追加情報も表示します（下の図を参照）。



Kaspersky Security Network でのファイルの評価

## 暗号化された接続のスキャン

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。


インストール後、Kaspersky Endpoint Security は、信頼する証明書のシステムストレージ（Windows 証明書ストア）に Kaspersky 証明書を追加します。Kaspersky Endpoint Security には、Firefox および Thunderbird の信頼する証明書のシステムストレージを使用して、これらのアプリケーションのトラフィックをスキャンする機能も含まれています。

[ウェブコントロール](#)、[メール脅威対策](#)、[ウェブ脅威対策](#)では、次のプロトコルで暗号化された接続を使用して送受信されるネットワークトラフィックを復号化しスキャンできます：

- SSL 3.0
- TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。

## 暗号化された接続のスキャンの設定

暗号化された接続のスキャンの設定を指定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[ネットワーク設定]** の順に選択します。
3. **[暗号化された接続のスキャン]** で、暗号化された接続のスキャンモードを選択します：

- **〔暗号化された接続をスキャンしない〕**。Kaspersky Endpoint Security は「https://」で始まるアドレスの Web サイトのコンテンツにアクセスしません。
- **〔保護機能の要求時に暗号化された接続をスキャンする〕**。Kaspersky Endpoint Security はファイル脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。
- **〔常に暗号化された接続をスキャンする〕**。Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。

トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。

4. 必要に応じて、信頼するオブジェクトを追加します。
5. 暗号化された接続のスキャンに関する設定を指定します（下記の表を参照）。
6. 変更内容を保存します。

暗号化された接続のスキャンの設定

パラメータ	説明
<b>信頼されない証明書を持つドメインにアクセスするとき</b>	<ul style="list-style-type: none"> <li>• <b>許可</b>：このオプションを選択した場合、信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続を許可します。</li> </ul> <p>信頼されていない証明書を持つドメインをブラウザで開こうとすると、Kaspersky Endpoint Security は、警告とそのドメインにアクセスすることが推奨されない理由が記載された HTML ページを表示します。ユーザーは HTML 警告ページのリンクをクリックすることで、要求された Web リソースにアクセスできます。このリンクを使用して対象の Web リソースにアクセスした後1時間の間は、同じドメインの他のリソースへのアクセス時に、信頼されない証明書に関する警告は表示されません。</p> <ul style="list-style-type: none"> <li>• <b>接続をブロックする</b>：このオプションを選択した場合、信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続をブロックします。</li> </ul> <p>信頼されていない証明書を持つドメインをブラウザで開こうとすると、Kaspersky Endpoint Security は、そのドメインがブロックされる理由が記載された HTML ページを表示します。</p>
<b>暗号化された接続のスキャンでエラーが発生するとき</b>	<ul style="list-style-type: none"> <li>• <b>接続をブロックする</b>：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はネットワーク接続をブロックします。</li> <li>• <b>除外リストにドメインを追加</b>：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はエラーが発生したドメインを [スキャンエラーの発生したドメイン] リストに追加し、このドメインへのアクセスでの暗号化されたネットワークトラフィックを監視しません。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインタ</li> </ul>



	<p>ーフェイスでのみ表示できます。リストに含まれる内容を消去して空にするには、<b>「接続をブロックする」</b>を選択する必要があります。</p>
<p><b>SSL 2.0 接続をブロック (推奨)</b></p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security は SSL 2.0 プロトコルで確立されたネットワーク接続をブロックします。</p> <p>このチェックボックスをオフにすると、Kaspersky Endpoint Security は SSL 2.0 プロトコルで確立されたネットワーク接続をブロックせず、これらの接続経由で送受信されるネットワークトラフィックを監視しません。</p>
<p><b>EV 証明書を使用した Web サイトへの暗号化接続を復号化する</b></p>	<p>EV (Extended Validation) 証明書は、Web サイトの信頼性を示すためのもので、接続のセキュリティを向上させます。Web サイトで EV 証明書が使用されている場合、ブラウザのアドレスバーの鍵アイコンでそのことが示されます。また、アドレスバーの全体や一部の色が緑色に変わるブラウザもあります。</p> <p>このチェックボックスをオンにすると、Kaspersky Endpoint Security は EV 証明書を使用している Web サイトの暗号化された接続を復号化して監視します。</p> <p>このチェックボックスをオフにすると、HTTPS トラフィックの通信内容に Kaspersky Endpoint Security はアクセスできません。そのため、HTTPS トラフィックは「https://google.com」などの URL のみに基づいて監視されます。</p> <p>EV 証明書を使用している Web サイトに最初にアクセスするときには、チェックボックスがオンかオフかにかかわらず、接続が復号されます。</p>

## Scanning encrypted connections in Firefox and Thunderbird


After installation, Kaspersky Endpoint Security adds a Kaspersky certificate to the system storage for trusted certificates (Windows certificate store). By default, Firefox and Thunderbird use their own proprietary Mozilla certificate store instead of the Windows certificate store. If Kaspersky Security Center is deployed in your organization and a policy is being applied to a computer, Kaspersky Endpoint Security automatically enables use of the Windows certificate store in Firefox and Thunderbird to scan the traffic of these applications. If a policy is not being applied to the computer, you can choose the certificate storage that will be used by Mozilla applications. If you selected the Mozilla certificate store, manually add a Kaspersky certificate to it. This will help avoid errors when working with HTTPS traffic.

To scan traffic in the Mozilla Firefox browser and the Thunderbird mail client, you must [enable the Encrypted Connections Scan](#). If Encrypted Connections Scan is disabled, Kaspersky Endpoint Security does not scan traffic in the Mozilla Firefox browser and Thunderbird mail client.

Prior to adding a certificate to the Mozilla store, export the Kaspersky certificate from the Windows Control Panel (browser properties). For details about exporting the Kaspersky certificate, please refer to the [Technical Support Knowledge Base](#)<sup>2</sup>. For details about adding a certificate to storage, visit the [Mozilla technical support website](#)<sup>2</sup>.

You can choose the certificate store only in the local interface of the application.

*To choose a certificate store for scanning encrypted connections in Firefox and Thunderbird:*

1. In the main application window, click the button .
2. In the application settings window, select **Advanced settings** → **Network settings**.

3. In the **Mozilla Firefox and Thunderbird** block, select the **Scan secure traffic in Mozilla applications** check box.

4. Select a certificate store:


- **Use Windows certificate store.** The Kaspersky root certificate is added to this store during installation of Kaspersky Endpoint Security.
- **Use Mozilla certificate store.** Mozilla Firefox and Thunderbird use their own certificate stores. If the Mozilla certificate store is selected, you need to manually add the Kaspersky root certificate to this store through the browser properties.

5. Save your changes.

## 暗号化された接続をスキャンから除外する

Web リソースの多くは暗号化された接続を使用しています。カスペルスキーは [\[暗号化された接続のスキャン\]](#) を有効にすることを推奨します。暗号化された接続のスキャンが業務に関連したアクティビティを妨げる場合などに、Web サイトを [\[信頼するアドレス\]](#) を参照する例外に追加します。信頼するアプリケーションが暗号化された接続を使用している場合は、[このアプリケーションの暗号化された接続のスキャンを無効にすることができます](#)。例えば、独自の認証で2ファクタ認証を使用するクラウドストレージアプリケーションなどに対して暗号化された接続のスキャンを無効にできます。

暗号化された接続のスキャンから Web アドレスを除外するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[\[詳細設定\]](#) → [\[ネットワーク設定\]](#) の順に選択します。
3. [\[暗号化された接続のスキャン\]](#) セクションで、[\[信頼するアドレス\]](#) をクリックします。
4. [\[追加\]](#) をクリックします。
5. Kaspersky Endpoint Security がドメインにアクセスするときに確立された暗号化された接続をスキャンしないようにする場合は、ドメイン名、または IP アドレスを入力します。

Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「\*」をサポートします。

Kaspersky Endpoint Security は IP アドレスのマスクをサポートしません。本製品のローカルインターフェイスで IP アドレス範囲を入力することができます (例：198.51.100.0/24)。Kaspersky Security Center コンソールでは IP アドレス範囲を入力することはできません。

例：


- 「[domain.com](#)」と入力すると次のアドレスが含まれます：<https://domain.com>、<https://www.domain.com>、<https://domain.com/page123>。サブドメイン (例：[subdomain.domain.com](https://subdomain.domain.com)) は含まれません。
- 「[subdomain.domain.com](#)」と入力すると次のアドレスが含まれます：<https://subdomain.domain.com>、<https://subdomain.domain.com/page123>。「[domain.com](#)」ドメインは含まれません。
- 「[\\*.domain.com](#)」と入力すると次のアドレスが含まれます：<https://movies.domain.com>、<https://images.domain.com/page123>。「[domain.com](#)」ドメインは含まれません。



## 6. 変更内容を保存します。

既定では、Kaspersky Endpoint Security はエラーが発生した場合は暗号化された接続のスキャンを行わず、[スキャンエラーの発生したドメイン] のリストに追加します。Kaspersky Endpoint Security は各ユーザーごとにリストを作成し、Kaspersky Security Center にはデータを送信しません。[スキャンエラーが発生したときに接続をブロック](#)することができます。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。


スキャンエラーが発生したドメインのリストを表示するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[詳細設定] → [ネットワーク設定] の順に選択します。
3. [暗号化された接続のスキャン] セクションの [スキャンエラーの発生したドメイン] をクリックします。

スキャンエラーの発生したドメインのリストが開きます。リストをリセットするには、ポリシー内でスキャンエラーが発生した場合の接続のブロックを有効にし、ポリシーを適用してからパラメータを初期値にリセットしてからポリシーを再度適用します。

カスペルスキーは、Kaspersky Endpoint Security が製品の設定に関係なくチェックの対象外にするグローバル除外リストを作成しています。

暗号化されたトラフィックのスキャンのグローバル除外リストを表示するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[詳細設定] → [ネットワーク設定] の順に選択します。
3. [暗号化された接続のスキャン] セクションの [Web サイト] をクリックします。

カスペルスキーによりまとめられた Web サイトのリストが開きます。Kaspersky Endpoint Security はこのリストに記載された Web サイトとの保護された接続はスキャンしません。このリストは、Kaspersky Endpoint Security の定義データベースとモジュールがアップデートされたときに更新される可能性があります。

# コンピューターのコントロール

## ウェブコントロール

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します（下図を参照）。

Kaspersky Endpoint Security では、HTTP プロトコルと HTTPS プロトコルのトラフィックのみが監視されません。

HTTPS トラフィックをスキャンするには、[暗号化された接続のスキャンを有効にする](#)必要があります。

## Web サイトへのアクセスの管理方法

ウェブコントロールでは、次の設定を使用して Web サイトへのアクセスを管理できます：

- **Web サイトのカテゴリ**：Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。例えば、「SNS」カテゴリまたは[その他のカテゴリ](#)のサイトに対してユーザーのアクセスを制限することができます。
- **データ種別**：Web サイトのデータへのユーザーのアクセスを制限して、画像を表示できないようにするなどの使い方ができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。

圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「圧縮ファイル」として識別し、「画像ファイル」とは識別しません。

- **個別のアドレス**：URL を入力したり、[マスクを使用](#)して Web アドレスを指定できます。

Web サイトへのアクセスを管理するために、複数の設定を同時に組み合わせて使用できます。たとえば、Web サイトのカテゴリが「Web メール」の場合にのみ「Office のファイル」へのアクセスを制限するような使い方ができます。

## Web サイトへのアクセスルール

ウェブコントロールは、アクセスルールを使用して Web サイトへのユーザーアクセスを管理します。Web サイトへのアクセスルールでは、次のような詳細設定を指定できます。

- ルールを適用するユーザー：

ブラウザーによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。

- ルールスケジュール：

ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

## アクセスルールの優先順位：

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。適用例として、たとえば、Kaspersky Endpoint Security によって企業ポータルが「ソーシャルネットワーク」サイトと判定されているケースを考えます。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「ソーシャルネットワーク」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 2 つのルールを作成します。この場合、企業ポータルへのアクセスルールには、ソーシャルネットワークカテゴリへのアクセスルールよりも高い優先順位を割り当てる必要があります。



 要求された Web ページを表示できません。

アドレス：<http://kaspersky.ru/>

この Web ページはルール「block」によってブロックされました。

理由：Web リソースがコンテンツカテゴリ「不明」とデータ種別カテゴリ「未定義」に属しています。

この Web リソースは社内での使用がブロックされています。誤ってブロックされたと思われる場合やこの Web リソースにアクセスする必要がある場合は、社内のネットワーク管理者([アクセスを要求](#))にお問い合わせください。

メッセージの作成時刻：29.10.2020 13:42:28



 要求された Web ページは安全でないか、社内のポリシーによってブロックされている可能性があります。

アドレス：<http://kaspersky.com/>

この Web ページはルール「warn」によってブロックされています。

理由：Web リソースがコンテンツカテゴリ「不明」とデータ種別カテゴリ「未定義」に属しています。

要求した Web ページを開くには、リンク「<http://kaspersky.com/>」をクリックしてください。

要求した Web ページが存在する Web サイトのコンテンツ全体にアクセスするには、リンク「[http://kaspersky.com/\\*](http://kaspersky.com/*)」をクリックしてください。

「\*」で示されたレベル以下の既存のドメインすべてにアクセスするには、リンク「[\\*/\\*.kaspersky.com/\\*](*/*.kaspersky.com/*)」をクリックしてください。

本製品の現在のセッションが終了するまでは、上記の Web リソースへのアクセスが許可されます。

誤って警告が表示されている場合は、社内のネットワーク管理者([アクセスを要求](#))に連絡してください。


メッセージの作成時刻：29.10.2020 13:42:12

ウェブコントロールによって表示されるメッセージ

## ウェブコントロールの有効化と無効化

既定では、ウェブコントロールは有効になっています。

ウェブコントロールの有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[ウェブコントロール]** の順に選択します。
3. **[ウェブコントロール]** を使用して機能を有効または無効にします。
4. 変更内容を保存します。

## Web リソースアクセスルールを使用した処理

1000 件を超える Web リソースアクセスルールを作成することは避けてください。システムが不安定になる可能性があります。

Web リソースアクセスルールは一連のフィルターと、ルールスケジュールに示されている期間中、ルールで指定されている Web リソースにユーザーがアクセスしたときに、Kaspersky Endpoint Security によって実行される一連の処理で構成されています。フィルターを使用することで、ウェブコントロールによってアクセスが管理される Web リソースの対象範囲を正確に指定できます。

次のフィルターを使用できます：


- **コンテンツによるフィルター**：ウェブコントロールでは、Web リソースが **コンテンツ** とデータの種類で分類されます。これらのカテゴリにあてはまるコンテンツとデータの種類の含む Web リソースへのユーザーアクセスを管理できます。選択したコンテンツカテゴリまたはデータ種別カテゴリに属する Web リソースにユーザーがアクセスすると、ルールで指定された処理が実行されます。
- **Web リソースアドレスによるフィルター**：すべての Web リソースアドレス、個別の Web リソースアドレス、Web リソースのアドレスグループのユーザーアクセスを管理できます。  
コンテンツによるフィルターと Web リソースアドレスによるフィルターの両方を指定していて、指定した Web リソースアドレスまたは Web リソースのアドレスグループが、選択したコンテンツカテゴリやデータ種別カテゴリに属しているときには、両方のフィルターの条件を満たす Web リソースへのアクセスが制限されます。選択したコンテンツカテゴリやデータ種別カテゴリに属するすべての Web リソースへのアクセスが制限されるわけではありません。代わりに、指定した Web リソースアドレスまたは Web リソースアドレスグループに限定してアクセスが制限されます。
- **ユーザー名またはユーザーグループ名によるフィルター**：ルールによって管理される Web リソースへのアクセス権を持つユーザーまたはユーザーグループの名前を指定できます。
- **ルールスケジュール**：ルールスケジュールを指定できます。ルールスケジュールは、Kaspersky Endpoint Security がルールによってカバーされた Web リソースへのアクセスを監視する期間を決定します。

Kaspersky Endpoint Security のインストール後、ウェブコントロールのルールリストは空ではありません。次の 2 つのルールが事前に設定されています：

- 「スクリプトとスタイルシート」ルール：アドレスに、css、js、または vbs の拡張子を持つファイル名が含まれている Web リソースにいつでもアクセスできる権限をすべてのユーザーに付与します。たとえば、<http://www.example.com/style.css> や <http://www.example.com/style.css?mode=normal> といったアドレスです。
- 既定のルール：このルールは他のルールの対象範囲に含まれないすべての Web リソースに適用され、すべてのユーザーによるこれらの Web リソースへのアクセスを許可またはブロックします。

## Web リソースへのアクセスルールの追加

Web リソースアクセスルールを追加または編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[ウェブコントロール]** の順に選択します。
3. **[設定]** ブロックで、**[Web リソースへのアクセスルール]** をクリックします。
4. **[追加]** をクリックします。  
**[Web リソースへのアクセスルール]** ウィンドウが表示されます。
5. **[ルール名]** にルール名を入力します。
6. Web リソースのアクセスルールに **[有効]** を選択します。  
トグルスイッチを使用していつでも [Web リソースのアクセスルールを無効にする](#) ことができます。
7. **[操作]** ブロックで、対応するオプションを選択します：
  - **許可**：この値を選択すると、Kaspersky Endpoint Security はルールパラメータと一致する Web リソースへのアクセスを許可します。
  - **ブロック**：この値を選択すると、Kaspersky Endpoint Security はルールパラメータと一致する Web リソースへのアクセスをブロックします。
  - **警告**：この値を選択すると、ユーザーがルールと一致する Web リソースへのアクセスを試みたときに、Web リソースが望ましくないことを示す警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。
8. **[コンテンツのフィルタリング]** で、関連するコンテンツフィルターを選択します。
  - **コンテンツカテゴリ** Web リソースへのユーザーのアクセスを [カテゴリ](#) (例えば SNS カテゴリなど) で制御することができます。
  - **データ種別** Web リソースへのユーザーのアクセスを公開されているデータの特定の種別 (例えば画像など) で制御することができます。

コンテンツフィルターを設定するには：

- a. **[設定]** をクリックします。
- b. 目的のコンテンツカテゴリまたはデータ種別名の横にあるチェックボックスをオンにします。

コンテンツカテゴリまたはデータ種別名の横にあるチェックボックスをオンにすると、Kaspersky Endpoint Securityはこのルールを適用して、選択したコンテンツカテゴリまたはデータ種別に属するWebリソースへのアクセスを管理します。

c. Webリソースのアクセスルールを設定するウィンドウに戻ります。

9. **[アドレス]** ブロックで、対応するWebリソースのアドレスのフィルターを選択します。

- **すべてのアドレス** Webリソースをアドレスでフィルターしません。
- **個別のアドレス** リストにあるWebリソースのアドレスのみをフィルターします。Webリソースのアドレスのリストを作成するには：
  - a. **[アドレスの追加]** または **[アドレスグループを追加]** をクリックします。
  - b. 表示されたウィンドウで、Webリソースのアドレスのリストを作成します。URLを入力したり、[マスクを使用](#)してWebアドレスを指定できます。また、[Webリソースのアドレスのリストをテキストファイルでエクスポート](#)することもできます。
- c. Webリソースのアクセスルールを設定するウィンドウに戻ります。

[暗号化された接続のスキャンがオフ](#)の場合、HTTPSプロトコルについてはサーバー名でのみフィルターできます。

10. **[ユーザー]** ブロックで、ユーザーのフィルターを選択します。

- **すべてのユーザー** Webリソースを特定のユーザーでフィルターしません。
- **個別のユーザーまたはグループ** Webリソースを特定のユーザーでのみフィルターします。ルールを適用するユーザーのリストを作成するには：
  - a. **[追加]** をクリックします。
  - b. 表示されたウィンドウで、Webリソースのアクセスルールを適用するユーザーまたはユーザーグループを選択します。
  - c. Webリソースのアクセスルールを設定するウィンドウに戻ります。

11. **[ルールのスケジュール]** で、目的のスケジュール名を選択するか、選択したルールスケジュールに基づく新しいスケジュールを作成します。次の手順に従います：

- a. **[編集または新規追加]** をクリックします。
- b. **[追加]** をクリックします。
- c. 表示されたウィンドウで、ルールスケジュール名を入力します。
- d. ユーザーのWebリソースのアクセスのスケジュールを設定します。
- e. Webリソースのアクセスルールを設定するウィンドウに戻ります。


12. 変更内容を保存します。



## Web リソースアクセスルールの優先度の割り当て


ルールリストでルールを並べる順序によって、各ルールに優先度を割り当てることができます。

Web リソースアクセスルールに優先度を割り当てるには

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**［セキュリティコントロール］** → **［ウェブコントロール］** の順に選択します。
3. **［設定］** ブロックで、**［Web リソースへのアクセスルール］** をクリックします。
4. 表示されたウィンドウで、優先度を変更するルールを選択します。
5. **［上へ］** と **［下へ］** を使用して、ルールをリソースアクセスルールのリスト内の適切なランクに移動します。
6. 変更内容を保存します。

## Web リソースへのアクセスルールの有効化と無効化

Web リソースアクセスルールを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**［セキュリティコントロール］** → **［ウェブコントロール］** の順に選択します。
3. **［設定］** ブロックで、**［Web リソースへのアクセスルール］** をクリックします。
4. 表示されたウィンドウで、有効または無効にするルールを選択します。
5. **［状態］** 列で、次の操作を行います：
  - ルールの使用を有効にする場合は、**［有効］** を選択します。
  - ルールの使用を無効にする場合は、**［無効］** を選択します。
6. 変更内容を保存します。

## 信頼する URL のリストのエクスポート / インポート

ウェブコントロールルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種類の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ウェブコントロールルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

## 管理コンソール (MMC) で信頼するウェブコントロールルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [セキュリティコントロール] → [ウェブコントロール] の順に選択します。
6. ウェブコントロールルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。複数のポートを選択するには、CTRL または SHIFT キーを使用します。  
ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
  - b. [エクスポート] をクリックします。
  - c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. [保存] をクリックします。  
Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
7. ウェブコントロールルールのリストをインポートするには：
  - a. [インポート] をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. [開く] をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。


## Web コンソールおよび Cloud コンソールでウェブコントロールルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ルールのリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[セキュリティコントロール]** → **[ウェブコントロール]** に移動します。
5. **[ルールリスト]** ブロックでルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択したルールのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。
  - d. **[エクスポート]** をクリックします。  
Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを XML ファイルでエクスポートします。
6. **[ルールリスト]** ブロックでルールのリストをインポートするには：
  - a. **[インポート]** をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. **[開く]** をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
7. 変更内容を保存します。

## Web リソースへのアクセスルールのテスト

ウェブコントロールルールの一貫性をチェックするには、そのルールをテストします。ウェブコントロールには、そのためのルール診断機能があります。

Web リソースへのアクセスルールをテストするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[ウェブコントロール]** の順に選択します。
3. **[設定]** ブロックで、**[ルールの診断]** をクリックします。  
**[ルールの診断]** ウィンドウが表示されます。


4. 特定の Web リソースへのアクセスを管理するルールをテストするには、**【アドレスの指定】** をオンにして、下のフィールドに Web リソースアドレスを入力します。
5. 特定のユーザーおよびユーザーグループ、またはそのいずれかに対して Web リソースへのアクセスを管理するルールをテストするには、ユーザーおよびユーザーグループのリストを指定します。
6. 特定のコンテンツカテゴリまたはデータ種別カテゴリの Web リソースへのアクセスを管理するルールをテストするには、**【コンテンツのフィルタリング】** から、**【コンテンツカテゴリ】**、**【データ種別】**、または**【コンテンツカテゴリとデータ種別】** を選択します。
7. ルール診断条件で指定された Web リソースへのアクセス試行の時間と曜日に関するルールをテストするには、**【アクセスを試みる時間】** をオンにします。次に、曜日と時間を指定します。
8. **【スキャン】** をクリックします。

テストの完了後、特定の Web リソースへのアクセス試行時に適用される最初のルールに従って、Kaspersky Endpoint Security によって実行された処理に関する情報を含むメッセージが表示されます（許可、ブロック、または警告）。最初に適用されるルールは、ウェブコントロールルールのリストにおいて、診断条件に合っている中で最上位に位置しているルールです。メッセージは、**【スキャン】** の右側に表示されます。次のテーブルには、Kaspersky Endpoint Security が実行した処理を指定する、適用されたルールの残りをリスト表示します。ルールは優先度の高い順に表示されます。

## Web リソースアドレスのリストのエクスポート / インポート

Web リソースアクセスルールで Web リソースアドレスのリストを作成した場合は、txt ファイルにエクスポートできます。その後、リストをこのファイルからインポートすることで、アクセスルールを設定するときに新しい Web リソースアドレスのリストを手動で作成する必要がなくなります。Web リソースアドレスのリストのエクスポートおよびインポートオプションは、類似したパラメータを使用してアクセスルールを作成する場合などに便利です。

Web リソースアドレスのリストをファイルにインポートまたはエクスポートするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【ウェブコントロール】** の順に選択します。
3. **【設定】** ブロックで、**【Web リソースへのアクセスルール】** をクリックします。
4. ファイルにインポートまたはエクスポートする Web リソースアドレスのリストを含むルールを選択します。
5. 信頼する URL のリストをエクスポートするには、**【アドレス】** ブロックで次の操作を行います：
  - a. エクスポートするアドレスを選択します。  
アドレスが何も選択されていない場合、すべてのアドレスがエクスポートされます。
  - b. **【エクスポート】** をクリックします。
  - c. 表示されたウィンドウで、Web リソースのアドレスのリストをエクスポートする TXT ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **【保存】** をクリックします。  
Web リソースのアドレスのリストがテキストファイルでエクスポートされます。

6. Web リソースのリストをインポートするには、**[アドレス]** ブロックで次の操作を行います：

a. **[インポート]** をクリックします。

表示されたウィンドウで、Web リソースのリストをインポートする TXT ファイルを選択します。

b. **[開く]** をクリックします。




コンピューターにアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、TXT ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

## ユーザーが行っているインターネット活動の監視

Kaspersky Endpoint Security では、許可されている Web サイトも含めて、すべての Web サイトへのユーザーのアクセスに関するデータをログに記録できます。この機能により、ブラウザでのすべての閲覧履歴を取得できます。Kaspersky Endpoint Security は、Kaspersky Security Center、[Kaspersky Endpoint Security のローカルログ](#)、Windows イベントログのそれぞれに、ユーザーの活動に関するイベント情報を送信できます。Kaspersky Security Center でイベントを受信するには、管理コンソールまたは Web コンソールを使用して、イベントに関するポリシー設定を指定する必要があります。ウェブコントロールイベントのメールによる通知と、ユーザーのコンピューター画面上への通知の表示も設定できます。


Kaspersky Endpoint Security では、ユーザーのインターネット活動に関して次のイベントが作成されます：

- Web サイトのブロック（緊急イベントステータス ）。
- 望ましくない Web サイトへのアクセス（警告ステータス ）。
- 許可されている Web サイトへのアクセス（情報メッセージステータス ）。

ユーザーのインターネット活動の監視を有効にする前に、以下の項目を実行してください：


- Web トラフィックへの Web ページと相互作用するスクリプトの埋め込み（下の手順を参照）。スクリプトはウェブコントロールのイベントの登録を有効にします。
- HTTPS トラフィックをスキャンするには、[暗号化された接続のスキャンを有効にする](#) 必要があります。

Web トラフィックに Web ページとの連携スクリプトを埋め込むには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[ネットワーク設定]** の順に選択します。
3. **[トラフィック処理]** で、**[Web ページと連携するため Web トラフィック内にスクリプトを埋め込む]** を選択します。
4. 変更内容を保存します。

Kaspersky Endpoint Security は Web トラフィックに Web ページと相互作用するスクリプトを埋め込みます。このスクリプトにより、ウェブコントロールのイベントをアプリケーションイベントログ、OS イベントログ、[レポート](#)に登録できるようになります。

ユーザーのコンピューター上で発生したウェブコントロールイベントに関する情報の保存を設定するには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【インターフェイス】** の順に選択します。
3. **【通知】** で、**【通知の設定】** をクリックします。
4. 表示されたウィンドウで、**【ウェブコントロール】** セクションを選択します。  
ウェブコントロールイベントと通知方法のリストが表示されます。
5. それぞれのイベントの通知方法を指定します（**ローカルレポートに保存**または**Windows イベントログに保存**）。  
許可されている Web サイトへのアクセスイベントもログに記録するには、ウェブコントロールの設定も編集する必要があります（下記の手順を参照）。  
イベントのリストで、画面上の通知とメール通知を有効にすることもできます。メールによる通知を送信するには、SMTP サーバー設定を指定する必要があります。メールによる通知の送信について詳しくは、[Kaspersky Security Centerのオンラインヘルプ](#)を参照してください。
6. 変更内容を保存します。

これにより、ユーザーのインターネット活動に関する情報のログへの記録が始まります。

ウェブコントロールは、ユーザーの活動に関するイベント情報を次のように Kaspersky Security Center に送信します：

- Kaspersky Security Center を使用している場合、ウェブコントロールは Web ページを構成するすべてのオブジェクトのイベントを送信します。そのため、1つの Web ページがブロックされたときに複数のイベントが作成される場合があります。たとえば、「<http://www.example.com>」という URL のページをブロックしたときに、Kaspersky Endpoint Security によって「<http://www.example.com>」「<http://www.example.com/icon.ico>」「<http://www.example.com/file.js>」などのオブジェクトに対するイベントが作成される可能性があります。
- Kaspersky Security Center Cloud コンソールを使用している場合、ウェブコントロールはイベントをグループ化し、Web サイトのプロトコルとドメインのみを送信します。たとえば、ユーザーが望ましくない Web ページ <http://www.example.com/main>、<http://www.example.com/contact>、および <http://www.example.com/gallery> を開いた場合、<http://www.example.com> オブジェクトを持つイベントを1つだけ送信します。

許可されている Web サイトへのアクセスイベントのログへの記録を有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【ウェブコントロール】** の順に選択します。
3. **【詳細】** ブロックで、**【詳細設定】** をクリックします。
4. 表示されたウィンドウで、**【許可対象のページの閲覧を記録する】** をオンにします。
5. 変更内容を保存します。

これにより、ブラウザーでのすべての閲覧履歴を確認できるようになります。

## ウェブコントロールメッセージのテンプレートの編集



ユーザーがインターネットリソースへのアクセスを試みると、Kaspersky Endpoint Security ではウェブコントロールルールのプロパティで指定された処理の種類に応じて次の種類のいずれかのメッセージが表示されます（アプリケーションでは HTTP サーバー応答の代わりにメッセージを含む HTML ページが使用されます）：

- **警告メッセージ**：このメッセージは、Web リソースの閲覧が推奨されないか企業ポリシーに違反することをユーザーに警告します。Kaspersky Endpoint Security では、この Web リソースを説明するルールの設定の [処理] の [警告] が選択されている場合に警告メッセージが表示されます。


警告が誤検知だと考えられる場合は、警告のリンクをクリックすると、あらかじめ作成されたメッセージを企業ネットワークの管理者に送信できます。

- **Web リソースのブロックを通知するメッセージ**：Kaspersky Endpoint Security では、この Web リソースを説明するルールの設定の [処理] から [ブロック] を選択すると、Web リソースがブロックされたことを通知するメッセージが表示されます。

Web リソースのブロックが誤検知だと考えられる場合は、Web リソースのブロックを通知するメッセージのリンクをクリックすると、あらかじめ作成されたメッセージを企業ネットワークの管理者に送信できます。

警告メッセージ、Web リソースのブロックを通知するメッセージ、LAN 管理者に送信するメッセージの専用テンプレートがあります。これらのテンプレートの内容を変更できます。

ウェブコントロールメッセージのテンプレートを変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[セキュリティコントロール] → [ウェブコントロール] の順に選択します。
3. [テンプレート] ブロックで、ウェブコントロールのメッセージのテンプレートを設定します。
  - **警告**この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。
  - **ブロックに関するメッセージ**：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。
  - **管理者に送信するメッセージ**：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**Web ページへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [ユーザー要求] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。
4. 変更内容を保存します。

## Web リソースアドレスマスクの編集

Web リソースアドレスマスク（「アドレスマスク」とも呼ばれます）は、Web リソースアクセスルールを作成する際に、多数の類似の Web リソースアドレスを入力する必要がある場合に役立つことがあります。アドレスマスクを適切に作成すると、多数の Web リソースアドレスを置換できます。

アドレスマスクの作成時には、次のルールに従います：

1. \* 文字はゼロ文字以上の文字を含むすべての文字シーケンスを置換します。  
たとえば、\*abc\* アドレスマスクを入力した場合、アクセスルールは文字シーケンス abc を含むすべての Web リソースに適用されます。例：http://www.example.com/page\_0-9abcdef.html
2. 連続する \*. 文字（ドメインマスク）を使用してアドレスのドメインをすべて選択することができます。ドメインマスク \*. はすべてのドメイン名、サブドメイン名、空白行を意味します。  
例：マスク \*.example.com は次のアドレスを表します：
  - http://pictures.example.com ドメインマスク \*. は pictures を表しています。
  - http://user.pictures.example.com ドメインマスク \*. は pictures. および user. を表しています。
  - http://example.com ドメインマスク \*. は空白を表しています。
3. アドレスマスクの頭にある www. 文字シーケンスは \*. シーケンスとして解釈されます。  
例：www.example.com のアドレスマスクは \*.example.com として解釈されます。このマスクは www2.example.com および www.pictures.example.com を表します。
4. アドレスマスクの先頭文字が \* ではない場合は、アドレスマスクの内容は \*. プリフィックスと同じになります。
5. アドレスマスクの末尾の文字が / または \* 以外の場合、アドレスマスクの内容は /\* ポストフィックスと同じになります。  
例：アドレスマスク http://www.example.com には http://www.example.com/abc などのアドレスも含まれます（a、b、c は任意の文字です）。
6. アドレスマスクの末尾の文字が / の場合、アドレスマスクの内容は /\*. ポストフィックスと同じになります。
7. アドレスマスクの末尾にある文字シーケンス /\* は、 /\* または空文字列として解釈されます。
8. Web リソースアドレスは、プロトコル（http または https）を考慮しながら、アドレスマスクに対して検証されます。
  - アドレスマスクにネットワークプロトコルがない場合は、このアドレスマスクにはすべてのネットワークプロトコルのアドレスが含まれます。  
例：アドレスマスク example.com には http://example.com および https://example.com も含まれます。
  - アドレスマスクにネットワークプロトコルがある場合は、このアドレスマスクにはそのアドレスマスクと同じネットワークプロトコルのアドレスのみが含まれます。  
例：アドレスマスク http://\*.example.com には http://www.example.com が含まれますが、https://www.example.com は含まれません。
9. 二重引用符で囲まれているアドレスマスクがアドレスマスクに最初に含まれている場合は、\* 文字が存在しない限り、その他の文字は考慮されません。ルール 5 および 7 は、「"」で囲まれたアドレスマスクには適用されません（下の表の例 14 - 18 を参照）。
10. Web リソースアドレスマスクと比較するときには、ユーザー名とパスワード、接続ポート、大文字と小文字の区別は考慮されません。

番号	アドレスマスク	検証する Web リソースアドレス	アドレスがアドレスマスクに含まれるか	コメント
1	*.example.com	http://www.123example.com	含まれない	ルール1を参照
2	*.example.com	http://www.123.example.com	含まれる	ルール2を参照
3	*example.com	http://www.123example.com	含まれる	ルール1を参照
4	*example.com	http://www.123.example.com	含まれる	ルール1を参照
5	http://www.*.example.com	http://www.123example.com	含まれない	ルール1を参照
6	www.example.com	http://www.example.com	含まれる	ルール1、3、2を参照。
7	www.example.com	https://www.example.com	含まれる	ルール1、3、2を参照。
8	http://www.*.example.com	http://123.example.com	含まれる	ルール1、3、4を参照。
9	www.example.com	http://www.example.com/abc	含まれる	ルール1、3、5を参照。
10	example.com	http://www.example.com	含まれる	ルール1、3を参照
11	http://example.com/	http://example.com/abc	含まれる	ルール6を参照
12	http://example.com/*	http://example.com	含まれる	ルール7を参照
13	http://example.com	https://example.com	含まれない	ルール8を参照
14	"example.com"	http://www.example.com	含まれない	ルール9を参照
15	"http://www.example.com"	http://www.example.com/abc	含まれない	ルール9を参照
16	"*.example.com"	http://www.example.com	含まれる	ルール9、1を参照
17	"http://www.example.com/*"	http://www.example.com/abc	含まれる	ルール9、1を参照
18	"www.example.com"	http://www.example.com、 https://www.example.com	含まれる	ルール8、9を参照
19	www.example.com/abc/123	http://www.example.com/abc	含まれない	アドレスマスクには Web リソースのアドレス以外の情報も含まれます。

## 以前のバージョンの製品から Web リソースのアクセスルールの移行

Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以前のバージョンを Kaspersky Endpoint Security for Windows 11.7.0 にアップグレードした場合、Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、次のように移行されます：

- 「チャットと掲示板」「Web メール」「ソーシャルネットワーク」からの1つ以上の Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、「インターネットコミュニケーション」の Web リソースのコンテンツカテゴリに移行されます。
- 「オンラインストア」と「決済システム」からの1つ以上の Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、「オンラインストア、銀行、決済システム」の Web リソースのコンテンツカテゴリに移行されます。
- 「ギャンブル」の Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、「ギャンブル、宝くじ、懸賞」のコンテンツカテゴリに移行されます。
- 「ブラウザーゲーム」の Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、「コンピューターゲーム」のコンテンツカテゴリに移行されます。
- 上記のリストに含まれていない Web リソースのコンテンツカテゴリに基づいた Web リソースのアクセスルールは、変更なしで移行されます。

## デバイスコントロール

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。

### デバイスへのアクセスの判定基準

デバイスコントロールは、次の情報に基づいてアクセスをコントロールできます。

- **デバイス種別**：プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。

次のようにデバイスアクセスを設定できます：

- 許可：
- ブロック：
- バスの種類に依存（Wi-Fi を除く）：
- 例外を除きブロック（Wi-Fi のみ）：
- **接続バス**：接続バスとは、コンピューターへのデバイスの接続に使用されるインターフェイスです（例：USB、FireWire）。これにより、たとえば USB など特定の接続バスを使用して接続されるすべてのデバイスの接続を制限できます。

次のようにデバイスアクセスを設定できます：

- 許可：
- ブロック：

- **信頼するデバイス**：「信頼するデバイス」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

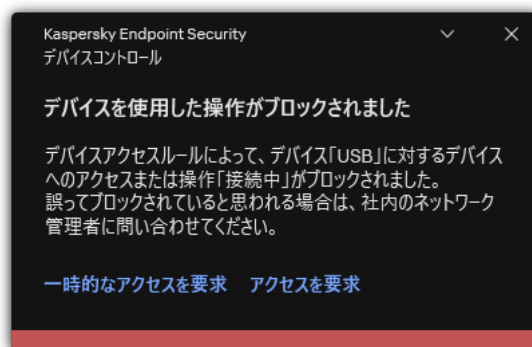
次のデータに基づいて信頼するデバイスを追加できます。

- **IDによるデバイス**：各デバイスには固有の識別子があります（ハードウェアID、またはHWID）。これらのIDは、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイスIDの例：SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000特定のデバイスを複数追加する場合は、IDでデバイスを追加すると便利です。
- **モデルによるデバイス**：各デバイスには製造元ID（VID）および製品ID（PID）があります。これらのIDは、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VIDおよびPIDの入力用テンプレート：VID\_1234&PID\_5678組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。
- **IDマスクによるデバイス**：IDが類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。**\***文字は、任意の文字列を置き換えます。Kaspersky Endpoint Securityでは、マスクでの「?」記号の使用をサポートしていません。例：WDC\_C\*
- **モデルマスクによるデバイス**：同一のVIDまたはPIDを持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。**\***文字は、任意の文字列を置き換えます。Kaspersky Endpoint Securityでは、マスクでの「?」記号の使用をサポートしていません。例：「VID\_05AC & PID\_ \*」。

デバイスコントロールは、[アクセスルール](#)を使用してデバイスへのユーザーアクセスを管理します。デバイスコントロールでは、デバイスの接続や切断のイベントを保存することもできます。イベントを保存するには、ポリシー内でイベントの記録を設定する必要があります。

デバイスへのアクセスが接続バスに依存する場合（🌐ステータスの場合）、Kaspersky Endpoint Securityではデバイスの接続イベントと切断イベントが保存されません。Kaspersky Endpoint Securityでデバイスの接続イベントと切断イベントを保存するには、デバイスへのアクセスを許可する（✅ステータス）か、デバイスを信頼リストに追加します。

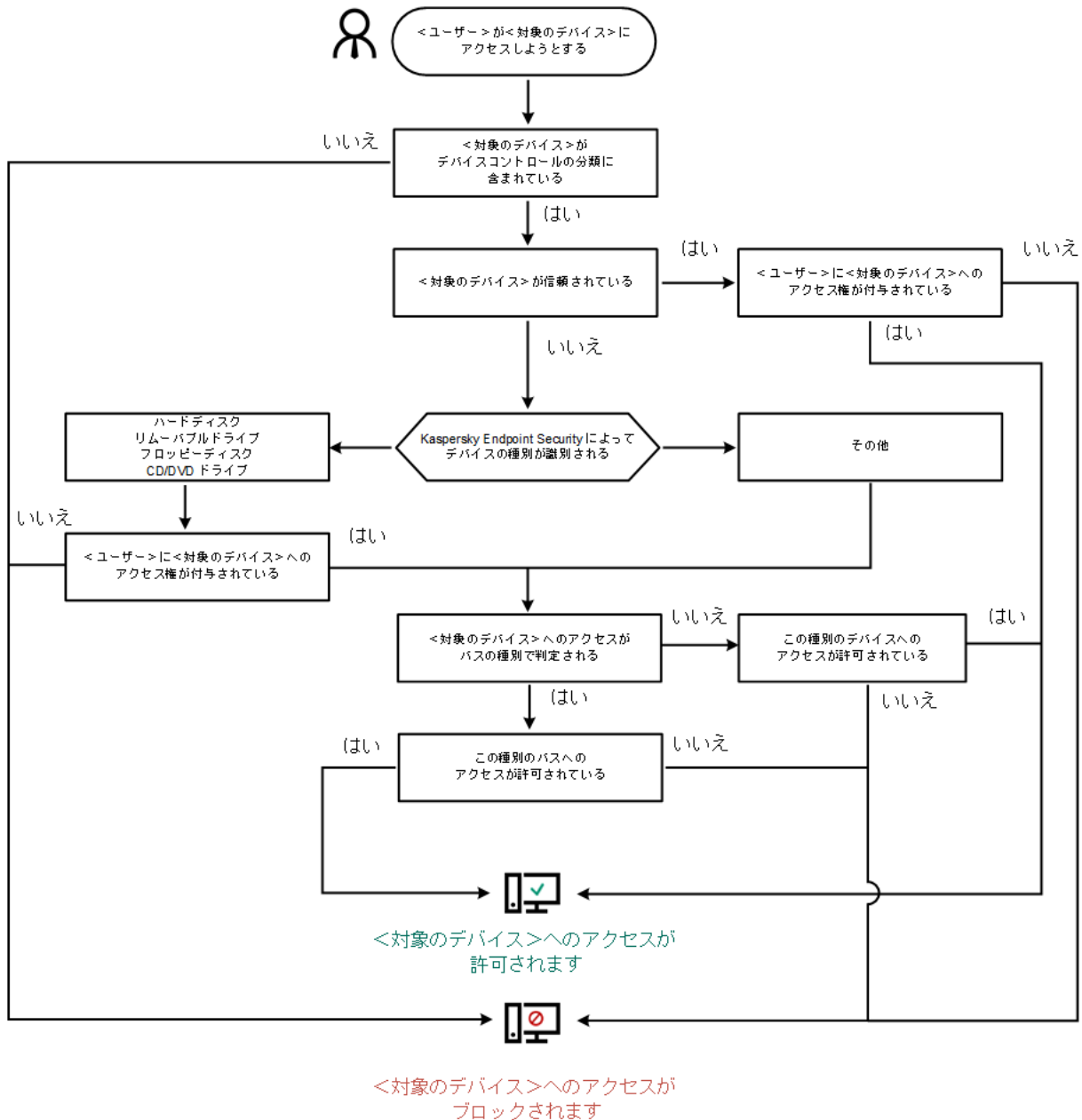
デバイスコントロールでブロックされているデバイスがコンピューターに接続された場合、Kaspersky Endpoint Securityはアクセスをブロックし通知を表示します（以下の図を参照）。



デバイスコントロールの通知

## デバイスコントロールの動作アルゴリズム

ユーザーがデバイスをコンピューターに接続すると、Kaspersky Endpoint Securityはデバイスへのアクセスを許可するかどうかを決定します（以下の図を参照）。



デバイスコントロールの動作アルゴリズム

デバイスが接続されてアクセスが許可されている状況で、アクセスをブロックするようにアクセスルールを編集できます。この場合、（フォルダーの内容の表示や、読み取りまたは書き込みの実行など）次にデバイスへのアクセスが試行されたときに、Kaspersky Endpoint Security はアクセスをブロックします。ファイルシステムのないデバイスは、次回デバイスが接続されたときのみブロックされます。

Kaspersky Endpoint Security がインストールされているコンピューターのユーザーが、誤ってブロックされたと考えられるデバイスへのアクセスを要求できるようにするには、[アクセス要求の手順](#)を伝えます。

## デバイスコントロールの有効化と無効化

既定では、デバイスコントロールは有効になっています。

デバイスコントロールを有効または無効にするには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【デバイスコントロール】** を使用して機能を有効または無効にします。
4. 変更内容を保存します。

デバイスコントロールが有効になると、本製品は接続されているデバイスの情報を Kaspersky Security Center に渡します。接続されたデバイスのリストは Kaspersky Security Center の **【ハードウェア】** フォルダで表示できます。

## アクセスルールの概要

アクセスルールは、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを指定する複数の設定項目から構成されます。デバイスコントロールの分類に含まれていないデバイスを追加することはできません。これらのデバイスへのアクセスはすべてのユーザーに対して許可されます。

### デバイスアクセスルール

アクセスルールで設定できる項目は、対象となるデバイスの種別に応じて異なります。詳しくは次の表を参照してください。

アクセスルールの設定

デバイス	アクセスコントロール	デバイスへのアクセスのスケジュール	ユーザーまたはユーザーのグループの割り当て	優先度	読み取り／書き込み権限
ハードディスク	✓	✓	✓	✓	✓
リムーバブルドライブ	✓	✓	✓	✓	✓
プリンター	✓	-	-	-	-
フロッピーディスク	✓	✓	✓	✓	✓
CD/DVD ドライブ	✓	✓	✓	✓	✓
モデム	✓	-	-	-	-
テープデバイス	✓	-	-	-	-
多機能デバイス	✓	-	-	-	-
スマートカードリーダー	✓	-	-	-	-
Windows CE USB ActiveSync デバイス	✓	-	-	-	-
外部ネットワークアダプター	✓	-	-	-	-
ポータブルデバイス (MTP)	✓	✓	✓	✓	✓






Bluetooth	✓	-	-	-	-
カメラとスキャナー	✓	-	-	-	-

## モバイルデバイスのアクセスルール



Android または iOS モバイルデバイスは、ポータブルデバイス (MTP) に分類されます。モバイルデバイスがコンピューターに接続されると、コンピューターのオペレーティングシステムがデバイスの種別を識別します。ADB (Android Debug Bridge) または iTunes (または同等のアプリケーション) がコンピューターにインストールされている場合、コンピューターのオペレーティングシステムはモバイルデバイスを ADB デバイスまたは iTunes デバイスとして認識します。それ以外の場合、オペレーティングシステムはモバイルデバイスを、ファイル転送用のポータブルデバイス (MTP) や画像転送用の PTP デバイス (カメラ) などの別のデバイスとして認識します。判定されるデバイスの種別は、モバイルデバイスの機種によって異なります。

ADB デバイスまたは iTunes デバイスへのアクセスについては、次の事項に留意してください：


- デバイスへのアクセスのスケジュールを設定することはできません。デバイスへのアクセスがルールによって制限されている場合は (ステータスが ) の場合)、ADB デバイスおよび iTunes デバイスに常時アクセスできません。
- 個別のユーザーのデバイスアクセスを設定したり、アクセス権 (読み取り / 書き込み) を設定したりすることはできません。デバイスへのアクセスがルールによって制限されている場合は (ステータスが ) の場合)、すべての権限を付与されているユーザーが ADB デバイスおよび iTunes デバイスにアクセスできます。
- 個別のユーザーに対して、信頼する ADB デバイスまたは iTunes デバイスへのアクセスを設定することはできません。デバイスが信頼されている場合は、すべてのユーザーが ADB デバイスおよび iTunes デバイスにアクセスできます。
- デバイスをコンピューターに接続してから ADB または iTunes のアプリケーションをインストールした場合は、デバイスの固有 ID がリセットされる場合があります。つまり、このデバイスは新しいデバイスとして認識されます。デバイスが信頼されている場合は、デバイスを信頼リストに再度追加します。

既定では、アクセスルールにより、各種デバイスの接続バスへのアクセスが許可されると、ユーザーにデバイスへのフルアクセス権 () ステータスが常に付与されるようになります。

## Wi-Fi ネットワークのアクセスルール

Wi-Fi ネットワークのアクセスルールでは、Wi-Fi ネットワークへの接続を許可するか (✓ ステータス)、あるいはブロックするか () ステータスを指定します。ルールに [信頼する Wi-Fi ネットワーク] () ステータスを追加できます。信頼する Wi-Fi ネットワークは制限なく使用が許可されます。既定では、Wi-Fi ネットワークのアクセスルールはすべての Wi-Fi ネットワークへのアクセスが許可されます。


## 接続バスアクセスルール

接続バスアクセスルールでは、デバイスの接続を許可するか (✓ ステータス)、あるいはブロックするか () ステータスを指定します。バスへのアクセスを許可するルールは、デバイスコントロールの分類時に存在するすべての接続バスに対して既定で作成されます。

## デバイスアクセスルールの編集

デバイスアクセスルールは、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを定義する複数の設定項目です。これらの設定には特定のデバイス、アクセススケジュール、読み取りまたは書き込み権限へのアクセスが含まれます。

デバイスアクセスルールを編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【アクセスの設定】** ブロックで、**【デバイスと Wi-Fi ネットワークのアクセスルール】** ボタンをクリックします。

ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。

4. **【ストレージ機器へのアクセス】** ブロックで、編集するアクセスルールを選択します。ブロックには、追加のアクセスを設定するファイルシステムを持つデバイスが表示されます。既定では、デバイスアクセスルールにより、指定した種類のデバイスへの常時フルアクセス権限がすべてのユーザーに付与されます。

- a. **【アクセス】** ブロックで、適切なデバイスのアクセスオプションを選択します。

- **許可：**

- **ブロック**

- **接続バスに依存する：**

デバイスへのアクセスをブロックまたは許可するには、[接続バスのアクセスを設定します](#)。

- **ルールによって制限する：**

このオプションでユーザーの権限やデバイスへのアクセスのスケジュールを設定できます。

- b. **【ユーザーの権限】** ブロックで、**【追加】** をクリックします。

新しいデバイスへのアクセスルールを追加するウィンドウが開きます。

- c. ルールの優先度の割り当て。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。


ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数のグループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

- d. デバイスアクセスルールに **【有効】** を設定します。

- e. ユーザーのデバイスのアクセスの読み取り、書き込み権限を設定します。
  - f. デバイスのアクセスルールを適用するユーザーまたはユーザーグループを選択します。
  - g. ユーザーのデバイスアクセススケジュールを設定します。
  - h. **[追加]** をクリックします。
5. **[外部デバイスへのアクセス]** ブロックで、ルールを選択して **[許可]**、**[ブロック]**、または **[接続バスに依存する]** のアクセスを設定します。必要に応じて [接続バスへのアクセスを設定](#) します。
6. **[Wi-Fi ネットワークへのアクセス]** ブロックで、**[Wi-Fi]** をクリックして **[許可]**、**[ブロック]**、または **[例外を除きブロック]** のアクセスを設定します。必要に応じて、[信頼リストに Wi-Fi ネットワークを追加](#) します。
7. 変更内容を保存します。

## 接続バスアクセスルールの編集


接続バスアクセスルールを編集するには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[デバイスコントロール]** の順に選択します。
3. **[アクセスの設定]** で、**[接続バス]** をクリックします。  
ウィンドウに、デバイスコントロールの分類に含まれるすべての接続バスのアクセスルールが表示されます。
4. 編集するアクセスルールを選択します。
5. **[アクセス]** 列で、接続バスへのアクセスを許可するかどうかを選択します：**許可**または**拒否**。
6. 変更内容を保存します。

## 信頼する Wi-Fi ネットワークの追加

企業の Wi-Fi ネットワークなど、安全だとみなされる Wi-Fi ネットワークに対する接続をユーザーに許可できます。そのためには、ネットワークを信頼する Wi-Fi ネットワークのリストに追加する必要があります。デバイスコントロールは、信頼リストで指定したもの以外のすべての Wi-Fi ネットワークへのアクセスをブロックします。

Wi-Fi ネットワークを信頼リストに追加するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[デバイスコントロール]** の順に選択します。
3. **[アクセスの設定]** ブロックで、**[デバイスと Wi-Fi ネットワーク]** ボタンをクリックします。

ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されま  
す。

4. **[Wi-Fi ネットワークへのアクセス]** ブロックで、**[Wi-Fi]** をクリックします。  
表示されたウィンドウで、Wi-Fi ネットワークのアクセスルールが表示されます。
5. **[アクセス]** 列で、**[例外を除きブロック]** を選択します。
6. **[信頼する Wi-Fi ネットワーク]** で、**[追加]** をクリックします。
7. 表示されたウィンドウで、次のいずれかの手順を実行します：
  - a. **[ネットワーク名]** で、信頼リストに追加する Wi-Fi ネットワークの名前を指定します。
  - b. **[認証種別]** で、信頼する Wi-Fi ネットワークの接続時に使用される認証の種別を選択します。
  - c. **[暗号化種別]** で、信頼する Wi-Fi ネットワークのトラフィックの保護に使用される暗号化の種別を選  
択します。
  - d. **[コメント]** で、追加する Wi-Fi ネットワークについての任意の情報を指定します。

すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされま  
す。

8. 変更内容を保存します。


## リムーバブルドライブの使用状況の監視

リムーバブルドライブの使用状況の監視には以下が含まれます：

- リムーバブルドライブ上のファイルの操作の監視。
- 信頼済みのリムーバブルドライブの接続および接続解除の監視。

Kaspersky Endpoint Security を使用して、リムーバブルドライブだけでなくすべての信頼済みデバイスの接  
続および接続解除を監視できます。イベントの記録はデバイスコントロール機能の[通知設定](#)で有効にする  
ことができます。イベントのセキュリティレベルは情報メッセージです。

リムーバブルドライブの使用状況の監視を有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[デバイスコントロール]** の順に選択しま  
す。
3. **[アクセスの設定]** ブロックで、**[デバイスと Wi-Fi ネットワーク]** ボタンをクリックします。  
ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されま  
す。
4. **[ストレージ機器へのアクセス]** ブロックで、**[リムーバブルドライブ]** を選択します。
5. **[ログ記録]** をクリックします。

6. 表示されたウィンドウで、**【ログ記録】** タブを選択します。
7. **【ログ記録】** をオンにします。
8. **【ファイルの操作】** で、監視する操作を選択します：**書き込み、削除**。
9. **【ファイル形式でフィルタリング】** ブロックで、デバイスコントロールで記録するファイル形式に関連付けられた操作を選択します。
10. 監視対象のリムーバブルドライブを使用するユーザーまたはユーザーグループを選択します。
11. 変更内容を保存します。

ユーザーが、リムーバブルドライブ上のファイルに書き込みをしたりリムーバブルドライブのファイルを削除すると、その操作に関する情報がイベントログに保存され、Kaspersky Security Center にイベントが送信されます。Kaspersky Security Center の管理コンソールに保存されているリムーバブルドライブのファイルに関するイベントは、**【管理サーバー】** ノードの作業領域内の **【イベント】** タブで確認できます。ローカルの Kaspersky Endpoint Security のイベントログにイベントを表示するには、デバイスコントロールの [通知設定](#) で **【ファイルの操作が実行されました】** をオンにしてください。

## キャッシュ期間の変更

デバイスコントロール機能は、監視対象デバイスに関連するイベント（デバイスからファイルを読み取り、ファイルをデバイスに書き込む、またその他のイベントのようなデバイスに接続したり接続を解除したりするイベント）を登録します。デバイスコントロールは次に Kaspersky Endpoint Security の設定に従って動作を許可したりブロックしたりします。

デバイスコントロールはキャッシュ期間とよばれると口絵の期間イベントに関する情報を保存します。イベントに関する情報がキャッシュされて登録された場合、デバイスへの接続などについて Kaspersky Endpoint Security に関連する情報を通知したり、関連する動作に関してアクセス件を付与するために別のプロンプトを表示する必要はありません。これによりデバイスでの作業がより簡便になります。

次のイベントの設定がキャッシュ内の記録と一致する場合、イベントは重複するイベントとして認識されません：

- デバイス ID
- アクセスを試行したユーザーアカウントの SID
- デバイスカテゴリ
- デバイスに対して実行された操作
- この操作に関するアプリケーションの権限の判断：許可または拒否
- 操作を実行するために使用されたプロセスのパス
- アクセスされたファイル

キャッシュ期間の変更より前に、[Kaspersky Endpoint Security のセルフディフェンスが無効](#)にしてください。キャッシュ期間を変更後、セルフディフェンスを有効にしてください。

キャッシュ期間を変更するには：

1. コンピューター上のレジストリエディタを開きます。
2. レジストリエディタで、次のセクションに移動します：
  - 64 ビットのオペレーティングシステムでは：  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
  - 32 ビットのオペレーティングシステムでは：  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]
3. DeviceControlEventsCachePeriod を開いて編集します。
4. デバイスコントロールがイベントに関する情報を保存する期間を定義します（分）。

## 信頼するデバイスを使用した処理

「信頼するデバイス」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

信頼するデバイスで作業するには、個々のユーザー、ユーザーグループ、または組織内のすべてのユーザーにアクセス権を付与できます。

たとえば、組織でリムーバブルドライブの使用を許可していないが、管理者が仕事でリムーバブルドライブを使用している場合、管理者グループのみにリムーバブルドライブを許可できます。これを行うには、信頼するリストにリムーバブルドライブを追加し、ユーザーのアクセス許可を設定します。

Kaspersky Endpoint Security では、次の方法でデバイスを信頼リストに追加できます：

- 組織に Kaspersky Security Center が導入されていない場合、デバイスをコンピューターに接続し、[アプリケーション設定の信頼リストに追加](#)できます。信頼するデバイスのリストを組織内のすべてのコンピューターに配布するには、ポリシー内の信頼するデバイスのリストの統合を有効にするか、[エクスポート/インポート手順](#)を使用できます。
- 組織に Kaspersky Security Center が導入されている場合、接続されているすべてのデバイスをリモートで検出し、[ポリシーで信頼するデバイスのリストを作成](#)できます。信頼するデバイスのリストは、ポリシーが適用されるすべてのコンピューターで利用できます。

Kaspersky Endpoint Security では、信頼済みデバイスの使用をコントロールできます（接続および接続解除）。イベントの記録はデバイスコントロール機能の[通知設定](#)で有効にすることができます。イベントのセキュリティレベルは情報です。

信頼するデバイスで作業する際に Kaspersky Endpoint Security には次の制限があります：

- Kaspersky Endpoint Security 管理プラグインのバージョン 11.0.0–11.2.0 は Kaspersky Endpoint Security のバージョン 11.3.0 および 11.4.0 で作成された信頼するデバイスのリストと動作しません。これらのバージョンで作成した信頼するデバイスのリストで作業する場合は、管理プラグインをバージョン 11.3.0 および 11.4.0 にアップグレードする必要があります。
- Kaspersky Endpoint Security 管理プラグインのバージョン 11.3.0 および 11.4.0 は Kaspersky Endpoint Security の 11.2.0 以前のバージョンで作成された信頼するデバイスのリストと動作しません。これらのバージョンで信頼するデバイスのリストを使用するには、製品をバージョン 11.3.0 および 11.4.0 にアップグレードしてください。状況の詳細な説明を入力して[カスペルスキーカンパニーアカウントからテクニカルサポート](#)にサポート依頼を送信することもできます。




- Kaspersky Endpoint Security のバージョン 11.2.0 からバージョン 11.3.0. に信頼するデバイスのリストを移行するには、状況の詳細な説明を入力して[カスペルスキーカンパニーアカウント](#)からテクニカルサポートにサポート依頼を送信してください。

## アプリケーションインターフェイスから信頼リストへのデバイスの追加

既定では、信頼するデバイスのリストにデバイスを追加すると、そのデバイスへのアクセス権がすべてのユーザー（「Everyone」グループに属するユーザー）に付与されます。

アプリケーションインターフェイスから信頼リストにデバイスを追加するには、次の操作を行います：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【アクセスの設定】** で、**【信頼するデバイス】** をクリックします。  
信頼するデバイスのリストが開きます。
4. **【選択】** をクリックします。  
接続されたデバイスのリストが開きます。デバイスのリストは、**【接続されているデバイスの表示】** で選択した値により異なります。
5. デバイスのリストで、信頼するデバイスのリストに追加するデバイスを選択します。
6. **【コメント】** フィールドで、その信頼するデバイスに関する情報を入力できます。
7. 信頼するデバイスへのアクセスを許可するユーザーまたはユーザーグループを選択します。
8. 変更内容を保存します。

## Kaspersky Security Center から信頼リストへのデバイスの追加

Kaspersky Security Center は、Kaspersky Endpoint Security がコンピューターにインストールされており、かつ[デバイスコントロールが有効](#)の場合に、デバイスに関する情報を取得します。デバイスに関する情報が Kaspersky Security Center で利用可能でない限り、デバイスを信頼できるリストに追加することはできません。

次のデータに従って、デバイスを信頼リストに追加できます：

- **ID によるデバイス**：各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000 特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。
- **モデルによるデバイス**：各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：VID\_1234&PID\_5678 組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。



- **ID マスクによるデバイス**：ID が類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。\* 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「?」記号の使用をサポートしていません。例：WDC\_C\*
- **モデルマスクによるデバイス**：同一の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。\* 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「?」記号の使用をサポートしていません。例：「VID\_05AC & PID\_\*」。

信頼するデバイスのリストにデバイスを追加するには、次の操作を行います：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **管理対象デバイス** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、**ポリシー** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**セキュリティコントロール** → **デバイスコントロール** の順に選択します。
6. ウィンドウの右側で、**信頼するデバイス** タブを選択します。
7. 組織内のすべてのコンピューターの信頼するデバイスのリストを作成する場合は **継承時に値を統合する** をオンにします。  
親ポリシーおよび子ポリシー内の信頼するデバイスのリストが統合されます。[継承時に値を統合する] がオンの時にリストが統合されます。親ポリシー内の信頼するデバイスは子ポリシー内では読み取り専用で表示されます。親ポリシー内の信頼するデバイスは編集または削除することはできません。
8. **追加** をクリックし、デバイスを信頼リストに追加する方法を選択します。
9. デバイスをフィルタリングするには、**デバイス種別** ドロップダウンリストで、デバイス種別を選択します（たとえば、**リムーバブルドライブ**）。
10. **名前またはモデル** フィールドに、選択した追加方法に応じて、ID、モデル（VID および PID）、またはマスクを入力します。

モデルマスク（VID および PID）によるデバイスの追加は次のように行われます：どのモデルにも一致しないモデルマスクを入力すると、デバイス ID（HWID）がマスクと一致するかどうかチェックされます。製作元とデバイス種別を識別するデバイス ID の一部のみがチェックされます（SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000）。モデルマスクがデバイス ID の一部と一致する場合、マスクと一致するデバイスがコンピューター上で信頼するデバイスのリストに追加されます。しかし、Kaspersky Security Center のデバイスリストは **更新** をクリックすると空のままになります。デバイスリストを正しく表示させるには、デバイス ID マスクを使用してデバイスを追加します。

11. デバイスをフィルタリングするには、**コンピューター** フィールドに、デバイスが接続されているコンピューター名またはコンピューター名のマスクを入力します。

\* 文字は、任意の文字列を置き換えます。? 文字は、任意の1文字を置き換えます。

12. **更新** をクリックします。

テーブルには、定義されたフィルタリング基準を満たすデバイスのリストが表示されます。

13. 信頼するデバイスのリストに追加するデバイス名の横にあるチェックボックスをオンにします。
14. **[コメント]** フィールドに、デバイスを信頼リストに追加する理由の説明を入力します。
15. **[許可するユーザーまたはユーザーグループ]** の右側にある **[選択]** をクリックします。
16. Active Directory のユーザーまたはグループを選択し、選択内容を確認します。  
既定では、信頼するデバイスへのアクセスは Everyone グループに対して許可されます。
17. 変更内容を保存します。

デバイスが接続されると、Kaspersky Endpoint Security は、認証済みユーザーの信頼するデバイスのリストを確認します。デバイスが信頼されている場合は、デバイス種別または接続バスへのアクセスが拒否された場合でも、Kaspersky Endpoint Security は、すべての権限でデバイスへのアクセスを許可します。デバイスが信頼されておらず、アクセスが拒否された場合は、[ロックされたデバイスへのアクセス要求](#)ができます。


## 信頼するデバイスのリストのエクスポート / インポート

信頼するデバイスのリストを組織内のすべてのコンピューターに配布するには、エクスポート/インポート手順を使用できます。

たとえば、信頼するリムーバブルドライブのリストを配布する必要がある場合、次のことを行う必要があります：

1. リムーバブルドライブをコンピューターに順次接続します。
2. Kaspersky Endpoint Security の設定で、[リムーバブルドライブを信頼するリストに追加します](#)。必要に応じて、ユーザーのアクセス許可を設定します。たとえば、管理者のみがリムーバブルドライブにアクセスできるようにします。
3. Kaspersky Endpoint Security の設定で信頼するデバイスのリストをエクスポートします（以下の手順を参照）。
4. 信頼するデバイスリストのファイルを組織内の他のコンピューターに配布します。たとえば、ファイルを共有フォルダーに配置します。
5. 組織内の他のコンピューターの Kaspersky Endpoint Security の設定で、信頼するデバイスのリストをインポートします（以下の手順を参照）。

信頼するデバイスのリストをインポートまたはエクスポートするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[デバイスコントロール]** の順に選択します。
3. **[アクセスの設定]** で、**[信頼するデバイス]** をクリックします。  
信頼するデバイスのリストが開きます。
4. 信頼するデバイスのリストをエクスポートするには：
  - a. 編集する信頼するデバイスを選択します。
  - b. **[エクスポート]** をクリックします。

c. 表示されたウィンドウで、信頼するデバイスのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. **【保存】** をクリックします。

Kaspersky Endpoint Security は、信頼するデバイスのリスト全体を XML ファイルにエクスポートします。

5. 信頼するデバイスのリストをインポートするには：

a. **【インポート】** で、関連する操作を選択します：**【インポートして既存に追加】** または **【インポートして既存を置換】**。

b. 表示されたウィンドウで、信頼するデバイスのリストをインポートする XML ファイルを選択します。

c. **【開く】** をクリックします。

コンピューターに信頼するデバイスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

デバイスが接続されると、Kaspersky Endpoint Security は、認証済みユーザーの信頼するデバイスのリストを確認します。デバイスが信頼されている場合は、デバイス種別または接続バスへのアクセスが拒否された場合でも、Kaspersky Endpoint Security は、すべての権限でデバイスへのアクセスを許可します。

## ブロックされたデバイスへのアクセスの取得

デバイスコントロールの設定次第では、業務で必要なデバイスを誤ってブロックしてしまう可能性があります。

組織内に Kaspersky Security Center が導入されていない場合、Kaspersky Endpoint Security のローカルの設定を使用して、デバイスへのアクセスを付与できます。たとえば、[そのデバイスを信頼リストに追加したり](#)、[デバイスコントロールを一時的に無効にすることができます](#)。

組織内に Kaspersky Security Center が導入されていてコンピューターにポリシーが適用されている場合、管理コンソールを使用して、デバイスへのアクセスを付与できます。

## オンラインモードでのアクセス権の付与

ブロックされたデバイスへのオンラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。このコンピューターは管理サーバーに接続できる必要があります。

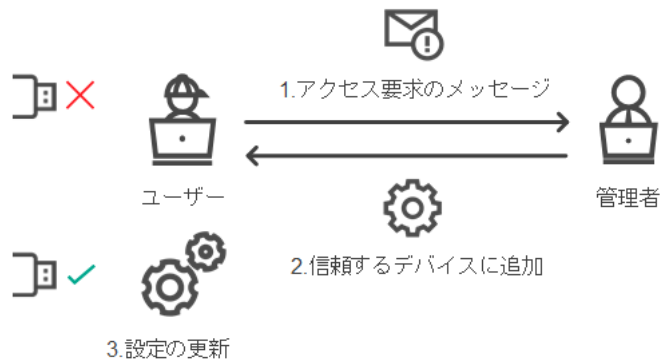
オンラインモードでのアクセス権が付与される流れは次の通りです：

1. ユーザーが管理者に、アクセス要求のメッセージを送信します。

2. 管理者が、該当するデバイスを信頼リストに追加します。

管理者は、管理グループのポリシーまたは個別のコンピューターのローカルでの製品設定で、信頼するデバイスを追加できます。

3. 管理者が、ユーザーのコンピューター上の Kaspersky Endpoint Security の設定を更新します。



オンラインモードでのデバイスへのアクセス権の付与のプロセス

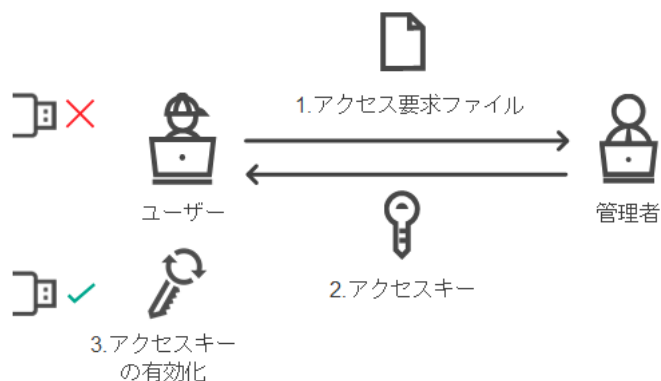
## オフラインモードでのアクセス権の付与

ブロックされたデバイスへのオフラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。ポリシー設定の **【デバイスコントロール】** セクションで、**【一時アクセスの要求を許可する】** がオンになっている必要があります。

デバイスを信頼リストに追加することはできない状況で、ブロックされているデバイスへの一時的なアクセス権を付与する場合は、デバイスへのオフラインモードでのアクセス権を付与できます。この方法を使用することで、コンピューターがネットワークに接続されていなかったり、企業ネットワークの外で動作している場合でも、ブロックされているデバイスへのアクセス権を付与できます。

オフラインモードでのアクセス権が付与される流れは次の通りです：

1. ユーザーがアクセス要求ファイルを作成し、管理者に送信します。
2. 管理者がアクセス要求ファイルからアクセスキーを作成して、ユーザーに送信します。
3. ユーザーはアクセスキーを有効化します。



オフラインモードでのデバイスへのアクセス権の付与のプロセス

## オンラインモードでのアクセス権の付与

ブロックされたデバイスへのオンラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。このコンピューターは管理サーバーに接続できる必要があります。

ユーザーがブロックされたデバイスへのアクセスを要求する方法は次の通りです：

1. コンピューターにデバイスを接続します。

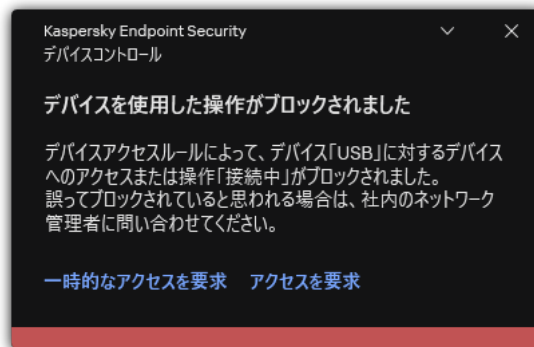
Kaspersky Endpoint Security によって、このデバイスへのアクセスがブロックされているという通知が表示されます（以下の図を参照）。

2. **【アクセス要求】** をクリックします。

**【管理者に送信するメッセージ】** ウィンドウが表示されます。このメッセージには、ブロックされているデバイスの情報が含まれています。

3. **【送信】** をクリックします。

管理者は、アクセスを要求するメッセージを指定されている方法で受け取ります（たとえば、電子メールなど）。ユーザーからの要求を処理する方法については、[Kaspersky Security Center のオンラインヘルプ](#)を参照してください。[デバイスの信頼リストへの追加](#)と Kaspersky Endpoint Security の設定の更新がコンピューター上で完了したら、ユーザーはデバイスへのアクセスを取得します。



デバイスコントロールの通知

## オフラインモードでのアクセス権の付与

ブロックされたデバイスへのオフラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。ポリシー設定の **【デバイスコントロール】** セクションで、**【一時アクセスの要求を許可する】** がオンになっている必要があります。

ユーザーがブロックされたデバイスへのアクセスを要求する方法は次の通りです：

1. コンピューターにデバイスを接続します。

Kaspersky Endpoint Security によって、このデバイスへのアクセスがブロックされているという通知が表示されます（以下の図を参照）。

2. **【一時的なアクセスを要求】** リンクをクリックします。

接続されているデバイスを含むウィンドウが開きます。

3. 接続されているデバイスのリストから、アクセス権を取得するデバイスを選択します。
4. **「アクセス要求ファイルを生成」** をクリックします。
5. **「アクセス期間」** で、デバイスにアクセスする期間を指定します。
6. ファイルをコンピューター上に保存します。

これにより、拡張子が「.akey」のアクセス要求ファイルがコンピューターにダウンロードされます。任意の受け渡し方法で、アクセス要求ファイルを企業 LAN の管理者に送信します。



デバイスコントロールの通知

### [管理コンソール \(MMC\) で、管理者がブロックされたデバイス向けのアクセスキーを作成する方法](#)




1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、対象のクライアントコンピューターが属する管理グループの名前のフォルダーを開きます。
3. 作業領域で、 **〔デバイス〕** タブを選択します。
4. クライアントコンピューターのリストで、ブロックされたデバイスへの一時アクセスをユーザーに許可する必要があるコンピューターを選択します。
5. コンピューターのコンテキストメニューで、 **〔オフラインモードでのアクセスを許可する〕** を選択します。
6. 表示されたウィンドウで、 **デバイスコントロール** タブを選択します。
7. **〔参照〕** をクリックして、ユーザーから受信したアクセス要求ファイルをダウンロードします。  
ユーザーがアクセスを要求した、ブロックされたデバイスの情報が表示されます。
8. 必要に応じて、 **〔アクセス期間〕** 設定の値を変更します。  
既定では、 **〔アクセス期間〕** の値は、アクセス要求ファイルの作成時にユーザーが指定した値となります。
9. **〔アクティベーション期限〕** 設定の値を指定します。  
この設定では、ユーザーがアクセスキーを使用して、ブロックされたデバイスへのアクセスを有効化できる期間を定義します。
10. アクセスキーファイルをコンピューター上に保存します。

[Web コンソールまたは Cloud コンソールで、管理者がブロックされたデバイス向けのアクセスキーを作成する方法](#)

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【管理対象デバイス】** の順に選択します。
2. クライアントコンピューターのリストで、ブロックされたデバイスへの一時アクセスをユーザーに許可する必要があるコンピューターを選択します。
3. コンピューターのリストの上にある省略記号の ( ) をクリックして、**【オフラインモードでのデバイスへのアクセスを許可】** をクリックします。
4. 表示されたウィンドウで、**【デバイスコントロール】** セクションを選択します。
5. **【参照】** をクリックして、ユーザーから受信したアクセス要求ファイルをダウンロードします。  
ユーザーがアクセスを要求した、ブロックされたデバイスの情報が表示されます。
6. 必要に応じて、**【アクセス期間 (時間)】** 設定の値を変更します。  
既定では、**【アクセス期間 (時間)】** の値は、アクセス要求ファイルの作成時にユーザーが指定した値となります。
7. デバイス上でのアクセスキーの有効期間を指定します。  
この設定では、ユーザーがアクセスキーを使用して、ブロックされたデバイスへのアクセスを有効化できる期間を定義します。
8. アクセスキーファイルをコンピューター上に保存します。

これにより、ブロックされたデバイスへのアクセスキーファイルがコンピューターにダウンロードされます。アクセスキーファイルの拡張子は「.acode」です。任意の受け渡し方法で、ブロックされたデバイスへのアクセスキーファイルをユーザーに送信します。

ユーザーは次の方法でアクセスキーを有効化します。

1. [メインウィンドウ](#)で、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** を選択します。
3. **【アクセス要求】** ブロックの **【デバイスへのアクセス要求】** をクリックします。
4. 表示されたウィンドウで、**【アクセスキーの有効化】** をクリックします。
5. 表示されたウィンドウで、企業 LAN 管理者から受け取ったデバイスへのアクセスキーを持つファイルを選択します。  
アクセスの提供に関する情報を確認できるウィンドウが表示されます。
6. **【OK】** をクリックします。


これにより、管理者が指定した期間、ユーザーにデバイスへのアクセス権が付与されます。ユーザーにはデバイスへのすべてのアクセス権（読み取りと書き込み）が付与されます。キーの有効期限が切れると、デバイスへのアクセスがブロックされます。ユーザーがデバイスへの恒久的なアクセス権を必要としている場合、[デバイスを信頼リストに追加](#)します。

## デバイスコントロールメッセージのテンプレートの編集

ブロックされているデバイスへのアクセスをユーザーが試行すると、そのデバイスへのアクセスはブロックされていること、またはデバイスの操作はブロックされていることを示すメッセージが表示されます。誤ってデバイスへのアクセスがブロックされているかデバイスの操作がブロックされていると考えられる場合、ユーザーはブロック処理についてのメッセージにあるリンクをクリックして、LAN 管理者にメッセージを送信できます。

デバイスへのアクセスがブロックされていることを示すメッセージ、デバイスの操作がブロックされていることを示すメッセージ、および管理者に送信するメッセージのテンプレートが用意されています。このメッセージテンプレートは変更することができます。

デバイスコントロールメッセージのテンプレートを編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【メッセージのテンプレート】** で、デバイスコントロールのメッセージのテンプレートを設定します：
  - **ブロックに関するメッセージ**：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。
  - **管理者に送信するメッセージ**：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**デバイスへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 **【ユーザー要求】** を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。
4. 変更内容を保存します。

## アンチブリッジ

アンチブリッジは、ネットワークブリッジの作成をブロックし、コンピューターで複数のネットワーク接続が同時に確立することを防止します。この機能を使用することで、セキュリティ保護が不十分で接続が許可されていないネットワークから社内ネットワークを保護できます。

アンチブリッジは、接続ルールを使用してネットワーク接続の確立を管理します。

以下の定義済みデバイス種別に対して接続ルールが作成されます：

- ネットワークアダプター
- Wi-Fi アダプター
- モデム


接続ルールが有効な場合、以下が実行されます：

- ルールで指定されたデバイス種別が両方の接続で使用されていた場合、新しい接続を確立する際に現在の接続をブロックします。
- 優先順位の低いルールが適用されるデバイス種別を使用して確立された接続をブロックします。

## アンチブリッジを有効にする

アンチブリッジは既定で無効です。


アンチブリッジを有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【アクセスの設定】** で、**【アンチブリッジ】** をクリックします。
4. **【アンチブリッジを有効にする】** トグルスイッチを使用して機能を有効または無効にします。
5. 変更内容を保存します。

アンチブリッジを有効にすると、接続ルールに従って、すでに確立されている接続がブロックされます。


## 接続ルールのステータスの変更

接続ルールのステータスを変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。
3. **【アクセスの設定】** で、**【アンチブリッジ】** をクリックします。
4. **【デバイスのルール】** ブロックで、ステータスを変更するルールを選択します。
5. **【コントロール】** 列のトグルスイッチを使用してルールを有効または無効にします。
6. 変更内容を保存します。

## 接続ルールの優先度の変更

接続ルールの優先度を変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【デバイスコントロール】** の順に選択します。

3. [アクセスの設定] で、[アンチブリッジ] をクリックします。
4. [デバイスのルール] ブロックで、優先度を変更するルールを選択します。
5. [上へ] と [下へ] を使用して接続ルールの優先度を設定します。  
リスト上の位置が高くなるほど、ルールの優先度が高くなります。アンチブリッジは、最も優先度が高いルールが使用されるデバイス種別によって確立された接続を除くすべての接続をブロックします。
6. 変更内容を保存します。

## アダプティブアノマリーコントロール

この機能は Kaspersky Endpoint Security for Business Advanced および Kaspersky Total Security for Business でのみ使用可能です。Kaspersky Endpoint Security for Business の詳細については、[カスペルスキーの Web サイト](#) を参照してください。

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「Office アプリケーションによる Microsoft PowerShell の起動」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートすると同様に、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。ルールのアップデートの適用は[手動で承認](#)する必要があります。

## アダプティブアノマリーコントロールの設定

アダプティブアノマリーコントロールの設定では、次のステップが必要です：

### 1. アダプティブアノマリーコントロールのトレーニング

アダプティブアノマリーコントロールを有効にすると、アダプティブアノマリーコントロールルールがトレーニングモードで動作します。トレーニング期間中、アダプティブアノマリーコントロールはルールを適用可能な動作が発生するかどうかを監視し、ルールを適用可能な動作が発生したらそのイベントを Kaspersky Security Center に送信します。ルールごとに、設定されているトレーニング期間は異なります。トレーニングモードの継続期間はカスペルスキーのエキスパートが設定しています。通常は、トレーニングモードの継続期間は 2 週間です。

特定のルールを適用可能な動作がトレーニング期間中に 1 回も発生しなかった場合、アダプティブアノマリーコントロールは、そのルールの対象となる動作は平常時には発生しない動作だと判断します。そのため、トレーニング終了後、該当するルールの適用対象となる動作はすべて Kaspersky Endpoint Security でブロックされるようになります。

特定のルールを適用可能な動作がトレーニング期間中に発生した場合、Kaspersky Endpoint Security は「[ルールの適用のレポート](#)」と「[スマートトレーニングでのルールの適用状況](#)」リポジトリにイベントのログ記録を保存します。

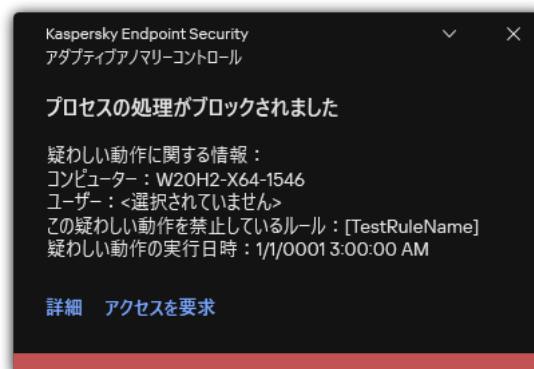
## 2. 「ルールの適用のレポート」の分析

管理者は「[ルールの適用のレポート](#)」または「[スマートトレーニングでのルールの適用状況](#)」リポジトリの内容を分析する必要があります。分析結果に基づき、管理者はそれぞれのルールが適用されたときのアダプティブアノマリーコントロールによる処理を、「ブロック」または「許可」から選択します。管理者は、ルールの適用状況に関する情報をさらに収集した上で判断を行うために、トレーニングモードの期間を延長することもできます。また、管理者がルールの適用状況のレポートに対する対応を行わなかった場合も、アダプティブアノマリーコントロールは引き続きトレーニングモードで動作します。トレーニングモードの残り期間もリセットされます。

アダプティブアノマリーコントロールの設定内容は、即座に動作に反映されます。アダプティブアノマリーコントロールの設定は、自動的に設定される場合と手動で設定する場合を合わせて、次の方法で設定されます：

- トレーニングモードの期間中に1回も適用可能な動作が発生しなかったルールについては、該当するルールが適用可能な動作をすべてブロックする設定が自動的に行われる。
- 新しいルールの追加や古くなったルールの削除が Kaspersky Endpoint Security によって行われる。
- 管理者がルール適用のレポートまたは[スマートトレーニングでのルールの適用状況](#)リポジトリの内容を確認した後、アダプティブアノマリーコントロールによる処理を設定します。ルール適用のレポートおよび[スマートトレーニングでのルールの適用状況](#)リポジトリの内容を確認することを推奨します。

悪意のあるアプリケーションによる動作が検知された場合、Kaspersky Endpoint Security はその動作をブロックし通知を表示します（以下の図を参照）。

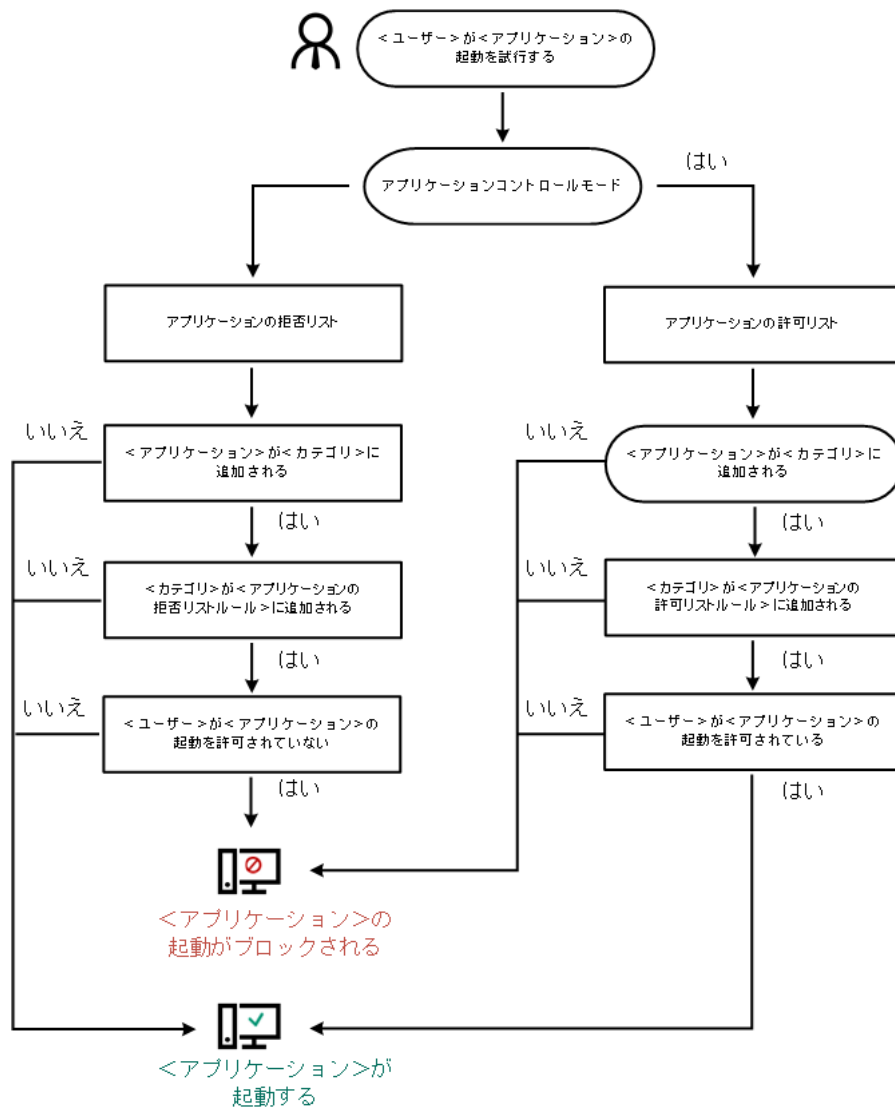


アダプティブアノマリーコントロールの通知

## アダプティブアノマリーコントロールの動作アルゴリズム

Kaspersky Endpoint Security は次の図のアルゴリズムに従って、ルールの適用対象となる動作の実行を許可するかブロックするかを判定します。






アダプティブアノマリーコントロールの動作アルゴリズム

## アダプティブアノマリーコントロールの有効化と無効化

アダプティブアノマリーコントロールは既定で有効になっています。

アダプティブアノマリーコントロールを有効または無効にするには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アダプティブアノマリーコントロール]** を選択します。
3. **[アダプティブアノマリーコントロール]** トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

この結果、アダプティブアノマリーコントロールは学習モードに切り替わります。学習モード中は、アダプティブアノマリーコントロールはルールの適用を監視します。学習モードが完了すると、アダプティブアノマリーコントロールは企業ネットワーク上のコンピューターで平常時には発生しない動作のブロックを開始します。

企業で新しいツールの使用を開始した場合など、アダプティブアノマリーコントロールがそのツールの動作をブロックしてしまう場合は、学習モードの結果をリセットして再度学習モードを実行してください。このためには、[ルールがトリガーされた場合の処理を変更](#)する必要があります（例えば、処理を[通知]に変更するなど）。それから、学習モードを再度有効にします（値を[スマート]にする）。


## アダプティブアノマリーコントロールルールの有効化と無効化

アダプティブアノマリーコントロールルールを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[セキュリティコントロール] → [アダプティブアノマリーコントロール]の順に選択します。
3. [ルール] ブロックで、[ルールの編集] ボタンをクリックします。  
アダプティブアノマリーコントロールルールのリストが開きます。
4. テーブルで、Office アプリケーションの動作など、ルールのセットを選択し、展開します。
5. Office アプリケーションによる Windows PowerShellの起動などのルールを選択します。
6. [ステータス] 列のトグルスイッチを使用してアダプティブアノマリーコントロールルールを有効または無効にします。
7. 変更内容を保存します。

## アダプティブアノマリーコントロールルールが適用されたときに実行する処理の変更

アダプティブアノマリーコントロールルールが適用されたときに実行する処理を編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[セキュリティコントロール] → [アダプティブアノマリーコントロール]の順に選択します。
3. [ルール] ブロックで、[ルールの編集] ボタンをクリックします。  
アダプティブアノマリーコントロールルールのリストが開きます。
4. ルールを選択します。
5. [編集] をクリックします。  
アダプティブアノマリーコントロールルールのプロパティウィンドウが開きます。
6. [処理] ブロックで、以下のオプションのいずれかを選択します：
  - **スマート**：このオプションを選択した場合、アダプティブアノマリーコントロールルールは、カスペルスキーのエキスパートが定義した期間、スマートトレーニングで動作します。このモードでは、アダプ

ティプアノマリーコントロールルールが適用されると、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、情報が Kaspersky Security Center 管理サーバーの [スマートトレーニングでのルールの適用状況] 保管領域にログとして記録されます。スマートトレーニングで動作するよう指定された期間が終了すると、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

- **ブロック** : この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。
- **通知する** : この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、ルールの適用対象となった動作の情報がログに記録されます。


7. 変更内容を保存します。

## Creating an exclusion for an Adaptive Anomaly Control rule

You cannot create more than 1,000 exclusions for Adaptive Anomaly Control rules. It is not recommended to create more than 200 exclusions. To reduce the number of exclusions used, it is recommended to use masks in the settings of exclusions.

An exclusion for an Adaptive Anomaly Control rule includes a description of the source and target objects. The *source object* is the object performing the actions. The *target object* is the object on which the actions are being performed. For example, you have opened a file named `file.xlsx`. As a result, a library file with the DLL extension is loaded into the computer memory. This library is used by a browser (executable file named `browser.exe`). In this example, `file.xlsx` is the source object, Excel is the source process, `browser.exe` is the target object, and Browser is the target process.

To create an exclusion for an Adaptive Anomaly Control rule:

1. In the main application window, click the button .
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the **Rules** block, click the **Edit rules** button.  
The Adaptive Anomaly Control rule list opens.
4. Select a rule in the table.
5. Click the **Edit** button.  
The Adaptive Anomaly Control rule properties window opens.
6. In the **Exclusions** block, click the **Add** button.  
The exclusion properties window opens.
7. Select the user for which you want to configure an exclusion.

Adaptive Anomaly Control does not support exclusions for user groups. If you select a user group, Kaspersky Endpoint Security does not apply the exclusion.

8. In the **Description** field, enter a description of the exclusion.

9. Define the settings of the source object or source process started by the object:

- **Source process.** Path or mask of the path to the file or folder containing files (for example, C:\Dir\File.exe or Dir\\*.exe).
- **Source process hash.** File hash code.
- **Source object.** Path or mask of the path to the file or folder containing files (for example, C:\Dir\File.exe or Dir\\*.exe). For example, file path document.docm, which uses a script or macro to start the target processes.

You can also specify other objects to exclude, such as a web address, macro, command in the command line, registry path, or others. Specify the object according to the following template: `object://<object>`, where `<object>` refers to the name of the object, for example, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. You can also use masks, for example, `object://*C:\Windows\temp\*`.

- **Source object hash.** File hash code.

The Adaptive Anomaly Control rule is not applied to actions performed by the object, or to processes started by the object.

10. Specify the settings of the target object or target processes started on the object.


- **Target process.** Path or mask of the path to the file or folder containing files (for example, C:\Dir\File.exe or Dir\\*.exe).
- **Target process hash.** File hash code.
- **Target object.** The command to start the target process. Specify the command using the following pattern `object://<command>`, for example, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage txt' "`. You can also use masks, for example, `object://*C:\Windows\temp\*`.
- **Target object hash.** File hash code.

The Adaptive Anomaly Control rule is not applied to actions taken on the object, or to processes started on the object.

11. Save your changes.

## アダプティブアノマリーコントロールルールの除外のエクスポートとインポート

選択したルールに除外リストをエクスポートまたはインポートするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アダプティブアノマリーコントロール]** の順に選択します。
3. **[ルール]** ブロックで、**[ルールの編集]** ボタンをクリックします。

アダプティブアノマリーコントロールルールが開きます。

4. ルールのリストをエクスポートするには：

- a. エクスポートする除外リストを含むルールを選択します。
- b. **【エクスポート】** をクリックします。
- c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
- d. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。
- e. **【保存】** をクリックします。

5. ルールのリストをインポートするには：

- a. **【インポート】** をクリックします。
- b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
- c. **【開く】** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。


6. 変更内容を保存します。

## アダプティブアノマリーコントロールルールへのアップデートの適用

定義データベースがアップデートされたときに、ルールのリストに新しいアダプティブアノマリーコントロールルールを追加したり、ルールのリストから既存のアダプティブアノマリーコントロールルールを削除したりできます。これらのルールへのアップデートが適用されていない場合、Kaspersky Endpoint Security はリストから追加または削除されるアダプティブアノマリーコントロールルールを他のルールから区別します。

アップデートが適用されるまで、アップデートによって削除される予定のアダプティブアノマリーコントロールルールもテーブルに表示されますが、**【無効】** ステータスが割り当てられます。これらのルールの設定は変更できません。

アダプティブアノマリーコントロールルールにアップデートを適用するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【アダプティブアノマリーコントロール】** の順に選択します。
3. **【ルール】** ブロックで、**【ルールの編集】** ボタンをクリックします。  
アダプティブアノマリーコントロールルールが開きます。
4. 表示されたウィンドウで、**【アップデートの承認】** をクリックします。

【**アップデートの承認**】は、アダプティブアノマリーコントロールルールで利用可能なアップデートが存在する場合にクリックできます。


5. 変更内容を保存します。

## アダプティブアノマリーコントロールのメッセージテンプレートの編集

ユーザーがアダプティブアノマリーコントロールルールによってブロックされている処理を実行しようとする、有害な可能性のある処理がブロックされることを示すメッセージが表示されます。処理が誤ってブロックされていると思われる場合は、メッセージテキストのリンクを使用して、メッセージをローカルエリアネットワーク管理者に送信できます。

有害な可能性のある処理がブロックされたときに表示されるメッセージと管理者に送信するメッセージについては、専用テンプレートを利用できます。このメッセージテンプレートは変更することができます。

メッセージテンプレートを編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、【セキュリティコントロール】 → 【アダプティブアノマリーコントロール】の順に選択します。
3. 【**テンプレート**】ブロックで、アダプティブアノマリーコントロールのメッセージのテンプレートを設定します。
  - **ブロックに関するメッセージ**：典型的でない動作をブロックするアダプティブアノマリーコントロールルールが適用された際に表示されるメッセージのテンプレート。
  - **管理者に送信するメッセージ**：ブロックが誤検知だと考えられる場合に、社内のローカルネットワークの管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの動作ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出【**ユーザー要求**】を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

4. 変更内容を保存します。

## アダプティブアノマリーコントロールのレポートの表示

アダプティブアノマリーコントロールのレポートを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの【**管理対象デバイス**】フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、【**ポリシー**】タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

5. ポリシーウィンドウで、[セキュリティコントロール] → [アダプティブアノマリーコントロール] の順に選択します。

ウィンドウの右側に、アダプティブアノマリーコントロールの設定が表示されます。

6. 次のいずれかの手順を実行します：

- アダプティブアノマリーコントロールルールの設定状況に関するレポートを表示するには、[アダプティブアノマリーコントロールルールのステータスに関するレポート] をクリックします。
- アダプティブアノマリーコントロールルールの適用状況に関するレポートを表示するには、[アダプティブアノマリーコントロールルールの適用に関するレポート] をクリックします。

7. レポートの生成プロセスが開始されます。

レポートが新しいウィンドウに表示されます。

## アプリケーションコントロール

アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。

アプリケーションコントロールの設定では、次のステップが必要です：

### 1. アプリケーションカテゴリの作成

管理者は、自身が管理するアプリケーションのカテゴリを作成します。アプリケーションのカテゴリは、管理グループに関係なく、企業ネットワーク内のすべてのコンピューターを対象としています。カテゴリを作成するには、KL カテゴリ（ブラウザーなど）、ファイルのハッシュ、アプリケーションの開発元、およびその他の条件を使用できます。

### 2. アプリケーションコントロールルールの作成

管理者は、管理グループのポリシーにアプリケーションコントロールルールを作成します。ルールには、アプリケーションのカテゴリと、「ブロック」または「許可」のカテゴリからのアプリケーションの起動ステータスが含まれます。

### 3. アプリケーションコントロールモードの選択

管理者は、拒否リストまたは許可リストのいずれのルールにも含まれていないアプリケーションを操作するモードを選択します。

ユーザーが禁止されたアプリケーションを起動しようとする時、Kaspersky Endpoint Security はアプリケーションの起動をブロックし、通知を表示します（下の図を参照）。

Application Control の構成を確認するためのテストモードが用意されています。このモードでは、Kaspersky Endpoint Security は次のことを行います：

- 禁止されているものも含めて、アプリケーションの起動を許可します。
- 禁止されているアプリケーションの起動に関する通知を表示し、ユーザーのコンピューターのレポートに情報を追加します。
- 禁止されたアプリケーションの起動に関するデータを Kaspersky Security Center に送信します。





アプリケーションコントロールの通知

## アプリケーションコントロールの操作モード

アプリケーションコントロールは2つのモードで動作します。

- **拒否リスト** このモードでは、アプリケーションコントロールルールで禁止されているアプリケーションを除くすべてのアプリケーションを、ユーザーが起動できます。

アプリケーションコントロールのこのモードは、規定では有効になっています。

- **許可リスト** このモードでは、アプリケーションコントロールルールで許可および禁止されていないアプリケーション以外のアプリケーションを、ユーザーが起動できないようにします。

必要なアプリケーションコントロールの許可ルールをすべて設定すると、LAN 管理者が検証していない新しいアプリケーションの起動はブロックされますが、オペレーティングシステムとユーザーが業務で使用している信頼するアプリケーションの動作は許可されます。

許可リストモードでは、[アプリケーションコントロールルールの設定における推奨事項](#)を確認できます。

アプリケーションコントロールは、Kaspersky Endpoint Security のローカルインターフェイスと Kaspersky Security Center の両方で、これらのモードで動作するように設定できます。

Kaspersky Security Center が提供するツールには、Kaspersky Endpoint Security のローカルインターフェイスで使用できないものもあります。これらは次の用途で必要となります：

- [アプリケーションカテゴリの作成](#)

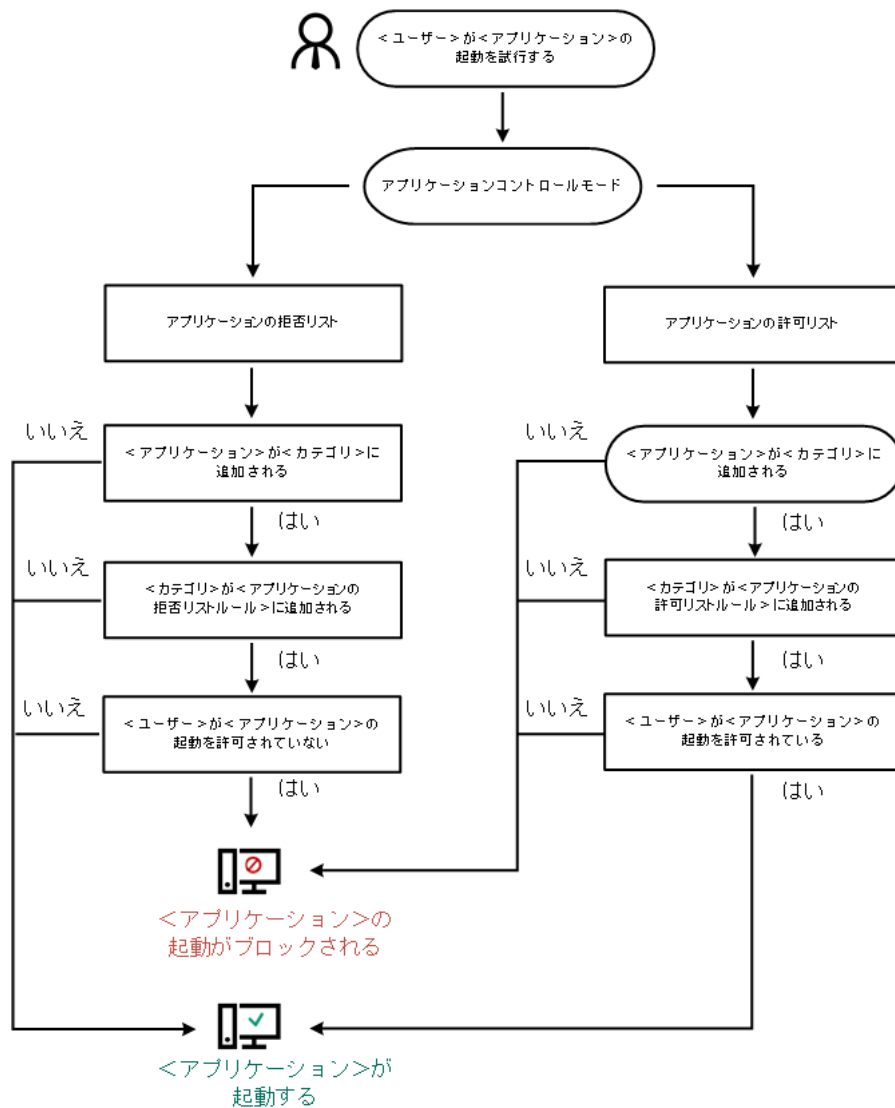
Kaspersky Security Center の管理コンソールで作成するアプリケーションコントロールルールは、カスタマイズされたアプリケーションカテゴリに基づき、Kaspersky Endpoint Security のローカルインターフェイスでの対象条件や除外条件には基づきません。

- [企業の LAN コンピューターにインストールされたアプリケーションについての情報の取得](#)

そのため、アプリケーションコントロールの動作設定には Kaspersky Security Center の使用を推奨します。

## アプリケーションコントロールの動作アルゴリズム

Kaspersky Endpoint Security は、アルゴリズムを使用して、アプリケーションの起動に関する決定を下します（下の図を参照）。



アプリケーションコントロールの動作アルゴリズム

## アプリケーションコントロールの機能の制限

アプリケーションコントロールの機能には、次のような制限があります：

- 本製品のバージョンをアップグレードするとき、アプリケーションコントロールの設定のインポートはサポートされません。
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降を Kaspersky Endpoint Security 11.7.0 for Windows にアップグレードする場合のみ、アプリケーションコントロールコンポーネントの設定のインポートがサポートされます。

Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以外のバージョンからアップグレードする場合、アプリケーションコントロールの設定を動作中の状態に復元するには、設定をやり直す必要があります。

- KSN サーバーと接続されていない場合、Kaspersky Endpoint Security はアプリケーションとモジュールの評価情報をローカル定義データベースからのみ取得します。

Kaspersky Endpoint Security が KL カテゴリ **【その他のアプリケーション\アプリケーション、KSN の評価によって信頼済み】** とするアプリケーションのリストは KSN サーバーへの接続が利用可能であるかによって異なることがあります。

- Kaspersky Security Center のデータベースには、処理したファイル 150,000 個分の情報を記録できます。保管されている記録が 150,000 個に到達すると、新しいファイルは処理されなくなります。処理を再開するには、以前 Kaspersky Endpoint Security がインストールされているコンピューターから Kaspersky Security Center のデータベースに保管したファイルを削除してください。
- スクリプトの起動は、スクリプトがコマンドラインを経由してインタープリターに送られる場合を除き、管理されません。

インタープリターの起動がアプリケーションコントロールルールによって許可されている場合、そのインタープリターから開始されるスクリプトはブロックされません。

インタープリターのコマンドラインで1つ以上のスクリプトの起動がアプリケーションコントロールルールによってブロックされた場合、インタープリターのコマンドラインで指定されたすべてのスクリプトがブロックされます。

- Kaspersky Endpoint Security でサポートされていないインタープリターから開始されるスクリプトは管理されません。

Kaspersky Endpoint Security は、以下のインタープリターをサポートします：

- Java
- PowerShell

以下の種別のインタープリターがサポートされます：


- %ComSpec%
- %SystemRoot%\system32\regedit.exe
- %SystemRoot%\regedit.exe
- %SystemRoot%\system32\regedt32.exe
- %SystemRoot%\system32\cscript.exe
- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe

- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

## アプリケーションコントロールの有効化と無効化

既定では、アプリケーションコントロールは無効になっています。


アプリケーションコントロールを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アプリケーションコントロール]** の順に選択します。
3. **[アプリケーションコントロール]** を使用して機能を有効または無効にします。
4. 変更内容を保存します。

アプリケーションコントロールが有効になると、本製品は動作中の実行ファイルの情報を Kaspersky Security Center に渡します。動作中の実行ファイルのリストは Kaspersky Security Center の **[実行ファイル]** フォルダで表示できます。動作中の実行ファイルのみのリストの代わりにすべての実行ファイルの情報を受け取るには、[インベントリタスク](#)を実行します。

## アプリケーションコントロールモードの選択

アプリケーションコントロールモードを選択するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アプリケーションコントロール]** の順に選択します。
3. **[アプリケーション起動コントロールモード]** ブロックで、以下のオプションのいずれかを選択します：
  - **拒否リスト** このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールの条件を満たす場合は除きます。
  - **許可リスト** このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールの条件を満たす場合は除きます。

【**ゴールデンイメージ**】ルールおよび【**信頼するアップデーター**】ルールは許可リストモードの初期設定です。アプリケーションコントロールはKL カテゴリに対応しています。「ゴールデンイメージ」KL カテゴリには、オペレーティングシステムの通常の動作を可能にするプログラムが含まれます。「信頼するアップデーター」KL カテゴリには、最も信頼できるソフトウェア開発元のアップデーターが含まれます。また、これらのルールは削除できません。これらのルールの設定は編集できません。既定では、【**ゴールデンイメージ**】ルールが有効で、【**信頼するアップデーター**】ルールは無効です。これらのルールを適用する条件に一致するアプリケーションは、すべてのユーザーが起動できます。

モードを選択した状態で作成したルールは、モードを変更しても保存され、再度使用できます。これらのルールの使用を元に戻すには、必要なモードを選択するのみです。

4. 【**ブロックされたアプリケーションの開始時の操作**】で、アプリケーションコントロールルールによってブロックされているアプリケーションを起動しようとする操作があった場合に実行する処理を選択します。
5. ユーザーがアプリケーションを起動するときに DLL モジュールの読み込みを監視するには、【**DLL モジュールの読み込みを管理(システムの負荷が大きくなります)**】をオンにします。

モジュールの情報およびモジュールを読み込んだアプリケーションの情報が、レポートに記録されます。

Kaspersky Endpoint Security は、【**DLL とドライバーを管理**】をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを監視するには、チェックボックスをオンにした後でコンピューターを再起動します。

どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、【**アプリケーションコントロール**】で、既定の【**ゴールデンイメージ**】ルールまたは「信頼する証明書」KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。【**ゴールデンイメージ**】ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。

アプリケーションの設定の編集に対する【**パスワードによる保護**】をオンにすることを推奨します。これにより、Kaspersky Security Center のポリシー設定を変更しなくても、重要な DLL モジュールとドライバーの起動をブロックしてしまっているルールをオフにできます。

6. 変更内容を保存します。

## 製品インターフェイスでのアプリケーションコントロールルールの操作

Kaspersky Endpoint Security は、ルールを使用してアプリケーションの起動をコントロールします。アプリケーションコントロールルールは、ルールを適用する条件と、ルールが適用されたときアプリケーションコントロールが実行する処理を指定します（ユーザーによってアプリケーションの起動を許可またはブロックします）。

### ルールを適用する条件

ルールを適用する条件には次の相互関係があります：「条件種別 - 条件判定基準 - 条検値」ルールを適用する条件に基づいて、Kaspersky Endpoint Security はルールをアプリケーションに適用します（あるいは適用しません）。

次の条件の種別がルール内で使用されます：

- 対象条件：アプリケーションが対象条件のうち1つ以上を満たす場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用します。
- 除外条件：アプリケーションが除外条件のうち1つ以上を満たしている一方で、どの対象条件も満たさない場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用しません。

ルールを適用する条件は、基準を使用して作成されます。Kaspersky Endpoint Security では、次の基準を使用してルールが作成されます：

- アプリケーションの実行ファイルが含まれているフォルダーのパス、またはアプリケーションの実行ファイルのパス。
- メタデータ：アプリケーションの実行ファイル名、アプリケーションの実行ファイルバージョン、アプリケーション名、アプリケーションのバージョン、アプリケーションの開発元。
- アプリケーションの実行ファイルのハッシュ。
- 証明書の発行元、発行先、ハッシュ値。
- アプリケーションが KL カテゴリに属しているかどうか。
- リムーバブルドライブ上のアプリケーション実行ファイルの場所。

条件で使用される基準のそれぞれに対して基準値を指定する必要があります。起動されるアプリケーションのパラメータが対象条件で指定されている基準値を満たす場合、ルールが適用されます。この場合、アプリケーションコントロールは、ルールで指定された処理を実行します。アプリケーションパラメータが除外条件で指定されている基準値を満たす場合、アプリケーションコントロールはアプリケーションの起動をコントロールしません。

ルールを適用する条件として証明書を選択した場合、その証明書が信頼するシステムの保管領域に追加されていることを確認し、[製品内の信頼するシステム保管領域の使用設定](#)を確認してください。

## ルールが適用されたときのアプリケーションコントロールの処理

ルールが適用されると、アプリケーションコントロールはそのルールに従って、ユーザーまたはユーザーグループに対してアプリケーションの起動を許可またはブロックします。ルールが適用されるアプリケーションの起動を許可または許可しないユーザーまたはユーザーグループを選択できます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されるユーザーを指定しないルールを、「ブロック」ルールと呼びます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されないユーザーを指定しないルールを、「許可」ルールと呼びます。

ブロックルールの優先度は、許可ルールの優先度よりも高くなります。たとえば、アプリケーションコントロールの許可ルールがユーザーグループに割り当てられていて、アプリケーションコントロールのブロックルールがそのユーザーグループの1人のユーザーに割り当てられている場合、そのユーザーはアプリケーションを起動できません。


## ルールの動作ステータス

アプリケーションコントロールルールの動作ステータスは、次のいずれかです：

- **有効**：このステータスは、アプリケーションコントロールが実施されているときにルールが使用されることを示します。
- **無効**：このステータスは、アプリケーションコントロールが実施されているときにルールが無視されることを示します。
- **テスト**：このステータスは、ルールが適用されるアプリケーションの起動は許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを示します。

## アプリケーションコントロールルールを追加する

アプリケーションコントロールルールを追加するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【セキュリティコントロール】** → **【アプリケーションコントロール】** の順に選択します。
3. **【ブロック対象のアプリケーション】** または **【許可するアプリケーション】** ボタンをクリックします。アプリケーションコントロールルールのリストのテーブルが開きます。
4. **【追加】** をクリックします。**【アプリケーションコントロールルール】** ウィンドウが表示されます。
5. **【全般設定】** タブでルールの主要な設定を定義します。
  - a. **【ルール名】** にルール名を入力します。
  - b. **【説明】** に、ルールの説明を入力します。
  - c. ルールの適用条件を満たすアプリケーションの起動を許可または拒否するユーザーまたはユーザーグループのリストを作成または編集します。そのためには、**【オブジェクトとその権限】** テーブルで **【追加】** をクリックします。

既定では、ユーザーのリストに「**すべてのユーザー**」が追加されています。このルールは、すべてのユーザーに適用されます。

テーブルでユーザーが指定されていない場合、ルールは保存できません。

- d. **【オブジェクトとその権限】** テーブルで、トグルスイッチを使用してユーザーがアプリケーションを開始する権限を定義します。
- e. **【オブジェクト】** 列に表示されておらず、**【オブジェクト】** 列で指定されているユーザーグループに属していないすべてのユーザーに対して、ルールを適用する条件を満たすアプリケーションの起動をブロックする場合、**【他のユーザーを拒否】** をオンにします。



「他のユーザーを拒否」をオフにすると、「オブジェクトとその権限」テーブルで指定されておらず「オブジェクトとその権限」テーブルで指定されたユーザーグループに属していないユーザーによるアプリケーションの起動は、管理されません。

f. ルールを適用する条件を満たすアプリケーションを信頼するアップデーターとみなし、そのアプリケーションが作成する別の実行ファイルの実行を許可するには、「信頼するアップデーター」をオンにします。

6. 「条件」タブで、ルールをトリガする対象条件のリストを作成または編集します。

7. 「例外」タブで、ルールをトリガする例外条件のリストを作成または編集します。

Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。

8. 変更内容を保存します。

## アプリケーションコントロールルールの適用条件の追加

アプリケーションコントロールルールの新しい適用条件を追加するには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、「セキュリティコントロール」→「アプリケーションコントロール」の順に選択します。

3. 「ブロック対象のアプリケーション」または「許可するアプリケーション」ボタンをクリックします。  
アプリケーションコントロールルールのリストのテーブルが開きます。

4. 適用する基準を設定するルールを選択します。

アプリケーションコントロールルールのプロパティが表示されます。

5. 「条件」タブまたは「除外」タブを選択し、「追加」をクリックします。

6. アプリケーションコントロールルールの適用条件を選択します。

- **起動したことがあるアプリケーションのプロパティによる条件設定**：実行中のアプリケーションのリストで、アプリケーションコントロールルールが適用されるアプリケーションを選択することができます。コンピューター上で以前実行されたアプリケーションのリストも表示されます。1つまたは複数のルールを適用する条件の作成に使用する次の条件を選択します：**ファイルのハッシュ**、**証明書**、**KL カテゴリ**、**メタデータ**または**フォルダーのパス**。

- **「KL カテゴリ」による条件設定**：KL カテゴリとは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe® Acrobat® などが含まれます。

- **カスタム条件設定**：アプリケーションのファイルを選択し、ルールを適用する条件を選択できます：**ファイルのハッシュ**、**証明書**、**メタデータ**または**フォルダーのパス**。

- **ドライブによる条件設定（リムーバブルドライブ）**：アプリケーションコントロールルールはリムーバブルドライブ上で実行されているファイルにのみ適用されます。

- **指定されたフォルダー内のファイルのプロパティによる条件設定**：アプリケーションコントロールルールは特定のフォルダーのファイルにのみ適用されます。サブフォルダーのファイルを含めたり除外することもできます。1つまたは複数のルールを適用する条件の作成に使用する次の条件を選択します：**ファイルのハッシュ、証明書、KL カテゴリ、メタデータ**または**フォルダーのパス**。


7. 変更内容を保存します。

条件を追加する際には、アプリケーションコントロールの次の事項に留意してください：

- Kaspersky Endpoint Security は、MD5 ファイルハッシュ値をサポートせず、MD5 ハッシュに基づいたアプリケーションの起動のコントロールを実行しません。ルールを適用する条件には SHA256 ハッシュが使用されます。
- ルールを適用する条件として **[発行元]** と **[発行先]** のみを使用することは避けてください。これらの条件は信頼されません。
- **[ファイルまたはフォルダーのパス]** でシンボリックリンクを使用している場合、アプリケーションコントロールルールが正しく動作するために、シンボリックリンクを解決してください。これを行うには、**[シンボリックリンクを解決する]** をクリックします。

## アプリケーションコントロールルールのステータスの変更

アプリケーションコントロールルールのステータスを変更するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アプリケーションコントロール]** の順に選択します。
3. **[ブロック対象のアプリケーション]** または **[許可するアプリケーション]** ボタンをクリックします。アプリケーションコントロールルールのリストのテーブルが開きます。
4. **[ステータス]** 列でコンテキストメニューを表示し、以下のいずれかを選択します：
  - **有効**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
  - **無効**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
  - **テスト**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。
5. 変更内容を保存します。

## Kaspersky Security Center でのアプリケーションコントロールルールの管理

Kaspersky Endpoint Security は、ルールを使用してアプリケーションの起動をコントロールします。アプリケーションコントロールルールは、ルールを適用する条件と、ルールが適用されたときアプリケーションコントロールが実行する処理を指定します（ユーザーによってアプリケーションの起動を許可またはブロックします）。

## ルールを適用する条件

ルールを適用する条件には次の相互関係があります：「条件種別 - 条件判定基準 - 条検値」ルールを適用する条件に基づいて、Kaspersky Endpoint Security はルールをアプリケーションに適用します（あるいは適用しません）。

次の条件の種別がルール内で使用されます：

- 対象条件：アプリケーションが対象条件のうち1つ以上を満たす場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用します。
- 除外条件：アプリケーションが除外条件のうち1つ以上を満たしている一方で、どの対象条件も満たさない場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用しません。

ルールを適用する条件は、基準を使用して作成されます。Kaspersky Endpoint Security では、次の基準を使用してルールが作成されます：

- アプリケーションの実行ファイルが含まれているフォルダーのパス、またはアプリケーションの実行ファイルのパス。
- メタデータ：アプリケーションの実行ファイル名、アプリケーションの実行ファイルバージョン、アプリケーション名、アプリケーションのバージョン、アプリケーションの開発元。
- アプリケーションの実行ファイルのハッシュ。
- 証明書の発行元、発行先、ハッシュ値。
- アプリケーションが KL カテゴリに属しているかどうか。
- リムーバブルドライブ上のアプリケーション実行ファイルの場所。

条件で使用される基準のそれぞれに対して基準値を指定する必要があります。起動されるアプリケーションのパラメータが対象条件で指定されている基準値を満たす場合、ルールが適用されます。この場合、アプリケーションコントロールは、ルールで指定された処理を実行します。アプリケーションパラメータが除外条件で指定されている基準値を満たす場合、アプリケーションコントロールはアプリケーションの起動をコントロールしません。

ルールを適用する条件として証明書を選択した場合、その証明書が信頼するシステムの保管領域に追加されていることを確認し、[製品内の信頼するシステム保管領域の使用設定](#)を確認してください。

## ルールが適用されたときのアプリケーションコントロールの処理

ルールが適用されると、アプリケーションコントロールはそのルールに従って、ユーザーまたはユーザーグループに対してアプリケーションの起動を許可またはブロックします。ルールが適用されるアプリケーションの起動を許可または許可しないユーザーまたはユーザーグループを選択できます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されるユーザーを指定しないルールを、「ブロック」ルールと呼びます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されないユーザーを指定しないルールを、「許可」ルールと呼びます。

ブロックルールの優先度は、許可ルールの優先度よりも高くなります。たとえば、アプリケーションコントロールの許可ルールがユーザーグループに割り当てられていて、アプリケーションコントロールのブロックルールがそのユーザーグループの1人のユーザーに割り当てられている場合、そのユーザーはアプリケーションを起動できません。

## ルールの動作ステータス

アプリケーションコントロールルールの動作ステータスは、次のいずれかです：

- **有効**：このステータスは、アプリケーションコントロールが実施されているときにルールが使用されることを示します。
- **無効**：このステータスは、アプリケーションコントロールが実施されているときにルールが無視されることを示します。

**テスト**：このステータスは、ルールが適用されるアプリケーションの起動は許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを示します。

## クライアン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についての情報の取得

最適なアプリケーション起動コントロールを作成するには、まず、企業のローカルエリアネットワークにあるコンピューターで使用されているアプリケーションを把握します。次の情報を取得できます：

- 企業のLANで使用されているアプリケーションの開発元、バージョン、およびローカライズ
- アプリケーションアップデートの頻度
- 企業で採用しているアプリケーション使用ポリシー（セキュリティポリシーまたは管理ポリシー）
- アプリケーション配布パッケージの保管場所

企業のLANで使用されているアプリケーションに関する情報は[\[アプリケーションレジストリ\]](#) フォルダと[\[実行ファイル\]](#) フォルダにあります。[\[アプリケーションレジストリ\]](#) フォルダと[\[実行ファイル\]](#) フォルダは、Kaspersky Security Center コンソールツリーの[\[アプリケーションの管理\]](#) フォルダにあります。

フォルダ [\[アプリケーションレジストリ\]](#) は、クライアントコンピューターにインストールされている[ネットワークエージェント](#)が検出したアプリケーションのリストを含みます。

[\[実行ファイル\]](#) フォルダには、クライアントコンピューター上で起動されたことのある実行ファイルおよび Kaspersky Endpoint Security のインベントリタスクの実行中に検出されたすべての実行ファイルのリストが含まれます。

アプリケーションやその実行ファイル、またアプリケーションがインストールされたコンピューターのリストに関する概要情報を見るには、[\[アプリケーションレジストリ\]](#) フォルダまたは [\[実行ファイル\]](#) フォルダで選択されたアプリケーションのプロパティウィンドウを開いてください。

[\[アプリケーションレジストリ\]](#) フォルダでアプリケーションのプロパティウィンドウを開くには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、[詳細] → [アプリケーションの管理] → [アプリケーションレジストリ] を選択します。
3. アプリケーションを選択します。
4. アプリケーションのコンテキストメニューから [プロパティ] を選択します。

[実行ファイル] フォルダーにある実行ファイルのプロパティウィンドウを開くには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、[詳細] → [アプリケーションの管理] → [実行ファイル] フォルダーの順に選択します。
3. 実行ファイルを選択します。
4. 実行ファイルのコンテキストメニューから [プロパティ] を選択します。

## アプリケーションカテゴリの作成

アプリケーションコントロールルールの作成を容易にするため、アプリケーションカテゴリを作成できます。

会社で使用されている標準セットのアプリケーションを網羅する「作業アプリケーション」カテゴリを作成すると有用です。さまざまなユーザーグループが仕事で異なるアプリケーションセットを使用している場合は、ユーザーグループごとに別個のアプリケーションカテゴリを作成できます。

アプリケーションカテゴリを作成するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、[詳細] → [アプリケーションの管理] → [アプリケーションカテゴリ] フォルダーの順に選択します。
3. 作業領域で [新規カテゴリ] をクリックします。  
ユーザーカテゴリの作成ウィザードが表示されます。
4. ユーザーカテゴリの作成ウィザードの指示に従います。

### ステップ 1: カテゴリ種別の選択

この手順では、次のいずれかのアプリケーションカテゴリ種別を選択します：

- **手動でコンテンツが追加されるカテゴリ**：このカテゴリ種別を選択した場合、「アプリケーションをカテゴリに含める条件の設定」および「アプリケーションをカテゴリから除外する条件の設定」ステップで、カテゴリに実行ファイルを含めるための条件を設定できます。
- **選択したデバイスの実行ファイルを含むカテゴリ**：このカテゴリ種別を選択した場合、「設定」ステップで、カテゴリに自動で追加する実行ファイルのコンピューターを指定できます。

- **特定のフォルダーの実行ファイルを含むカテゴリ**：このカテゴリ種別を選択した場合、「リポジトリフォルダー」ステップで、カテゴリに自動で追加する実行ファイルのフォルダーを指定できます。

自動でコンテンツが追加されるカテゴリを作成すると、Kaspersky Security Center によって、以下の形式のファイルに対してインベントリが実行されます：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX、SCR。

## ステップ 2：ユーザーカテゴリ名の入力

この手順では、アプリケーションカテゴリの名前を指定します。

## ステップ 3：アプリケーションをカテゴリに含める条件の設定

この手順は、**【手動でコンテンツを追加するカテゴリ】** カテゴリ種別を選択した場合に使用できます。

この手順の **【追加】** ドロップダウンリストで、アプリケーションをカテゴリに含める条件を選択します。

- **実行ファイルのリストから**：クライアントデバイス上の実行ファイルのリストからカスタムカテゴリへアプリケーションを追加します。
- **ファイルのプロパティ**：アプリケーションをカスタムカテゴリに追加する条件として、実行ファイルの詳細なデータを指定します。
- **フォルダーのファイルのメタデータ**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダーに含まれるファイルのチェックサム**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダー内のファイルの証明書**：証明書で署名された実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルの証明書が、アプリケーションをカスタムカテゴリに追加する条件として示されます。

プロパティで **【証明書のハッシュ値】** パラメータが指定されていない条件の使用は推奨されません。

- **MSI インストーラーファイルのメタデータ**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーに含まれるファイルのチェックサム**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **KL カテゴリから選択**：アプリケーションをカスタムカテゴリに追加する条件として KL カテゴリを指定します。KL カテゴリとは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。  
すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。



- **アプリケーションへのパスを指定する**：クライアントデバイス上のフォルダーを選択します。Kaspersky Security Center により、そのフォルダーにある実行ファイルがカスタムカテゴリに追加されます。
- **リポジトリから証明書を選択**：カスタムカテゴリにアプリケーションを追加するための条件として、実行可能ファイルの署名に使用された証明書を選択します。

プロパティで [証明書のハッシュ値] パラメータが指定されていない条件の使用は推奨されません。

- **ドライブ種別**：アプリケーションをカスタムカテゴリに追加する条件として、ストレージデバイスの種別（すべてのハードディスクとリムーバブルドライブ、またはリムーバブルドライブのみ）を選択します。

## ステップ 4：アプリケーションをカテゴリから除外する条件の設定

この手順は、[手動でコンテンツを追加するカテゴリ] カテゴリ種別を選択した場合に使用できます。

この手順で指定したアプリケーションは、「アプリケーションをカテゴリに含める条件の設定」ステップで指定されていても、カテゴリから除外されます。

この手順の [追加] ドロップダウンリストで、アプリケーションをカテゴリから除外する条件を選択します。

- **実行ファイルのリストから**：クライアントデバイス上の実行ファイルのリストからカスタムカテゴリへアプリケーションを追加します。
- **ファイルのプロパティ**：アプリケーションをカスタムカテゴリに追加する条件として、実行ファイルの詳細なデータを指定します。
- **フォルダーのファイルのメタデータ**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダーに含まれるファイルのチェックサム**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダー内のファイルの証明書**：証明書で署名された実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルの証明書が、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーファイルのメタデータ**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーに含まれるファイルのチェックサム**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **KL カテゴリから選択**：アプリケーションをカスタムカテゴリに追加する条件として KL カテゴリを指定します。KL カテゴリとは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。  
すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。



- **アプリケーションへのパスを指定する**：クライアントデバイス上のフォルダーを選択します。Kaspersky Security Center により、そのフォルダーにある実行ファイルがカスタムカテゴリに追加されます。
- **リポジトリから証明書を選択**：カスタムカテゴリにアプリケーションを追加するための条件として、実行可能ファイルの署名に使用された証明書を選択します。
- **ドライブ種別**：アプリケーションをカスタムカテゴリに追加する条件として、ストレージデバイスの種別（すべてのハードディスクとリムーバブルドライブ、またはリムーバブルドライブのみ）を選択します。

## ステップ 5：設定

この手順は、**【選択したデバイスの実行ファイルを含むカテゴリ】** カテゴリ種別を選択した場合に使用できます。

この手順では、**【追加】** をクリックしてコンピューターを指定します。そのコンピューターにある実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。**【実行ファイル】** フォルダーに表示される、指定されたコンピューターのすべての実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。

この手順では、以下の設定も指定できます：

- Kaspersky Security Center によるハッシュ関数計算のアルゴリズム。アルゴリズムを選択するには、以下のチェックボックスを1つ以上オンにします：
  - **このカテゴリのファイルの SHA-256 の値を計算する**（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）
  - **このカテゴリのファイルの MD5 の値を計算する**（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）
- **データを管理サーバーのリポジトリと同期**：Kaspersky Security Center によって、定期的にアプリケーションカテゴリを空にした後、**【実行ファイル】** フォルダーに表示される、指定されたコンピューターのすべての実行ファイルをアプリケーションカテゴリに追加する場合、このチェックボックスをオンにします。  
**【データを管理サーバーのリポジトリと同期】** がオフの場合、アプリケーションカテゴリの作成後、Kaspersky Security Center はカテゴリへの変更を行いません。
- **スキャン期間（時間）**：このフィールドで、Kaspersky Security Center がアプリケーションカテゴリを空にして、**【実行ファイル】** フォルダーに表示される、指定されたコンピューターのすべての実行ファイルをアプリケーションカテゴリに追加する間隔（時間）を指定できます。  
 このフィールドは、**【データを管理サーバーのリポジトリと同期】** をオンにした場合に使用できます。

## ステップ 6：【リポジトリ】フォルダー

この手順は、**【特定のフォルダーの実行ファイルを含むカテゴリ】** カテゴリ種別を選択した場合に使用できます。

この手順では、**【参照】** をクリックしてフォルダーを指定すると、Kaspersky Security Center によってそのフォルダー内の実行ファイルが検索され、アプリケーションがアプリケーションカテゴリに自動的に追加されます。

この手順では、以下の設定も指定できます：

- **ダイナミックリンクライブラリ (DLL) をこのカテゴリに含める** : ダイナミックリンクライブラリ (DLL ファイル) をアプリケーションカテゴリに含める場合は、このチェックボックスをオンにします。

DLL ファイルをアプリケーションカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

- **このカテゴリ内のスクリプトデータを含める** : アプリケーションカテゴリにスクリプトを含める場合は、このチェックボックスをオンにします。

スクリプトをアプリケーションカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

- Kaspersky Security Center によるハッシュ関数計算のアルゴリズム。アルゴリズムを選択するには、以下のチェックボックスを1つ以上オンにします :

- **このカテゴリのファイルの SHA-256 の値を計算する** (Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート)
- **このカテゴリのファイルの MD5 の値を計算する** (Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート)

- **変更のあったフォルダーを強制スキャンする** : アプリケーションカテゴリへの自動追加に使用されたフォルダーに対して、Kaspersky Security Center によって定期的に行われる実行ファイルを検索する場合、このチェックボックスをオンにします。

「**変更のあったフォルダーを強制スキャンする**」がオフの場合、Kaspersky Security Center は、アプリケーションカテゴリへの自動追加に使用されたフォルダーでファイルの追加または削除があった場合のみ、そのフォルダー内の実行ファイルを検索します。

- **スキャン期間 (時間)** : このフィールドで、アプリケーションカテゴリへの自動追加に使用されるフォルダー内の実行ファイルを検索する Kaspersky Security Center が検索する間隔 (時間) を指定できます。

このフィールドは、「**変更のあったフォルダーを強制スキャンする**」がオンの場合に使用できます。

## ステップ 7 : カスタムカテゴリの作成

セットアップウィザードを終了するには、「**終了**」をクリックします。

## 実行ファイルフォルダーからアプリケーションカテゴリへの実行ファイルの追加

「**実行ファイル**」フォルダーに、コンピューター上で検出された実行ファイルが表示されます。Kaspersky Endpoint Security ではインベントリタスクの実行後に実行ファイルのリストが生成されます。

「**実行ファイル**」フォルダーからアプリケーションカテゴリに実行ファイルを追加するには :

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、「**詳細**」 → 「**アプリケーションの管理**」 → 「**実行ファイル**」フォルダーの順に選択します。
3. 作業領域で、アプリケーションカテゴリに追加する実行ファイルを選択します。

4. 選択した実行ファイルを右クリックしてコンテキストメニューを開き、**【カテゴリに追加】**を選択します。
5. 表示されたウィンドウで、次のいずれかの手順を実行します：
  - ウィンドウの上部で、次のいずれかのオプションを選択します：
    - **新規アプリケーションカテゴリへ追加**：新しいアプリケーションカテゴリを作成して実行ファイルを追加する場合、このオプションを選択します。
    - **アプリケーションカテゴリへ追加**：既存のアプリケーションカテゴリを選択して実行ファイルを追加する場合、このオプションを選択します。
  - **【ルール種別】** セクションで、次のいずれかを選択します：
    - **除外しない場合のルール**：実行ファイルをアプリケーションカテゴリに追加する条件を作成する場合、このオプションを選択します。
    - **除外に追加する場合のルール**：実行ファイルをアプリケーションカテゴリから除外する条件を作成する場合、このオプションを選択します。
  - **【条件として使用する情報】** ブロックで、以下のオプションのいずれかを選択します：
    - **証明書の詳細情報（証明書がないファイルの場合 SHA-256 ハッシュ）**
    - **証明書の詳細情報（証明書のないファイルはスキップ）**
    - **SHA-256 のみ（ハッシュのないファイルはスキップ）**
    - **MD5（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**
6. **【OK】** をクリックします。

## イベントに関連した実行ファイルのアプリケーションカテゴリへの追加

アプリケーションコントロールによるイベントに関連する実行ファイルをアプリケーションカテゴリに追加するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **【管理サーバー】** フォルダーで、**【イベント】** タブを選択します。
3. **【イベントの抽出】** で、アプリケーションコントロールの動作に関連するイベントの抽出を選択します（[アプリケーションコントロールの動作によるイベントの表示](#)、[アプリケーションコントロールのテスト動作によるイベントの表示](#)）。
4. **【抽出を実行】** をクリックします。
5. 関連する実行ファイルをアプリケーションカテゴリに追加するイベントを選択します。
6. 選択したイベントを右クリックしてコンテキストメニューを開き、**【カテゴリに追加】** を選択します。
7. 表示されたウィンドウで、アプリケーションカテゴリの設定をします：

- ウィンドウの上部で、次のいずれかのオプションを選択します：
    - **新規アプリケーションカテゴリへ追加**：新しいアプリケーションカテゴリを作成して実行ファイルを追加する場合、このオプションを選択します。
    - **アプリケーションカテゴリへ追加**：既存のアプリケーションカテゴリを選択して実行ファイルを追加する場合、このオプションを選択します。
  - [ルール種別] セクションで、次のいずれかを選択します：
    - **除外しない場合のルール**：実行ファイルをアプリケーションカテゴリに追加する条件を作成する場合、このオプションを選択します。
    - **除外に追加する場合のルール**：実行ファイルをアプリケーションカテゴリから除外する条件を作成する場合、このオプションを選択します。
  - [条件として使用する情報] ブロックで、以下のオプションのいずれかを選択します：
    - **証明書の詳細情報（証明書がないファイルの場合 SHA-256 ハッシュ）**
    - **証明書の詳細情報（証明書のないファイルはスキップ）**
    - **SHA-256 のみ（ハッシュのないファイルはスキップ）**
    - **MD5（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**
8. [OK] をクリックします。

## Kaspersky Security Center を使用したアプリケーションコントロールルールの追加と変更

*Kaspersky Security Center* を使用してアプリケーションコントロールルールを追加および変更するには：

1. Kaspersky Security Center の管理コンソールを開きます。
  2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
  3. 作業領域で、[ポリシー] タブを選択します。
  4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
  5. ポリシーウィンドウで、[セキュリティコントロール] → [アプリケーションコントロール] の順に選択します。  
ウィンドウの右側に、アプリケーションコントロールの設定が表示されます。
  6. 次のいずれかの手順を実行します：
    - ルールを追加するには、[追加] をクリックします。
    - 既存のルールを編集するには、ルールをリストから選択し、[編集] をクリックします。
- [アプリケーションコントロールルール] ウィンドウが開きます。

7. 次のいずれかの手順を実行します：

- 新しいカテゴリを作成する場合：
  - a. **【カテゴリの作成】** をクリックします。  
ユーザーカテゴリの作成ウィザードが表示されます。
  - b. ユーザーカテゴリの作成ウィザードの指示に従います。
  - c. **【カテゴリ】** で、作成したアプリケーションカテゴリを選択します。
- 既存のカテゴリを編集する場合：
  - a. **【カテゴリ】** で、編集する既存のアプリケーションカテゴリを選択します。
  - b. **【プロパティ】** をクリックします。
  - c. 選択したアプリケーションカテゴリの設定を変更します。
  - d. **【OK】** をクリックします。
  - e. **【カテゴリ】** で、ルール作成のために作成したアプリケーションカテゴリを選択します。

8. **【オブジェクトとその権限】** テーブルで **【追加】** をクリックします。

9. **【ユーザーまたはグループの選択】** ウィンドウで、選択したカテゴリに属するアプリケーションの起動権限を設定する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。

10. **【オブジェクトとその権限】** テーブルで、以下を実行します：

- 選択したカテゴリに属するアプリケーションの起動をユーザーまたはユーザーグループに許可する場合、該当する行にある **【許可】** をオンにします。
- 選択したカテゴリに属するアプリケーションの起動をユーザーまたはユーザーグループに許可しない場合、該当する行にある **【拒否】** をオンにします。

11. **【オブジェクト】** 列に表示されておらず、**【オブジェクト】** 列で指定されているユーザーグループに属していないすべてのユーザーに対して、選択したカテゴリに属するアプリケーションの起動をブロックする場合、**【他のユーザーを拒否】** をオンにします。

12. 選択したアプリケーションカテゴリに含まれるアプリケーションを信頼するアップデーターとみなし、そのアプリケーションが作成する別の実行ファイルの実行を許可するには、**【信頼するアップデーター】** をオンにします。

Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。

13. 変更内容を保存します。

## Kaspersky Security Center を使用したアプリケーションコントロールルールのステータス変更

アプリケーションコントロールルールのステータスを変更するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[セキュリティコントロール] → [アプリケーションコントロール] の順に選択します。  
ウィンドウの右側に、アプリケーションコントロールの設定が表示されます。
6. [ステータス] 列をクリックしてコンテキストメニューを表示し、以下のいずれかを選択します：
  - **有効**：このステータスは、アプリケーションコントロールが実施されているときにルールが使用されることを示します。
  - **無効**：このステータスは、アプリケーションコントロールが実施されているときにルールが無視されることを示します。
  - **テスト**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

[処理] で [ルールを適用] が選択されている場合、一部のルールに対して **[ルールをテスト運用] と同等の処理** を割り当てるには、[テスト] ステータスを使用します。

7. 変更内容を保存します。

## アプリケーションコントロールルールのエクスポートおよびインポート

アプリケーションコントロールルールを XML ファイルにエクスポートすることができます。また、エクスポートまたはインポート機能を使用して、アプリケーションコントロールルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

アプリケーションコントロールルールをエクスポートまたはインポートする際、次の留意事項にご注意ください：

- Kaspersky Endpoint Security は、有効なアプリケーションコントロールモードのルールのリストのみをエクスポートします。言い換えると、アプリケーションコントロールが拒否リストモードで動作している場合、Kaspersky Endpoint Security はこのモードのルールのみをエクスポートします。許可リストモードのルールのリストをエクスポートするには、モードを変更してエクスポート操作を再度実行してください。
- Kaspersky Endpoint Security はアプリケーションコントロールルールが動作するためにアプリケーションカテゴリを使用します。アプリケーションコントロールルールのリストを別のサーバーに抗する場合、アプリケーションカテゴリのリストも移行する必要があります。アプリケーションカテゴリのエクスポートまたはインポートの詳細については、[Kaspersky Security Center のヘルプ](#) を参照してください。

**[管理コンソール \(MMC\) で信頼するアプリケーションコントロールルールのリストをエクスポートおよびインポートする方法](#)**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔セキュリティコントロール〕** → **〔アプリケーションコントロール〕** の順に選択します。
6. アプリケーションコントロールルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。  
ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
  - b. **〔エクスポート〕** をクリックします。
  - c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. **〔保存〕** をクリックします。  
Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
7. アプリケーションコントロールルールのリストをインポートするには：
  - a. **〔インポート〕** をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. **〔開く〕** をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

[Web コンソールおよび Cloud コンソールでアプリケーションコントロールルールのリストをエクスポートおよびインポートする方法](#) 



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ルールのリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[セキュリティコントロール]** → **[アプリケーションコントロール]** の順に選択します。
5. **[ルールリストの設定]** をクリックします。
6. ルールのリストを選択します：アプリケーションの拒否リストまたは許可リスト。
7. アプリケーションコントロールルールのリストをエクスポートするには：
  - a. エクスポートするルールを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択したルールのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。
  - d. **[エクスポート]** をクリックします。  
Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを XML ファイルでエクスポートします。
8. アプリケーションコントロールルールのリストをインポートするには：
  - a. **[インポート]** をクリックします。  
表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
  - b. **[開く]** をクリックします。  
コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
9. 変更内容を保存します。

## Kaspersky Security Center を使用したアプリケーションコントロールルールのテスト

アプリケーションコントロールルールが業務に必要なアプリケーションをブロックしないことを確認するため、新しくルールを作成したあとでテストを有効にして動作を検証してください。アプリケーションコントロールルールのテストを有効にすると、Kaspersky Endpoint Security は、アプリケーションコントロールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

アプリケーションコントロールルールの動作を検証するには、動作の結果として Kaspersky Security Center に報告されるアプリケーションコントロールのイベントを確認します。テストモードの結果、コンピューターのユーザーの業務に必要なすべてのアプリケーションについて起動ブロックイベントがなければ、適切なルールが作成されています。そうでない場合、作成したルールの設定の変更、追加のルールの作成、既存のルールの削除を行ってください。

既定では、Kaspersky Endpoint Security は、ルールで禁止されているアプリケーションを除くすべてのアプリケーションの起動を許可します。

Kaspersky Security Center でアプリケーションコントロールルールのテストを有効または無効にするには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[セキュリティコントロール] → [アプリケーションコントロール] の順に選択します。  
ウィンドウの右側に、アプリケーションコントロールの設定が表示されます。
6. [コントロールモード] ドロップダウンリストから、次のいずれかを選択します：
  - **拒否リスト** このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールの条件を満たす場合は除きます。
  - **許可リスト** このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールの条件を満たす場合は除きます。
7. 次のいずれかの手順を実行します：
  - アプリケーションコントロールルールのテストを有効にする場合、[処理] で [ルールをテスト運用] を選択します。
  - アプリケーションコントロールを有効にしてユーザーのコンピューター上のアプリケーションの起動を管理する場合は、[ルールを適用] を選択します。
8. 変更内容を保存します。

## アプリケーションコントロールのテスト動作によるイベントの表示

Kaspersky Security Center が受信した、アプリケーションコントロールのテストイベントを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理サーバー] フォルダーで、[イベント] タブを選択します。
3. [抽出の作成] をクリックします。

抽出のプロパティウィンドウが表示されます。

4. [イベント] セクションを開きます。
5. [すべてクリア] をクリックします。
6. [イベント] テーブルで [アプリケーションの起動がテストモードでブロックされています] と [アプリケーションの起動がテストモードで許可されています] をオンにします。
7. [OK] をクリックします。
8. [イベントの抽出] で、作成した抽出を選択します。
9. [抽出を実行] をクリックします。

## 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の表示

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. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理サーバー] フォルダーで、 [レポート] タブを選択します。
3. [新規レポートテンプレート] をクリックします。  
新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。 [レポートテンプレートの種別の選択] 手順で、 [その他] → [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] の順に選択します。  
新規レポートテンプレートウィザードが完了すると、 [レポート] タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

## アプリケーションコントロールの動作によるイベントの表示

Kaspersky Security Center が受信した、アプリケーションコントロールの動作によるイベントを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理サーバー] フォルダーで、 [イベント] タブを選択します。
3. [抽出の作成] をクリックします。  
抽出のプロパティウィンドウが表示されます。
4. [イベント] セクションを開きます。
5. [すべてクリア] をクリックします。

6. [イベント] テーブルで、[アプリケーションの起動が禁止されました] をオンにします。
7. [OK] をクリックします。
8. [イベントの抽出] で、作成した抽出を選択します。
9. [抽出を実行] をクリックします。

## ブロックされたアプリケーションに関するレポートの表示

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. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理サーバー] フォルダーで、[レポート] タブを選択します。
3. [新規レポートテンプレート] をクリックします。  
新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。[レポートテンプレートの種別の選択] 手順で、[その他] → [ブロック対象アプリケーションのレポート] の順に選択します。  
新規レポートテンプレートウィザードが完了すると、[レポート] タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。  
  
レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

## アプリケーションコントロールルールのテスト

アプリケーションコントロールルールが業務に必要なアプリケーションをブロックしないことを確認するため、新しくルールを作成したあとでテストを有効にして動作を検証してください。

アプリケーションコントロールルールの動作を検証するには、動作の結果として Kaspersky Security Center に報告されるアプリケーションコントロールのイベントを確認します。テストモードの結果、コンピューターのユーザーの業務に必要なすべてのアプリケーションについて起動ブロックイベントがなければ、適切なルールが作成されています。そうでない場合、作成したルールの設定の変更、追加のルールの作成、既存のルールの削除を行ってください。

アプリケーションコントロールルールのテストを有効にするか、アプリケーションコントロールのブロック処理を選択するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[セキュリティコントロール] → [アプリケーションコントロール] の順に選択します。  
アプリケーションコントロールルールのリストのテーブルが開きます。
3. [ステータス] 列で [テスト] をオンにします。  
このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

#### 4. 変更内容を保存します。

Kaspersky Endpoint Security は、アプリケーションコントロールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

## Application activity monitor

*Application Activity Monitor* is a tool designed for viewing information about the activity of applications on a user's computer in real time.

Using the Application Activity Monitor requires installing the Application Control and Host Intrusion Prevention components. If these components are not installed, the Application Activity Monitor section in the [main application window](#) is hidden.

*To start Application Activity Monitor:*

In the main application window, under **Monitoring**, click the **Application Activity Monitor** tile.

The **Application Activity** window opens. In this window, information about the activity of applications on the user's computer is presented on three tabs:

- The **All applications** tab displays information about all applications installed on the computer.
- The **Running** tab displays information about the computer resource consumption by each application in real time. From this tab, you can also proceed to configure permissions for an individual application.
- The **Run at startup** tab displays the list of applications that are started when the operating system starts.

If you want to hide application activity information on the user's computer, you can restrict user access to the Application Activity Monitor tool.

### [How to hide Application Activity Monitor in the application interface using the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **General settings** → **Interface**.
6. Use the **Hide Application Activity Monitor section** check box to grant or revoke access to the tool.
7. Save your changes.

### [How to hide Application Activity Monitor in the application interface using the Web Console and Cloud Console](#)

1. In the main window of Web Console, select **Devices** → **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.  
The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **General settings** → **Interface**.
5. Use the **Hide Application Activity Monitor section** check box to grant or revoke access to the tool.
6. Save your changes.

## Rules for creating name masks for files or folders

A *mask of a file or folder name* is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following common characters to create a file or folder name mask:


- The **\*** (asterisk) character, which takes the place of any set of characters (including an empty set). For example, the `C:\*.txt` mask will include all paths to files with the `.txt` extension located in folders and subfolders on the (C:) drive.
- The **?** (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the `TXT` extension and a name consisting of three characters.

## アプリケーションコントロールのメッセージテンプレートの編集

ユーザーがアプリケーションコントロールルールによってブロックされているアプリケーションを起動しようと試みると、Kaspersky Endpoint Security はアプリケーションの起動がブロックされていることを示すメッセージを表示します。アプリケーションの起動が誤ってブロックされていると思われる場合は、メッセージテキストのリンクを使用して、メッセージを LAN 管理者に送信できます。

アプリケーションの起動がブロックされたときに表示されるメッセージと管理者に送信するメッセージについては、専用テンプレートを利用できます。このメッセージテンプレートは変更することができます。

メッセージテンプレートを編集するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[セキュリティコントロール]** → **[アプリケーションコントロール]** の順に選択します。
3. **[テンプレート]** ブロックで、アプリケーションコントロールのメッセージのテンプレートを設定します：

- **ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。
- **管理者に送信するメッセージ**：アプリケーションが誤ってブロックされるとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの起動ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [**ユーザー要求**] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

4. 変更内容を保存します。

## 許可されるアプリケーションのリストの実装のベストプラクティス

許可されるアプリケーションのリストの実装を計画する場合、以下を実行してください：

1. 以下のグループを作成します：

- **ユーザーグループ**：各種アプリケーションの使用を許可するユーザーのグループ。
- **管理グループ**：Kaspersky Security Center によって許可されるアプリケーションのリストを割り当てるコンピューターのグループ。異なる許可リストの設定をグループに対して使用する場合は、複数のコンピューターのリストを作成する必要があります。

2. 起動を許可するアプリケーションのリストを作成します。

リストを作成する前に、以下を実行してください：

- インベントリタスクを実行します。  
インベントリタスクの作成、設定、開始に関する情報は、「タスクの管理」セクションにあります。
- [実行ファイルのリスト](#)を表示します。

## アプリケーションの許可リストモードの設定

許可リストモードを設定する際は、以下の操作を実行してください：

1. 起動を許可するアプリケーションを含む[アプリケーションカテゴリ](#)を作成します。

次のいずれかのアプリケーションカテゴリ作成方法を選択できます：

- **手動でコンテンツが追加されるカテゴリ**：このカテゴリには、以下の条件を使用して手動で追加できます：
  - **ファイルのメタデータ**：Kaspersky Security Center により、指定されたメタデータを伴うすべての実行ファイルがアプリケーションカテゴリに追加されます。
  - **ファイルのハッシュ値**。Kaspersky Security Center により、指定されたハッシュを持つすべての実行ファイルがアプリケーションカテゴリに追加されます。



異なるバージョンのファイルのハッシュは異なるため、この条件を使用すると、アップデートの自動インストールが使用できなくなります。

- ファイルの証明書：Kaspersky Security Center により、指定された証明書で署名されたすべての実行ファイルがアプリケーションカテゴリに追加されます。
- KL カテゴリ：Kaspersky Security Center により、指定された KL カテゴリにあるすべてのアプリケーションがアプリケーションカテゴリに追加されます。
- アプリケーションフォルダー：Kaspersky Security Center により、そのフォルダーにあるすべての実行ファイルがアプリケーションカテゴリに追加されます。

アプリケーションフォルダーの条件を使用すると、指定されたフォルダー内の任意のアプリケーションに対して起動が許可されるため、安全でない場合があります。アプリケーションフォルダーを条件としたアプリケーションカテゴリは、アップデートの自動インストールが許可されているユーザーに対して適用されるルールでのみ使用してください。

- **特定のフォルダーの実行ファイルを含むカテゴリ**：指定したフォルダーの実行ファイルを、作成されたアプリケーションカテゴリに自動的に割り当てるように設定できます。
- **選択したデバイスの実行ファイルを含むカテゴリ**：指定したコンピューターのすべての実行ファイルを、作成されたアプリケーションカテゴリに自動的に割り当てるように設定できます。

この方法でアプリケーションカテゴリを作成すると、Kaspersky Security Center は **実行ファイルフォルダー** からコンピューター上のアプリケーションに関する情報を受け取ります。

2. アプリケーションコントロールの **許可リストモード** を選択します。

3. 作成したアプリケーションカテゴリを使用して **アプリケーションコントロールルール** を作成します。

【**ゴールデンイメージ**】ルールおよび【**信頼するアップデーター**】ルールは許可リストモードの初期設定です。アプリケーションコントロールは KL カテゴリに対応しています。「ゴールデンイメージ」KL カテゴリには、オペレーティングシステムの通常の動作を可能にするプログラムが含まれます。「信頼するアップデーター」KL カテゴリには、最も信頼できるソフトウェア開発元のアップデーターが含まれます。また、これらのルールは削除できません。これらのルールの設定は編集できません。既定では、【**ゴールデンイメージ**】ルールが有効で、【**信頼するアップデーター**】ルールは無効です。これらのルールを適用する条件に一致するアプリケーションは、すべてのユーザーが起動できます。

4. アップデートの自動インストールを許可するアプリケーションを特定します。

次のいずれかの方法で、アップデートの自動インストールを許可できます：

- KL カテゴリに属するすべてのアプリケーションの起動を許可することで、許可するアプリケーションのリストを指定する。
- 証明書で署名されたすべてのアプリケーションの起動を許可することで、許可するアプリケーションのリストを指定する。

証明書で署名されたすべてのアプリケーションの起動を許可するには、証明書に基づく条件のカテゴリを作成し、【**発行先**】パラメータのみを使用して値を「\*」にします。

- アプリケーションコントロールルールで **【信頼するアップデーター】** をオンにする。このチェックボックスをオンにすると、ルールに含まれるアプリケーションが信頼するアップデーターとみなされます。ルールに含まれるアプリケーションによってインストールまたはアップデートされたアプリケーションの起動は、ブロックルールが適用されなければ許可されます。

Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。

- フォルダーを作成し、その中にアップデートの自動インストールを許可するアプリケーションの実行ファイルを置きます。続いて、**【アプリケーションフォルダー】** 条件を設定したアプリケーションカテゴリを作成し、フォルダーのパスを指定します。許可ルールを作成し、対象としてこのアプリケーションカテゴリを選択します。

アプリケーションフォルダーの条件を使用すると、指定されたフォルダー内の任意のアプリケーションに対して起動が許可されるため、安全でない場合があります。アプリケーションフォルダーを条件としたアプリケーションカテゴリは、アップデートの自動インストールが許可されているユーザーに対して適用されるルールでのみ使用してください。

## 許可リストモードのテスト

アプリケーションコントロールルールが業務に必要なアプリケーションをブロックしないことを確認するため、新しくルールを作成したあとでテストを有効にして動作を検証してください。テストを有効にすると、Kaspersky Endpoint Security は、アプリケーションコントロールルールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

許可リストモードをテストする場合、以下を実行してください：

1. テスト期間を決定します（数日間から2か月）。
2. [アプリケーションコントロールルールのテスト](#) を有効にします。
3. [アプリケーションコントロールの動作テストによるイベントと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](#) を検証することにより、テスト結果を分析します。
4. 分析の結果に基づいて、許可リストモードの設定を変更します。  
特に、テスト結果に基づいて、[イベントに関連する実行ファイルをアプリケーションカテゴリに追加](#) できます。

## 許可リストモードのサポート

[アプリケーションコントロールのブロック処理を選択](#) した後、以下を実行して許可リストモードのサポートを継続してください：

- [アプリケーションコントロールの動作によるイベントと実行ブロックのレポート](#) を検証することにより、アプリケーションコントロールの有効性を分析します。
- アプリケーションへのアクセスを求めるユーザーからのリクエストを分析します。

- 見慣れない実行ファイルについて、[Kaspersky Security Network](#)で評価を確認して分析します。
- オペレーティングシステムやソフトウェアのアップデートをインストールする前に、アップデートをテストグループのコンピューターにインストールして、アプリケーションコントロールルールでの処理を確認します。
- アプリケーションコントロールルールで使用されているカテゴリに、必要なアプリケーションを追加します。


## ネットワークポートの監視

Kaspersky Endpoint Security の動作中、[ウェブコントロール](#)、[メール脅威対策](#)、[ウェブ脅威対策](#)は、特定のプロトコルで送信される、もしくはコンピューターの開いている TCP および UDP ポートを通過するデータストリームを監視します。たとえば、メール脅威対策は SMTP を使用して送信される情報を分析し、ウェブ脅威対策は HTTP または FTP を使用して送信される情報を分析します。

Kaspersky Endpoint Security は、ユーザーのコンピューターの TCP ポートと UDP ポートを、侵害される可能性に応じていくつかのグループに分割します。一部のネットワークポートは、脆弱なサービスのために予約されています。これらのポートはネットワーク攻撃の標的となる可能性が大きいため、より重点的に監視してください。非標準ネットワークポートに依存する非標準サービスを使用する場合も、これらのネットワークポートが攻撃側のコンピューターの標的になる可能性があります。ネットワークポートのリスト、およびネットワークアクセスを要求するアプリケーションのリストを指定できます。こうすると、メール脅威対策とウェブ脅威対策がネットワークトラフィックを監視する際に、これらのポートとアプリケーションに特別な注意がはられます。


## すべてのネットワークポートの監視の有効化

すべてのネットワークポートの監視を有効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[ネットワーク設定]** の順に選択します。
3. **[監視対象のポート]** セクションで、**[すべてのネットワークポートを監視する]** を選択します。
4. 変更内容を保存します。

## 監視対象ネットワークポートのリストの作成

監視するネットワークポートのリストを作成するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[ネットワーク設定]** の順に選択します。
3. **[監視対象のポート]** セクションで、**[選択されたネットワークポートのみを監視する]** を選択します。
4. **[選択]** をクリックします。

メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。

5. **[ステータス]** 列のトグルスイッチを使用してネットワークポートの監視を有効または無効にします。
6. 目的のネットワークポートがリストに表示されていない場合は、次の手順を実行してそのポートを追加します：
  - a. **[追加]** をクリックします。
  - b. 表示されたウィンドウで、ネットワークポート番号と短い説明を入力します。
  - c. ネットワークポートの **[有効]** または **[無効]** を設定します。
7. 変更内容を保存します。


FTP プロトコルがパッシブモードで動作している場合、監視対象のネットワークポートのリストに追加されていないランダムネットワークポートを経由して接続を確立することもできます。接続を保護するには、[すべてのネットワークポートの監視を有効化](#)するか、[FTP 接続を確立するアプリケーションのネットワークポートの制御を設定](#)します。

## すべてのネットワークポートを監視するアプリケーションのリストの作成

Kaspersky Endpoint Security がすべてのネットワークポートを監視するアプリケーションのリストを作成できます。

Kaspersky Endpoint Security がすべてのネットワークポートを監視するアプリケーションのリストに、FTP プロトコル経由でデータを受信または送信するアプリケーションを含めるようにしてください。

すべてのネットワークポートを監視するアプリケーションのリストを作成するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[ネットワーク設定]** の順に選択します。
3. **[監視対象のポート]** セクションで、**[選択されたネットワークポートのみを監視する]** を選択します。
4. **[カスペルスキーが推奨するリストに含まれるアプリケーションのすべてのポートを監視する]** チェックボックスをオンにします。

このチェックボックスをオンにすると、Kaspersky Endpoint Security は次のアプリケーションのポートすべてを監視します：

- Adobe Reader
- Apple Application Support
- Google Chrome
- Microsoft Edge

- Mozilla Firefox
  - Internet Explorer
  - Java
  - mIRC
  - Opera
  - Pidgin
  - Safari
  - Mail.ru Agent
  - Yandex Browser
5. **[選択したアプリケーションのすべてのポートを監視する]** をオンにします。
  6. **[選択]** をクリックします。  
Kaspersky Endpoint Security がネットワークポートを監視するアプリケーションのリストが開きます。
  7. **[ステータス]** 列のトグルスイッチを使用してネットワークポートの監視を有効または無効にします。
  8. アプリケーションがリストに含まれていない場合は、次の手順に従って追加します：
    - a. **[追加]** をクリックします。
    - b. 表示されたウィンドウで、アプリケーションの実行ファイルへのパスおよび短い説明を入力します。
    - c. ネットワークポートの **[有効]** または **[無効]** を設定します。
  9. 変更内容を保存します。

## 監視対象のポートのリストのエクスポートまたはインポート

Kaspersky Endpoint Security は次のリストを使用してネットワークポートを監視します：ネットワークポートのリストおよび Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリスト。監視対象のポートのリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ説明を持つ多数のポートをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、監視対象のポートのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

**[管理コンソール \(MMC\) で監視対象のポートのリストをエクスポートおよびインポートする方法](#)** 

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [全般設定] → [ネットワークの設定] の順に選択します。
6. [監視対象のポート] セクションで、 [選択されたネットワークポートのみを監視する] を選択します。
7. [設定] をクリックします。

[ネットワークポート] ウィンドウが開きます。 [ネットワークポート] ウィンドウに、メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。
8. ネットワークポートのリストをエクスポートするには：
  - a. ネットワークポートのリストで、エクスポートするポートを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。

ポートが何も選択されていない場合、すべてのポートがエクスポートされます。
  - b. [エクスポート] をクリックします。
  - c. 表示されたウィンドウで、ネットワークポートのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. [保存] をクリックします。

Kaspersky Endpoint Security は、 ネットワークポートのリスト全体を XML ファイルにエクスポートします。
9. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをエクスポートするには：
  - a. [選択したアプリケーションのすべてのポートを監視する] をオンにします。
  - b. アプリケーションのリストで、エクスポートするアプリケーションを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。

アプリケーションが何も選択されていない場合、すべてのアプリケーションがエクスポートされます。
  - c. [エクスポート] をクリックします。
  - d. 表示されたウィンドウで、アプリケーションをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - e. [保存] をクリックします。

Kaspersky Endpoint Security は、 アプリケーションのリスト全体を XML ファイルにエクスポートします。

10. ネットワークポートのリストをインポートするには：

a. ネットワークポートのリストで、**【インポート】** をクリックします。

表示されたウィンドウで、ネットワークポートのリストをインポートする XML ファイルを選択します。

b. **【開く】** をクリックします。

コンピューターにネットワークポートのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

11. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをインポートするには：

a. アプリケーションのリストで、**【インポート】** をクリックします。

表示されたウィンドウで、アプリケーションのリストをインポートする XML ファイルを選択します。

b. **【開く】** をクリックします。

コンピューターにアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

12. 変更内容を保存します。

[Web コンソールおよび Cloud コンソールで監視対象のポートのリストをエクスポートおよびインポートする方法](#) 



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 監視対象のポートのリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[全般設定]** - **[ネットワークの設定]** を選択します。
5. ネットワークポートのリストをエクスポートするには：
  - a. **[監視対象のポート]** セクションで、**[選択されたネットワークポートのみを監視する]** を選択します。
  - b. **[<N>個のポートを選択済み]** リンクをクリックします。  
**[ネットワークポート]** ウィンドウが開きます。**[ネットワークポート]** ウィンドウに、メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。
  - c. ネットワークポートのリストで、エクスポートするポートを選択します。
  - d. **[エクスポート]** をクリックします。
  - e. 表示されたウィンドウで、ネットワークポートのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - f. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、ネットワークポートのリスト全体を XML ファイルにエクスポートします。
6. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをエクスポートするには：
  - a. **[監視対象のポート]** ブロックで、**[選択したアプリケーションのすべてのポートを監視する]** をオンにします。
  - b. **[<N>個のアプリケーションを選択済み]** リンクをクリックします。
  - c. アプリケーションのリストで、エクスポートするアプリケーションを選択します。
  - d. **[エクスポート]** をクリックします。
  - e. 表示されたウィンドウで、アプリケーションをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - f. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、アプリケーションのリスト全体を XML ファイルにエクスポートします。
7. ネットワークポートのリストをインポートするには：
  - a. ネットワークポートのリストで、**[インポート]** をクリックします。

表示されたウィンドウで、ネットワークポートのリストをインポートする XML ファイルを選択します。

b. **【開く】** をクリックします。

コンピューターにネットワークポートのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをインポートするには：

a. アプリケーションのリストで、**【インポート】** をクリックします。

表示されたウィンドウで、アプリケーションのリストをインポートする XML ファイルを選択します。

b. **【開く】** をクリックします。

コンピューターにアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

9. 変更内容を保存します。

## データの消去

Kaspersky Endpoint Security では、タスクを使用してユーザーのコンピューターからデータをリモート消去できます。

Kaspersky Endpoint Security は次の方法でデータを削除します：

- サイレントで実行
- ハードディスクおよびリムーバブルドライブのデータが対象
- コンピューター上のすべてのユーザーアカウントが対象

Kaspersky Endpoint Security は、使用しているライセンスの種別に関わりなく、ライセンスの有効期限が切れている場合でも、データの消去タスクを実行します。

### データ消去で利用できるモード

このタスクでは、次のいずれかのモードでデータを削除できます：

- 即座にデータを削除  
このモードは、ディスク上の空き容量を確保するために古くて不要になったデータを削除する用途などで使用できます。
- 接続が一定期間なかったときにデータを削除  
このモードは、ノート PC の紛失や盗難時に、ノート PC のデータが流出しないように保護する目的などで使用できます。社内ネットワークの外に持ち出されたノート PC が、長期間 Kaspersky Security Center に接続しなかった場合にデータを自動的に削除するように設定できます。

タスクのプロパティでデータを削除するスケジュールを設定することはできません。データを削除するタイミングは、「タスクを手動で開始した直後」または「Kaspersky Security Center と接続していないまま一定期間が経過した場合」のいずれかのかたちでのみ指定できます。

### 制限事項

データ消去には次の制限事項があります：

- Kaspersky Security Center の管理者のみが、データ消去タスクを管理できます。Kaspersky Endpoint Security のローカルインターフェイスでは、タスクの開始を設定できません。
- NTFS ファイルシステムの場合、Kaspersky Endpoint Security はメインデータストリームの名前のみ削除します。代替データストリーム名は削除できません。
- シンボリックリンクファイルを削除すると、Kaspersky Endpoint Security はシンボリックリンクでパスが指定されているファイルも削除します。

### データの消去タスクの作成

ユーザーのコンピューター上でデータを削除するには：

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **[タスク種別]** で、**[データの消去]** を選択します。
  - c. **[タスク名]** に「データの消去（盗難対策として）」などの簡潔な名前を付けます。
  - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。**[次へ]** をクリックします。

タスクの範囲内の管理グループに新しいコンピューターが追加された場合、即座にデータを消去するタスクについては、タスクが完了してから5分以内にコンピューターが追加された場合にのみ、この新しいコンピューターでもタスクが実行されます。

5. **[終了]** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
6. Kaspersky Endpoint Security の **[データの消去]** タスクを選択します。  
タスクのプロパティウィンドウが表示されます。
7. **[アプリケーション設定]** タブを選択します。
8. データの削除方法を選択します：
  - **OS の機能で削除する** : Kaspersky Endpoint Security は OS の機能を使用して、ファイルをごみ箱には送らずに削除します。
  - **完全に削除し、復元できないようにする** : Kaspersky Endpoint Security はランダムなデータを使用してファイルを上書きします。削除後にデータを復元することは、事実上不可能です。
9. 接続が一定期間なかったときにデータを削除する場合、**[Kaspersky Security Center への接続がない期間が次を超えた場合、自動的にデータを削除する]** をオンにします。日数を指定します。

接続が一定期間なかったときにデータを削除するタスクは、Kaspersky Security Center に接続されていない期間が指定した期間を超えるたびに毎回実行されます。

接続が一定期間なかったときにデータを削除するタスクを設定する場合は、従業員が長期休暇取得前にコンピューターの電源をオフにしてしまう可能性などを十分に考慮してください。長期間コンピューターの電源がオフになっていた場合、指定した期間を超えて接続が確立されず、データが消去される可能性があります。また、オフラインでコンピューターを使用するユーザーなどの業務スケジュールも考慮に入れてください。オフラインのコンピューターとモバイルユーザーについては詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

チェックボックスをオフにすると、Kaspersky Security Center と同期されたタイミングで即座にタスクが実行されます。

10. 削除するオブジェクトのリストを作成します：

- **フォルダー**：Kaspersky Endpoint Security は、指定したフォルダーとそのサブフォルダーに含まれるファイルをすべて削除します。マスクや環境変数を使用してのフォルダーのパスの指定はサポートされません。
- **ファイルの拡張子による指定**：Kaspersky Endpoint Security は、リムーバブルドライブも含めたコンピューター上のすべてのドライブで、指定した拡張子のファイルを検出します。複数の拡張子を指定するには、区切り文字として「;」または「,」を使用してください。
- **定義済みフォルダー**：次の領域からファイルが削除されます。
  - **ドキュメント**：オペレーティングシステムの標準の [ドキュメント] フォルダー内のファイルとそのサブフォルダー。
  - **Cookie**：ユーザーがアクセスした Web サイトのデータ（ユーザー認証データなど）をブラウザが保存するファイル。
  - **デスクトップ**：オペレーティングシステムの標準の [デスクトップ] フォルダー内のファイルとそのサブフォルダー。
  - **Internet Explorer の一時ファイル**：Web ページ、画像、メディアファイルのコピーなど、Internet Explorer の動作に関連する一時ファイル。
  - **一時ファイル**：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の動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。
  - **Outlook ファイル**：Outlook メールクライアントの動作に関連するファイル（データファイル (PST)、オフラインデータファイル (OST)、オフラインアドレス帳ファイル (OAB)、および個人のアドレス帳ファイル (PAB))。
  - **ユーザープロファイル**：ローカルユーザーアカウントのオペレーティングシステム設定を保存している一連のファイルおよびフォルダー。

各タブで削除するオブジェクトのリストを作成できます。Kaspersky Endpoint Security は、統合リストを作成し、タスクの完了時にこのリストからファイルを削除します。

Kaspersky Endpoint Security の動作に関連するファイルは削除できません。

11. **[保存]** をクリックします。

12. タスクの横にあるチェックボックスをオンにします。

13. **[開始]** をクリックします。

選択したモードに応じて、ユーザーのコンピューターのデータが削除されます（即座にまたは一定期間接続がなかったときに）。ユーザーがファイルを使用中だったなどの理由で、一部のファイルを Kaspersky Endpoint Security が削除できなかった場合、これらのファイルの削除が再試行されることはありません。データの削除を完了するには、タスクをもう一度実行してください。

# パスワードによる保護

企業などでは、コンピューターリテラシーのレベルが異なる複数のユーザーで1台のPCを共有することがあります。ユーザーに Kaspersky Endpoint Security およびその設定へのアクセスが制限なく許可されている場合、全体的なコンピューター保護のレベルが低下することがあります。パスワードによる保護を使用することで、ユーザーに付与された権限（例：アプリケーションの終了権限）に応じて、ユーザーが Kaspersky Endpoint Security で行える操作を制限できます。

Windows セッションを開始したユーザー（セッションユーザー）に操作を実行する権限が付与されている場合、Kaspersky Endpoint Security はユーザー名とパスワードの入力または一時パスワードの入力を要求しません。付与されている権限に応じて、ユーザーは Kaspersky Endpoint Security の機能にアクセスできます。

セッションユーザーに操作を実行する権限が付与されていない場合、ユーザーは次の方法でアクセスを取得できます：

- ユーザー名とパスワードを入力してください。

日常的なコンピューター使用では、この方法が最適です。パスワードによって保護されている操作を実行するには、必要な権限を付与されているユーザーのドメインアカウントの認証情報を入力する必要があります。この場合、コンピューターはドメイン内にある必要があります。コンピューターがドメインにない場合は、KLAdmin アカウントを使用できます。

- 一時パスワードを入力する。

この方法は、組織のネットワーク外のユーザーに、ブロックされている操作（例：本製品の終了）の権限を一時的に付与する場合に最適です。一時パスワードの有効期限が切れたりセッションが終了した場合、Kaspersky Endpoint Security の設定は元に戻ります。

パスワードによって保護されている操作をユーザーが試行した場合、Kaspersky Endpoint Security はユーザー名とパスワードの組み合わせまたは一時パスワードの入力を求めます（以下の図を参照）。

パスワードの入力ウィンドウでは、**ALT+SHIFT**を押すことでのみ言語を切り替えられます。オペレーティングシステムでその他のショートカットが設定されていても、その他のショートカットで言語を切り替えることはできません。

カスペルスキー

製品の設定を変更しますか？

ユーザー名:  
[ KLAdmin ]  
ユーザー名の既定値: KLAdmin

パスワードの入力:  
[ ]

この確認画面を非表示にする時間:  
非表示にしない

入力言語を切り替えるには、ALT+SHIFT キーを使用してください。 ENU

確認 キャンセル

Kaspersky Endpoint Security にアクセスするパスワードの入力

## ユーザー名とパスワード

Kaspersky Endpoint Security にアクセスするには、ドメインアカウントの認証情報を入力する必要があります。パスワードによる保護では次のアカウントがサポートされます：

- **KLAdmin** : Kaspersky Endpoint Security に制限なくアクセスできる管理者アカウント。KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。KLAdmin アカウントに対する権限を取り消すことはできません。パスワードによる保護を有効にすると、Kaspersky Endpoint Security では KLAdmin アカウントのパスワードの指定が要求されます。
- **Everyone グループ** : Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。Everyone グループに含まれるユーザーは、グループに対して付与されている権限に応じて本製品にアクセスできます。
- **個別のユーザーまたはグループ** : ユーザーアカウントに対して個別に権限を設定できます。たとえば、Everyone グループに対してはブロックされている操作を、個別のユーザーやグループに対して許可することができます。
- **セッションユーザー** : Windows セッションを開始したユーザーのアカウント。パスワードの入力を要求されたときに、別のセッションユーザーに切り替えることができます（**[本製品の終了までパスワードを記憶する]**）。この場合、Kaspersky Endpoint Security は、Windows セッションを開始したユーザーではなく、認証情報を入力したユーザーアカウントをセッションユーザーとして認識します。

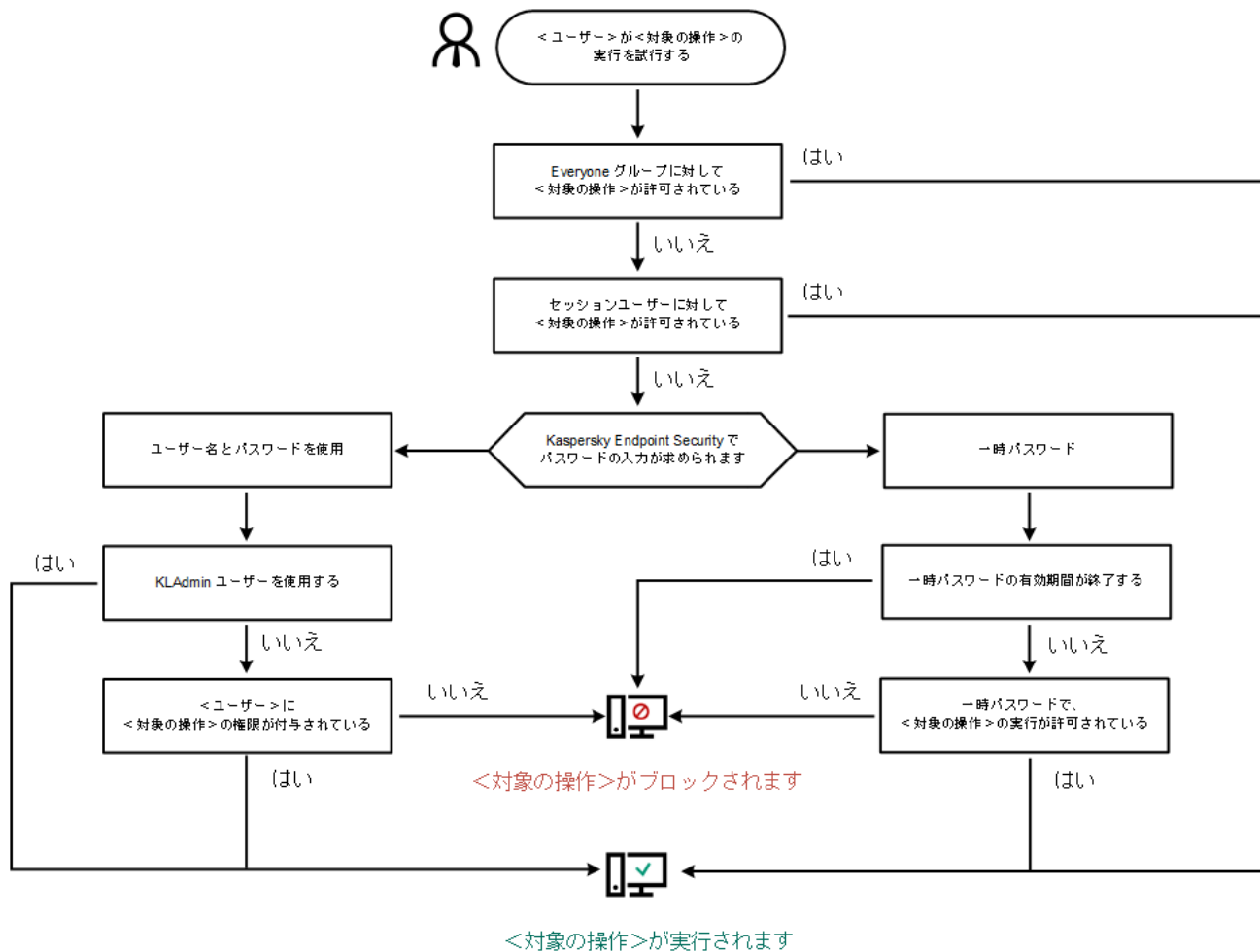
## 一時パスワード

一時パスワードを使用すると、組織ネットワーク外の個別のコンピューターに対して Kaspersky Endpoint Security への一時的なアクセス権を付与できます。管理者は、Kaspersky Security Center で、対象コンピューターのプロパティを使用して個別のコンピューターに対して一時パスワードを生成できます。管理者は、一時パスワードで保護される操作を選択し、一時パスワードの有効期間を指定します。

## パスワードによる保護の判定アルゴリズム

Kaspersky Endpoint Security は次のアルゴリズムに従って、パスワードによって保護されている処理の実行を許可するかブロックするかを判定します。






パスワードによる保護の判定アルゴリズム

## パスワードによる保護を有効にする

パスワードによる保護を使用することで、ユーザーに付与された権限（例：アプリケーションの終了権限）に応じて、ユーザーが Kaspersky Endpoint Security で行える操作を制限できます。

パスワードによる保護を有効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【インターフェイス】** の順に選択します。
3. **【パスワードによる保護】** を使用して機能を有効または無効にします。
4. KLAdmin アカウントのパスワードを入力し、確認します。

KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。

コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、管理者はポリシーのプロパティで KLAdmin アカウントのパスワードをリセットできます。コンピューターが Kaspersky Security Center に接続していない状態で KLAdmin アカウントのパスワードを忘れてしまうと、パスワードを復元することはできません。

5. 組織ネットワーク内のすべてのユーザーの権限を設定します。

- a. [権限] リストで、[編集] をクリックして Everyone グループの権限のリストを表示します。

Everyone グループは Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。

- b. ユーザーがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。

チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、**[本製品の終了]** 権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

- c. [OK] をクリックします。

6. 変更内容を保存します。

パスワードによる保護をオンにすると、Everyone グループに付与された権限に応じて、ユーザーが Kaspersky Endpoint Security で行える操作が制限されます。Everyone グループに対してブロックされている動作は、KLAdmin アカウントを使用している場合、必要な権限を付与されたその他のアカウントを使用している場合、あるいは一時パスワードを入力した場合にのみ実行できます。

KLAdmin としてログインしている場合にのみ、パスワードによる保護をオフにできます。その他のユーザーアカウントでログインしている場合または一時パスワードを使用してログインしている場合は、パスワードによる保護をオフにできません。


パスワードの確認時に、**[本製品の終了までパスワードを記憶する]** をオンにできます。この場合、セッションの継続中は、その他のパスワードによって保護された操作を実行しようとしてもパスワードの入力を要求されることはありません。

## 個別のユーザーまたはグループへの権限付与

Kaspersky Endpoint Security へのアクセス権を、個別のユーザーまたはグループに付与できます。たとえば、Everyone グループに対して「本製品の終了」操作がブロックされている場合でも、「**本製品の終了**」権限を個別のユーザーに対して付与できます。これにより、権限を付与されたユーザーまたは KLAdmin としてログインしている場合にのみ、本製品を終了できます。

コンピューターがドメイン内にある時のみ、本製品にアクセスするアカウントの認証情報を使用できます。コンピューターがドメインにない場合は、KLAdmin アカウントまたは一時パスワードを使用できます。

個別のユーザーまたはグループに権限を付与するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、[詳細設定] → [インターフェイス] の順に選択します。

3. **パスワードによる保護** テーブルで、**追加** をクリックします。
4. 表示されたウィンドウで、**ユーザーまたはグループの選択** 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。
5. Active Directory のユーザーまたはグループを選択し、選択内容を確認します。
6. **権限** リストで、選択したユーザーまたはグループがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。

チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、**本製品の終了** 権限のチェックボックスをオフにすると、KAdmin アカウントでログインしている場合、または 必要な権限を付与された個別のユーザーでログインしている場合、あるいは 一時パスワード を入力した場合にのみ本製品の終了を実行できます。

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの 留意事項 があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

7. 変更内容を保存します。

これにより、Everyone グループに対して Kaspersky Endpoint Security へのアクセスが制限されている場合でも、個別に権限を付与されたユーザーはその権限に応じて Kaspersky Endpoint Security にアクセスできます。

## 一時パスワードを使用した権限の付与

一時パスワードを使用すると、組織ネットワーク外の個別のコンピューターに対して Kaspersky Endpoint Security への一時的なアクセス権を付与できます。該当するユーザーに KAdmin アカウントの認証情報を共有せずに、ブロックされている操作の実行を許可するには、この手順が必要です。一時パスワードを使用するには、Kaspersky Security Center の管理対象にコンピューターを追加する必要があります。

一時パスワードを使用して、ブロックされている操作の実行をユーザーに許可するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **管理対象デバイス** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、**デバイス** タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、**アプリケーション** セクションを選択します。
6. コンピューターにインストールされているカスペルスキー製品のリストから **Kaspersky Endpoint Security for Windows** を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。
7. 本製品の設定ウィンドウで、**全般設定** → **インターフェイス** の順に選択します。
8. **パスワードによる保護** セクションで、**設定** をクリックします。  
**パスワードによる保護** ウィンドウが表示されます。
9. **一時パスワード** セクションで、**設定** をクリックします。

[一時パスワードを作成] ウィンドウが表示されます。

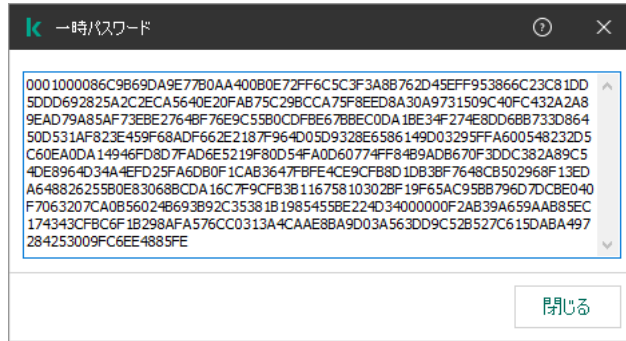
10. [有効期限] で、一時パスワードの有効期限が切れる日付を指定します。

11. [一時パスワードを要求する操作] リストで、一時パスワードの入力後にユーザーが使用できるようにする操作の横にあるチェックボックスをオンにします。

12. [新規作成] をクリックします。

ウィンドウが開き、一時パスワードが表示されます（以下の図を参照）。

13. パスワードをコピーし、ユーザーに共有します。




一時パスワード

## パスワードによる保護で付与する権限に関する留意事項

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作など、いくつかの留意事項があります。


### 製品設定

コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。

### 本製品の終了


特別な留意事項はありません。

### 保護機能の停止

- Everyone グループの保護機能を無効にする権限を付与することはできません。KLAdmin 以外のユーザーに保護機能の無効化を許可する場合は、パスワードによる保護の設定で [保護機能の停止] 権限を持つ ユーザーまたはグループを追加 してください。
- コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。
- ユーザーが本製品の設定で保護機能を停止するには、[本製品の設定] 権限も付与されている必要があります。

- コンテキストメニューから保護機能を無効にするには（**〔保護機能の一時停止〕**メニュー項目を使用し  
て）、ユーザーは**〔保護機能の停止〕**権限に加えて、**〔管理コンポーネントの停止〕**権限が必要です。

## 管理コンポーネントの停止

- Everyone グループの管理コンポーネントを停止する権限を付与することはできません。KAdmin 以外のユーザーに管理コンポーネントの無効化を許可する場合は、パスワードによる保護の設定で**〔管理コンポーネントの停止〕**権限を持つユーザーまたはグループを追加してください。
- コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。
- ユーザーが本製品の設定で管理コンポーネントを停止するには、**〔本製品の設定〕**権限も付与されている必要があります。
- コンテキストメニューから管理コンポーネントを無効にするには（**〔保護機能の一時停止〕**メニュー項目を使用し  
て）、ユーザーは**〔管理コンポーネントの停止〕**権限に加えて、**〔保護機能の停止〕**権限が必要です。

## Kaspersky Security Center ポリシーを無効にする

Kaspersky Security Center ポリシーを無効にする権限を「Everyone」グループに付与することはできません。KAdmin 以外のユーザーにポリシーの無効化を許可する場合は、パスワードによる保護の設定でユーザーまたはグループを追加し、このユーザーまたはグループに**〔Kaspersky Security Center ポリシーを無効にする〕**権限を付与してください。

## ライセンスの削除

特別な留意事項はありません。

## 本製品の削除 / 変更 / 修復

「すべて」のグループに本製品の削除、変更、修復を許可した場合、ユーザーがこれらの操作を実行しようとした場合に Kaspersky Endpoint Security はパスワードを要求しません。そのため、ドメイン外のユーザーを含むすべてのユーザーが本製品をインストール、変更、復元することができます。

## 暗号化されたドライブ上のデータへのアクセスの復元

暗号化されたドライブ上のデータへのアクセスは、KAdmin としてログインしている場合にのみ復元できます。この操作を実行する権限は、その他のユーザーには付与できません。

## レポートの表示

特別な留意事項はありません。

## バックアップから復元

特別な留意事項はありません。

# 信頼ゾーン

信頼ゾーンは Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。

管理者は処理されるオブジェクトとコンピューターにインストールされるアプリケーションの特徴を考慮しながら、信頼ゾーンを個別に定義します。Kaspersky Endpoint Security がアクセスをブロックする特定のオブジェクトやアプリケーションが無害であることが確実なときには、オブジェクトやアプリケーションを信頼ゾーンに含めなければならない場合があります。管理者が、ユーザーが特定のコンピューターに対してローカルの信頼するゾーンを作成するよう許可することも可能です。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。

## 信頼するオブジェクトの作成

信頼するオブジェクトとは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。

信頼するオブジェクトにより、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアを安全に使用できるようになります。悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアについて詳しくは、カスペルスキーの[ウイルス百科事典](#)を参照してください。

このようなアプリケーションは Kaspersky Endpoint Security によってブロックされる場合があります。ブロックしないようにするには、使用している製品を信頼するオブジェクトに設定できます。これを行うには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクを信頼ゾーンに追加します。たとえば、ユーザーがコンピューターのリモート管理用に Radmin アプリケーションを使用しているとします。Kaspersky Endpoint Security はこの処理を疑わしいものとみなして、ブロックする可能性があります。アプリケーションがブロックされないようにするには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクによって信頼するオブジェクトを作成します。

情報を収集し、それを処理するために送信するアプリケーションがコンピューターにインストールされていると、Kaspersky Endpoint Security がそのアプリケーションをマルウェアに分類する可能性があります。それを防ぐために、ヘルプ内で説明する方法で Kaspersky Endpoint Security を設定することで、そのアプリケーションをスキャン対象から除外できます。

システム管理者が設定した以下のコンポーネントとタスクによって信頼するオブジェクトを使用できます：

- [ふるまい検知](#)
- [脆弱性攻撃ブロック](#)：
- [ホスト侵入防止](#)：
- [ファイル脅威対策](#)：
- [ウェブ脅威対策](#)
- [メール脅威対策](#)
- [スキャンタスク](#)：

スキャンタスクの開始時にこのオブジェクトを含むドライブやフォルダーがスキャン範囲に含まれている場合、オブジェクトはスキャンされません。ただし、ある特定のオブジェクトについてオブジェクトスキャンタスクが開始された場合、信頼するオブジェクトは適用されません。

#### **管理コンソール (MMC) で信頼するオブジェクトを作成する方法**



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [全般設定] → [除外リスト] の順に選択します。
6. [信頼するオブジェクトとアプリケーション] セクションで、 [設定] をクリックします。
7. [信頼ゾーン] ウィンドウで、 [信頼するオブジェクト] タブを選択します。  
除外リストを含むウィンドウが開きます。
8. 組織内のすべてのコンピューターの除外リストを作成する場合は [継承時に値を結合する] をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。 [継承時に値を統合する] がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。
9. ローカルの除外リストをユーザーが作成できるようにするには、 [ローカルの除外リストの使用を許可する] を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。  
チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。ローカルのリストが作成された場合、この機能を無効にした後でも Kaspersky Endpoint Security は除外リストのファイルをスキャンから除外し続けます。
10. [追加] をクリックします。
11. ファイルまたはフォルダーをスキャンから除外するには：
  - a. [プロパティ] セクションで、 [ファイルまたはフォルダー] をオンにします。
  - b. [信頼するオブジェクトの説明] セクションの [ファイルまたはフォルダーの選択] をクリックして、 [ファイルまたはフォルダーの名前] ウィンドウを開きます。
  - c. ファイルまたはフォルダー名あるいはファイルまたはフォルダー名のマスクを指定するか、 [参照] をクリックしてフォルダーツリーからファイルまたはフォルダーを選択します。  
マスクを使用する
    - 「\*」 (アスタリスク) 文字。「\」 および 「/」 (ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字) を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
    - 2つの連続した「\*」 (アスタリスク) 文字。ファイル名またはフォルダー名内の、「\」 および 「/」 (ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字) を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子がtxtでファイル名が3文字のすべてのファイルのパスを含みます。

d. **【ファイルまたはフォルダーの名前】** ウィンドウで **【OK】** をクリックします。

追加されたファイルまたはフォルダーへのリンクが **【信頼するオブジェクト】** ウィンドウの **【信頼するオブジェクトの説明】** セクションに表示されます。

12. 特定の名前を持つオブジェクトをスキャンから除外するには：

a. **【プロパティ】** セクションで、**【オブジェクト名】** をオンにします。

b. **【信頼するオブジェクトの説明】** セクションの **【オブジェクト名の入力】** をクリックして、**【オブジェクト名】** ウィンドウを開きます。

c. **【ウイルス百科事典<sup>2</sup>】** の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、**【Rootkit】**、**【RemoteAdmin】**）。

任意の1文字を置き換える「?」と複数の文字を置き換える「\*」を使用してマスクを使用することができます。たとえば、マスク「Client\*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。

d. **【オブジェクト名】** ウィンドウで **【OK】** をクリックします。

追加されたオブジェクト名へのリンクが **【信頼するオブジェクト】** ウィンドウの **【信頼するオブジェクトの説明】** セクションに表示されます。

13. 個別のファイルをスキャンから除外する場合：

a. **【プロパティ】** セクションで、**【オブジェクトハッシュ】** をオンにします。

b. **【オブジェクトハッシュ】** ウィンドウを開くには、オブジェクトハッシュの項目のリンクをクリックします。

c. ファイルハッシュを入力するか、**【参照】** をクリックしてファイルを選択します。

ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

d. **【オブジェクトハッシュ】** ウィンドウで **【OK】** をクリックします。

追加されたオブジェクトへのリンクが **【信頼するオブジェクト】** ウィンドウの **【信頼するオブジェクトの説明】** ブロックに表示されます。

14. 必要に応じて、**【コメント】** に、作成する信頼するオブジェクトの簡単なコメントを入力します。

15. 次の手順に従って、信頼するオブジェクトを使用する Kaspersky Endpoint Security コンポーネントを指定します：

a. **【信頼するオブジェクトの説明】** セクションで **【すべての保護機能】** をクリックすると、**【コンポーネントの指定】** が表示されます。

b. **【コンポーネントの指定】** をクリックして **【保護機能】** ウィンドウを開きます。

c. スキャンからの除外を適用するコンポーネントの横にあるチェックボックスをオンにします。

d. **【保護機能】** ウィンドウで **【OK】** をクリックします。

信頼するオブジェクトの設定でコンポーネントが指定されている場合、Kaspersky Endpoint Security のこれらのコンポーネントによるスキャン時にのみ、この信頼するオブジェクトが適用されます。

信頼するオブジェクトの設定でコンポーネントが指定されていない場合、Kaspersky Endpoint Security のどのコンポーネントによるスキャン時にも、この信頼するオブジェクトが適用されます。

16. このチェックボックスを使用していつでも除外を停止することができます。


17. 変更内容を保存します。

#### Web コンソールと Cloud コンソールで信頼するオブジェクトを作成する方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. 信頼するオブジェクトを追加するコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [全般設定] → [除外リスト] を選択します。
5. [信頼するオブジェクトとアプリケーション] セクションで、[信頼するオブジェクト] をクリックします。
6. 組織内のすべてのコンピューターの除外リストを作成する場合は [継承時に値を結合する] をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。[継承時に値を統合する] がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。
7. ローカルの除外リストをユーザーが作成できるようにするには、[ローカルの除外リストの使用を許可する] を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。  
チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。ローカルのリストが作成された場合、この機能を無効にした後でも Kaspersky Endpoint Security は除外リストのファイルをスキャンから除外し続けます。
8. [追加] をクリックします。
9. 除外を追加する方法を選択します： [ファイルまたはフォルダー]、[オブジェクト名] または [オブジェクトハッシュ]。
10. ファイルまたはフォルダーをスキャンから除外する場合は、[参照] をクリックしてファイルまたはフォルダーを選択します。  
手動でパスを入力することもできます。Kaspersky Endpoint Security はマスクの入力時の文字「\*」および「?」をサポートします。
  - 「\*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
  - 2つの連続した「\*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。
  - 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\??.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。

11. 特定のオブジェクトをスキャンから除外する場合は、**【オブジェクト】**フィールドで、「[ウイルス百科事典](#)」の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、「Rootkit」、「RemoteAdmin」）。  
任意の1文字を置き換える「?」と複数の文字を置き換える「\*」を使用してマスクを使用することができます。たとえば、マスク「Client\*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。
12. 個別のファイルをスキャンから除外する場合は、**【ファイルハッシュ】**フィールドにファイルのハッシュを入力します。  
ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。
13. **【保護機能】**ブロックで、スキャンの例外を適用するコンポーネントを選択します。
14. 必要に応じて、**【コメント】**に、作成する信頼するオブジェクトの簡単なコメントを入力します。
15. このトグルスイッチを使用していつでも[除外を停止](#)することができます。
16. 変更内容を保存します。

### **製品インターフェイスで信頼するオブジェクトを作成する方法**

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[脅威と除外リスト]** を選択します。
3. **[除外リスト]** ブロックで、**[除外リストの管理]** をクリックします。
4. **[追加]** をクリックします。
5. ファイルまたはフォルダーをスキャンから除外する場合は、**[参照]** をクリックしてファイルまたはフォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Endpoint Security はマスクの入力時の文字「\*」および「?」をサポートします。

- 「\*」（アスタリスク）文字。「\」（バックスラッシュ）および「/」（スラッシュ）（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
- 2つの連続した「\*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」（バックスラッシュ）および「/」（スラッシュ）（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下の「C:\\*\*\\*.txt」というマスクの指定は無効です。
- 「?」（クエスチョンマーク）。「\」（バックスラッシュ）および「/」（スラッシュ）（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。

6. 特定のオブジェクトをスキャンから除外する場合は、**[オブジェクト]** フィールドで、**[ウイルス百科事典]** の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、「Rootkit」、「RemoteAdmin」）。

任意の1文字を置き換える「?」と複数の文字を置き換える「\*」を使用してマスクを使用することができます。たとえば、マスク「Client\*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。

7. 個別のファイルをスキャンから除外する場合は、**[ファイルハッシュ]** フィールドにファイルのハッシュを入力します。

ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

8. **[保護機能]** ブロックで、スキャンの例外を適用するコンポーネントを選択します。
9. 必要に応じて、**[コメント]** に、作成する信頼するオブジェクトの簡単なコメントを入力します。
10. 信頼するオブジェクトのステータスに **[有効]** を選択します。  
このトグルスイッチを使用していつでも**除外を停止**することができます。
11. 変更内容を保存します。

パスマスクの例：

任意のフォルダーにあるファイルへのパス：



- 「\*.exe」というマスクには、拡張子が「exe」のファイルへのすべてのパスが含まれます。
- 「example\*」というマスクには、名前が「example」のファイルへのすべてのパスが含まれます。

特定のフォルダーにあるファイルへのパス：


- 「C:\dir\\*.\*」というマスクには、「C:\dir\」フォルダーにあるすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「C:\dir\\*」というマスクには、「C:\dir\」フォルダーにあるすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「C:\dir\」というマスクには、「C:\dir\」フォルダーにあるすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「C:\dir\\*.exe」というマスクには、「C:\dir\」フォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「C:\dir\test」というマスクには、「C:\dir\」フォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「C:\dir\\*\test」というマスクには、「C:\dir\」フォルダーとそのサブフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれます。

特定の名前のすべてのフォルダーにあるファイルへのパス：

- 「dir\\*.\*」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「dir\\*」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「dir\」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「dir\\*.exe」というマスクには、名前が「dir」のフォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「dir\test」というマスクには、名前が「dir」のフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。

## 信頼するオブジェクトの有効化と無効化

信頼するオブジェクトを有効または無効にするには、次の操作を行います：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【脅威と除外リスト】** を選択します。
3. **【除外リスト】** ブロックで、**【除外リストの管理】** をクリックします。
4. 信頼するオブジェクトのリストで必要なオブジェクトを選択します。



5. オブジェクトの横にあるトグルスイッチを使用して、オブジェクトをスキャン範囲に含めるか除外するかを指定します。
6. 変更内容を保存します。

## Editing the list of trusted applications

The *list of trusted applications* is a list of applications whose file and network activity (including malicious activity) and access to the system registry are not monitored by Kaspersky Endpoint Security. By default, Kaspersky Endpoint Security scans objects that are opened, executed, or saved by any application process and controls the activity of all applications and network traffic that is generated by them. However, an application that has been added to the list of trusted applications is excluded from scans by Kaspersky Endpoint Security.

For example, if you consider objects that are used by the standard Microsoft Windows Notepad application to be safe without scanning, meaning that you trust this application, you can add Microsoft Windows Notepad to the list of trusted applications. Scanning then skips objects that are used by this application.

In addition, certain actions that are classified by Kaspersky Endpoint Security as suspicious may be safe within the context of the functionality of a number of applications. For example, the interception of text that is typed from the keyboard is a routine process for automatic keyboard layout switchers (such as Punto Switcher). To take account of the specifics of such applications and exclude their activity from monitoring, we recommend that you add such applications to the trusted applications list.

Excluding trusted applications from scanning allows avoiding compatibility conflicts between Kaspersky Endpoint Security and other programs (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Endpoint Security and by another anti-virus application), and also increases the computer's performance, which is critical when using server applications.

At the same time, the executable file and process of the trusted application are still scanned for viruses and other malware. An application can be fully excluded from Kaspersky Endpoint Security scanning by means of scan exclusions.

[How to add an application to the trusted list in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **General settings** → **Exclusions**.
6. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
7. In the **Trusted zone** window, select the **Trusted applications** tab.  
This opens a window containing a list of trusted applications.
8. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company. The lists of trusted applications in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted applications from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted applications of the parent policy is not possible.
9. Select the **Allow use of local trusted applications** check box if you want to enable the user to create a local list of trusted applications. This way, a user can create their own local list of trusted applications in addition to the general list of trusted applications generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.  
If the check box is cleared, the user can access only the general list of trusted applications generated in the policy. If a local list was generated, after this functionality is disabled Kaspersky Endpoint Security continues excluding the listed trusted applications from scans.
10. Click the **Add** button.
11. In the opened window, enter the path to the executable file of the trusted application.  
Kaspersky Endpoint Security supports environment variables and the **\*** and **?** characters when entering a mask.  

Kaspersky Endpoint Security does not support the %userprofile% environment variable when generating a list of trusted applications on the Kaspersky Security Center console. To apply the entry to all user accounts, you can use the \* character (for example, C:\Users\\*\Documents\File.exe).


Whenever you add a new environment variable, you need to restart the application.
12. Configure the advanced settings for the trusted application (see the table below).
13. You can use the check box to [exclude an application from the trusted zone](#) at any time.
14. Save your changes.

1. In the main window of Web Console, select **Devices** → **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to add the application to the trusted list.  
The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **General settings** → **Exclusions**.
5. In the **Scan exclusions and trusted applications** block, click the **Trusted applications** link.  
This opens a window containing a list of trusted applications.
6. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company. The lists of trusted applications in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted applications from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted applications of the parent policy is not possible.
7. Select the **Allow use of local trusted applications** check box if you want to enable the user to create a local list of trusted applications. This way, a user can create their own local list of trusted applications in addition to the general list of trusted applications generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.  
If the check box is cleared, the user can access only the general list of trusted applications generated in the policy. If a local list was generated, after this functionality is disabled Kaspersky Endpoint Security continues excluding the listed trusted applications from scans.
8. Click the **Add** button.
9. In the opened window, enter the path to the executable file of the trusted application.  
Kaspersky Endpoint Security supports environment variables and the **\*** and **?** characters when entering a mask.  

Kaspersky Endpoint Security does not support the %userprofile% environment variable when generating a list of trusted applications on the Kaspersky Security Center console. To apply the entry to all user accounts, you can use the \* character (for example, C:\Users\\*\Documents\File.exe).

Whenever you add a new environment variable, you need to restart the application.
10. Configure the advanced settings for the trusted application (see the table below).
11. You can use the check box to [exclude an application from the trusted zone](#) at any time.
12. Save your changes.

## [How to add an application to the trusted list in the application interface](#)

1. In the main application window, click the button .
2. In the application settings window, select the **Advanced settings** → **Threats and Exclusions** section.
3. In the **Exclusions** block, click the **Specify trusted applications** link.
4. In the window, click the **Add** button.
5. Select the executable file of the trusted application.

You can also manually enter the path. Kaspersky Endpoint Security supports environment variables and the `*` and `?` characters when entering a mask.

Kaspersky Endpoint Security supports environment variables and converts the path in the local interface of the application. In other words, if you enter the file path `%userprofile%\Documents\File.exe`, a `C:\Users\Fred123\Documents\File.exe` record is added in local interface of the application for user Fred123. Accordingly, Kaspersky Endpoint Security ignores the `File.exe` trusted program for other users. To apply the entry to all user accounts, you can use the `*` character (for example, `C:\Users\*\Documents\File.exe`).

Whenever you add a new environment variable, you need to restart the application.

6. In the trusted application properties window, configure the advanced settings (see the table below).
7. You can use the toggle to [exclude an application from the trusted zone](#) at any time.
8. Save your changes.


Trusted application settings

Parameter	Description
<b>Do not scan opened files</b>	All files that are opened by the application are excluded from scans by Kaspersky Endpoint Security. For example, if you are using applications to back up files, this feature helps reduce the consumption of resources by Kaspersky Endpoint Security.
<b>Do not monitor application activity</b>	Kaspersky Endpoint Security will not monitor the application's file- and network activity in the operating system. Application activity is monitored by the following components: <a href="#">Behavior Detection</a> , <a href="#">Exploit Prevention</a> , <a href="#">Host Intrusion Prevention</a> , <a href="#">Remediation Engine</a> and <a href="#">Firewall</a> .
<b>Do not inherit restrictions of the parent process (application)</b>	The restrictions configured for the parent process will not be applied by Kaspersky Endpoint Security to a child process. The parent process is started by an application for which <a href="#">application rights</a> (Host Intrusion Prevention) and <a href="#">application network rules</a> (Firewall) are configured.
<b>Do not monitor child application activity</b>	Kaspersky Endpoint Security will not monitor the file activity or network activity of applications that are started by this application.
<b>Allow interaction with the application interface</b>	<a href="#">Kaspersky Endpoint Security Self-Defense</a> blocks all attempts to manage application services from a remote computer. If the check box is selected, the remote access application is allowed to manage Kaspersky Endpoint Security settings through the Kaspersky Endpoint Security interface.

<b>Do not block interaction with AMSI Protection component</b> <i>(available only in the Kaspersky Security Center Console)</i>	Kaspersky Endpoint Security will not monitor the trusted application's requests for objects to be scanned by the <a href="#">AMSI Protection component</a> .
<b>Do not scan network traffic</b>	Network traffic initiated by the application will be excluded from scans by Kaspersky Endpoint Security. You can exclude either all traffic or only encrypted traffic from scans. You can also exclude individual IP addresses and port numbers from scans.
<b>Comment</b>	If necessary, you can provide a brief comment for the trusted application. Comments help simplify searches and sorting of trusted applications.
<b>Status</b>	Status of the trusted application: <ul style="list-style-type: none"> <li>• <b>Active</b> status means that the application is in the trusted zone.</li> <li>• <b>Inactive</b> status means that the application is excluded from the trusted zone.</li> </ul>

## 信頼するアプリケーションのリストでのアプリケーションに対する信頼ゾーンルールの有効化と無効化


信頼するアプリケーションのリストで、アプリケーションに適用される信頼ゾーンルールの処理を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【脅威と除外リスト】** を選択します。
3. **【除外リスト】** ブロックで、**【信頼するアプリケーションの指定】** をクリックします。
4. 信頼するアプリケーションのリストで、目的の信頼するアプリケーションを選択します。
5. **【ステータス】** 列のトグルスイッチを使用して、信頼するアプリケーションをスキャン範囲に含めるか除外するかを指定します。
6. 変更内容を保存します。

## 信頼するシステム証明書ストアの使用

システム証明書ストアを使用することで、信頼されるデジタル署名で署名されたアプリケーションをウイルススキャンから除外できます。Kaspersky Endpoint Security はこのようなアプリケーションを信頼済みグループに割り当てます。

信頼するシステム証明書ストアの使用を開始するには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、**〔詳細設定〕** → **〔脅威と除外リスト〕** を選択します。
3. **〔信頼するシステム証明書ストア〕** で、信頼するシステムストアを選択します。
4. 変更内容を保存します。

## バックアップの管理

バックアップ保管領域には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。バックアップコピーは、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルのバックアップコピーは、フォルダー C:\ProgramData\Kaspersky Lab\KES\QB に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。


駆除中にファイルの整合性を維持できない場合があります。駆除後に、駆除されたファイルに含まれている重要な情報の一部または全体にアクセスできなくなった場合、バックアップコピーからファイルを元のフォルダーに復元を試みる可以尝试することができます。

Kaspersky Endpoint Security が Kaspersky Security Center の管理下で動作している場合、ファイルのバックアップコピーが Kaspersky Security Center の管理サーバーに送信される場合があります。Kaspersky Security Center でのファイルのバックアップコピーの管理について詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。

## バックアップファイルの最大保管期間の設定

既定では、最大保管期間は 30 日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。

バックアップファイルの最大保管期間を設定するには：

1. メインウィンドウで、 をクリックします。
2. 製品の設定ウィンドウで、**[詳細設定]** → **[レポートと保管領域]** を選択します。
3. バックアップ内のコピーの保管期限を設定する場合は、**[バックアップ]** ブロックで **[保存期間]** チェックボックスをクリックします。**[保存期間]** の右側のフィールドに、バックアップにあるファイルのコピーの最大保管期間を指定します。
4. 変更内容を保存します。

## バックアップの最大サイズの設定

バックアップの最大サイズを設定できます。既定では、バックアップのサイズは制限されていません。最大サイズに到達すると、データの最大保管サイズの超過を防ぐために、最も古いファイルがバックアップから自動的に削除されます。

バックアップの最大サイズを設定するには：

1. メインウィンドウで、 をクリックします。



2. 製品の設定ウィンドウで、**〔詳細設定〕** → **〔レポートと保管領域〕** を選択します。
3. バックアップのサイズを制限するには、**〔バックアップ〕** で **〔バックアップのサイズを制限する〕** を選択します。バックアップの最大サイズを指定します。
4. 変更内容を保存します。

## バックアップからのファイルの復元

悪意のあるコードがファイル内で検知された場合、Kaspersky Endpoint Security はそのファイルをブロックし、「感染」ステータスを割り当て、コピーをバックアップに保存してから駆除を試みます。ファイルの駆除に成功すると、ファイルのバックアップコピーのステータスが「駆除済み」に変わります。ファイルは元のフォルダーで利用可能になります。ファイルを駆除できない場合、元のフォルダーからファイルを削除します。バックアップコピーから元のフォルダーにファイルを復元できます。

「コンピューターの再起動後に駆除」ステータスのファイルは復元できません。コンピューターを再起動すると、ステータスが「駆除済み」または「削除済み」に変更されます。バックアップコピーから元のフォルダーにファイルを復元することもできます。

Windows ストアアプリの一部であるファイルに悪意のあるコードが検知されると、Kaspersky Endpoint Security は即座にそのファイルを削除します。ファイルのコピーがバックアップに移動されることはありません。Windows ストアアプリの整合性を復元するには、Microsoft Windows 8 オペレーティングシステムの適切なツールを使用します（Windows ストアアプリの復元の詳細については、Microsoft Windows 8 のヘルプファイルを参照してください）。

ファイルのバックアップコピーはテーブル形式で表示されます。ファイルのバックアップコピーでは、ファイルの元のフォルダーのパスが表示されます。ファイルの元のフォルダーのパスには個人情報が含まれる場合があります。

同じフォルダーにある名前が同一で内容が異なる複数のファイルがバックアップに移動された場合、最後にバックアップに移動されたファイルのみを復元できます。

バックアップからファイルを復元するには：

1. 製品のメインウィンドウの **〔監視〕** で、**〔バックアップ〕** をクリックします。
2. バックアップにあるファイルのリストが表示されます。リストから復元したいファイルを選択して **〔復元〕** をクリックします。

選択したバックアップコピーのファイルが元のフォルダーに復元されます。

## バックアップからのファイルのバックアップコピーの削除

Kaspersky Endpoint Security は、製品の設定で指定した保管期間を過ぎると、バックアップコピーのステータスに関係なく、ファイルのバックアップコピーをバックアップから自動的に削除します。また、ファイルのコピーは、バックアップから手動で削除することもできます。

バックアップからファイルのバックアップコピーを削除するには：

1. 製品のメインウィンドウの **〔監視〕** で、**〔バックアップ〕** をクリックします。

2. バックアップにあるファイルのリストが表示されます。リストから、バックアップから削除するファイルを選択して「削除」をクリックします。「すべて削除」ボタンをクリックすることで、バックアップ内のすべてのファイルを削除することができます。

選択したバックアップファイルがバックアップから削除されます。

# 通知サービス

Kaspersky Endpoint Security の動作中には、あらゆる種類のイベントが発生します。イベントの通知には、単にお知らせのものもあれば重要な情報が含まれるものもあります。たとえば、定義データベースとソフトウェアモジュールのアップデートが正常に完了したことを通知したり、修復が必要なコンポーネントエラーを記録したりします。

Kaspersky Endpoint Security では、Microsoft Windows のアプリケーションログや Kaspersky Endpoint Security のイベントログの動作のイベントに関する情報の記録をサポートします。

Kaspersky Endpoint Security は次の方法で通知を配信します：

- Microsoft Windows タスクバーの通知領域でポップアップ通知を表示する
- メールで送信する


イベント通知の配信を設定できます。通知配信の方法はイベントの種類ごとに設定します。

イベントのテーブルを使用して通知サービスを設定する場合は、次のことができます：

- 通知サービスイベントを列の値または絞り込み条件でフィルター処理する。
- 通知サービスイベントの検索機能を使用する。
- 通知サービスイベントを並べ替える。
- 通知サービスイベントのリストに表示される順番と列を変更する。

## イベントログ設定の指定

イベントログ設定を指定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[インターフェイス]** の順に選択します。
3. **[通知]** で、**[通知の設定]** をクリックします。

Kaspersky Endpoint Security のコンポーネントとタスクがウィンドウの左側に表示されます。ウィンドウの右側に、選択したコンポーネントまたはタスクで発生したイベントが表示されます。

イベントには、以下のユーザーデータが含まれる場合があります：

- Kaspersky Endpoint Security がスキャンしたファイルのパス
- Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
- Microsoft Windows のユーザー名
- ユーザーが開いた Web ページのアドレス

4. ウィンドウの左側で、イベントログを設定するコンポーネントまたはタスクを選択します。


5. [ローカルレポートに保存] および [Windows イベントログに保存] 列で、該当するイベントのチェックボックスをオンにします。

[ローカルレポートに保存] 列のチェックボックスがオンになっているイベントは、[アプリケーションとサービス ログ] の [Kaspersky イベントログ] セクションに表示されます。[Windows イベントログに保存] 列のチェックボックスがオンになっているイベントは、[Windows ログ] の [アプリケーション] セクションに表示されます。イベントログを開くには、[スタート] → [コントロール パネル] → [管理ツール] → [イベント ビューアー] の順に選択します。

6. 変更内容を保存します。

## 通知の表示と配信の設定

通知の表示と配信を設定するには：

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、[詳細設定] → [インターフェイス] の順に選択します。

3. [通知] で、[通知の設定] をクリックします。

Kaspersky Endpoint Security のコンポーネントとタスクがウィンドウの左側に表示されます。ウィンドウの右側に、選択したコンポーネントまたはタスクで発生したイベントが表示されます。

イベントには、以下のユーザーデータが含まれる場合があります：

- Kaspersky Endpoint Security がスキャンしたファイルのパス
- Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
- Microsoft Windows のユーザー名
- ユーザーが開いた Web ページのアドレス

4. ウィンドウの左側で、通知の配信を設定するコンポーネントまたはタスクを選択します。

5. [画面で通知] 列で、必要なイベントの横のチェックボックスをオンにします。

選択したイベントに関する情報が、Microsoft Windows タスクバーの通知領域にポップアップメッセージとして画面に表示されます。

6. [メールで通知] 列で、必要なイベントの横のチェックボックスをオンにします。

メール通知配信が設定されている場合、選択したイベントに関する情報がメールで配信されます。

7. [OK] をクリックします。

8. 通知を有効にする場合は、メール配信を設定します：

a. [メール通知の設定] をクリックします。

b. [イベントを通知する] をオンにして、[メールで通知] 列でオンにした Kaspersky Endpoint Security イベントに関する通知の配信を有効にします。


c. メール通知の配信設定を指定してください。



d. [OK] をクリックします。

9. 変更内容を保存します。

## 製品のステータスに関する通知領域での警告の表示設定

製品のステータスに関する警告の通知領域での表示を設定するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【インターフェイス】** の順に選択します。
3. **【通知エリアに製品のステータスを表示する】** セクションで、Microsoft Windows の通知領域に通知を表示するイベントカテゴリの横にあるチェックボックスをオンにします。
4. 変更内容を保存します。

選択したカテゴリに属するイベントが発生すると、通知領域の[製品アイコン](#)が、警告の重要度に応じて  または  に変わります。


## レポートの管理

レポートには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

レポートは、フォルダー「C:\ProgramData\Kaspersky Lab\KES\Report」に保存されます。

レポートには、以下のユーザーデータが含まれる場合があります：

- Kaspersky Endpoint Security がスキャンしたファイルのパス
- Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
- Microsoft Windows のユーザー名
- ユーザーが開いた Web ページのアドレス


レポートのデータはテーブル形式で表示されます。テーブルの各行には、各イベントの情報が含まれます。イベント属性はテーブルの列に表示されます。特定の列は、詳細属性に入れ子にされた列を含んだ複合列です。追加の属性を表示するには、列の名前の横にある  ボタンをクリックします。さまざまなコンポーネントの操作中またはさまざまなタスクの実行中にログに記録されるイベントには、異なる属性セットがあります。


次のレポートを使用できます：

- **システム監査**レポート。ユーザーと製品の相互作用および一般的な製品操作で発生し、特定の Kaspersky Endpoint Security コンポーネントまたはタスクとは無関係なイベントに関する情報が含まれます。
- Kaspersky Endpoint Security コンポーネントの操作に関するレポート。
- Kaspersky Endpoint Security のタスクに関するレポート。
- **データ暗号化**レポート。データの暗号化および復号化の処理中に発生したイベントに関する情報が含まれます。

以下は、レポートで使用するイベントの重要度レベルです：


 **情報イベント**。通常は重要な情報が含まれていない参照イベントです。

 **警告**。Kaspersky Endpoint Security の処理における重要な状況が反映されているので、注意が必要なイベントです。


 **緊急イベント**。Kaspersky Endpoint Security の処理上の問題やユーザーのコンピューター保護における脆弱性を示す、きわめて重大なイベントです。

レポートを処理しやすくするために、データの表示方法を次のように変更できます：

- イベントリストを各種基準でフィルタリングする。
- 検索機能を使用して、具体的なイベントを検索する。
- 選択したイベントをセクションごとに表示する。
- イベントのリストをレポートの列ごとに分類する。

-  ボタンを使用して、イベントのフィルターによってグループ化されたイベントを表示または非表示にする。
- レポートに表示される列の順番と配置を変更する。

必要に応じて、生成されたレポートをテキストファイルに保存できます。Kaspersky Endpoint Security コンポーネントおよびグループに統合されたタスクに関する [レポート情報を削除](#) することもできます。

Kaspersky Endpoint Security が Kaspersky Security Center の管理下で実行されている場合、イベントに関する情報が Kaspersky Security Center 管理サーバーに転送される場合があります。詳細については、[Kaspersky Security Center のオンラインヘルプ](#)  を参照してください。

## レポートの表示

ユーザーがレポートを表示できる場合、そのユーザーはレポートに関連するすべてのイベントを表示することもできます。

レポートを表示するには、次の手順を実行します：


1. 製品のメインウィンドウの **[監視]** で、**[レポート]** をクリックします。
2. **[レポート]** ウィンドウの左側にあるコンポーネントとタスクのリストで、コンポーネントまたはタスクを選択します。  
ウィンドウの右側に、選択したコンポーネントまたは選択したタスクの動作の結果であるイベントのリストを含むレポートが表示されます。レポート内のイベントは、列の値で並べ替えることができます。既定では、レポートイベントは **[イベントの日付]** 列の値の昇順に並べ替えられます。
3. イベントの詳細な情報を表示するには、レポート内のイベントを選択します。

ウィンドウの下部のセクションに、イベントのサマリーが表示されます。

## レポート最長保管期間の設定

既定では、Kaspersky Endpoint Security によってログに記録されるイベントに関するレポートの最長保管期間は 30 日間です。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。

レポート最長保管期間を変更するには：


1. メインウィンドウで、 をクリックします。
2. 製品の設定ウィンドウで、**[詳細設定]** → **[レポートと保管領域]** を選択します。
3. レポートの保管期限を設定する場合は、**[レポート]** ブロックで **[保存期間]** チェックボックスをクリックします。レポート最長保管期間を設定します。
4. 変更内容を保存します。



## レポートファイルの最大サイズの設定

レポートを含むファイルの最大サイズを指定できます。既定では、レポートの最大ファイルサイズは1024 MBです。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。

レポートファイルの最大サイズを設定するには：

1. メインウィンドウで、 をクリックします。
2. 製品の設定ウィンドウで、**[詳細設定]** → **[レポートと保管領域]** を選択します。
3. レポートファイルのサイズを制限する場合は、**[レポート]** ブロックで、**[レポートファイルの最大サイズ]** を選択します。レポートファイルの最大サイズを設定します。
4. 変更内容を保存します。

## レポートのファイルへの保存

ファイルに保存したレポート内の情報の保護、特にその情報へのアクセスの管理と制限については、ユーザーが責任を負います。

生成したレポートはテキスト形式 (txt) ファイルとして、または CSV ファイルとして保存できます。

Kaspersky Endpoint Security では、イベントを画面に表示されるとおり、つまり同一セットおよびシーケンスのイベント属性とともにレポートに記録します。


レポートをファイルに保存するには：

1. 製品のメインウィンドウの **[監視]** で、**[レポート]** をクリックします。
2. 表示されるウィンドウでコンポーネントまたはタスクを選択します。  
レポートがウィンドウの右側に表示されます。このレポートには、選択した Kaspersky Endpoint Security コンポーネントの操作またはタスクに関するイベントがリスト表示されます。
3. 次の方法で、レポートに表示されるデータを必要に応じて変更できます：
  - イベントをフィルター処理する
  - イベント検索を実行する
  - 列の配置を変更する
  - イベントを並べ替える
4. ウィンドウの右上にある **[レポートを保存]** をクリックします。
5. 表示されたウィンドウで、レポートファイルの保存先フォルダーを指定します。

6. **【ファイル名】** にレポートファイル名を入力します。
7. **【ファイル種別】** で必要なレポートファイル形式を TXT または CSV から選択します：
8. 変更内容を保存します。

## レポートの削除

レポートから情報を削除するには：

1. メインウィンドウで、 をクリックします。
2. 製品の設定ウィンドウで、**【詳細設定】** → **【レポートと保管領域】** を選択します。
3. **【レポート】** セクションの **【消去】** をクリックします。
4. パスワードによる保護が有効な場合は、ユーザーアカウントの認証情報が求められます。ユーザーに十分な権限がなかった場合は、アカウントの認証情報が求められます。

すべてのアプリケーションコンポーネントおよびタスクのレポートがすべて削除されます。

# Kaspersky Endpoint Security Self-Defense

セルフディフェンスは、他のアプリケーションが Kaspersky Endpoint Security の動作を妨害したり、Kaspersky Endpoint Security をコンピューターから削除したりする操作を実行できないようにします。使用できる Kaspersky Endpoint Security セルフディフェンス技術は、オペレーティングシステムが 32 ビットか 64 ビットかで異なります（下の表を参照してください）。


Kaspersky Endpoint Security セルフディフェンス技術

技術	説明	x86 コンピューター	x64 コンピューター
<b>セルフディフェンス機構</b>	次の製品コンポーネントへのアクセスをブロックします： <ul style="list-style-type: none"><li>• Kaspersky Endpoint Security のインストールフォルダーにあるファイルおよび本製品のファイル</li><li>• 本製品に属する項目を含むレジストリキー</li><li>• 本製品が実行するプロセス</li></ul>	✓	✓
<b>AM-PPL (Antimalware Protected Process Light)</b>	Kaspersky Endpoint Security のプロセスを悪意のある処理から保護します。AM-PPL 技術について詳しくは、 <a href="#">Microsoft の Web サイトの情報</a> を参照してください。  AM-PPL 技術は Windows 10 バージョン 1703 (RS2) 以降および Windows Server 2019 で利用できます。	✓	✓
<b>外部からの管理に対する防御機構</b>	この技術は、TeamViewer または RemotelyAnywhere などの遠隔管理アプリケーションからの Kaspersky Endpoint Security へのアクセスをブロックします。	✓	– (Windows 7 以外)

## セルフディフェンスの有効化と無効化

既定では、Kaspersky Endpoint Security のセルフディフェンス機構は有効です。

セルフディフェンスを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[全般設定]** の順に選択します。
3. **[セルフディフェンスを有効にする]** を使用してセルフディフェンスを有効または無効にします。
4. 変更内容を保存します。

## AM-PPL のサポートの有効化と無効化

Kaspersky Endpoint Security は Microsoft の Antimalware Protected Process Light 技術（以降、「AM-PPL」）をサポートします。AM-PPL は、Kaspersky Endpoint Security のプロセスを悪意のある処理（アプリケーションの終了など）から保護します。AM-PPL が実行を許可するのは信頼するプロセスのみです。Kaspersky Endpoint Security のプロセスは Windows のセキュリティ要件に従って署名されているため、信頼するプロセスとして扱われます。AM-PPL 技術について詳しくは、[Microsoft の Web サイトの情報](#)を参照してください。既定では、AM-PPL 技術が有効です。

また、Kaspersky Endpoint Security には製品のプロセスを保護するための機構が組み込まれています。AM-PPL のサポートにより、プロセスのセキュリティ機能をオペレーティングシステムに委任できます。したがって、本製品の動作速度を向上し、コンピューターリソースの消費量を削減できます。

AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。

AM-PPL 技術を有効または無効にするには：

1. [製品のセルフディフェンス機構を無効](#)にします。

セルフディフェンス機構は、AM-PPL の状態の変更を含めて、コンピューターメモリ内で本製品のプロセスが変更されたり削除されたりしないようにします。

2. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。

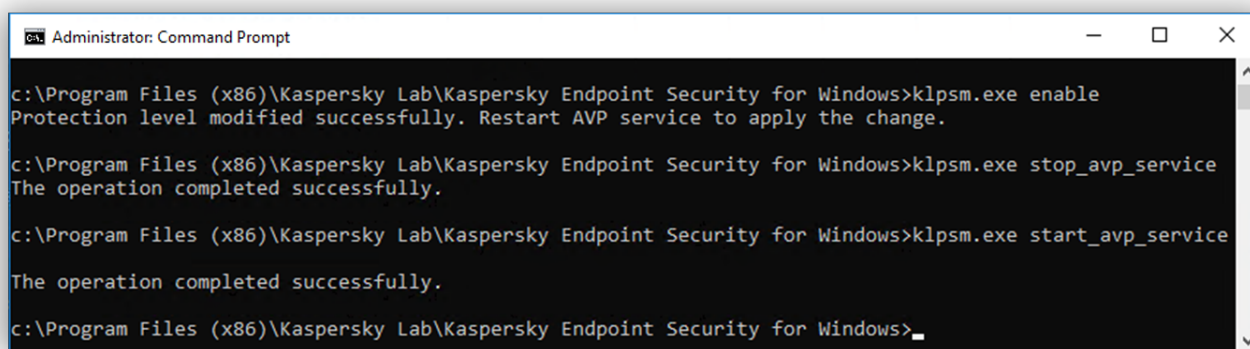
3. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

4. コマンドラインに以下のように入力します：

- `klpsm.exe enable` – AM-PPL 技術のサポートを有効にします（次の図を参照）。
- `klpsm.exe disable` – AM-PPL 技術のサポートを無効にします。

5. Kaspersky Endpoint Security を再起動します。

6. [製品のセルフディフェンス機構を再び有効](#)にします。



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

AM-PPL 技術のサポートの有効化


## 外部からの管理に対する防御の有効化と無効化

外部からの管理に対する防御は、TeamViewer または RemotelyAnywhere などの遠隔管理アプリケーションからの Kaspersky Endpoint Security へのアクセスをブロックします。この機構には次の外部からの管理に対する防御機能が含まれます：

- Kaspersky Endpoint Security の設定の変更からの保護。
- Kaspersky Endpoint Security サービス（AVP サービスなど）の保護。
- 製品プロセスの保護。

外部からの管理に対する保護は、Windows 7 を除く 32 ビットのオペレーティングシステムを実行するコンピューターにのみ使用可能です。Windows 7 に関しては、32 ビットおよび 64 ビットのオペレーティングシステムで使用できます。

外部からの管理に対する保護を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【全般設定】** の順に選択します。
3. **【遠隔操作アプリケーションを利用した Kaspersky Endpoint Security 設定の変更を許可する】** を使用して、外部からの管理に対する防御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、遠隔管理アプリケーションを使用して Kaspersky Endpoint Security を設定したり、サービスやプロセスを管理することができます。  
チェックボックスをオフにすると、外部からの管理に対する防御により、遠隔管理アプリケーションを使用して Kaspersky Endpoint Security にアクセスすることができなくなります。特定の遠隔管理アプリケーションを使用した Kaspersky Endpoint Security の設定を許可することができます。そのためには、[信頼リストに遠隔管理アプリケーションを追加](#)する必要があります。この場合も、遠隔管理に対する防御機構は Kaspersky Endpoint Security のサービスやプロセスへの遠隔管理アプリケーションからのアクセスをブロックします。
4. **【外部からの管理を有効にする】** を使用して Kaspersky Endpoint Security の外部からの管理に対する保護を有効または無効にします。

コマンドラインから本製品を停止するには、Kaspersky Endpoint Security サービスの外部からの管理に対する保護を無効にします。


5. 変更内容を保存します。

外部からの管理に対する保護を有効にすると、Kaspersky Endpoint Security は製品ウィンドウにマウスポインタを合わせる動作をブロックします。リモートユーザーが製品サービスをシャットダウンしようとする、エラーメッセージが表示されたシステムウィンドウが表示されます。

## リモート管理アプリケーションのサポート

外部からの管理に対する防御が有効になっているとき、リモート管理アプリケーションの使用が必要になる場合があります。

リモート管理アプリケーションの操作を有効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【脅威と除外リスト】** を選択します。
3. **【除外リスト】** ブロックで、**【信頼するアプリケーションの指定】** をクリックします。

4. **【追加】** をクリックします。
5. リモート管理アプリケーションの実行ファイルを選択します。  
手動でパスを入力することもできます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。
6. **【アプリケーションの動作を監視しない】** をオンにします。
7. 変更内容を保存します。

# Kaspersky Endpoint Security のパフォーマンスと他のアプリケーションとの互換性

## Kaspersky Endpoint Security のパフォーマンス

Kaspersky Endpoint Security のパフォーマンスは、電力の消費量やコンピューターリソースの使用率だけでなく、コンピューターに損害を与える可能性があるオブジェクトのうち、どの種別のオブジェクトを検知対象に含めるかにも影響されます。

### 検知可能なオブジェクトの選択

Kaspersky Endpoint Security では、コンピューターで実行する保護機能の内容を詳細に調整し、動作中に検知する オブジェクトの種別 を選択できます。Kaspersky Endpoint Security は必ずオペレーティングシステムのウイルス、ワーム、トロイの木馬をスキャンします。これらのオブジェクト種別のスキャンを無効にすることはできません。このようなマルウェアはコンピューターに重大な損害を与える可能性があります。コンピューターのセキュリティをさらに強化する場合は、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアの監視を有効にして、検知できるオブジェクト種別の範囲を拡大できます。

### 省エネモードの使用

アプリケーションの電力使用量は、ノートパソコンにとって重要な考慮事項です。Kaspersky Endpoint Security のスケジュールタスクは、通常、大量のリソースを消費します。コンピューターがバッテリー電源で稼働しているときには、省エネモードを使用することで、電力消費量を抑えることができます。

省エネモードでは、次のスケジュールされているタスクが自動的に延期されます：

- アップデートタスク
- 完全スキャンタスク
- 簡易スキャンタスク
- オブジェクトスキャンタスク
- 整合性チェックタスク

省エネモードが有効になっているかどうかとは関係なく、ノートパソコンの電源がバッテリー電源に切り替わると、Kaspersky Endpoint Security は暗号化タスクを一時停止します。ノートパソコンがバッテリー電源から主電源に切り替わると、暗号化タスクが再開されます。

### 他のアプリケーションに対するコンピューターリソースの優先割り当て

Kaspersky Endpoint Security によるコンピューターリソースの使用は、他のアプリケーションのパフォーマンスに影響する可能性があります。CPU およびハードディスクサブシステムの負荷が増大しているときに複数のアプリケーションが同時に動作することで発生する問題を解決するために、Kaspersky Endpoint Security は、スケジュールタスクを一時停止して他のアプリケーションにシステムリソースを優先的に割り当てることができます。

ただし、CPU リソースが使用可能な状態になった時点で、多数のアプリケーションがすぐに開始され、バックグラウンドで稼働し続けます。スキャンが他のアプリケーションのパフォーマンスに依存しないようにするには、オペレーティングシステムのリソースを他のアプリケーションに割り当てないでください。



必要に応じて、このようなタスクは手動で開始できます。

## 特別な駆除技術の使用

最近の悪意のあるアプリケーションは、オペレーティングシステムの最も深いレベルに侵入できるため、除去は、ほとんど不可能です。Kaspersky Endpoint Security はオペレーティングシステムで悪意のある活動を検知した後、特別な駆除技術を使用した広範囲な駆除処理を実行します。この特別な駆除技術の目的は、RAM 内部でそのプロセスを既に開始している悪意のあるプログラムをオペレーティングシステムから除去して Kaspersky Endpoint Security が他の方法でそれらのアプリケーションを除去しないようにすることです。その結果、脅威が駆除されます。特別な駆除を実行している間は、新しいプロセスの起動やオペレーティングシステムレジストリの修正を行わないように指示されます。特別な駆除には大量のオペレーティングシステムリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。


クライアントコンピューター用 Microsoft Windows が実行されているコンピューターで、特別な駆除処理が完了した後、Kaspersky Endpoint Security は、ユーザーにコンピューターを再起動する許可を求めます。システムの再起動後、Kaspersky Endpoint Security はマルウェアファイルを削除し、コンピューターで「簡易版」の完全スキャンを開始します。

Kaspersky Endpoint Security の特性のため、サーバー用の Microsoft Windows が実行されているコンピューターではユーザーに再起動を実行してよいか確認メッセージを表示してから再起動することはできません。サーバーの予定外の再起動が問題を引き起こし、サーバーのデータが一時的に使用できなくなったり、保存されていないデータが失われたりする原因となることがあります。サーバーの再起動は、スケジュールに厳密に従ってください。この理由で、サーバーでは特別な駆除技術が既定で無効になっています。

サーバーでアクティブな感染が検知された場合、特別な駆除が必要であるという情報とともにイベントが Kaspersky Security Center へ送信されます。サーバーのアクティブな感染を駆除するには、サーバーの特別な駆除技術を有効化し、サーバーユーザーの都合のよい時間に、ウイルススキャングループタスクを開始します。

## 検知可能なオブジェクトの選択

検知可能なオブジェクトを選択するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[脅威と除外リスト]** を選択します。
3. **[検知するオブジェクトの種別]** セクションで、チェックボックスを使用して Kaspersky Endpoint Security が検知するオブジェクトの種類を選択します：

- **ウイルス、ワーム**

## サブカテゴリ：ウイルスやワーム (Viruses\_and\_Worms)

危険性：高

古典的なウイルスやワームは、ユーザーが許可していない処理を実行します。このようなウイルスやワームは、自己複製が可能な自身のコピーを作成することができます。

### 古典的ウイルス

古典的ウイルスがコンピューターに侵入すると、ファイルに感染して活動を開始し、悪意のある処理を実行し、それ自体のコピーを他のファイルに追加します。

古典的ウイルスは、コンピューターのローカルリソースでしか増殖しないため、自力で他のコンピューターに侵入できません。このウイルスが別のコンピューターに感染するのは、ウイルス自身のコピーを共有フォルダーに保管されているファイルまたは挿入された CD に追加したときや、ユーザーが感染したファイルを添付したメールを転送したときです。

古典的ウイルスのコードはコンピューター、オペレーティングシステム、アプリケーションの各種領域に侵入する可能性があります。環境により、ウイルスは、ファイルウイルス、ブートウイルス、スクリプトウイルス、およびマクロウイルスに分けられます。

ウイルスはさまざまな技法を駆使してファイルを感染させます。上書きウイルスは、そのコードを、感染したファイルのコードに上書きして、そのファイルの内容を消去します。感染したファイルは機能しなくなり、復元できません。寄生ウイルスは、ファイルを変更しますが、ファイルが完全にまたは部分的に機能する状態を維持します。コンパニオンウイルスは、ファイルを変更しませんが、代わりに複製を作成します。感染したファイルが開かれると、ウイルスの複製（実際にはこれがウイルス）が起動します。他にも、次のような種別のウイルスが見つかっています：リンクウイルス、OBJウイルス、LIBウイルス、ソースコードウイルスなど多数。

### ワーム

古典的ウイルスのコードと同様に、ワームのコードは、コンピューターに侵入してから活動を開始し、悪意のある処理を実行します。ワームは、コンピューターから別のコンピューターに「這うように移動」し、ユーザーの許可なく多数のデータチャネルを経由してコピーを拡散させることから、この名が付けられました。

さまざまなワームの種類を区別する主な特徴は、その拡散方法です。次のテーブルに、拡散方法によって分類される各種ワームの概要を示します：

ワームの拡散方法

種別	Name	説明
メールワーム	メールワーム	これらのワームはメールを介して広がります。 感染したメールには、ワームのコピーを含んだ添付ファイル、あるいは感染した Web サイトまたは感染させる目的で作成された Web サイトにアップロードされるファイルへのリンクが含まれています。添付ファイルを開くと、ワームが起動します。リンクをクリックし、ファイルをダウンロードして開くと、ワームも悪意のある処理を実行し始めます。その後、ワームは他のメールアドレスを検索して、これらのアドレスに感染メールを送信しながら、自身のコピーを拡散し続けます。
IMワーム	IMクライアントワーム	インスタントメッセージ (IM) クライアント経由で拡散します。 通常、このようなワームは、ユーザーの連絡先リストを使用して、ワームのコピーに感染した Web サイト上のファイルへのリンクを含んだメールを送信します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。

IRC ワーム	インターネットチャットワーム	<p>このワームはインターネットリレーチャット（インターネット上の別のユーザーとリアルタイムで通信できるサービスシステム）を介して拡散します。</p> <p>この種のワームは、インターネットチャットで自身のコピーを含むファイルまたはそのファイルへのリンクを公開します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。</p>
インターネットワーム (Net-Worm)	ネットワークワーム	<p>これらのワームは、コンピューターネットワークを介して広がります。</p> <p>通常のネットワークワームは、他の種類のワームと異なり、ユーザーが参加していなくても拡散します。このワームはプライベートネットワークに、脆弱性のあるプログラムがインストールされたコンピューターがないか探します。この操作を行うために、このワームはワームコードまたはその一部を含む特別に形成されたネットワークパケット（エクスプロイト）を送信します。ネットワーク上に「脆弱な」コンピューターが存在すると、そのコンピューターはこのようなネットワークパケットを受信します。ワームが完全にコンピューターに侵入すると、ワームが起動します。</p>
P2P ワーム	ファイル共有ネットワークワーム	<p>peer-to-peer のファイル共有ネットワーク経由で拡散します。</p> <p>P2P ネットワークに潜入するために、ワームはそれ自身をファイル共有フォルダーにコピーします。このフォルダーは通常、ユーザーのコンピューター上にあります。P2P ネットワークでは、ネットワーク上の感染したファイルをユーザーが他のファイルと同様に「見つけ」、このファイルをダウンロードして開くように、このファイルに関する情報が表示されます。</p> <p>さらに巧妙なワームは特定の P2P ネットワークのネットワークプロトコルを装って検索クエリに肯定応答を返し、自身のコピーをダウンロードさせます。</p>
ワーム	他の種類のワーム	<p>他の種類のワームには、以下のものがあります：</p> <ul style="list-style-type: none"> <li>自身のコピーをネットワークリソースを介して拡散するワーム。このようなワームは、オペレーティングシステムの機能を使って使用可能なネットワークフォルダーを検索し、インターネット上のコンピューターへ接続し、このコンピューターのディスクドライブへのフルアクセス権を取得しようと試みます。他の種類のワームは上記種類のワームとは異なり、自力で起動するのではなく、ユーザーがワームのコピーを含むファイルを開いたときに起動します。</li> <li>上記のどの拡散方法も使用しないワーム（携帯電話を通じて拡散するワームなど）。</li> </ul>

• [トロイの木馬](#)

## サブカテゴリ：トロイの木馬

危険性：高

ワームやウイルスとは異なり、トロイの木馬は自己複製しません。たとえば、ユーザーが感染している Web サイトにアクセスすると、トロイの木馬はメールやブラウザからコンピューターに侵入します。トロイの木馬は、ユーザーの関与によって起動します。起動直後に、悪意のある処理を実行し始めます。

トロイの木馬は多種多様で、感染コンピューター上でのふるまいも多岐にわたります。トロイの木馬の主な機能は、情報のブロック、改変、破壊、およびコンピューターまたはネットワークの無効化です。また、トロイの木馬はファイルの送受信、ファイルの実行、画面上へのメッセージの表示、Web サイトの要求、プログラムのダウンロードとインストール、コンピューターの再起動を行うこともできます。

多くの場合、ハッカーはトロイの木馬の「セット」を使用します。

次のテーブルでは、トロイの木馬における動作の種類について説明します。

感染コンピューターにおけるトロイの木馬の動作種類

種別	Name	説明
Trojan-ArcBomb	トロイの木馬 - 「圧縮爆弾」	このアーカイブは、解凍するとコンピューターの動作に影響を与える程度のサイズにまで膨張します。  ユーザーがこのようなアーカイブを解凍しようとする、コンピューターは処理速度が低下したりフリーズしたりすることがあります。また、ハードディスクが「空の」データで満杯になることがあります。「圧縮爆弾」は、特にファイルサーバーやメールサーバーにとって危険です。サーバーが自動システムを使用して受信情報を処理すると、「圧縮爆弾」によってサーバーが停止することがあります。
バックドア	リモート管理用のトロイの木馬	このプログラムは、トロイの木馬の中でも最も危険なものと考えられます。機能面で、コンピューターにインストールされるリモート管理アプリケーションに似ています。  これらのプログラムは、ユーザーに気付かれずにコンピューターにインストールされるので、侵入者はコンピューターを遠隔管理できます。
トロイの木馬	トロイの木馬	トロイの木馬には、次のような悪意のあるアプリケーションがあります：  <ul style="list-style-type: none"><li>• <b>古典的なトロイの木馬</b>：これらのプログラムはトロイの木馬の主な機能（情報のブロック、改変または破壊、およびコンピューターまたはネットワークの無効化）のみを実行し、テーブルに示す他の種類のトロイの木馬とは異なり、高度な機能を持っていません。</li><li>• <b>多目的なトロイの木馬</b>：これらのプログラムは、数種類のトロイの木馬に特徴的な先進機能を備えています。</li></ul>
Trojan-Ransom	トロイの木馬型ランサムウェア	このプログラムは、ユーザーの情報を「人質」にとって改変したり、ブロックしたりします。また、ユーザーが情報を使用する能力を喪失するように、コンピューターの動作に影響を与えます。侵入者は、コンピューターのパフォーマンスと保存されていたデータを復元するアプリケーションを送るという約束と引き替えに、ユーザーから身代金を要求します。
Trojan-Clicker	トロイの木馬	このプログラムは、ブラウザにコマンドを送信するか、オペレーティングシステムファイルで指定されている Web アドレスを変更する

	クリッカー	<p>ことによって、ユーザーのコンピューターから Web サイトにアクセスします。</p> <p>侵入者はこのようなプログラムを使用することによって、ネットワーク攻撃を行って Web サイトのアクセス数を増やし、バナー広告の表示回数を増やします。</p>
Trojan-Downloader	トロイの木馬ダウンロード	<p>これは侵入者の Web サイトにアクセスして、そこから他の悪意のあるアプリケーションをダウンロードし、ユーザーのコンピューターにインストールします。このプログラムには、悪意のあるアプリケーションをダウンロードまたは受信するためにアクセスした Web サイトのファイル名が含まれていることがあります。</p>
Trojan-Dropper	トロイの木馬ドロッパー	<p>このプログラムは他のトロイの木馬を内包しており、この内包されたプログラムがハードディスクにインストールされ、実行されます。</p> <p>侵入者は、トロイの木馬ドロッパー型プログラムを次のような目的で使用することがあります：</p> <ul style="list-style-type: none"> <li>• ユーザーに気付かれずに悪意のあるプログラムをインストールする：トロイの木馬ドロッパー型プログラムは、メッセージを表示しないか、たとえば、アーカイブ中にエラーが発生したことやオペレーティングシステムが互換性のないバージョンであることを示すといった偽のメッセージを表示します。</li> <li>• 既知の悪意のある別のアプリケーションが検知されないようにする：すべてのアンチウイルスのソフトウェアがトロイの木馬ドロッパー型アプリケーション内の悪意のあるアプリケーションを検知できるわけではありません。</li> </ul>
Trojan-Notifier	トロイの木馬型ノーティファイア	<p>このプログラムは、感染したコンピューターにアクセスできることを侵入者に教えるため、コンピューターの次のような情報を侵入者に送信します：IP アドレス、開いているポートの番号、メールアドレスなど。このプログラムはこれらの情報をメール、FTP、侵入者の Web サイトへのアクセス、あるいはこれら以外の方法で侵入者に送ります。</p> <p>トロイの木馬型ノーティファイアプログラムは、多くの場合、複数のトロイの木馬からなるセットとして使用されます。また、このプログラムはトロイの木馬がユーザーのコンピューターにインストールされたことを侵入者に知らせます。</p>
Trojan-Proxy	トロイの木馬型プロキシ	<p>これらのトロイの木馬により、侵入者は、ユーザーのコンピューターを使って匿名で Web サイトにアクセスします。このトロイの木馬はスパムの送信によく利用されます。</p>
Trojan-PSW	パスワード窃盗ソフトウェア	<p>パスワード窃盗ソフトウェアは、ソフトウェア登録データなどのユーザーアカウントを盗むトロイの木馬の一種です。このトロイの木馬はシステムファイルおよびレジストリ内の機密データを見つけ、そのデータを「攻撃者」にメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって送信します。</p> <p>これらのトロイの木馬のうち、いくつかがこのテーブルに示す種類に分類されます。これらは、銀行のアカウント情報 (Trojan-Banker)、メッセンジャークライアントのユーザーのデータ (Trojan-IM)、およびオンラインゲームのユーザーの情報 (Trojan-GameThief) を盗むトロイの木馬です。</p>
Trojan-Spy	スパイウェア型トロイの木馬	<p>このトロイの木馬はコンピューター上で動作しながら、ユーザーが行う処理に関する情報を収集して、ユーザーの行動を秘密裏に監視します。このトロイの木馬は、ユーザーがキーボードで入力するデータの傍受、スクリーンショットの撮影、あるいはアクティブなアプリケーションのリストの収集などを行うことがあります。このプログラムが</p>



		<p>情報を入力すると、その情報をメールやFTPで送信する、あるいは侵入者のWebサイトにアクセスするなどによって侵入者に転送します。</p>
<b>Trojan-DDoS</b>	<p>トロイの木馬ネットワークアタッカー</p>	<p>このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、またはDoS攻撃）。ハッカーは、1台のサーバーを多数のコンピューターから同時に攻撃できるように、このプログラムを利用して多数のコンピューターを感染させることがあります。</p> <p>DoSプログラムは1台のコンピューターから、ユーザーに気付かれることなく攻撃を実行します。DDoS（分散DoS）プログラムは、感染したコンピューターのユーザーに気付かれずに、複数のコンピューターから分散して攻撃を行います。</p>
<b>Trojan-IM</b>	<p>メッセージクライアントのユーザーから情報を盗むトロイの木馬</p>	<p>このトロイの木馬は、メッセージクライアントのユーザーのアカウント番号とパスワードを盗みます。このプログラムは、データをメールやFTPで送信する、あるいは侵入者のWebサイトにアクセスするなどによって侵入者に転送します。</p>
<b>ルートキット</b>	<p>ルートキット</p>	<p>ルートキットは、他の悪意のあるアプリケーションやその活動を隠蔽します。そのため、このアプリケーションはオペレーティングシステムに長期間潜入します。また、ルートキットはファイル、感染しているコンピューターのメモリ内のプロセス、または悪意のあるアプリケーションを実行するレジストリキーを隠蔽することもできます。さらにルートキットは、ユーザー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とネットワーク上の他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間で行われるデータ交換を隠蔽できます。</p>
<b>Trojan-SMS</b>	<p>SMSメッセージ形式のトロイの木馬</p>	<p>このトロイの木馬は携帯電話を感染させ、高額の通話料が発生する電話番号にSMSメッセージを送信します。</p>
<b>Trojan-GameThief</b>	<p>オンラインゲームのユーザーから情報を盗むトロイの木馬</p>	<p>このトロイの木馬は、オンラインゲームのユーザーのアカウント情報を盗み、このデータを侵入者にメールやFTPで送信するか、侵入者のWebサイトにアクセスするなどによって送信します。</p>
<b>Trojan-Banker</b>	<p>銀行のアカウント情報を盗むトロイの木馬</p>	<p>このトロイの木馬は、銀行のアカウント情報や電子マネーシステムのデータを盗み、このデータをメールやFTPを使用して侵入者に送信するか、侵入者のWebサイトにアクセスするなどして送信します。</p>

Trojan-Mailfinder	メールアドレスを収集するトロイの木馬	このトロイの木馬は、コンピューターに保存されているメールアドレスを収集し、侵入者にメールやFTPで送信するか、侵入者のWebサイトにアクセスするなどによって送信します。侵入者が収集したアドレスにスパムを送信することがあります。
-------------------	--------------------	---

- [悪意のあるツール](#) 



## サブカテゴリ：悪意のあるツール

危険度：中

悪意のあるツールは、他の種類のマルウェアとは異なり、起動した直後に処理を実行しません。このプログラムはユーザーのコンピューターに安全に侵入し、そこで起動することができます。侵入者は、多くの場合、悪意のあるツールの機能を悪用して、ウイルス、ワーム、トロイの木馬を作成したり、リモートサーバーに対してネットワーク攻撃を仕掛けたりします。

悪意のあるツールのさまざまな機能を、次のテーブルに示す種類別に分類しています：

悪意のあるツールの機能

種別	Name	説明
コンストラクター	コンストラクター	このツールを使用して、新しいウイルス、ワームおよびトロイの木馬を作成します。一部のコンストラクターは標準的なウィンドウベースのインターフェイスを備えています。このインターフェイスでは、悪意のあるアプリケーションの種類を選択して、デバッガを無効にする手段やその他の機能を作成できます。
Dos	ネットワーク攻撃	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。
エクスプロイト	エクスプロイト	<p>エクスプロイトは、処理されるアプリケーションの脆弱性を利用する一連のデータまたはプログラムコードで、コンピューター上で悪意のある処理を実行します。たとえば、エクスプロイトは、ファイルの書き込みまたは読み取り、あるいは「感染している」Web サイトの要求を行うことができます。</p> <p>それぞれのエクスプロイトは、さまざまなアプリケーションまたはネットワークサービスの脆弱性を利用します。ネットワークパケットに偽装したエクスプロイトは、ネットワーク経由で多数のコンピューターに送信され、脆弱なネットワークサービスを備えるコンピューターを探します。DOC ファイルのエクスプロイトは、テキストエディターの脆弱性を利用します。このエクスプロイトは、ユーザーが感染したファイルを開いたときに、ハッカーが事前にプログラミングした処理を開始することがあります。メールに組み込まれたエクスプロイトは、メールクライアントの脆弱性を探します。このエクスプロイトは、ユーザーがメールクライアントの感染メールを開くとすぐに悪意のある処理を実行します。</p> <p>エクスプロイトを使用してネットワーク上に拡散するのがネットワームです。ヌーカー型エクスプロイトは、コンピューターを無効にするネットワークパケットです。</p>
FileCryptor	エンクリプター	このプログラムは、他の悪意のあるアプリケーションを暗号化してアンチウイルス製品から隠蔽します。
Flooder	ネットワークを「汚染する」ため	<p>このプログラムは大量のメールをネットワークチャネル上に送信します。この種のツールには、インターネットリレーチャットなどを汚染するプログラムがあります。</p> <p>Flooder 型ツールには、メール、IM クライアントおよびモバイル通信システムで使用されるチャネルを「汚染する」プログラムは含まれません。これらのプログラムは、テーブルに示す別種（Email-Flooder、IM-Flooder および SMS-Flooder）として区別されます。</p>

	のプログラム	
HackTool	ハッキングツール	このプログラムは、たとえば、ユーザーの許可なしに新しいシステムアカウントを追加したり、システムログを消去してオペレーティングシステムにおける存在の痕跡を隠蔽したりすることによって、このプログラムがインストールされたコンピュータをハッキングすることや別のコンピュータを攻撃することを可能にします。この種のツールには、パスワードの傍受などの悪意のある機能の特徴とする一部のスニファーが含まれます。スニファーは、ネットワークトラフィックの監視を可能にするプログラムです。
Hoax	デマウイルス	このプログラムはウイルスメッセージに似たメッセージでユーザーに注意を喚起します。具体的には、感染していないファイルで「ウイルスを検知した」というメッセージや、実際にはディスクのフォーマットが発生しなかったのに、ディスクがフォーマットされたというメッセージを表示します。
スプーファ	スプーフィングツール	このツールは、メッセージ要求やネットワーク要求を送信者の偽装アドレスで送信します。たとえば、侵入者はスプーファ型のツールを使用して、ツール本体をメールの実際の送信者として渡します。
VirTool	悪意のあるアプリケーションを改変するツール	このツールを使用すると、他のマルウェアを改変して、アンチウイルス製品から隠蔽することができます。
Email-Flooder	メールアドレスを「汚染する」プログラム	このプログラムはさまざまなメールアドレスに大量のメールを送信して、これらのメールアドレスを「汚染」します。大量の受信メールによって、ユーザーは必要なメールを受信ボックスで表示できなくなります。
IM-Flooder	メッセージクライアントのトラフィックを「汚染する」	IMクライアントのユーザーをメッセージであふれさせます。大量のメールが送られてくるため、ユーザーは必要な受信メールを表示できなくなります。

	プログラム	
SMS-Flooder	トラフィックをSMSメッセージで「汚染する」プログラム	このプログラムは携帯電話に大量のSMSメッセージを送信します。

- [アドウェア](#)

**サブカテゴリ**：広告ソフトウェア（アドウェア）

**危険性**：中

アドウェアはユーザーに対して広告情報を表示します。アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。このようなプログラムには、ユーザーに関するマーケティング情報を収集し、それを開発者に送信するものがあります。この情報には、ユーザーが表示した Web サイトの名前や、ユーザーの検索の内容などが含まれます。スパイウェア型のトロイの木馬とは異なり、アドウェアは、このような情報をユーザーの同意を得てから開発者に送ります。

- [オートダイヤラー](#)

**サブカテゴリ：**ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェア。

**危険度：**中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

種別	Name	説明
Client-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダイヤラー	オートダイヤラー	これらのプログラムは、モデムを介してひそかに電話接続を確立できます。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他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とどのようにデータをやり取りしているかを監視する）。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理プログラム	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。

		合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。
Server-FTP	FTPサーバー	このプログラムはFTPサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、FTP経由でコンピュータへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnetサーバー	このプログラムはTelnetサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、Telnet経由でコンピュータへのリモートアクセスを開きます。
Server-Web	Webサーバー	このプログラムはWebサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、HTTP経由でコンピュータへのリモートアクセスを開きます。
RiskTool	ローカルコンピュータで動作するツール	このプログラムは、ユーザーのコンピュータで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピュータで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピュータを再起動して、開いているポートを検知し、コンピュータにインストールされているアプリケーションを起動することができます。
Client-P2P	P2Pネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
Client-SMTP	SMTPクライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピュータに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Webツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

- ユーザーに損害を与える目的で悪用される可能性があるその他のソフトウェアを検出する ②

**サブカテゴリ：**ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェア。

**危険度：**中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

種別	Name	説明
Client-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダイヤラー	オートダイヤラー	これらのプログラムは、モデムを介してひそかに電話接続を確立できます。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他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とどのようにデータをやり取りしているかを監視する）。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理プログラム	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。



		合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。
Server-FTP	FTPサーバー	このプログラムはFTPサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、FTP経由でコンピュータへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnetサーバー	このプログラムはTelnetサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、Telnet経由でコンピュータへのリモートアクセスを開きます。
Server-Web	Webサーバー	このプログラムはWebサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピュータに埋め込み、HTTP経由でコンピュータへのリモートアクセスを開きます。
RiskTool	ローカルコンピュータで動作するツール	このプログラムは、ユーザーのコンピュータで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピュータで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピュータを再起動して、開いているポートを検知し、コンピュータにインストールされているアプリケーションを起動することができます。
Client-P2P	P2Pネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
Client-SMTP	SMTPクライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピュータに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Webツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

## • 悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト

Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に圧縮オブジェクトやアンパッカーモジュールがないかスキャンします。

侵入者は、危険なプログラムをアンチウイルス製品から隠蔽するために、特殊なパッカーを使用して危険なプログラムを保存するか、多重圧縮したファイルを作成します。

カスペルスキーのウイルスアナリストは、ハッカーの中で最も使用されているパッカーを識別しています。

Kaspersky Endpoint Security によってそのようなパッカーがファイル内に検知された場合、そのファイルには非常に高い確率で、悪意のあるアプリケーションやユーザーに損害を与える目的で悪用される可能性があるアプリケーションが含まれています。

Kaspersky Endpoint Security は、次のようなプログラムを検知します：

- 損害を与える可能性がある圧縮ファイル - マルウェア（ウイルス、ワーム、トロイの木馬など）を圧縮するために使用されます。
- 多重圧縮ファイル（危険性「中」） - 1個以上のパッカーによって3回圧縮されたオブジェクト。

## • 多重圧縮オブジェクト

Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に圧縮オブジェクトやアンパッカーモジュールがないかスキャンします。

侵入者は、危険なプログラムをアンチウイルス製品から隠蔽するために、特殊なパッカーを使用して危険なプログラムを保存するか、多重圧縮したファイルを作成します。

カスペルスキーのウイルスアナリストは、ハッカーの中で最も使用されているパッカーを識別しています。

Kaspersky Endpoint Security によってそのようなパッカーがファイル内に検知された場合、そのファイルには非常に高い確率で、悪意のあるアプリケーションやユーザーに損害を与える目的で悪用される可能性があるアプリケーションが含まれています。

Kaspersky Endpoint Security は、次のようなプログラムを検知します：

- 損害を与える可能性がある圧縮ファイル - マルウェア（ウイルス、ワーム、トロイの木馬など）を圧縮するために使用されます。
- 多重圧縮ファイル（危険性「中」） - 1個以上のパッカーによって3回圧縮されたオブジェクト。


4. 変更内容を保存します。

## サーバー向けの特別な駆除の有効化または無効化

Kaspersky Endpoint Security がマルウェアの実行を停止できない場合、特別な駆除技術を使用することができません。特別な駆除には大量のコンピューターリソースが必要になるため、既定では特別な駆除は無効になっています。そのため、特別な駆除は アクティブな脅威に対する操作 を行うときのみ有効にしてください。

特別な駆除はワークステーションとサーバーに対して異なる動作をします。サーバーでこの技術を使用する場合は、ウイルススキャンタスクのプロパティで [\[すぐに特別な駆除を実行する\]](#) を有効にする必要があります。ワークステーションでこの技術を使う場合、事前準備は必要ありません。


サーバー向けの特別な駆除を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[全般設定]** の順に選択します。
3. **[操作モード]** で、**[特別な駆除を有効にする]** をオンまたはオフにして、特別な駆除技術を有効または無効にします。
4. 変更内容を保存します。

特別な駆除が実行されている間、ユーザーはオペレーティングシステムの多くの機能を使用できなくなります。駆除が完了すると、コンピューターは再起動されます。

## 省エネモードの有効化または無効化

省エネモードを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[脅威と除外リスト]** を選択します。
3. **[パフォーマンス]** セクションで、**[バッテリー使用中はスケジュールタスクを延期する]** を使用して省エネモードを有効または無効にします。


省エネモードが有効のときは、コンピューターがバッテリーの電力で動作している場合、以下のタスクがスケジュールされていても実行されません。

- アップデートタスク
- 完全スキャンタスク
- 簡易スキャンタスク
- オブジェクトスキャンタスク
- 整合性チェックタスク

4. 変更内容を保存します。

## 他のアプリケーションへのリソースの供与の有効化または無効化

他のアプリケーションへのリソースの供与を有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**[詳細設定]** → **[全般設定]** の順に選択します。

3. [パフォーマンス] セクションで、[他のアプリケーションにシステムリソースを優先的に割り当てる] を使用して他のアプリケーションへのリソースの供与を有効または無効にします。

他のアプリケーションにリソースを割り当てるように設定されている場合、Kaspersky Endpoint Security は、他のアプリケーションの実行速度を遅くするような、スケジュールされているタスクを延期します。

- アップデートタスク
- 完全スキャンタスク
- 簡易スキャンタスク
- オブジェクトスキャンタスク
- 整合性チェックタスク

既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。


4. 変更内容を保存します。

## 設定ファイルの作成と使用

Kaspersky Endpoint Security の設定を含む設定ファイルを使用すると、次の作業を実行できます：

- 定義済みの設定を使用してコマンドラインから Kaspersky Endpoint Security のローカルインストールを実行する。  
そのためには、設定ファイルを配布パッケージと同じフォルダーに保存する必要があります。
- 定義済みの設定を使用して Kaspersky Security Center から Kaspersky Endpoint Security のリモートインストールを実行する。
- Kaspersky Endpoint Security の設定を別のコンピューターに移行する。


設定ファイルを作成するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【設定の管理】** の順に選択します。
3. **【エクスポート】** をクリックします。
4. 表示されたウィンドウで、設定ファイルを保存するパスを指定し、ファイル名を入力します。

設定ファイルを Kaspersky Endpoint Security のローカルインストールまたはリモートインストールに使用するには、ファイル名を install.cfg にします。

5. **【保存】** をクリックします。

Kaspersky Endpoint Security の設定を設定ファイルから読み込むには：


1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【設定の管理】** の順に選択します。
3. **【インポート】** をクリックします。
4. 表示されたウィンドウで、設定ファイルのパスを入力します。
5. **【開く】** をクリックします。

Kaspersky Endpoint Security のすべての設定値が、選択された設定ファイルに従って設定されます。

## 既定の設定の復元

Kaspersky Endpoint Security の設定は、カスペルスキーが推奨する設定にいつでも戻すことができます。この設定が復元されると、すべての保護機能のセキュリティレベルが **【推奨】** に設定されます。

既定の設定を復元するには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【設定の管理】** の順に選択します。
3. **【復元】** をクリックします。
4. 変更内容を保存します。

## ユーザーと管理者間のメッセージ

[アプリケーションコントロール](#)、[デバイスコントロール](#)、[ウェブコントロール](#)、[アダプティブアノマリーコントロール](#)では、Kaspersky Endpoint Security がインストールされているコンピューターを使用している LAN ユーザーが管理者にメッセージを送信できます。

次の場合に、ユーザーが LAN 管理者にメッセージを送信することがあります：

- デバイスコントロールがデバイスへのアクセスをブロックした。  
ブロックされたデバイスへのアクセスを要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの [[デバイスコントロール](#)] セクションにあります。
- アプリケーションコントロールがアプリケーションの起動をブロックした。  
ブロックされたアプリケーションの起動許可を要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの [[アプリケーションコントロール](#)] セクションにあります。
- ウェブコントロールが Web リソースへのアクセスをブロックした。  
ブロックされた Web リソースへのアクセスを要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの [[ウェブコントロール](#)] セクションにあります。

メッセージの送信方法および使用するテンプレートは、Kaspersky Endpoint Security がインストールされているコンピューター上での Kaspersky Security Center ポリシーの実行状況、および Kaspersky Security Center 管理サーバーとの接続状況によって異なります。可能なシナリオは次のとおりです：

- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center のポリシーが実行中でない場合、ユーザーのメッセージがローカルエリアネットワークの管理者にメールで送信されます。  
本文のフィールドには、Kaspersky Endpoint Security のローカルインターフェイスで定義されたテンプレートのフィールドの値が入力されます。
- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center のポリシーが実行中の場合、標準のメッセージが Kaspersky Security Center 管理サーバーに送信されます。  
この場合、ユーザーメッセージは、Kaspersky Security Center イベント保管領域で確認できます（以下の手順を参照）。本文のフィールドには、Kaspersky Security Center のポリシーで定義されたテンプレートのフィールドの値が入力されます。
- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center モバイルユーザーポリシーが実行中の場合、メッセージの送信方法は Kaspersky Security Center との接続状況によって異なります。
  - Kaspersky Security Center との接続が確立されている場合、標準のメッセージが Kaspersky Security Center 管理サーバーに送信されます。
  - Kaspersky Security Center との接続がない場合、ユーザーのメッセージがローカルエリアネットワークの管理者にメールで送信されます。

どちらの場合も、本文のフィールドには Kaspersky Security Center のポリシーで定義されたテンプレートのフィールドの値が入力されます。

Kaspersky Security Center イベント保管領域にあるユーザーのメッセージを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [**管理サーバー**] フォルダーで、 [**イベント**] タブを選択します。



Kaspersky Security Center の作業領域に、LAN ユーザーから受信した管理者向けメッセージを含む、Kaspersky Endpoint Security の動作時に発生したすべてのイベントが表示されます。

3. イベントのフィルターを設定するには、**「イベントの抽出」** で **「ユーザー要求」** を選択します。
4. 管理者に送信するメッセージを選択します。
5. 管理コンソールの作業領域の右側にある **「イベントのプロパティウィンドウの表示」** をクリックします。

# データ暗号化

Kaspersky Endpoint Security では、ローカルドライブおよびリムーバブルドライブに保存されているファイルやフォルダー、またはリムーバブルドライブおよびハードディスク全体を暗号化できます。データを暗号化すると、ノートパソコン、リムーバブルドライブ、ハードディスクの消失や盗難、承認されていないユーザーやアプリケーションによるデータへのアクセスなどに伴って発生する情報漏洩のリスクを最小限に抑えることができます。Kaspersky Endpoint Security では、Advanced Encryption Standard (AES) 暗号アルゴリズムが使用されます。

ライセンスの有効期間が終了すると、新しいデータの暗号化は行いませんが、暗号化された既存のデータは暗号化されたままで、使用可能です。この場合、新たにデータを暗号化するには、暗号化の使用が許可された新しいライセンスで製品をアクティベートする必要があります。

ライセンスの有効期間が終了した場合や、使用許諾契約書の違反が発生した場合、ライセンスや Kaspersky Endpoint Security、暗号化のコンポーネントが削除された場合、以前に暗号化されたファイルの暗号化状態は保証されなくなります。これは、Microsoft Office Word など一部のアプリケーションが、編集時にファイルの一時的なコピーを作成するためです。元のファイルが保存される時、一時コピーが元のファイルと入れ替わります。その結果、暗号化機能がないコンピューターや暗号化機能にアクセスできないコンピューターでは、ファイルは暗号化されていない状態になります。

Kaspersky Endpoint Security は、次に示すようにデータを多面的に保護します：

- **ローカルコンピュータードライブでのファイルレベルの暗号化**：拡張子や拡張子グループ、ローカルコンピューターのドライブに保存されているフォルダーのリストに基づいて、[ファイルのリストを作成](#)できます。また、[特定のアプリケーションで作成されたファイルを暗号化するルール](#)を作成できます。ポリシーが適用されると、Kaspersky Endpoint Security は以下のファイルを暗号化および復号化します：
  - 暗号化および復号化のリストに追加されたファイル
  - 暗号化および復号化のリストに追加されたフォルダーにあるファイル
  - 別々のアプリケーションによって作成されたファイル
- **リムーバブルドライブの暗号化**：既定の暗号化ルールを指定すると、そのルールに基づいてすべてのリムーバブルドライブに同じ処理を適用できます。また、個々のリムーバブルドライブの暗号化ルールを指定することもできます。

既定の暗号化ルールの優先度は、個々のリムーバブルドライブに対して作成された暗号化ルールよりも低くなります。指定されたデバイスモデルのリムーバブルドライブについて作成された暗号化ルールの優先度は、指定されたデバイス ID のリムーバブルドライブについて作成された暗号化ルールよりも低くなります。

Kaspersky Endpoint Security は、リムーバブルドライブ上のファイルの暗号化ルールを選択するために、デバイスモデルと ID が既知かどうかをチェックします。チェック後、次のいずれかの操作が行われます：

- デバイスモデルのみが既知の場合は、特定のデバイスモデルのリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。
- デバイス ID のみが既知の場合は、特定のデバイス ID のリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。
- デバイスモデルもデバイス ID も既知の場合は、特定のデバイス ID のリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。そのようなルールが存在せず、特定のデバイスモデルのリムーバブルドライブを対象に作成された暗号化ルールが存在する場合、そのルールが適用されます。特定のデバイス ID についても特定のデバイスモデルについても暗号化ルールが設定されていない場合は、既定の暗号化ルールが適用されます。

- デバイスモデルもデバイスIDも未知の場合は、既定の暗号化ルールが適用されます。

ユーザーは、リムーバブルドライブに保存されている暗号化データをポータブルモードで使用できるようリムーバブルドライブを準備できます。ポータブルモード有効にすると、暗号化機能を持たないコンピューターに接続されているリムーバブルドライブ上の暗号化ファイルにアクセスできます。

- **アプリケーションの暗号化ファイルアクセスルールの管理**：任意のアプリケーションについて、暗号化ファイルへのアクセスをブロックしたり暗号化ファイルへのアクセスを暗号文（暗号化が適用された状態の文字列）としてのみ許可したりする暗号化ファイルアクセスルールを作成できます。
- **暗号化されたパッケージへの追加**：暗号化されたアーカイブを作成して、そのアーカイブに対するアクセスをパスワードで保護できます。暗号化されたアーカイブの内容には、アーカイブへのアクセスの保護に使用したパスワードを入力しないとアクセスできません。このアーカイブは、ネットワーク経由またはリムーバブルドライブを使用して安全に転送できます。
- **ディスク全体の暗号化**次の暗号化技術を選択できます：Kaspersky Disk Encryption、BitLocker ドライブ暗号化（単に BitLocker とも）。

*BitLocker* は、Windows オペレーティングシステムの一部です。コンピューターに Trusted Platform Module (TPM) が搭載されている場合、BitLocker は、暗号化されたハードディスクにアクセスするための回復キーを TPM に保管します。コンピューターの起動時、BitLocker は Trusted Platform Module からハードディスク回復キーを要求し、ドライブのロックを解除します。回復キーにアクセスするためにパスワードや暗証番号を使用するよう設定できます。

既定のディスク暗号化のルールを指定して、暗号化から除外するハードディスクのリストを作成できます。Kaspersky Endpoint Security は、Kaspersky Security Center ポリシーが適用されると、ディスク全体をセクター単位で暗号化します。本製品は、ハードディスクのすべての論理パーティションを同時に暗号化します。

システムハードディスクが暗号化されると、次のコンピューターの起動時、ユーザーはハードディスクにアクセスしてオペレーティングシステムを読み込む前に[認証エージェント](#)による認証を完了する必要があります。それには、コンピューターに接続されているトークンまたはスマートカードのパスワードを入力するか、[認証エージェントアカウントの管理](#)タスクを使用して LAN 管理者により作成される認証エージェントアカウントのユーザー名とパスワードを入力します。これらのアカウントは、ユーザーがオペレーティングシステムにログインする際にログインアカウントとして使用する Microsoft Windows アカウントに基づいています。また、認証エージェントアカウントのユーザー名とパスワードを使用してオペレーティングシステムに自動的にログインできる[シングルサインオン \(SSO\) 技術を使用する](#)こともできます。

コンピューターをバックアップしてから、そのコンピューターのデータを暗号化した場合、その後、コンピューターのバックアップコピーを復元し、コンピューターのデータをもう一度暗号化すると、Kaspersky Endpoint Security により、認証エージェントアカウントの複製が作成されます。この複製されたアカウントを削除するには、klmover ユーティリティを dupfix キーを指定して使用します。klmover ユーティリティは、Kaspersky Security Center のビルドに含まれています。この操作の詳細については、Kaspersky Security Center のオンラインヘルプを参照してください。

暗号化されたハードディスクにアクセスできるコンピューターは、ディスク全体の暗号化機能を含む Kaspersky Endpoint Security がインストールされたコンピューターに限定されています。この予防策により、企業のローカルエリアネットワークの外からアクセスが試みられ、暗号化されたハードディスクからデータが漏出するリスクが最小限に抑えられます。

ハードディスクとリムーバブルドライブを暗号化する際、**「使用されているディスク領域のみを暗号化」**機能を使用できます。この機能は、まだ使用されていない新しいデバイスでのみ使用するようにしてください。すでに使用されているデバイスに暗号化を適用する場合、デバイス全体を暗号化するようにしてください。それにより、削除されているが取り出すことのできる情報を含む可能性があるデータを含め、すべてのデータが保護されます。

Kaspersky Endpoint Security は、暗号化を開始する前に、ファイルシステムセクターのマッピングを取得します。暗号化の第1段階では、暗号化を開始した時点でファイルによって占められているセクターが対象になります。暗号化の第2段階で、暗号化が開始された後に書き込まれたセクターが対象になります。暗号化が完了すると、データを含んでいるすべてのセクターが暗号化されます。

暗号化が完了した後にユーザーがファイルを削除すると、削除されたファイルが格納されていたセクターはファイルシステムレベルで新しい情報を格納するために使用可能になりますが、引き続き暗号化されます。このように、ファイルが新しいデバイスに書き込まれ、そのデバイスが **【使用されているディスク領域のみを暗号化】** 機能が有効な状態で定期的に暗号化されていくことで、しばらくするとすべてのセクターが暗号化されます。

ファイルの復号化に必要なデータは、暗号化時にこのコンピューターをコントロールしていた Kaspersky Security Center 管理サーバーから提供されます。暗号化されたオブジェクトを持つコンピューターが何らかの理由で別の管理サーバーによって管理されていた場合、次のいずれかの方法で暗号化されたデータへのアクセスを取得できます：

- 同じ階層の管理サーバー：
  - 追加のアクションを実行する必要はありません。ユーザーは暗号化されたオブジェクトに引き続きアクセスできる。すべての管理サーバーに暗号鍵が配布される。
- 独立した管理サーバー：
  - LAN 管理者に暗号化されたオブジェクトへのアクセスを要求します。
  - 暗号化されたデバイスのデータの復元ツールを使用して復元する。
  - 暗号化時にこのコンピューターを管理していた Kaspersky Security Center 管理サーバーの構成をバックアップコピーから復元し、暗号化されたオブジェクトを持つコンピューターを現在管理している管理サーバーでこの構成を使用する。

暗号化されたデータへのアクセスがない場合は、暗号化されたデータを操作するための特別な指示に従ってください ([暗号化されたファイルへのアクセスの復元処理](#)、[暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用](#))。

## 暗号化機能の制限

データ暗号化には次の制限があります：

- 暗号化時にサービスファイルが作成されます。これらのファイルを保存するために、ハードディスク上でフラグメント化していない約 0.5% の空き容量が必要です。ハードディスク上のフラグメント化していない空き容量が足りない場合は、十分な空き容量が用意されるまで暗号化が開始されません。
- Kaspersky Security Center の管理コンソール および Kaspersky Security Center の Web コンソールですべてのデータ暗号化を管理できます。Kaspersky Security Center Cloud コンソールでは、BitLocker のみ管理できます。
- Kaspersky Security Center 管理システムまたは Kaspersky Security Center Cloud コンソール (BitLocker のみ) とともに Kaspersky Endpoint Security を使用する場合のみ、データ暗号化を利用できます。Kaspersky Endpoint Security は暗号鍵を Kaspersky Security Center に保存するため、Kaspersky Endpoint Security をオフラインモードで使用している場合、データ暗号化は不可能です。
- [サーバー用の Microsoft Windows](#) を実行するコンピューターに Kaspersky Endpoint Security がインストールされている場合、BitLocker ドライブ暗号化技術を使用したディスク全体の暗号化のみ使用できます。ワー

クステーション用の Windows を実行するコンピューターに Kaspersky Endpoint Security がインストールされている場合、データ暗号化機能が完全に利用できます。

Kaspersky Disk Encryption 技術を使用したディスク全体の暗号化は、ハードウェアおよびソフトウェア要件を満たさないハードディスクでは使用できません。

Kaspersky Endpoint Security と Kaspersky Anti-Virus for UEFI のディスク全体の暗号化機能との互換性はサポートされていません。Kaspersky Anti-Virus for UEFI はオペレーティングシステムの読み込み前に起動します。ディスク全体の暗号化を使用している場合、コンピューターにオペレーティングシステムがインストールされていないという検知を行います。これにより、Kaspersky Anti-Virus for UEFI でエラーが発生して動作が終了します。ファイルレベルの暗号化 (FLE) は、Kaspersky Anti-Virus for UEFI の動作に影響しません。

Kaspersky Endpoint Security は、以下の設定をサポートします：

- HDD、SSD および USB ドライブ。

Kaspersky Disk Encryption (FDE) 技術は SSD ドライブのパフォーマンスおよびサービス残存期間が保持されている間は SSD をサポートします。

- バス経由で接続されているドライブ：SCSI、ATA、IEEE1394、USB、RAID、SAS、SATA、NVME。
- SD または MMC バス経由で接続されている非リムーバブルドライブ。
- 512 バイトセクタのドライブ。
- 512 バイトをエミュレートする 4096 バイトセクタのドライブ。
- 次の種別のパーティションを持つドライブ：GPT、MBR、および VBR (リムーバブルドライブ)。
- UEFI 64 およびレガシー BIOS 標準の埋め込みソフトウェア。
- UEFI 標準で Secure Boot がサポートされる埋め込みソフトウェア。

*Secure Boot* は UEFI ローターアプリケーションおよびドライバー向けにデジタル署名を検証するために設計された技術です。Secure Boot は未署名または不明な発行元により署名された UEFI アプリケーションおよびドライバーの開始をブロックします。Kaspersky Disk Encryption (FDE) は Secure Boot をサポートしています。認証エージェントは Microsoft Windows UEFI Driver Publisher 証明書により署名されています。

一部のデバイスでは (例えば Microsoft Surface Pro および Microsoft Surface Pro 2 など)、デジタル署名検証証明書の日付の古いリストが既定でインストールされていることがあります。ドライブを暗号化する前に、これらの証明書のリストをアップデートする必要があります。

- UEFI 標準で Fast Boot がサポートされる埋め込みソフトウェア。

*Fast Boot* は、コンピューターの起動速度向上に役立つ技術です。Fast Boot 技術が有効になっていると、通常コンピューターはオペレーティングシステムの開始に必要な最低限の UEFI ドライバー設定のみ読み込みます。Fast Boot 技術が有効になっていると、認証エージェントが実行している最中に USB キーボード、マウス、USB トークン、タッチパッドおよびタッチスクリーンが正常に動作しないことがあります。

Kaspersky Disk Encryption (FDE) を使用するには、Fast Boot 技術を無効にすることを推奨します。[FDE テストユーティリティ](#) を使用して、Kaspersky Disk Encryption (FDE) の動作をテストすることもできます。

Kaspersky Endpoint Security は、以下の構成をサポートしません：

- ブートローダーが配置されているドライブとオペレーティングシステムが配置されているドライブが異なる。
- システムに UEFI 32 標準の組み込みソフトウェアが含まれている。
- システムが Intel® Rapid Start Technology を持ち、ハイバネーション用パーティションがあるドライブ（Intel® Rapid Start Technology を無効にしている場合も含む）。
- 10 以上の拡張パーティションを含む MBR 形式のドライブ。
- スワップファイルがシステムドライブ以外のドライブに配置されている。
- 複数のオペレーティングシステムがインストールされているマルチブートシステム。
- 動的パーティション（最初のパーティションのみがサポートされます）。
- 断片化していない空き容量が 0.5% 未満のドライブ。
- セクターサイズが 512 バイト（または 512 バイトをエミュレートする 4096 バイト）以外であるドライブ。
- ハイブリッドドライブ。
- システムにサードパーティローダーがある。
- 圧縮 NTFS ディレクトリのドライブ。
- Kaspersky Disk Encryption（FDE）技術はほかのディスク全体の暗号化技術（BitLocker、McAfee Drive Encryption、および WinMagic SecureDoc など）とは互換性がありません。
- Kaspersky Disk Encryption（FDE）技術は Express Cache 技術とは互換性がありません。
- 暗号化されたドライブ上のパーティションの作成、削除、変更はサポートされていません。データ損失の可能性あります。
- ファイルシステムのフォーマットはサポートされていません。データ損失の可能性あります。  
Kaspersky Disk Encryption（FDE）技術で暗号化されたドライブをフォーマットする必要がある場合、Kaspersky Endpoint Security for Windows がインストールされていないコンピューター上で、ディスク全体の暗号化のみ使用してドライブをフォーマットしてください。  
クイックフォーマットオプションでフォーマットされた暗号化されたドライブは、次に Kaspersky Endpoint Security for Windows がインストールされたコンピューターに接続した際に暗号化されたものと誤認される可能性があります。ユーザーデータは利用できなくなります。
- 認証エージェントは100アカウント以上はサポートしません。
- シングルサインオン技術はサードパーティ開発元によるその他の技術とは互換性がありません。
- Kaspersky Disk Encryption（FDE）技術は次のデバイスのモデルではサポートされていません：
  - Dell Latitude E6410（UEFI モード）
  - HP Compaq nc8430（レガシー BIOS モード）
  - Lenovo Think Center 8811（レガシー BIOS モード）
- 認証エージェントはレガシー USB サポートが有効になっている場合は USB トークンの動作はサポートしません。コンピューター上ではパスワードによる認証のみ可能です。



- レガシー BIOS モードでドライブを暗号化する場合は、次のモデルのデバイスではレガシー USB サポートを有効にすることをお勧めします：
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530
  - Lenovo ThinkPad T510
  - Lenovo ThinkPad W540
  - Lenovo ThinkPad X121e
  - Lenovo ThinkPad X200s (74665YG)
  - Samsung R530
  - Toshiba Satellite A350



- Toshiba Satellite U400 100
- MSI 760GM-E51 (マザーボード)

## 暗号鍵 (AES56 / AES256) の鍵長の変更

Kaspersky Endpoint Security では、Advanced Encryption Standard (AES) 暗号アルゴリズムが使用されます。Kaspersky Endpoint Security では、鍵長が 256 ビットまたは 56 ビットの AES 暗号アルゴリズムがサポートされます。データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります (強度の高い暗号化 (AES256) または相対的に強度の低い暗号化 (AES56))。AES 暗号化ライブラリは本製品と合わせてインストールされます (※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません)。

暗号鍵の鍵長の変更は Kaspersky Endpoint Security 11.2.0 以降でのみ利用できます。

暗号鍵長の変更は、次の手順で行います：

1. 暗号鍵長を変更する前に Kaspersky Endpoint Security によって暗号化されているオブジェクトを復号します。
  - a. [ハードディスクを復号](#)します。
  - b. [ローカルドライブでファイルを復号](#)します。
  - c. [リムーバブルドライブを復号](#)します。

暗号鍵長を変更すると、それ以前に暗号化されたオブジェクトは使用できなくなります。

2. [Kaspersky Endpoint Security をアンインストール](#)します。
3. 鍵長が異なる暗号化ライブラリを含む配布パッケージから [Kaspersky Endpoint Security をインストール](#)します。

あるいは、本製品をアップグレードすることで暗号鍵長を変更することもできます。次の条件を満たす場合にのみ、本製品のアップグレードによって鍵長を変更できます：

- Kaspersky Endpoint Security 10 Service Pack 2 以降がコンピューターにインストールされている。
- データ暗号化コンポーネント (ファイルレベルの暗号化、ディスク全体の暗号化) がコンピューターにインストールされていない。  
既定では、データ暗号化コンポーネントは Kaspersky Endpoint Security のインストールに含まれていません。BitLocker の管理コンポーネントは暗号鍵長の変更に影響しません。

暗号鍵長を変更するには、目的の暗号化ライブラリを含む配布パッケージから kes\_win.msi または setup\_kes.exe ファイルを実行します。インストールパッケージを使用してリモートで本製品をアップグレードすることもできます。

コンピューターにインストールされている製品をアンインストールせずに、この製品と同じバージョンの配布パッケージを使用して暗号鍵の鍵長を変更することはできません。

## Kaspersky Disk Encryption

Kaspersky Disk Encryption は、ワークステーション用の Windows オペレーティングシステム上でのみ使用できます。サーバー用の Windows オペレーティングシステムを実行しているコンピューターには、BitLocker ドライブ暗号化技術を使用してください。

Kaspersky Endpoint Security は、FAT32、NTFS および exFat ファイルシステムの暗号化に対応していません。

ディスク全体の暗号化を開始する前に、多数のチェックが実行され、暗号化をデバイスに適用できるかどうか判断されます。このチェックには、システムのハードディスクと認証エージェントまたは BitLocker 暗号化との互換性チェックも含まれます。互換性をチェックするため、コンピューターを再起動する必要があります。コンピューターの再起動後、必要なチェックがすべて自動的に行われます。互換性チェックが正常に終了すると、オペレーティングシステムが起動し本製品が読み込まれます。その後、ディスク全体の暗号化が実行されます。システムのハードディスクに認証エージェントおよび BitLocker 暗号化との互換性がないことがわかった場合は、ハードウェアリセットボタンを押して、コンピューターを再起動する必要があります。互換性がないという情報は、Kaspersky Endpoint Security によりレポートに記録されます。この情報に基づき、オペレーティングシステムの起動時に、ディスク全体の暗号化は開始されません。このイベントに関する情報は、Kaspersky Security Center レポートに記録されます。

コンピューターのハードウェア構成の変更後、システムのハードディスクと認証エージェントおよび BitLocker 暗号化との互換性をチェックするには、前述のチェック中に記録された非互換性情報を削除する必要があります。そのためには、ディスク全体を暗号化する前に、コマンドラインに `avp pbatestreset` と入力します。システムのハードディスクで認証エージェントとの互換性がチェックされた後にオペレーティングシステムを読み込めない場合は、復元ツールを使用して[認証エージェントのテスト操作後に残ったオブジェクトとデータを削除する必要があります](#)。その後 Kaspersky Endpoint Security を起動し、`avp pbatestreset` コマンドを再度実行します。

ディスク全体の暗号化の開始後、Kaspersky Endpoint Security は、ハードディスクに書き込まれているデータをすべて暗号化します。

ディスク全体の暗号化の実行中にユーザーがコンピューターをシャットダウンまたは再起動した場合、次のオペレーティングシステムの起動前に、認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ディスク全体の暗号化を再開します。

ディスク全体の暗号化の進行中にオペレーティングシステムがハイバネーションモードに切り替わった場合は、オペレーティングシステムがハイバネーションモードから通常モードに復帰した時点で認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ディスク全体の暗号化を再開します。

ディスク全体の暗号化の進行中にオペレーティングシステムがスリープモードに入った場合、オペレーティングシステムがスリープモードから復帰したときにディスク全体の暗号化が再開されます。認証エージェントは読み込まれません。

認証エージェントでのユーザー認証は 2 通りの方法で実行できます：

- LAN 管理者が Kaspersky Security Center ツールを使用して作成した認証エージェントアカウントの名前とパスワードを入力する。
- コンピューターに接続されたトークンまたはスマートカードのパスワードを入力する。

トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合にのみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

認証エージェントは、以下の言語のキーボード配列をサポートします：

- 英語（英国）
- 英語（米国）
- アラビア語（アルジェリア、モロッコ、チュニジア、AZERTY 配列）
- スペイン語（ラテンアメリカ）
- イタリア語
- ドイツ語（ドイツ、オーストリア）
- ドイツ語（スイス）
- ポルトガル語（ブラジル、ABNT2 配列）
- ロシア語（IBM / Windows 105 キーボード、QWERTY 配列）
- トルコ語（QWERTY 配列）
- フランス語（フランス）
- フランス語（スイス）
- フランス語（ベルギー、AZERTY 配列）
- 日本語（106 キーボード、QWERTY 配列）

キーボードの配列がオペレーティングシステムの言語と地域の規格の設定に追加されており、Microsoft Windows のログイン画面で使用可能である場合に、認証エージェントでその配列が使用できるようになります。

認証エージェントのアカウント名に、認証エージェントで使用できるキーボード配列で入力できない記号が含まれている場合、暗号化されたハードディスクは、復元ユーティリティを使用して復元してから、または[認証エージェントのアカウント名とパスワードを復元](#)してからでないと、アクセスできません。

## SSD ドライブ暗号化の特別な機能

本製品は SSD ドライブ、ハイブリッド SSHD ドライブ、Intel Smart Response を持つドライブをサポートします。本製品は Intel Rapid Start を持つドライブの暗号化はサポートしません。このようなドライブを暗号化する前に Intel Rapid Start を無効にしてください。

SSD ドライブの暗号化には、次の特別な機能があります：

- SSD ドライブが新しい、または SSD に重要なデータがない場合は、[使用済みのスペースのみの暗号化を有効](#)にしてください。関連するドライブセクターを上書きできます。
- SSD ドライブが使用中で、重要なデータがある場合は、次のオプションから1つ選択します：
  - SSD ドライブを完全に消去し、オペレーティングシステムをインストールしてから [使用済みのスペースのみの暗号化を有効するオプションを使用して SSD ドライブの暗号化を実行する](#)
  - 使用済みのスペースのみの暗号化を有効するオプションを無効にして SSD ドライブの暗号化を実行する

SSD ドライブの暗号化には 5~10 GB の空き容量が必要です。暗号化した管理データの保存に必要な空き容量は下の表に記載されています。

暗号化した管理データの保存に必要な空き容量

SSD ドライブのサイズ (GB)	SSD ドライブのプライマリパーティションの空き容量 (MB)	SSD ドライブのセカンダリパーティションの空き容量 (MB)
128	250	64
256	250	640
512	300	128

## Kaspersky Disk Encryption 技術を使用したディスク全体の暗号化

ディスク全体の暗号化を行う前に、コンピューターが感染していないことを確認してください。確認するには、完全スキャンか簡易スキャンを開始します。ルートキットによって感染したコンピューターでディスク全体の暗号化を行うと、ハードディスクが動作しなくなる可能性があります。

*Kaspersky Disk Encryption* 技術を使用してディスク全体を暗号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [ディスク全体の暗号化] の順に選択します。
6. [暗号化技術] で、[Kaspersky Disk Encryption] を選択します。

Kaspersky Disk Encryption 技術は、コンピューターに BitLocker で暗号化されたハードディスクがある場合は使用できません。

7. [暗号化モード] で、[すべてのハードディスクを暗号化する] を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、すべてのディスクの暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。

いくつかのハードディスクを暗号化から除外する必要がある場合は、[除外するハードディスクのリストを作成します](#)。

8. ディスクの暗号化中に認証エージェントアカウントを追加するルールを設定します。エージェントを使用して認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。自動的に認証エージェントアカウントを追加するには、以下のように設定します：

- **暗号化中に Windows ユーザー向けの認証エージェントアカウントを自動的に作成する**：このチェックボックスをオンにすると、コンピューター上の Windows ユーザーアカウントのリストに基づいて認証エージェントアカウントを作成します。既定では、Kaspersky Endpoint Security は、過去 30 日間にユーザーがオペレーティングシステムにログインしたすべてのローカルアカウントとドメインアカウントを使用します。
- **このコンピューターのすべてのユーザーの初回ログイン時に認証エージェントアカウントを自動で作成する**：このチェックボックスをオンにすると、認証エージェントの開始前にコンピューター上の Windows ユーザーアカウントに関する情報をチェックします。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。認証エージェントアカウントには次の既定の設定（パスワードで保護されているログインのみ、初回認証時のパスワード変更を要求）が適用されています。そのため、すでに暗号化されたドライブを持つコンピューター用に認証エージェントアカウントの管理タスクを使用して[認証エージェントを手動で追加](#)する必要はありません。

認証エージェントアカウントの自動作成を無効にした場合、アカウントの管理タスクを使用して[手動で認証エージェントを追加](#)できます。このタスクを使用して、自動で作成された認証エージェントアカウントの設定を変更することもできます。

9. 認証エージェントのメモリーにユーザー名を保存しておけば、ユーザーは次回パスワードを入力するだけでシステムにログインすることができます。ユーザー名を保存するには、**「認証エージェントに入力したユーザー名を保存する」**をオンにします。

10. 次のいずれかの暗号化方法を選択します：

- ファイルによって占められているハードディスクセクターにのみ暗号化を適用する場合、**「使用されているディスク領域のみを暗号化」**をオンにします。

既に使用されているドライブに暗号化を適用する場合、ドライブ全体を暗号化してください。それにより、削除されているが取り出すことのできる情報を含む可能性があるデータを含め、すべてのデータが保護されます。**「使用されているディスク領域のみを暗号化」**は、まだ使用されていない新しいドライブに推奨します。

- ハードディスク全体に暗号化を適用する場合、**「使用されているディスク領域のみを暗号化」**をオフにします。

デバイスが既に**「使用されているディスク領域のみを暗号化（暗号化時間を短縮）」**をオンにして暗号化されている場合、**「すべてのハードディスクを暗号化する」**をオンにしたポリシーを適用しても、ファイルが占有していないセクターは暗号化されません。

11. コンピューターの暗号化中にハードウェアの非互換性の問題が発生した場合は、**「レガシー USB サポートを使用する」**チェックボックスをオンにできます。



レガシー USB サポートは BIOS / UEFI 機能であり、オペレーティングシステム (BIOS モード) を起動する前のコンピューターのブートフェーズ中に USB デバイス (セキュリティトークンなど) を使用することができます。レガシー USB サポートは、オペレーティングシステムが起動した後の USB デバイスのサポートには影響しません。

レガシー USB サポートが有効になっている場合、BIOS モードの認証エージェントでは USB を介してトークンを操作することはできません。ハードウェアの互換性の問題が発生しているコンピューターでのみ、このオプションをオンにしてください。

## 12. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品の[メインウィンドウ](#)から実行できます。

システムのハードディスクが暗号化されている場合、オペレーティングシステムの起動前に認証エージェントが読み込まれます。認証エージェントを使用して認証を完了し、暗号化されたハードディスクへのアクセス権を得てオペレーティングシステムを読み込みます。認証手順が問題なく完了したら、オペレーティングシステムが読み込まれます。認証プロセスは、オペレーティングシステムが再起動するたびに繰り返されます。

## 暗号化から除外するハードディスクのリスト作成

暗号化から除外するリストは、Kaspersky Disk Encryption 技術でのみ作成できます。

暗号化から除外するハードディスクのリストを作成するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [ディスク全体の暗号化] の順に選択します。
6. [暗号化技術] で、[Kaspersky Disk Encryption] を選択します。  
[次のハードディスクを暗号化しない] テーブルに、暗号化から除外するハードディスクに対応するエントリが表示されます。暗号化から除外するハードディスクのリストを以前に作成していない場合、このテーブルは空白です。
7. 暗号化から除外するハードディスクのリストにハードディスクを追加するには：
  - a. [追加] をクリックします。
  - b. [Kaspersky Security Center のリストからのデバイスの追加] ウィンドウで、[名前]、[コンピューター]、[ディスク種別]、[Kaspersky Disk Encryption] の各パラメータの値を指定します。
  - c. [更新] をクリックします。

d. **[名前]** 列で、暗号化から除外するハードディスクのリストに追加するハードディスクのテーブル列の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。

**[次のハードディスクを暗号化しない]** テーブルに、選択したハードディスクが表示されます。

8. 除外するリストからハードディスクを削除するには、**[次のハードディスクを暗号化しない]** テーブルで1つまたは複数の行を選択して **[削除]** をクリックします。

テーブルで複数の行を選択するには、**CTRL** キーを押しながら選択します。

9. 変更内容を保存します。

## 暗号化から除外するハードディスクのリストのエクスポートおよびインポート

暗号化から除外するハードディスクのリストをXMLファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の除外リストをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーに除外リストを移行することができます。

[管理コンソール \(MMC\) で暗号化から除外するハードディスクのリストをエクスポートおよびインポートする方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダで、設定を適用するクライアントコンピューターが属している管理グループのフォルダを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔データ暗号化〕** → **〔ディスク全体の暗号化〕** の順に選択します。
6. **〔暗号化技術〕** で、 **〔Kaspersky Disk Encryption〕** を選択します。  
**〔次のハードディスクを暗号化しない〕** テーブルに、暗号化から除外するハードディスクに対応するエントリが表示されます。
7. 除外リストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。複数のポートを選択するには、 **CTRL** または **SHIFT** キーを使用します。  
除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。
  - b. **〔エクスポート〕** をクリックします。
  - c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダを指定します。
  - d. **〔保存〕** をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
8. ルールのリストをインポートするには：
  - a. **〔インポート〕** をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. **〔開く〕** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
9. 変更内容を保存します。

## Web コンソールで暗号化から除外するハードディスクのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. 除外リストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **データ暗号化** → **ディスク全体の暗号化** に移動します。
5. **[Kaspersky Disk Encryption]** 技術を選択し、設定するためのリンクをクリックします。  
暗号化の設定が開きます。
6. **[除外リスト]** をクリックします。
7. ルールのリストをエクスポートするには：
  - a. エクスポートする除外リストを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。
  - d. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - e. **[保存]** をクリックします。  
Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。
8. ルールのリストをインポートするには：
  - a. **[インポート]** をクリックします。
  - b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
  - c. **[開く]** をクリックします。  
コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
9. 変更内容を保存します。

## シングルサインオン (SSO) 技術の有効化

シングルサインオン (SSO) 技術を使用すると、認証エージェントの認証情報を使用してオペレーティングシステムに自動的にログインできます。

シングルサインオン技術を使用する場合、認証エージェントは Kaspersky Security Center で指定されたパスワードの強度の要件を無視します。パスワードの強度の要件は、オペレーティングシステムの設定で設定できます。

シングルサインオン技術は、アカウント認証情報のサードパーティプロバイダーとは互換性がありません。

### 管理コンソール (MMC) でシングルサインオン技術の使用を有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [暗号化の共通設定] の順に選択します。
6. [パスワードの設定] ブロックで、[設定] をクリックします。
7. 開いたウィンドウの [認証エージェント] タブで、[シングルサインオン (SSO) 技術を使用する] をオンにします。
8. 変更内容を保存します。

その結果、ユーザーは、エージェントで一度だけ認証手順を完了する必要があります。認証手順は、オペレーティングシステムの読み込みには必要ありません。オペレーティングシステムが自動的にロードされます。

### Web コンソールでシングルサインオンの使用を有効にする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. シングルサインオンの使用を有効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **データ暗号化** → **ディスク全体の暗号化** に移動します。
5. **[Kaspersky Disk Encryption]** 技術を選択し、設定するためのリンクをクリックします。  
暗号化の設定が開きます。
6. **パスワードの設定** セクションで、**シングルサインオン (SSO) 技術を使用する** チェックボックスをオンにします。
7. **[OK]** をクリックします。

その結果、ユーザーは、エージェントで一度だけ認証手順を完了する必要があります。認証手順は、オペレーティングシステムの読み込みには必要ありません。オペレーティングシステムが自動的にロードされます。

シングルサインオンが機能するには、Windows アカウントのパスワードと認証エージェントアカウントのパスワードが一致する必要があります。パスワードが一致しない場合、ユーザーは認証手順を2回実行する必要があります。認証エージェントのインターフェイス上および、オペレーティングシステムをロードする前です。その後、Kaspersky Endpoint Security は、認証エージェントアカウントのパスワードを Windows アカウントのパスワードに置き換えます。

## 認証エージェントアカウントの管理

Kaspersky Disk Encryption (FDE) 技術を使用して保護されているドライブを操作するには、認証エージェントが必要です。オペレーティングシステムを読み込む前に、ユーザーはエージェントで認証を完了する必要があります。認証エージェントアカウントの管理タスクは、ユーザー認証設定を設定するために構成されています。個別のコンピューターにローカルタスクを使用できるだけでなく、個別の管理グループまたは選択されたコンピューターにグループタスクを使用できます。

認証エージェントアカウントの管理タスクを開始するスケジュールを構成することはできません。タスクを強制的に停止することもできません。

### [管理コンソール \(MMC\) で認証エージェントアカウントの管理タスクを作成する方法](#)

1. 管理コンソールで、**〔管理サーバー〕** → **〔タスク〕** のフォルダーに移動します。  
タスクのリストが表示されます。

2. **〔新規タスク〕** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

**〔Kaspersky Endpoint Security for Windows (11.7.0)〕** → **〔認証エージェントアカウントの管理〕** を選択します。

## ステップ 2：認証エージェントアカウント管理コマンドの選択

認証エージェントアカウント管理コマンドのリストを生成します。管理コマンドを使用すると、認証エージェントアカウントを追加、変更、および削除できます。認証エージェントアカウントを持つユーザーのみが認証手順を完了し、オペレーティングシステムをロードし、暗号化されたドライブにアクセスできます。

## ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 4：タスク名の定義

タスクの名前を入力します。たとえば、「管理者アカウント」など。

## ステップ 5：タスク作成の完了

ウィザードを終了します。必要に応じて、**〔ウィザードの完了後にタスクを実行〕** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
2. **【タスク種別】** で、**【認証エージェントアカウントの管理】** を選択します。
3. **【タスク名】** に「管理者アカウント」などの簡潔な名前を付けます。
4. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。

## ステップ 2：認証エージェントアカウントの管理

認証エージェントアカウント管理コマンドのリストを生成します。管理コマンドを使用すると、認証エージェントアカウントを追加、変更、および削除できます。認証エージェントアカウントを持つユーザーのみが認証手順を完了し、オペレーティングシステムをロードし、暗号化されたドライブにアクセスできます。

## ステップ 3：タスク作成の完了

**【終了】** をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。

タスクを実行するには、タスクのチェックボックスをオンにし、**【開始】** をクリックします。

その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

認証エージェントアカウントを追加するには、認証エージェントアカウントの管理タスクに特別なコマンドを追加する必要があります。たとえば、すべてのコンピューターに管理者アカウントを追加するには、グループタスクを使用すると便利です。

Kaspersky Endpoint Security では、ドライブを暗号化する前に認証エージェントアカウントを自動的に作成できます。[ディスク全体の暗号化ポリシー設定](#)で認証エージェントアカウントの自動作成を有効にできます。[シングルサインオン \(SSO\) 技術の使用](#)もできます。

### [管理コンソール \(MMC\) を使用して認証エージェントアカウントを追加する方法](#)

1. 認証エージェントアカウントの管理タスクのプロパティを開きます。
2. タスクのプロパティで、**【オプション】** セクションを選択します。
3. **【追加】** → **【アカウント追加コマンド】** をクリックします。
4. 開いたウィンドウの **【Windows アカウント】** フィールドで、認証エージェントアカウントの作成に使用される Microsoft Windows アカウントの名前を指定します。
5. Windows アカウント名を手動で入力した場合は、**【許可】** をクリックして、アカウントのセキュリティ識別子 (SID) を定義します。  
 **【許可】** をクリックしてセキュリティ識別子 (SID) を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、認証エージェントアカウントの管理タスクはエラーで終了します。

6. 認証エージェントのために以前に作成されたアカウントを、作成されるアカウントで置き換える場合、**【既存のアカウントの置き換え】** をオンにします。

このステップは、認証エージェントアカウントの管理用のグループタスクのプロパティに認証エージェントアカウント作成コマンドを追加する場合に使用できます。このステップは、ローカルタスクの **【認証エージェントアカウントの管理】** のプロパティに認証エージェントアカウント作成コマンドを追加する場合には使用できません。

7. **【ユーザー名】** に、暗号化されたハードディスクへのアクセスのための認証時に入力する必要がある認証エージェントアカウントの名前を入力します。
8. 暗号化されたハードディスクへのアクセスのための認証時に、認証エージェントアカウントのパスワードの入力を求めるメッセージをユーザーに表示する場合は、**【パスワードベースの認証を有効にする】** をオンにします。認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。
9. 暗号化されたハードディスクへのアクセスのための認証時に、トークンまたはスマートカードをコンピューターに接続することを求める場合は、**【証明書ベースの認証を有効にする】** をオンにします。スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。
10. 必要に応じて、**【コマンドの説明】** に、コマンド管理に必要な認証エージェントアカウントの詳細情報を入力します。
11. 次のいずれかの手順を実行します：
  - コマンドで指定されたアカウントを使用しているユーザーに、認証エージェントで認証ダイアログにアクセスすることを許可する場合は、**【認証を許可】** をオンにします。
  - コマンドで指定されたアカウントを使用しているユーザーが認証エージェントで認証ダイアログにアクセスできないようにする場合は、**【認証をブロック】** をオンにします。
12. 変更内容を保存します。



1. Web コンソールのメインウィンドウで、[デバイス] → [タスク] の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Endpoint Security の [認証エージェントアカウントの管理] タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. 認証エージェントアカウントのリストで、[追加] をクリックします。  
これにより、認証エージェントアカウント管理ウィザードが起動します。
5. [アカウントの追加] コマンドタイプを選択します。
6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。[次へ] をクリックします。  
  
Kaspersky Endpoint Security は、アカウントセキュリティ識別子 (SID) を決定します。これは、アカウントを確認するために必要です。ユーザー名を誤って入力した場合、Kaspersky Endpoint Security はエラーでタスクを終了します。
7. 認証エージェントのアカウント設定を設定します。
  - **認証エージェントアカウントを新規に作成して既存のアカウントを置き換えます** : Kaspersky Endpoint Security は、コンピューター上の既存のアカウントをスキャンします。コンピューターとタスクのユーザーセキュリティ識別子が一致する場合、Kaspersky Endpoint Security はタスクに従ってアカウント設定を変更します。
  - **ユーザー名** : 認証エージェントアカウントの既定のユーザー名は、ユーザーのドメイン名に対応しています。
  - **パスワードベースの認証を有効にする** : 認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。このようにして、各ユーザーは独自のパスワードを持ちます。ポリシーで、認証エージェントアカウントのパスワードの強度要件を設定することもできます。
  - **証明書ベースの認証を有効にする** : スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。この方法では、ユーザーはスマートカードまたはトークンのパスワードを入力する必要があります。
  - **暗号化されたデータへのアカウントのアクセス** : 暗号化されたドライブへのユーザーアクセスを設定します。たとえば、認証エージェントアカウントを削除する代わりに、ユーザー認証を一時的に無効にすることができます。
  - **コメント** : 必要に応じて、アカウントの説明を入力します。
8. 変更内容を保存します。
9. タスクの横のチェックボックスをオンにし、[開始] をクリックします。

その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

認証エージェントアカウントのパスワードおよびその他の設定を変更するには、認証エージェントアカウントの管理タスクに特別なコマンドを追加する必要があります。たとえば、すべてのコンピューターの管理者トークン証明書を置き換えるには、グループタスクを使用すると便利です。

### **管理コンソール (MMC) を使用して認証エージェントアカウントを変更する方法**

1. 認証エージェントアカウントの管理タスクのプロパティを開きます。
2. タスクのプロパティで、**【オプション】** セクションを選択します。
3. **【追加】** → **【アカウント編集コマンド】** をクリックします。
4. 開いたウィンドウの **【Windows アカウント】** フィールドで、変更する Microsoft Windows ユーザーアカウントの名前を指定します。
5. Windows アカウント名を手動で入力した場合は、**【許可】** をクリックして、アカウントのセキュリティ識別子 (SID) を定義します。  
 **【許可】** をクリックしてセキュリティ識別子 (SID) を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、認証エージェントアカウントの管理タスクはエラーで終了します。

6. **【Windows アカウント】** で示される名前を持つ Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントのユーザー名をその下にあるフィールドに入力した名前に変更する場合は、**【ユーザー名の変更】** をオンにして、認証エージェントユーザーアカウントの新しい名前を入力します。
7. パスワードベースの認証設定を編集できるようにするには、**【パスワードベースの認証設定を変更する】** をオンにします。
8. 暗号化されたハードディスクへのアクセスのための認証時に、認証エージェントアカウントのパスワードの入力を求めるメッセージをユーザーに表示する場合は、**【パスワードベースの認証を有効にする】** をオンにします。認証エージェントアカウントのパスワードを設定します。
9. **【Windows アカウント】** に表示された名前を持つ Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントについて、パスワード変更設定の値をその下で指定する設定値に変更する場合は、**【認証エージェントでの認証時のパスワード変更ルールの編集】** をオンにします。
10. 認証エージェントでの認証時のパスワード変更設定の値を指定します。
11. トークンまたはスマートカードの電子証明書に基づく認証の設定を編集できるようにするには、**【証明書ベースの認証設定を変更する】** をオンにします。
12. 暗号化されたハードディスクへのアクセスのための認証プロセスで、コンピューターに接続されたトークンまたはスマートカードに対するパスワードの入力を求めるメッセージをユーザーに表示する場合は、**【証明書ベースの認証を有効にする】** をオンにします。スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。
13. **【Windows アカウント】** に表示されている名前の Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントのコマンド説明を変更する場合は、**【コマンドの説明の編集】** をオンにして、コマンド説明を編集します。
14. **【Windows アカウント】** に表示されている名前の Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントについて、認証エージェントでの認証ダイアログへのユーザーアクセスのルールを、その下で指定する値に変更する場合は、**【認証エージェントでの認証アクセスルールの編集】** をオンにします。

15. 認証エージェントでの認証ダイアログへのアクセスのルールを指定します。
16. 変更内容を保存します。

#### [Web コンソールを使用して認証エージェントアカウントを変更する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **[認証エージェントアカウントの管理]** タスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. 認証エージェントアカウントのリストで、**[追加]** をクリックします。  
これにより、認証エージェントアカウント管理ウィザードが起動します。
5. **アカウントの編集** コマンドタイプを選択します。
6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。**[次へ]** をクリックします。  
  
Kaspersky Endpoint Security は、アカウントセキュリティ識別子 (SID) を決定します。これは、アカウントを確認するために必要です。ユーザー名を誤って入力した場合、Kaspersky Endpoint Security はエラーでタスクを終了します。
7. 編集する設定の横にあるチェックボックスをオンにします。
8. 認証エージェントのアカウント設定を設定します。
  - **認証エージェントアカウントを新規に作成して既存のアカウントを置き換えます** : Kaspersky Endpoint Security は、コンピューター上の既存のアカウントをスキャンします。コンピューターとタスクのユーザーセキュリティ識別子が一致する場合、Kaspersky Endpoint Security はタスクに従ってアカウント設定を変更します。
  - **ユーザー名** : 認証エージェントアカウントの既定のユーザー名は、ユーザーのドメイン名に対応しています。
  - **パスワードベースの認証を有効にする** : 認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。このようにして、各ユーザーは独自のパスワードを持ちます。ポリシーで、認証エージェントアカウントのパスワードの強度要件を設定することもできます。
  - **証明書ベースの認証を有効にする** : スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。この方法では、ユーザーはスマートカードまたはトークンのパスワードを入力する必要があります。
  - **暗号化されたデータへのアカウントのアクセス** : 暗号化されたドライブへのユーザーアクセスを設定します。たとえば、認証エージェントアカウントを削除する代わりに、ユーザー認証を一時的に無効にすることができます。
  - **コメント** : 必要に応じて、アカウントの説明を入力します。
9. 変更内容を保存します。
10. タスクの横のチェックボックスをオンにし、**[開始]** をクリックします。

認証エージェントアカウントを削除するには、認証エージェントアカウントの管理タスクに特別なコマンドを追加する必要があります。たとえば、解雇された従業員のアカウントを削除するには、グループタスクを使用すると便利です。

## 管理コンソール (MMC) を使用して認証エージェントアカウントを削除する方法②

1. 認証エージェントアカウントの管理タスクのプロパティを開きます。
2. タスクのプロパティで、**【オプション】** セクションを選択します。
3. **【追加】** → **【アカウント削除コマンド】** をクリックします。
4. 開いたウィンドウの **【Windows アカウント】** フィールドで、削除する認証エージェントアカウントの作成に使用された Windows ユーザーアカウントの名前を指定します。
5. Windows アカウント名を手動で入力した場合は、**【許可】** をクリックして、アカウントのセキュリティ識別子 (SID) を定義します。  
 **【許可】** をクリックしてセキュリティ識別子 (SID) を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、認証エージェントアカウントの管理タスクはエラーで終了します。

6. 変更内容を保存します。

## Web コンソールを使用して認証エージェントアカウントを削除する方法②

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
 タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **【認証エージェントアカウントの管理】** タスクをクリックします。  
 タスクのプロパティウィンドウが表示されます。
3. **【アプリケーション設定】** タブを選択します。
4. 認証エージェントアカウントのリストで、**【追加】** をクリックします。  
 これにより、認証エージェントアカウント管理ウィザードが起動します。
5. **アカウントの削除コマンドタイプ**を選択します。
6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。
7. 変更内容を保存します。
8. タスクの横のチェックボックスをオンにし、**【開始】** をクリックします。

その結果、コンピューターの次回起動時にタスクが完了した後、ユーザーは認証手順を完了してオペレーティングシステムを読み込むことができなくなります。Kaspersky Endpoint Security は、暗号化されたデータへのアクセスを拒否します。

エージェントで認証を完了し、オペレーティングシステムの読み込みができるユーザーのリストを表示するには、管理されたコンピューターのプロパティに移動する必要があります。

### 管理コンソール (MMC) を使用して認証エージェントアカウントのリストを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [デバイス] タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、 [タスク] セクションを選択します。  
ローカルタスクのリストが表示されます。
6. **認証エージェントアカウントの管理** タスクを選択します。
7. タスクのプロパティで、 [オプション] セクションを選択します。

その結果、このコンピューター上の認証エージェントアカウントのリストにアクセスできるようになります。リストのユーザーのみが、エージェントで認証を完了し、オペレーティングシステムの読み込みができます。

### Web コンソールを使用して認証エージェントアカウントのリストを表示する方法

1. Web コンソールのメインウィンドウで、 [デバイス] → [管理対象デバイス] の順に選択します。
2. 認証エージェントアカウントのリストを表示するコンピューターの名前をクリックします。  
コンピューターのプロパティが表示されます。
3. コンピューターのプロパティウィンドウで、 [タスク] セクションを選択します。  
ローカルタスクのリストが表示されます。
4. **認証エージェントアカウントの管理** タスクを選択します。
5. タスクのプロパティで、 **アプリケーション設定** タブを選択します。

その結果、このコンピューター上の認証エージェントアカウントのリストにアクセスできるようになります。リストのユーザーのみが、エージェントで認証を完了し、オペレーティングシステムの読み込みができます。

## 認証エージェントでのトークンまたはスマートカードの使用

暗号化されたハードディスクにアクセスする際、認証にトークンまたはスマートカードを使用できます。これを行うには、トークンまたはスマートカードの電子証明書ファイルを認証エージェントアカウントの管理タスクに追加する必要があります。



トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合のみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

Kaspersky Endpoint Security は、以下のトークン、スマートカードリーダー、およびスマートカードをサポートします：

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K Java
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511
- Rutoken ECP
- Rutoken ECP Flash
- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI.

トークンまたはスマートカードの電子証明書ファイルを認証エージェントアカウント作成コマンドに追加するには、まず、証明書を管理するサードパーティソフトウェアを使用してファイルを保存する必要があります。

トークンまたはスマートカードの証明書は、次の属性を満たす必要があります：

- 証明書が X.509 標準に準拠し、証明書ファイルが DER で符号化されている。
- 証明書が、長さ 1024 ビット以上の RSA キーを含む。

トークンまたはスマートカードの電子証明書がこれらの要件を満たしていない場合、認証エージェントアカウントを作成するためのコマンドに証明書ファイルを読み込むことはできません。

証明書の KeyUsage パラメーターには、値 keyEncipherment または dataEncipherment が必要です。KeyUsage パラメーターは、証明書の目的を決定します。パラメーターの値が異なる場合、Kaspersky Security Center は証明書ファイルをダウンロードしますが、警告を表示します。

ユーザーがトークンまたはスマートカードを紛失してしまった場合、管理者は、トークンまたはスマートカードの電子署名ファイルを、認証エージェントアカウントの作成コマンドに追加する必要があります。その後、[暗号化されたデバイスへのアクセス権を取得するか暗号化されたデバイスのデータを復元するための手順](#)をユーザー側で完了させます。

# ハードディスクの復号化

現在のライセンスでデータの暗号化が許可されていない場合でも、ハードディスクの復号化は可能です。

ハードディスクを復号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [データ暗号化] → [ディスク全体の暗号化] の順に選択します。
6. [暗号化技術] で、ハードディスクを暗号化する技術を選択します。
7. 次のいずれかの手順を実行します：
  - 暗号化されているすべてのハードディスクを復号化するには、 [暗号化モード] で [すべてのハードディスクを復号化する] を選択します。
  - 復号化する暗号化されたハードディスクを [次のハードディスクを暗号化しない] 表に追加します。

このオプションは、Kaspersky Disk Encryption 技術でのみ使用できます。

8. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品の[メインウィンドウ](#)から実行できます。

Kaspersky Disk Encryption 技術で暗号化されたハードディスクの復号化中にユーザーがコンピューターをシャットダウンまたは再起動した場合、次のオペレーティングシステムの起動前に、認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ハードディスクの復号化を再開します。

Kaspersky Disk Encryption 技術で暗号化されたハードディスクの復号化中にオペレーティングシステムがハイバネーションモードに切り替わった場合は、オペレーティングシステムがハイバネーションモードから復帰した時点で認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ハードディスクの復号化を再開します。ハードディスクの復号化後、オペレーティングシステムを再起動するまで、ハイバネーションモードは使用できません。

ハードディスクの復号化中にオペレーティングシステムがスリープモードに入った場合、オペレーティングシステムがスリープモードから復帰したときにハードディスクの復号化が再開されます。認証エージェントは読み込まれません。

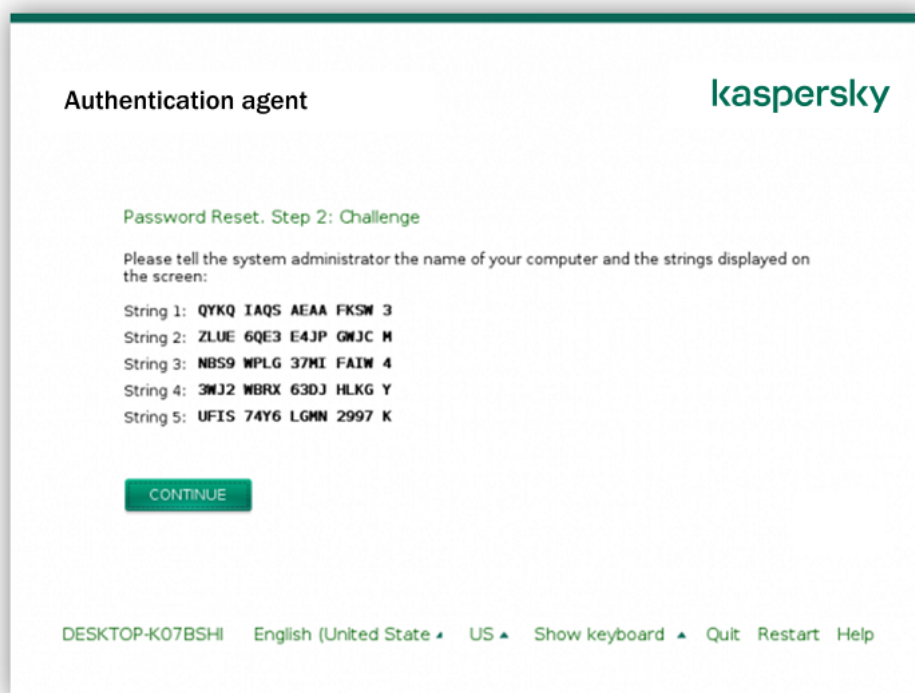
# Kaspersky Disk Encryption 技術で保護されたドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたハードドライブにアクセスするためのパスワードをユーザーが忘れた場合、復元手順（要求と応答）を開始する必要があります。

## システムのハードドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたシステムハードドライブへのアクセスを復元するには、次の手順を実行します：

1. ユーザーは、要求ブロックを管理者に報告します（以下の図を参照）。
2. 管理者は要求ブロックを Kaspersky Security Center に入力し、応答ブロックを受け取り、応答ブロックをユーザーに報告します。
3. ユーザーは、認証エージェントのインターフェイスに応答ブロックを入力し、ハードドライブへのアクセスを取得します。



Kaspersky Disk Encryption 技術で保護されたシステムハードドライブへのアクセスの復元

復元手順を開始するには、ユーザーは、認証エージェントのインターフェイスの **[パスワードを忘れた場合]** をクリックする必要があります。

[管理コンソール（MMC）で Kaspersky Disk Encryption 技術で保護されたシステムハードドライブの応答ブロックを取得する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [デバイス] タブを選択します。
4. [デバイス] タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
5. コンテキストメニューで、 [オフラインモードでのアクセスを許可する] を選択します。
6. 表示されたウィンドウで、 [認証エージェント] タブを選択します。
7. [使用されている暗号化アルゴリズム] セクションで、 [AES56] または [AES256] の暗号化アルゴリズムを選択します。  
データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（強度の高い暗号化（AES256）または相対的に強度の低い暗号化（AES56））。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。
8. [アカウント] で、認証エージェントのアカウント名とパスワードの復元を要求しているユーザーの認証エージェントアカウント名を選択します。
9. [ハードディスク] で、アクセスを復元する暗号化されたハードディスクを選択します。
10. [ユーザーの要求] セクションに、ユーザーが提示した要求ブロックを入力します。

その結果、認証エージェントアカウントのユーザー名とパスワードの復元を求めるユーザー要求に対する応答ブロックの内容が、**アクセスキー**フィールドに表示されます。応答ブロックの内容をユーザーに伝えます。

### Web コンソールで Kaspersky Disk Encryption 技術で保護されたシステムハードドライブの応答ブロックを取得する方法

1. Web コンソールのメインウィンドウで、 [デバイス] → [管理対象デバイス] の順に選択します。
2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。
4. 表示されたウィンドウで、 [認証エージェント] セクションを選択します。
5. [アカウント] で、認証エージェントのアカウント名とパスワードの復元を要求しているユーザーのために作成された認証エージェントアカウントの名前を選択します。
6. ユーザーから伝えられた要求ブロックを入力します。

認証エージェントのアカウントのユーザー名とパスワードの復元に関するユーザー要求に対する応答ブロックの内容は、ウィンドウの下部に表示されます。応答ブロックの内容をユーザーに伝えます。

復元手順が完了すると、認証エージェントはユーザーにパスワードの変更を求めます。

## システム以外のハードドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたシステム以外のハードドライブへのアクセスを復元するには、次の手順を実行します：

1. ユーザーがアクセス要求ファイルを管理者に送信します。
2. 管理者はアクセス要求ファイルを Kaspersky Security Center に追加し、アクセスキーファイルを作成してユーザーに送信します。
3. ユーザーはアクセスキーファイルを Kaspersky Endpoint Security に追加し、ハードドライブへのアクセスを取得します。

復元手順を開始するには、ユーザーはハードドライブにアクセスする必要があります。その結果、Kaspersky Endpoint Security はアクセス要求ファイル（拡張子が KESDC のファイル）を作成します。ユーザーは、このファイルを管理者に電子メールなどで送信する必要があります。

### 管理コンソール (MMC) で暗号化されたシステム以外のハードドライブのアクセスキーファイルを取得する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[デバイス] タブを選択します。
4. [デバイス] タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
5. コンテキストメニューで、[オフラインモードでのアクセスを許可する] を選択します。
6. 表示されたウィンドウで、[データ暗号化] タブを選択します。
7. [データ暗号化] タブで [参照] をクリックします。
8. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。

### Web コンソールで暗号化されたシステム以外のハードドライブのアクセスキーファイルを取得する方法

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[管理対象デバイス]** の順に選択します。
2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. **[オフラインモードでのデバイスへのアクセスを許可]** をクリックします。
4. **[データ暗号化]** セクションを選択します。

5. **[ファイルを選択]** をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。

Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。

6. **[ライセンスを保存]** をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

## オペレーティングシステムのアップデート

ディスク全体の暗号化（FDE）を使用して保護しているコンピューターのオペレーティングシステムのアップデートでは、いくつか特別に留意すべき事項が存在します。次の順序でオペレーティングシステムをアップデートします：1台のコンピューターで最初に OS をアップデートします。次に、数台のコンピューターで OS をアップデートします。その後、ネットワーク内のすべての OS をアップデートします。

Kaspersky Disk Encryption 技術を使用している場合、オペレーティングシステムの起動前に認証エージェントが読み込まれます。認証エージェントを使用することで、ユーザーはシステムにサインインして暗号化されたディスクにアクセスできます。これに続いて、オペレーティングシステムが読み込まれます。

Kaspersky Disk Encryption 技術を使用して保護されているコンピューター上のオペレーティングシステムのアップデートを開始すると、OS のアップデートウィザードによって認証エージェントが削除されます。その結果、OS ローターは暗号化されたドライブにアクセスできないため、コンピューターをロックできます。

オペレーティングシステムの安全なアップデートについては、[テクニカルサポートのナレッジベースの記事](#)を参照してください。

オペレーティングシステムの自動アップデートは、次の条件下で使用できます：

1. オペレーティングシステムが WSUS（Windows Server Update Services）を使用してアップデートされる。
2. Windows 10 バージョン 1607（RS1）以降がコンピューターにインストールされている。
3. Kaspersky Endpoint Security 11.2.0 以降がコンピューターにインストールされている。

すべての条件が満たされている場合は、通常の方法でオペレーティングシステムをアップデートできます。

Kaspersky Disk Encryption（FDE）技術を使用していて、Kaspersky Endpoint Security for Windows のバージョン 11.1.0 または 11.1.1 がコンピューターにインストールされている場合、Windows 10 にアップデートする際にハードドライブを復号化する必要はありません。



オペレーティングシステムをアップデートするには、次の操作を実行する必要があります：

1. システムをアップデートする前に、cm\_km.inf、cm\_km.sys、klfde.cat、klfde.inf、klfde.sys、klfdefsf.cat、klfdefsf.inf、klfdefsf.sys という名前のドライバーをローカルフォルダーにコピーしてください。たとえば「C:\fde\_drivers」などです。
2. システムアップデートのインストールを実行し、`/ReflectDrivers` スイッチを使用して保存されたドライバーが置かれたフォルダーを指定します。  
`setup.exe /ReflectDrivers C:\fde_drivers`

BitLocker ディスク暗号化技術を使用している場合、Windows 10 をアップデートするためにハードドライブを復号化する必要はありません。BitLocker について詳しくは、[Microsoft の Web サイトの情報](#)を参照してください。

## 暗号化機能のアップデートのエラーの解決

以前のバージョンの製品が Kaspersky Endpoint Security for Windows 11.7.0 にアップグレードされると、ディスク全体の暗号化がアップデートされます。

ディスク全体の暗号化機能のアップデートの開始時に、次のエラーが発生する場合があります：

- アップグレードを開始できませんでした
- デバイスと認証エージェントとの互換性がありません

ディスク全体の暗号化機能のアップデートを新しいバージョンの製品で開始したときに発生するエラーを解決するには：

1. [ハードディスクを復号](#)します。
2. もう一度[ハードディスクを暗号化](#)します。

ディスク全体の暗号化機能のアップデートを実行中に、次のエラーが発生する場合があります：

- アップグレードを完了できませんでした。
- ディスク全体の暗号化のアップグレードのロールバックがエラーで終了した。

ディスク全体の暗号化機能のアップデートを実行中に発生するエラーを解決するには：

[復元ツールを使用して、暗号化されたデバイスへのアクセスを回復](#)します。

## 認証エージェントのトレースレベルの選択

本製品は、認証エージェントが行う操作のサービス情報と、ユーザーが認証エージェントに対して行う操作の情報をトレースファイルに記録します。

認証エージェントのトレースレベルを選択するには：

1. 暗号化されたハードディスクでコンピューターが起動したら、すぐに **F3** キーを押して認証エージェントを設定するウィンドウを表示します。
2. 認証エージェントの設定ウィンドウで、トレースレベルを選択します：



- **Disable debug logging (default)** : このオプションを選択すると、認証エージェントのイベントに関する情報がトレースファイルに記録されません。
- **Enable debug logging** : このオプションを選択すると、認証エージェントの動作と、認証エージェントに対してユーザーが実行する操作に関する情報がトレースファイルに記録されます。
- **Enable verbose logging** : このオプションを選択すると、認証エージェントの動作と、認証エージェントに対してユーザーが実行する操作に関する詳細な情報がトレースファイルに記録されます。

このオプションは、[**Enable debug logging**] と比較して、項目の詳細レベルが高くなります。項目の詳細レベルを高くすると、認証エージェントとオペレーティングシステムの起動が遅くなる場合があります。

- **Enable debug logging and select serial port** : このオプションを選択すると、認証エージェントが行う操作と、認証エージェントに対してユーザーが実行する操作に関する情報がトレースファイルに記録され、COMポート経由で送信されます。

暗号化されたハードディスクのあるコンピューターがCOMポート経由で別のコンピューターに接続されている場合、この別のコンピューターから認証エージェントのイベントを確認できます。

- **Enable verbose debug logging and select serial port** : このオプションを選択すると、認証エージェントが行う操作と、認証エージェントに対してユーザーが実行する操作に関する詳細な情報がトレースファイルに記録され、COMポート経由で送信されます。

このオプションは、[**Enable debug logging and select serial port**] と比較して、項目の詳細レベルが高くなります。項目の詳細レベルを高くすると、認証エージェントとオペレーティングシステムの起動が遅くなる場合があります。

コンピューターに暗号化されたハードディスクがある場合、またはディスク全体の暗号化を実行中の場合、データは認証エージェントのトレースファイルに記録されます。

認証エージェントのトレースファイルは、本製品の他のトレースファイルと異なり、カスペルスキーに送信されません。必要に応じて、認証エージェントのトレースファイルを分析するため、手動でカスペルスキーに送信できます。

## 認証エージェントのヘルプテキストの編集

認証エージェントのヘルプメッセージを編集する前に、起動前環境でサポートされる文字のリストを参照してください（以下を参照）。

認証エージェントのヘルプメッセージを編集するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [**管理対象デバイス**] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [**ポリシー**] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [**データ暗号化**] → [**暗号化の共通設定**] の順に選択します。

6. [テンプレート] セクションで、[ヘルプ] をクリックします。  
[認証エージェントのヘルプメッセージ] ウィンドウが表示されます。

7. 次の手順に従います：

- [認証] タブを選択して、アカウント情報を入力するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。
- [パスワードの変更] タブを選択して、認証エージェントアカウントのパスワードを変更するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。
- [パスワードの復元] タブを選択して、認証エージェントアカウントのパスワードを復元するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。

8. ヘルプメッセージを編集します。

元のテキストを復元する場合は、[既定] をクリックします。

ヘルプのテキストは 16 行以内で入力してください。1 行に入力できる最大文字数は 64 です。

9. 変更内容を保存します。

## 認証エージェントのヘルプメッセージでサポートされる文字

起動前環境では、以下のユニコード文字がサポートされます：

- 基本ラテン文字 (0000 ~ 007F)
- ラテン1補助 (0080 ~ 00FF)
- ラテン文字拡張 A (0100 ~ 017F)
- ラテン文字拡張 B (0180 ~ 024F)
- 前進を伴う修飾文字 (02B0 ~ 02FF)
- ダイアクリティカルマーク (0300 ~ 036F)
- ギリシア文字およびコプト文字 (0370 ~ 03FF)
- キリル文字 (0400 ~ 04FF)
- ヘブライ文字 (0590 ~ 05FF)
- アラビア文字 (0600 ~ 06FF)
- ラテン文字拡張追加 (1E00 ~ 1EFF)
- 一般句読点 (2000 ~ 206F)
- 通貨記号 (20A0 ~ 20CF)
- 文字様記号 (2100 ~ 214F)

- 幾何学模様 (25A0 ~ 25FF)
- アラビア表示形 B (FE70 ~ FEFF)

このリストに示されていない文字は、起動前環境ではサポートされません。それらの文字は認証エージェントのヘルプメッセージに使用しないでください。

## 認証エージェントの動作テスト後に残存するオブジェクトとデータの削除

製品のアンインストール時に、認証エージェントのテスト操作後のオブジェクトとデータがシステムのハードディスクに残っていることを製品が検出した場合、製品のアンインストールは中断され、そのようなオブジェクトとデータが削除されるまで再開できません。

認証エージェントのテスト操作後のオブジェクトとデータは、例外的な場合のみ、システムのハードディスクに残ることがあります。たとえば、暗号化設定を含む Kaspersky Security Center ポリシーを適用した後にコンピューターを再起動していない場合や、認証エージェントのテスト操作の後、本製品の起動に失敗した場合などです。

認証エージェントのテスト操作後に、システムのハードディスクに残っているオブジェクトやデータを削除するには次の方法があります：

- Kaspersky Security Center のポリシーを使用する。
- [復元ツールを使用する](#)。

Kaspersky Security Center のポリシーを使用して認証エージェントのテスト操作後に残っているオブジェクトとデータを削除するには：

1. コンピューターのすべてのハードディスクを[復号化](#)するよう設定した Kaspersky Security Center ポリシーを、コンピューターに適用します。
2. Kaspersky Endpoint Security を起動します。

認証エージェントとアプリケーションとの非互換性に関する情報を削除するには：

コマンドラインに「avp pbatestreset」コマンドを入力します。

## BitLocker の管理

BitLocker は、Windows オペレーティングシステムに組み込まれた暗号化技術です。Kaspersky Endpoint Security を使用して、Kaspersky Security Center で BitLocker を制御および管理できます。BitLocker は論理ボリュームを暗号化します。BitLocker はリムーバブルドライブの暗号化には使用できません。BitLocker について詳しくは、[Microsoft 社の資料](#)を参照してください。

BitLocker 信頼済みプラットフォームモジュールを使用して、安全なアクセスキーの保管領域を提供します。Trusted Platform Module (TPM) は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。TPM は起動前のシステム整合性検証を行うため、TPM を使用すると最も安全に BitLocker アクセスキーを保管できます。TPM なしでもコンピューター上のドライブを暗号化することは可能です。この場合は、アクセスキーはパスワードで暗号化されます。BitLocker は次の暗号化の方法を使用します：

- TPM。
- TPM と PIN。
- パスワード。

ドライブを暗号化した後、BitLocker はマスター鍵を作成します。Kaspersky Endpoint Security はこのマスター鍵を Kaspersky Security Center に送るため、ユーザーがパスワードを忘れた場合などに[ディスクへのアクセスを復元](#)することができます。

ユーザーが BitLocker を使用してディスクを暗号化すると、Kaspersky Endpoint Security は [Kaspersky Security Center にディスク暗号化に関する情報](#) を送ります。一方、Kaspersky Endpoint Security はマスター鍵を Kaspersky Security Center に送らないため、Kaspersky Security Center を使用してディスクへのアクセスを復元することはできません。Kaspersky Security Center と BitLocker が正しく動作するために、[ドライブの復号化および再暗号化](#)にはポリシーを使用してください。ローカルで、またはポリシーを使用してドライブを復号化できます。

システムの暗号化後、ユーザーはオペレーティングシステムを起動するために BitLocker 認証の手順を完了する必要があります。認証手順完了後、BitLocker はユーザーのログインを許可します。BitLocker はシングルサインオン (SSO) をサポートしていません。

Windows のグループポリシーを使用している場合、ポリシーで BitLocker の管理をオフにしてください。Windows のポリシー設定は Kaspersky Endpoint Security のポリシー設定と競合する可能性があります。ドライブの暗号化の際にエラーが発生する可能性があります。

## BitLocker ドライブ暗号化の開始

ディスク全体の暗号化を行う前に、コンピューターが感染していないことを確認してください。確認するには、完全スキャンか簡易スキャンを開始します。ルートキットによって感染したコンピューターでディスク全体の暗号化を行うと、ハードディスクが動作しなくなる可能性があります。

Windows サーバーのオペレーティングシステムが搭載されたコンピューターで BitLocker ドライブ暗号化を使用するには、BitLocker ドライブ暗号化機能をインストールする必要がある場合があります。オペレーティングシステムツール (ロールとコンポーネントを追加するウィザード) を使用して機能をインストールしてください。BitLocker ドライブ暗号化のインストールについては、[Microsoft 社の資料](#)を参照してください。

### [管理コンソール \(MMC\) を使用した BitLocker ドライブ暗号化を実行する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **〔管理対象デバイス〕** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 **〔ポリシー〕** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 **〔データ暗号化〕** → **〔ディスク全体の暗号化〕** の順に選択します。
6. **〔暗号化技術〕** で、 **〔BitLocker ドライブ暗号化〕** を選択します。
7. **〔暗号化モード〕** で、 **〔すべてのハードディスクを暗号化する〕** を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化すると、暗号化を実行したオペレーティングシステムのみを読み込みます。

8. BitLocker ドライブ暗号化の詳細なオプションを設定します（下記の表を参照）。
9. 変更内容を保存します。

### **Web コンソールおよび Cloud コンソールを使用した BitLocker ドライブ暗号化を実行する方法**

1. Web コンソールのメインウィンドウで **〔デバイス〕** → **〔ポリシーとプロファイル〕** の順に選択します。
2. BitLocker 暗号化を開始するコンピューターで使用する Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **〔アプリケーション設定〕** タブを選択します。
4. **データ暗号化** → **ディスク全体の暗号化** に移動します。
5. **〔暗号化の管理〕** セクションで、 **〔BitLocker ドライブ暗号化〕** を選択します。
6. **BitLocker ドライブ暗号化** のリンクをクリックします。  
BitLocker ドライブ暗号化の設定ウィンドウが開きます。
7. **〔暗号化モード〕** で、 **〔すべてのハードディスクを暗号化する〕** を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化すると、暗号化を実行したオペレーティングシステムのみを読み込みます。

8. BitLocker ドライブ暗号化の詳細なオプションを設定します（下記の表を参照）。
9. **〔OK〕** をクリックします。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品の[メインウィンドウ](#)から実行できます。

ポリシーの適用後、認証の設定によって次の内容が表示されます：

- TPM のみ：ユーザーの入力は必要ありません。ディスクはコンピューターの再起動時に暗号化されます。
- TPM および PIN / パスワード：TPM モジュールが利用可能な場合、PIN コードの入力ウィンドウが表示されます。TPM モジュールが利用できない場合、起動前認証用のパスワードの入力ウィンドウが表示されません。
- パスワードのみ：起動認証用のパスワードを求めるウィンドウが表示されます。

コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、Windows 8 以前のオペレーティングシステムでは、回復キーのファイルを保存するのに USB デバイスなどのストレージデバイスの接続を求めるウィンドウが表示されます。複数の回復キーのファイルを、単一のストレージデバイスに保存できます。

パスワードまたは PIN を設定したあと、暗号化を完了するために BitLocker は再起動を求めます。次に、BitLocker の認証の手順を完了します。認証手順の後に、システムにログオンする必要があります。オペレーティングシステムが読み込まれると、BitLocker は暗号化を完了します。

暗号鍵にアクセスできない場合、[回復キーを付与してもらうよう、ユーザーからローカルネットワークの管理者にリクエストできます](#)（回復キーが事前にストレージデバイスに保存されていない場合、または回復キーを紛失した場合）。

#### BitLocker ドライブ暗号化の設定

パラメータ	説明
<b>タブレットでブリーフキーボード入力が必要な BitLocker 認証を使用できるようにする</b>	<p>このチェックボックスでは、起動前の環境でデータ入力を必要とする認証を使用するかしないかを選択します。この設定は、起動前に入力できる機能がないプラットフォームに対しても適用されます（例：タブレットのタッチスクリーンキーボード）。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"><p>タブレットコンピューターのタッチスクリーンは起動前環境では利用できません。タブレットコンピューターで BitLocker 認証を完了するには、ユーザーは USB キーボードなどを接続する必要があります。</p></div> <p>このチェックボックスをオンにすると、起動前の入力を必要とする認証の使用が許可されます。この設定は、起動前の環境でデータ入力ができるツールがあるデバイスに対してのみ使用してください（例：タッチスクリーンキーボードだけでなく USB キーボードも付いているデバイスなど）。</p> <p>チェックボックスをオフにすると、タブレットコンピューターで BitLocker ドライブ暗号化が使用できなくなります。</p>
<b>ハードウェア暗号化を使用 (Windows 8 以降)</b>	<p>このチェックボックスをオンにすると、ハードウェア暗号化が適用されます。ハードウェア暗号化を使用すると、より少ないコンピューターリソースで、より速く暗号化することができます。</p>
<b>使用されているディスク領域のみを暗号化 (Windows 8 以降)</b>	<p>このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。</p>



暗号化の開始後に [ **使用されているディスク領域のみを暗号化 (暗号化時間を短縮)** ] を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン/オフは、暗号化が開始する前に選択してください。

このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。

チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。

データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。すでに使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。

既定では、このチェックボックスはオフです。

## 認証設定

### パスワードを使用 (Windows 8 以降)

このオプションを選択すると、暗号化されたドライブにアクセスしようとした際に、パスワードの入力が要求されます。

このオプションは、Trusted Platform Module (TPM) が使用されていない場合に選択できます。

### Trusted Platform Module (TPM) を使用

このオプションを選択すると、BitLocker は Trusted Platform Module (TPM) を使用します。

*Trusted Platform Module (TPM)* は、セキュリティ関連の基本機能 (暗号化鍵の保存など) を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。

Windows 7 と Windows 2008 R2 では、TPM モジュールを使用した暗号化のみを利用できます。TPM モジュールがインストールされていない場合、BitLocker 暗号化は実行できません。これらのオペレーティングシステムを使用しているコンピューターでは、パスワードを使用した暗号化はサポートされません。

Trusted Platform Module を搭載したデバイスで作成された暗号鍵は、そのデバイスでしか復号化できません。Trusted Platform Module は、各 TPM が保持するストレージルートキーを使って暗号鍵を暗号化します。ストレージルートキーは Trusted Platform Module 内部に格納されています。そのため、暗号鍵を盗もうとする試みに対して、より強固な保護を提供することができます。

既定では、この処理が選択されています。

暗号化鍵およびパスワードまたは PIN で保護された暗号化鍵へのアクセスに、より強固な保護を提供することが可能です。

- **TPM の PIN を使用する** : このチェックボックスをオンにすると、Trusted Platform Module (TPM) 内に格納されている暗号鍵にアクセスする際に暗証番号を使用できます。  
このチェックボックスをオフにすると、PIN コードの使用が禁止されます。暗号鍵へのアクセスには、パスワードの入力が必要となります。



ユーザーに拡張 PIN の使用を許可することができます。拡張 PIN を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります。

- **Trusted Platform Module (TPM) を使用する。使用できない場合はパスワードを使用する**：このチェックボックスをオンにすると、Trusted Platform Module (TPM) が使用できない場合、パスワードを使用して暗号鍵にアクセスできます。

チェックボックスがオフの場合は TPM は使用できず、ディスク全体の暗号化は開始されません。

## BitLocker で保護されたハードドライブの復号化

ユーザーはオペレーティングシステムを使用してディスクを復号化することができます (BitLocker 機能をオフにしてください)。その後、Kaspersky Endpoint Security はディスクを再度暗号化するように求められます。Kaspersky Endpoint Security は、ポリシー内でディスク暗号化を有効にするまでディスクを暗号化するように求めます。

### 管理コンソール (MMC) で BitLocker で保護されたハードドライブを復号化する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [ディスク全体の暗号化] の順に選択します。
6. [暗号化技術] で、[BitLocker ドライブ暗号化] を選択します。
7. [暗号化モード] で、[すべてのハードディスクを復号化する] を選択します。
8. 変更内容を保存します。

### BitLocker で暗号化されたハードドライブを Web コンソールおよび Cloud コンソールで復号化するには

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ハードドライブを復号化するコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **データ暗号化** → **ディスク全体の暗号化** に移動します。
5. **[BitLocker ドライブ暗号化]** 技術を選択し、設定するためのリンクをクリックします。  
暗号化の設定が開きます。
6. **[暗号化モード]** で、**[すべてのハードディスクを復号化する]** を選択します。
7. **[OK]** をクリックします。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品の[メインウィンドウ](#)から実行できます。

## BitLocker で保護されたハードドライブへのアクセスの復元

ユーザーが BitLocker で暗号化されたハードドライブにアクセスするためのパスワードを忘れた場合は、復元手順（要求と応答）を開始する必要があります。

コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、Windows 8 以前のオペレーティングシステムでは、暗号化の前に回復キーのファイルがリムーバブルドライブに保存されます。ドライブへのアクセスを復旧するには、リムーバブルドライブを接続し、画面上の指示に従います。

BitLocker によって暗号化されたハードドライブへのアクセスは、次の復元手順で構成されます：

1. ユーザーは、管理者に回復キーの ID を伝えます（下の図を参照）。
2. 管理者は、Kaspersky Security Center のコンピューターのプロパティで回復キーの ID を確認します。ユーザーが提供した ID は、コンピューターのプロパティに表示される ID と一致する必要があります。
3. 回復キーの ID が一致する場合、管理者はユーザーに回復キーを提供するか、回復キーのファイルを送信します。

回復キーのファイルは、次のオペレーティングシステムを実行しているコンピューターに使用されます：

- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2011

- Windows Server 2012

他のすべてのオペレーティングシステムでは、回復キーが使用されます。

4. ユーザーは回復キーを入力し、ハードドライブにアクセスします。



BitLocker で暗号化されたハードドライブへのアクセスの復元

## システムドライブへのアクセスの復元

復元手順を開始するには、ユーザーはプリブート認証段階で **Esc** キーを押す必要があります。

**[管理コンソール \(MMC\) で BitLocker によって暗号化されたシステムドライブの回復キーを表示する方法](#)** 

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [デバイス] タブを選択します。
4. [デバイス] タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
5. コンテキストメニューで、 [オフラインモードでのアクセスを許可する] を選択します。
6. 表示されたウィンドウで、 BitLocker で保護されたシステムドライブへのアクセスタブを選択します。
7. BitLocker パスワード入力ウィンドウに示されている回復キーの ID をユーザーに尋ね、 [回復キーの ID] の値と比較します。

ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。

## Web コンソールまたは Cloud コンソールで BitLocker で暗号化されたシステムドライブの回復キーを表示する方法



1. Web コンソールのメインウィンドウで、 [デバイス] → [管理対象デバイス] の順に選択します。
2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。
4. 表示されたウィンドウで、 [BitLocker] セクションを選択します。
5. 回復キーの ID を確認します。ユーザーが提供する ID は、コンピューターの設定に表示される ID と一致する必要があります。

ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

6. [予備のライセンス] をクリックします。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。

オペレーティングシステムが読み込まれた後、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促します。新しいパスワードまたは PIN コードを設定した後、BitLocker は新しいマスター鍵を作成し、その鍵を Kaspersky Security Center に送ります。回復キーおよび回復キーファイルが更新されます。ユーザーがパスワードを変更していない場合は、オペレーティングシステムが次に読み込まれるときに古い回復キーを使用できます。

Windows 7 搭載のコンピューターでは、パスワードまたは PIN コードの変更が許可されません。回復キーが入力され、オペレーティングシステムが読み込まれた後は、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促しません。このため、新しいパスワードまたは PIN コードを設定することはできません。この問題はオペレーティングシステムの実行によるものです。続行するには、ハードドライブを再度暗号化する必要があります。

## システムドライブ以外のドライブへのアクセスの復元

復元手順を開始するには、ユーザーがドライブへのアクセスを提供するウィンドウで **パスワードを忘れた場合** のリンクをクリックする必要があります。暗号化されたドライブにアクセスした後、ユーザーは BitLocker の設定で Windows 認証中にドライブの自動ロック解除を有効にできます。

### 管理コンソール (MMC) で BitLocker によって暗号化されたシステムドライブ以外のドライブの回復キーを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、**[詳細]** → **[データ暗号化と保護機能]** → **[暗号化されたドライブ]** フォルダの順に選択します。
3. 作業領域で、アクセスキーファイルを作成する暗号化されたデバイスを選択し、デバイスのコンテキストメニューで **[Kaspersky Endpoint Security for Windows のデバイスへのアクセス]** をクリックします。
4. BitLocker パスワード入力ウィンドウに示されている回復キーの ID をユーザーに尋ね、**[回復キーの ID]** の値と比較します。

ID が一致しない場合、キーは無効であり、指定されたドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

5. **[回復キー]** に表示されているキーをユーザーに送信します。

### Web コンソールおよび Cloud コンソールで BitLocker で暗号化されたシステムドライブ以外のドライブの回復キーを表示する方法

1. Web コンソールのメインウィンドウで、[操作] → [データ暗号化と保護機能] → [暗号化されたドライブ] の順に選択します。
2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。  
これにより、デバイスへのアクセスを許可するためのウィザードが開始されます。
4. ウィザードの指示に従って、デバイスへのアクセスを許可します。
  - a. **Kaspersky Endpoint Security for Windows** のプラグインを選択します。
  - b. 回復キーの ID を確認します。ユーザーが提供する ID は、コンピューターの設定に表示される ID と一致する必要があります。

ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

- c. [予備のライセンス] をクリックします。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。

## ソフトウェアアップデート時の BitLocker 保護の一時停止

BitLocker 保護が有効な状態でのオペレーティングシステムのアップデート、オペレーティングシステムへのアップデートパッケージのインストール、またはその他のソフトウェアのアップデート時には留意事項が少なくありません。アップデートのインストールには、コンピューターの再起動が複数回必要になることがあります。再起動ごとにユーザーは BitLocker 認証を完了する必要があります。アップデートを正常にインストールするために、一時的に BitLocker 認証をオフにすることができます。この場合ディスクは暗号化されたままで、ユーザーはシステムにサインインした後にデータにアクセスすることができます。BitLocker 認証を管理するには、*BitLocker* 保護の管理タスクを使用できます。このタスクを使用して、BitLocker 認証を必要としないコンピューターの再起動の回数を指定することができます。アップデートがインストールされて *BitLocker* 保護の管理タスクが完了すると、BitLocker 認証は自動的にオンになります。いつでも BitLocker 認証をオンにできます。

### [管理コンソール \(MMC\) を使用して BitLocker 保護を一時停止する方法](#)

1. 管理コンソールで、**[管理サーバー]** → **[タスク]** のフォルダーに移動します。  
タスクのリストが表示されます。

2. **[新規タスク]** をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

**[Kaspersky Endpoint Security for Windows (11.7.0)]** → **[BitLocker 保護の管理]** を選択します。

## ステップ 2：BitLocker 保護の管理

BitLocker 認証を設定します。BitLocker 保護を一時停止するには、**[一時的に BitLocker 認証のスキップを許可する]** を選択して BitLocker 認証をスキップする再起動の回数を入力します (1 ~ 15 回)。必要に応じて、タスクの有効期限の日時を入力します。指定した回数でタスクは自動的にオフになり、ユーザーはその後コンピューターが再起動した際に BitLocker 認証を完了する必要があります。

## ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 4：タスク名の定義

「Windows 10 のアップデート」などのタスクの名前を入力します。

## ステップ 5：タスク作成の完了

ウィザードを終了します。必要に応じて、**[ウィザードの完了後にタスクを実行]** をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

[Web コンソールを使用して BitLocker 保護を一時停止する方法](#) 



1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
2. **【タスク種別】** で、**【BitLocker 保護の管理】** を選択します。
3. **【タスク名】** に「Windows 10 のアップデート」などの簡潔な名前を付けます。
4. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。

## ステップ 2：BitLocker 保護の管理

BitLocker 認証を設定します。BitLocker 保護を一時停止するには、**【一時的に BitLocker 認証のスキップを許可する】** を選択して BitLocker 認証をスキップする再起動の回数を入力します（1～15 回）。必要に応じて、タスクの有効期限の日時を入力します。指定した回数でタスクは自動的にオフになり、ユーザーはその後コンピューターが再起動した際に BitLocker 認証を完了する必要があります。

## ステップ 3：タスク作成の完了

**【終了】** をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。

タスクを実行するには、タスクのチェックボックスをオンにし、**【開始】** をクリックします。

その結果、タスクの実行中は次のコンピューターの再起動以降 BitLocker がユーザー認証を求めることはありません。BitLocker 認証を省略してコンピューターを再起動するたびに、Kaspersky Endpoint Security は対応するイベントを作成し、残りの再起動回数を記録します。Kaspersky Endpoint Security は次にそのイベントを Kaspersky Security Center に送り、管理者が監視できるようにします。Kaspersky Security Center のコンソールで、コンピューターのプロパティから残りの再起動の回数を確認することができます。

指定した再起動の回数に到達する、もしくはタスクの有効期間が終了すると、BitLocker 認証は自動的に有効になります。データにアクセスするためには、ユーザーは BitLocker 認証を完了する必要があります。

Windows 7 を実行しているコンピューターでは、BitLocker はコンピューターの再起動の回数を記録できません。Windows 7 のコンピューターの再起動回数は、Kaspersky Endpoint Security 側で記録します。このため、再起動ごとに自動的に BitLocker 認証をオンにするには、Kaspersky Endpoint Security が開始されている必要があります。

事前に BitLocker 認証をオンにするには、*BitLocker* 保護の管理タスクのプロパティを開いて、**【常に起動前認証を要求する】** を選択してください。

## ローカルコンピュータドライブでのファイルレベルの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピュータに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピュータに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ファイル暗号化には、次の特別な機能があります：

- Kaspersky Endpoint Security は、オペレーティングシステムのローカルユーザープロファイルについてのみ定義済みフォルダーのファイルの暗号化や復号化を行います。Kaspersky Endpoint Security は、移動ユーザープロファイル、固定ユーザープロファイル、一時ユーザープロファイル、またはリダイレクトされたフォルダーの、定義済みフォルダー内のファイルを暗号化または復号化しません。
- Kaspersky Endpoint Security は、暗号化が原因でオペレーティングシステムやインストールされたアプリケーションに損害を与える可能性がある場合は、ファイルを暗号化しません。たとえば、次のファイルおよびフォルダーは、入れ子になっているすべてのフォルダーとともに、暗号化しないファイルまたはフォルダーのリストに含まれます：
  - %WINDIR%;
  - %PROGRAMFILES% and %PROGRAMFILES(X86)%;
  - Windows のレジストリファイル

暗号化しないファイルまたはフォルダーのリストは、表示することも編集することもできません。暗号化除外リストにあるファイルとフォルダーは暗号化リストに追加できますが、ファイルの暗号化中は暗号化されません。

## ローカルコンピュータドライブのファイルの暗号化

Kaspersky Endpoint Security では、OneDrive クラウドストレージに置かれているファイルを暗号化しません。また、暗号化されたファイルが[復号化ルール](#)に追加されていない限り、暗号化されたファイルの OneDrive クラウドストレージへのコピーをブロックします。

ローカルドライブでファイルを暗号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **管理対象デバイス** フォルダーで、設定を適用するクライアントコンピュータが属している管理グループのフォルダーを開きます。
3. 作業領域で、**ポリシー** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**データ暗号化** → **ファイルレベルの暗号化** の順に選択します。

6. ウィンドウの右側で、**〔暗号化〕** タブを選択します。
  7. **〔暗号化モード〕** で、**〔ルールに従う〕** を選択します。
  8. **〔暗号化〕** タブで **〔追加〕** をクリックし、ドロップダウンリストから次のいずれかを選択します：
    - a. カスペルスキーが推奨するローカルユーザープロファイルフォルダーのファイルを暗号化ルールに追加するには、**〔定義済みフォルダー〕** を選択します。
      - **ドキュメント**：オペレーティングシステムの標準の **〔ドキュメント〕** フォルダー内のファイルとそのサブフォルダー。
      - **お気に入り**：オペレーティングシステムの標準の **〔お気に入り〕** フォルダー内のファイルとそのサブフォルダー。
      - **デスクトップ**：オペレーティングシステムの標準の **〔デスクトップ〕** フォルダー内のファイルとそのサブフォルダー。
      - **一時ファイル**：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の動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。
      - **Outlook ファイル**：Outlook メールクライアントの動作に関連するファイル(データファイル(PST)、オフラインデータファイル(OST)、オフラインアドレス帳ファイル(OAB)、および個人のアドレス帳ファイル(PAB))。
    - b. 暗号化ルールに追加するフォルダーのパスを手動で入力するには、**〔カスタムフォルダー〕** を選択します。

フォルダーのパスを追加するときは、次のルールに従います：

      - 環境変数を使用します(たとえば、%FOLDER%\UserFolder\)。環境変数は、パスの先頭で一度だけ使用できます。
      - 相対パスは使用しないでください。**〔\..\〕** のセットを使用できます(例：  
C:\Users\..\UserFolder\)。**〔\..\〕** のセットは、親フォルダーへの移動を意味します。
      - **〔\*および?〕** の文字は使用しないでください。
      - UNC パスは使用しないでください。
      - 区切り文字として、**〔;〕** または **〔,〕** を使用してください。
    - c. **〔ファイルの拡張子による指定〕** を選択して、暗号化ルールに個々のファイルの拡張子を追加します。Kaspersky Endpoint Security は、コンピューターのすべてのローカルドライブ上の指定された拡張子を持つファイルを暗号化します。
    - d. **〔ファイルの拡張子のグループによる指定〕** を選択して、ファイルの拡張子のグループを暗号化ルールに追加します(たとえば、*Microsoft Office Documents*)。拡張子のグループに含まれるファイル拡張子を持つ、コンピューターのローカルドライブにあるすべてのファイルが暗号化されます。
  9. 変更内容を保存します。
- ポリシーを適用すると、Kaspersky Endpoint Security は、暗号化ルールに含まれ **復号化ルール** に含まれていないファイルをただちに暗号化します。

ファイル暗号化には、次の特別な機能があります：

- 同じファイルが暗号化ルールと復号化ルールの両方に追加されている場合、Kaspersky Endpoint Security は次の処理を実行します：
  - ファイルが暗号化されていない場合、Kaspersky Endpoint Security はファイルを暗号化しません。
  - ファイルが暗号化されている場合は、Kaspersky Endpoint Security はファイルを復号化します。
- 暗号化ルールの条件に一致する新しいファイルがある場合、Kaspersky Endpoint Security は続けて暗号化します。例えば、暗号化されていないファイルのパスや拡張子などの属性を変更した場合、暗号化ルールの条件に一致することになります。Kaspersky Endpoint Security はこのファイルを暗号化します。
- 新しいファイルが作成され、そのファイルのプロパティが暗号化ルールの条件と一致する場合、Kaspersky Endpoint Security はそのファイルが開かれると同時に暗号化します。
- Kaspersky Endpoint Security は、開かれているファイルについては、閉じられるまで暗号化を延期します。
- 暗号化されているファイルを同じローカルドライブ上の別のフォルダーに移動する場合、移動先のフォルダーが暗号化ルールに含まれるかどうかとは関係なく、ファイルの暗号化は維持されます。
- ファイルを復号化して、復号化ルールに含まれていない別のローカルのフォルダーにコピーした場合、このファイルのコピーは暗号化される可能性があります。コピーしたファイルが暗号化されないようにするには、対象のフォルダーに復号化ルールを作成します。

## アプリケーションを対象にした暗号化ファイルへのアクセスルールの策定

アプリケーションを対象に暗号化ファイルへのアクセスルールを策定するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **【管理対象デバイス】** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、**【ポリシー】** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**【データ暗号化】** → **【ファイルレベルの暗号化】** の順に選択します。
6. ウィンドウの右側で、**【暗号化】** タブを選択します。
7. **【暗号化モード】** で、**【ルールに従う】** を選択します。

アクセスルールは、**【ルールに従う】** が選択されている場合のみ適用されます。**【ルールに従う】** を選択した後、**【変更しない】** に変更すると、すべてのアクセスルールが無視されます。すべてのアプリケーションがすべての暗号化されたファイルへアクセスできるようになります。

8. ウィンドウの右側で、**【アプリケーションのルール】** タブを選択します。
9. Kaspersky Security Center のリストからのみアプリケーションを選択するには、**【追加】** をクリックして、ドロップダウンリストで **【Kaspersky Security Center のリストからのアプリケーションの追加】** を選択します。

- a. テーブルのアプリケーションリストの項目を絞るためのフィルターを指定します。そのためには、**[アプリケーション]**、**[製造元]**、**[追加された期間]** の各パラメータと **[グループ]** セクションのすべてチェックボックスの値を指定します。
- b. **[更新]** をクリックします。
- c. テーブルに適用されたフィルターの基準を満たすアプリケーションが表示されます。
- d. **[アプリケーション]** 列で、暗号化ファイルアクセスルールの策定の対象にするアプリケーションの横にあるチェックボックスをオンにします。
- e. **[アプリケーションのルール]** で、暗号化ファイルへのアプリケーションのアクセスを決定するルールを選択します。
- f. **[以前に選択したアプリケーションの処理]** で、アプリケーションに対して以前に作成された暗号化ファイルアクセスルールに対する処理を選択します。

アプリケーションの暗号化ファイルアクセスルールの詳細が **[アプリケーションのルール]** タブのテーブルに表示されます。

10. 手動でアプリケーションを選択するには、**[追加]** をクリックして、ドロップダウンリストで **[カスタムアプリケーション]** を選択します。
  - a. エントリフィールドに、アプリケーションの実行ファイルの名前または名前のリストを拡張子を含めて入力します。

**[Kaspersky Security Center のリストからの追加]** をクリックすることで、Kaspersky Security Center のリストからアプリケーションの実行ファイルの名前を追加することもできます。
  - b. 必要に応じて、**[説明]** にアプリケーションリストの説明を入力します。
  - c. **[アプリケーションのルール]** で、暗号化ファイルへのアプリケーションのアクセスを決定するルールを選択します。

アプリケーションの暗号化ファイルアクセスルールの詳細が **[アプリケーションのルール]** タブのテーブルに表示されます。

11. 変更内容を保存します。

## 特定のアプリケーションによって作成または変更されたファイルの暗号化

ルールで指定されたアプリケーションによって作成または変更されたすべてのファイルを暗号化するようなルールを作成できます。

その暗号化ルールが適用される前に、指定されたアプリケーションで作成または変更されたファイルは、暗号化されません。

特定のアプリケーションによって作成または変更されたファイルを暗号化するよう設定するには：

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [データ暗号化] → [ファイルレベルの暗号化] の順に選択します。
6. ウィンドウの右側で、 [暗号化] タブを選択します。
7. [暗号化モード] で、 [ルールに従う] を選択します。

暗号化ルールは、 [ルールに従う] が選択されている場合のみ適用されます。 [ルールに従う] を選択した後、 [変更しない] に変更すると、すべての暗号化ルールが無視されます。すでに暗号化されたファイルは暗号化されたままになります。

8. ウィンドウの右側で、 [アプリケーションのルール] タブを選択します。
9. Kaspersky Security Center のリストからのみアプリケーションを選択するには、 [追加] をクリックして、ドロップダウンリストで [Kaspersky Security Center のリストからのアプリケーションの追加] を選択します。
  - a. テーブルのアプリケーションリストの項目を絞るためのフィルターを指定します。そのためには、 [アプリケーション]、 [製造元]、 [追加された期間] の各パラメータと [グループ] セクションのすべてチェックボックスの値を指定します。
  - b. [更新] をクリックします。  
テーブルに適用されたフィルターの基準を満たすアプリケーションが表示されます。
  - c. [アプリケーション] 列で、作成したファイルを暗号化するアプリケーションの横にあるチェックボックスを選択します。
  - d. [アプリケーションのルール] で、 [作成されたすべてのファイルを暗号化する] を選択します。
  - e. [以前に選択したアプリケーションの処理] で、アプリケーションに対して以前に作成されたファイル暗号化ルールに対する処理を選択します。

選択されたアプリケーションによって作成または変更されたファイルの暗号化ルールの情報が [アプリケーションのルール] タブのテーブルに表示されます。

10. 手動でアプリケーションを選択するには、 [追加] をクリックして、ドロップダウンリストで [カスタムアプリケーション] を選択します。
  - a. エントリフィールドに、アプリケーションの実行ファイルの名前または名前のリストを拡張子を含めて入力します。  
[Kaspersky Security Center のリストからの追加] をクリックすることで、Kaspersky Security Center のリストからアプリケーションの実行ファイルの名前を追加することもできます。
  - b. 必要に応じて、 [説明] にアプリケーションリストの説明を入力します。
  - c. [アプリケーションのルール] で、 [作成されたすべてのファイルを暗号化する] を選択します。

選択されたアプリケーションによって作成または変更されたファイルの暗号化ルールの情報が [アプリケーションのルール] タブのテーブルに表示されます。



11. 変更内容を保存します。

## 復号化ルールの作成

復号化ルールを作成するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [ファイルレベルの暗号化] の順に選択します。
6. ウィンドウの右側で、[復号化] タブを選択します。
7. [暗号化モード] で、[ルールに従う] を選択します。
8. [復号化] タブで [追加] をクリックし、ドロップダウンリストから次のいずれかを選択します：
  - a. カスペルスキーが推奨するローカルユーザープロファイルフォルダーのファイルを復号化ルールに追加するには、[定義済みフォルダー] を選択します。
  - b. 復号化ルールに追加するフォルダーのパスを手動で入力するには、[カスタムフォルダー] を選択します。
  - c. [ファイルの拡張子による指定] を選択して、暗号化ルールに個々のファイルの拡張子を追加します。Kaspersky Endpoint Security は、コンピューターのすべてのローカルドライブ上のファイルのうち指定された拡張子を持つものについては暗号化を行いません。
  - d. [ファイルの拡張子のグループによる指定] を選択して、ファイルの拡張子のグループを暗号化ルールに追加します（たとえば、*Microsoft Office Documents*）。拡張子のグループに含まれるファイル拡張子を持つ、コンピューターのローカルドライブにあるすべてのファイルが暗号化されません。
9. 変更内容を保存します。

同じファイルが暗号化ルールと復号化ルールの両方に追加されると、そのファイルが暗号化されていない場合は暗号化されず、暗号化されている場合は復号化されます。

## ローカルコンピュータードライブでのファイルの復号化

ローカルドライブでファイルを復号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。



3. 作業領域で、**［ポリシー］** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**［データ暗号化］** → **［ファイルレベルの暗号化］** の順に選択します。
6. ウィンドウの右側で、**［暗号化］** タブを選択します。
7. 復号化するファイルとフォルダーを暗号化リストから削除します。リストからの削除には、ファイルを選択して、**［削除］** のコンテキストメニューから **［ルールの削除とファイルの復号化］** を選択します。  
暗号化リストから、複数の項目を一度に削除することもできます。複数項目を削除するには、**CTRL** キーを押しながら、必要なファイルを左クリックして選択し、**［削除］** のコンテキストメニューから **［ルールの削除とファイルの復号化］** を選択します。  
暗号化リストから削除されたファイルやフォルダーは、自動的に復号化リストに追加されます。
8. [ファイル復号化リストを作成します。](#)
9. 変更内容を保存します。

Kaspersky Endpoint Security は、ポリシーが適用されると、復号化リストに追加された暗号化ファイルをすぐに復号化します。

Kaspersky Endpoint Security は、暗号化されているファイルのパラメータ（ファイルパス / ファイル名 / ファイル拡張子）が変更され、復号化リストに追加されているオブジェクトのパラメータと一致すると、そのファイルを復号化します。

Kaspersky Endpoint Security は、開かれているファイルについては、閉じられるまで復号化を延期します。

## 暗号化されたパッケージへの追加

企業ネットワーク外のユーザーへのファイル送付時にデータを保護する目的で、暗号化されたパッケージを使用できます。メールクライアントには添付ファイルのサイズ制限があるため、暗号化されたパッケージは、リムーバブルドライブ上にあるサイズが大きなファイルを送付するのに便利です。

暗号化されたパッケージの作成前に、パスワードの設定が要求されます。データ保護の信頼性を高めるため、パスワードの強度チェックと、パスワードの強度の指定の有効化が可能です。有効にすると、「1234」のような短く単純なパスワードが使用できなくなります。

[暗号化されたアーカイブを管理コンソール \(MMC\) で作成するときにパスワードの強度チェックを有効にする方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [データ暗号化] → [暗号化の共通設定] の順に選択します。
6. [パスワードの設定] ブロックで、 [設定] をクリックします。
7. 表示されたウィンドウで、 [暗号化されたパッケージ] タブを選択します。
8. 暗号化されたパッケージの作成時のパスワードの複雑さを設定します。

### **暗号化されたアーカイブを Web コンソールで作成するときにパスワードの強度チェックを有効にする方法**

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. パスワードの強度チェックを有効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [データ暗号化] → [ファイルレベルの暗号化] の順に移動します。
5. [暗号化されたパッケージのパスワード設定] ブロックで、暗号化されたパッケージの作成時に必要なパスワードの強度の条件を設定します。

暗号化されたパッケージは、ファイルレベルの暗号化機能とともに Kaspersky Endpoint Security がインストールされたコンピューターで作成できます。

OneDrive クラウドストレージ上にある暗号化されたパッケージにファイルを追加すると、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードして暗号化を実行します。

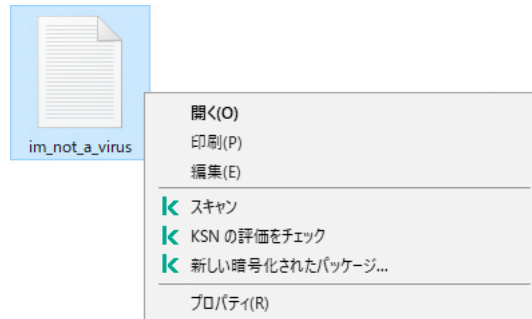
暗号化されたパッケージを作成するには：

1. 任意のファイル管理アプリケーションで、暗号化されたパッケージに追加するファイルまたはフォルダーを選択します。右クリックして、ファイルまたはフォルダーのコンテキストメニューを開きます。
2. コンテキストメニューで、 [新しい暗号化されたパッケージ] を選択します（下の図を参照）。
3. 表示されたウィンドウで、暗号化されたパッケージを保存するリムーバブルドライブ上の場所を選択し、パッケージ名を指定して [保存] をクリックします。
4. 表示されたウィンドウで、パスワードを指定し、入力して確認します。

パスワードは、ポリシーで指定したパスワードの複雑さの基準を満たす必要があります。

##### 5. [新規作成] をクリックします。

暗号化されたパッケージの作成プロセスが開始されます。Kaspersky Endpoint Security は、暗号化されたパッケージの作成時に、ファイルの圧縮は行いません。プロセスが終了すると、パスワードで保護されており暗号化された自己解凍形式パッケージ (🔒) が、選択した保存先フォルダーに作成されます。



暗号化されたパッケージの作成

暗号化されたパッケージ内のファイルにアクセスするには、ダブルクリックして解凍ウィザードを開始し、パスワードを入力します。忘れたり紛失したりしたパスワードは復旧できず、暗号化されたパッケージ内のファイルへのアクセスもできなくなります。暗号化されたパッケージを再作成してください。

## 暗号化されたファイルへのアクセスの復元処理

ファイルが暗号化されると、Kaspersky Endpoint Security は、暗号化されたファイルに直接アクセスするために必要な暗号化鍵を受け取ります。この暗号化鍵を使用すると、ファイルの暗号化中にアクティブだった Windows アカウントで作業しているユーザーは、暗号化ファイルに直接アクセスできます。ファイルの暗号化中、アクティブではなかった Windows アカウントで作業しているユーザーは、暗号化ファイルにアクセスするには、Kaspersky Security Center に接続する必要があります。

次の状況では、暗号化されたファイルにアクセスできないことがあります：

- ユーザーのコンピューターに暗号鍵が保存されているが、Kaspersky Security Center と接続されていないため鍵の管理ができない。この場合、ユーザーは LAN 管理者に暗号化ファイルへのアクセスを要求する必要があります。

Kaspersky Security Center にアクセスする手段がない場合は、次を行ってください：

- コンピューターのハードディスクにある暗号化されたファイルにアクセスするためのアクセスキーを要求する。
- リムーバブルドライブに保存されている暗号化ファイルにアクセスするには、各リムーバブルドライブの暗号化ファイルに対してそれぞれアクセスキーを要求する。
- 暗号化機能がユーザーのコンピューターから削除されている。この場合、ローカルドライブおよびリムーバブルドライブ上の暗号化されたファイルを開くことはできますが、ファイルの内容は暗号化された状態で表示されます。

ユーザーは次の場合に、暗号化されたファイルにアクセスできます：

- Kaspersky Endpoint Security がインストールされているコンピューターで作成された 暗号化パッケージ の中にファイルが保存されている。
- ポータブルモード が許可されたリムーバブルドライブにファイルが保存されている。

暗号化されたファイルにアクセスするには、ユーザーは復元手順（要求と応答）を開始する必要があります。

暗号化されたファイルへのアクセスを復元するには、次の手順を実行します：

1. ユーザーがアクセス要求ファイルを管理者に送信します（以下の図を参照）。
2. 管理者はアクセス要求ファイルを Kaspersky Security Center に追加し、アクセスキーファイルを作成してユーザーに送信します。
3. ユーザーはアクセスキーファイルを Kaspersky Endpoint Security に追加し、ファイルへのアクセスを取得します。



暗号化されたファイルへのアクセスの復元処理

復元手順を開始するには、ユーザーはファイルにアクセスを試みる必要があります。その結果、Kaspersky Endpoint Security はアクセス要求ファイル（拡張子が KESDC のファイル）を作成します。ユーザーは、このファイルを管理者に電子メールなどで送信する必要があります。

Kaspersky Endpoint Security は、コンピューターのドライブ（ローカルドライブまたはリムーバブルドライブ）に保存されているすべての暗号化されたファイルにアクセスするためのアクセス要求ファイルを生成します。

### [管理コンソール（MMC）で暗号化されたデータアクセスキーファイルを取得する方法](#)

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [デバイス] タブを選択します。
4. [デバイス] タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
5. コンテキストメニューで、 [オフラインモードでのアクセスを許可する] を選択します。
6. 表示されたウィンドウで、 [データ暗号化] タブを選択します。
7. [データ暗号化] タブで [参照] をクリックします。
8. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。

### Web コンソールで暗号化されたデータアクセスキーファイルを取得する方法

1. Web コンソールのメインウィンドウで、 [デバイス] → [管理対象デバイス] の順に選択します。
2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。
4. [データ暗号化] セクションを選択します。

5. [ファイルを選択] をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。

Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。

6. [ライセンスを保存] をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

暗号化されたデータアクセスキーファイルを受信した後、ユーザーはファイルをダブルクリックして実行する必要があります。その結果、Kaspersky Endpoint Security はドライブに保存されているすべての暗号化されたファイルへのアクセスを許可します。他のドライブに保存されている暗号化ファイルにアクセスするには、ドライブごとに別々のアクセスキーファイルを入手する必要があります。

# オペレーティングシステム障害が発生した後の暗号化されたデータへのアクセスの復元

オペレーティングシステム障害が発生した場合は、ファイルレベルの暗号化（FLE）を使用していた場合のみ、データへのアクセスを復元できます。ディスク全体の暗号化（FDE）を使用していた場合は、データへのアクセスは復元できません。

オペレーティングシステム障害が発生した後に、暗号化されたデータへのアクセスを復元するには：

1. ハードディスクをフォーマットせずにオペレーティングシステムを再インストールします。
2. [Kaspersky Endpoint Security をインストール](#)します。
3. コンピューターと、データの暗号化時にコンピューターを管理していた Kaspersky Security Center の管理サーバーとの接続を確立します。

オペレーティングシステム障害が発生する前と同じ条件で、暗号化されたデータへのアクセスが許可されます。

## 暗号化ファイルアクセスメッセージのテンプレートの編集

暗号化ファイルアクセスメッセージのテンプレートを編集するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **管理対象デバイス** フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、**ポリシー** タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、**データ暗号化** → **暗号化の共通設定** の順に選択します。
6. **テンプレート** セクションで、**テンプレート** をクリックします。  
**テンプレート** ウィンドウが表示されます。
7. 次の手順に従います：
  - ユーザーメッセージテンプレートを編集するには、**ユーザーのメッセージ** タブを選択します。コンピューター上に暗号化ファイルへのアクセスに使用できるキーがない場合、ユーザーが暗号化されたファイルにアクセスを試みると、**データへのアクセスがブロックされました** ウィンドウが表示されます。**データへのアクセスがブロックされました** ウィンドウで **メールで送信** をクリックすると、ユーザーメッセージが自動的に作成されます。このメッセージが、暗号化ファイルへのアクセスを要求するファイルとともに企業の LAN 管理者に送信されます。
  - 管理者メッセージテンプレートを編集するには、**管理者のメッセージ** タブを選択します。このメッセージは、**暗号化されたファイルへのアクセスの要求** ウィンドウで **メールで送信** がクリックされると自動で作成され、ユーザーが暗号化ファイルへのアクセス権を付与された後でユーザーに送信されます。



8. メッセージテンプレートを編集します。

[既定] と [変数] を使用できます。

9. 変更内容を保存します。

## リムーバブルドライブの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムのファイルの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、このリムーバブルドライブの暗号化タスクはエラーにより失敗し、リムーバブルドライブが読み取り専用になります。

リムーバブルドライブ上のデータを保護するには、次の暗号化種別を使用できます：

- ディスク全体の暗号化 (FDE)

ファイルシステムを含むリムーバブルドライブ全体の暗号化。

企業ネットワークの外部で暗号化されたデータにアクセスすることはできません。Kaspersky Security Center へ接続されていないコンピューターの場合 (ゲストコンピューターなど) も、企業ネットワーク内の暗号化されたデータへアクセスできません。

- ファイルレベルの暗号化 (FLE)

リムーバブルドライブ上のファイルのみの暗号化。ファイルシステムは変更されません。

リムーバブルドライブ上のファイルの暗号化は、[ポータブルモード](#)と呼ばれる特別なモードを使用して、企業ネットワークの外部のデータにアクセスする機能を提供します。

暗号化中に、Kaspersky Endpoint Security はマスター鍵を作成します。Kaspersky Endpoint Security は、マスター鍵を次のリポジトリに保存します：

- Kaspersky Security Center

- ユーザーのコンピューター

マスター鍵はユーザーの秘密鍵で暗号化されます。

- リムーバブルドライブ

マスター鍵は、Kaspersky Security Center の公開鍵で暗号化されています。

暗号化が完了すると、従来のリムーバブルドライブを暗号化せずに使用しているかのように、企業ネットワーク内でリムーバブルドライブ上のデータにアクセスできます。



## 暗号化されたデータへのアクセス

暗号化されたデータのリムーバブルドライブが接続されると、Kaspersky Endpoint Security は次のアクションを実行します：

1. ユーザーのコンピューターのローカル保管領域でマスター鍵を確認します。  
マスター鍵が見つかった場合、ユーザーはリムーバブルドライブ上のデータにアクセスできます。  
マスター鍵が見つからない場合、Kaspersky Endpoint Security は次のアクションを実行します：
  - a. Kaspersky Security Center に要求を送信します。  
要求を受け取った後、Kaspersky Security Center はマスター鍵を含む応答を送信します。
  - b. Kaspersky Endpoint Security は、暗号化されたリムーバブルドライブを使用した、それ以降の操作のために、ユーザーのコンピューターのローカル保管領域にマスター鍵を保存します。
2. データを復号化します。

## リムーバブルドライブ暗号化の特別な機能

リムーバブルドライブの暗号化には、次の特別な機能があります：

- リムーバブルドライブの暗号化に関する事前設定はポリシーに含まれます。このポリシーは、管理対象コンピューターの特定のグループに対して作成されています。このため、リムーバブルドライブの暗号化または復号化の設定を含む Kaspersky Security Center ポリシーの適用結果は、そのリムーバブルドライブがどのコンピューターに接続しているかによって異なります。
- Kaspersky Endpoint Security は、リムーバブルドライブに保存されている読み取り専用ステータスのファイルの暗号化や復号化は行いません。
- リムーバブルドライブとして、次のデバイス種別がサポートされています：
  - USB バス経由で接続されているリムーバブルドライブ
  - USB および FireWire バス経由で接続されているハードディスク
  - USB および FireWire バス経由で接続されている SSD ドライブ

## リムーバブルドライブの暗号化の開始

ポリシーを使用して、リムーバブルドライブを復号化できます。リムーバブルドライブの暗号化の設定が定義されたポリシーが、特定の管理グループに対して生成されます。このため、リムーバブルドライブに対するデータ復号化の結果は、リムーバブルドライブが接続されているコンピューターによって異なります。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、リムーバブルドライブの暗号化はエラーにより失敗し、このリムーバブルドライブは読み取り専用になります。

リムーバブルドライブを暗号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [データ暗号化] → [リムーバブルドライブの暗号化] の順に選択します。
6. [暗号化モード] ドロップダウンリストで、リムーバブルドライブに対して実行する既定の処理を選択します。

- **リムーバブルドライブ全体の暗号化 (FDE)** : Kaspersky Endpoint Security によって、リムーバブルドライブのすべてのセクションが暗号化されます。その結果、リムーバブルドライブに保存されているファイルだけでなく、ファイル名やフォルダー構造を含むファイルシステムも暗号化されます。
- **すべてのファイルの暗号化 (FLE)** : Kaspersky Endpoint Security によって、リムーバブルドライブ上のすべてのファイルが暗号化されます。ファイルの名前やフォルダー構造を含めて、リムーバブルドライブのファイルシステムは暗号化されません。
- **新しいファイルのみ暗号化 (FLE)** : Kaspersky Security Center ポリシーが前回適用された後でリムーバブルドライブに追加されたファイルと、以前からリムーバブルドライブに保存されていたがポリシーの前の適用後に変更されたファイルだけを暗号化します。

Kaspersky Endpoint Security は、既に暗号化されているリムーバブルドライブは暗号化しません。

7. リムーバブルドライブの暗号化で ポータブルモードを使用する 場合は、 [ポータブルモード] をオンにします。

[ポータブルモード] は、リムーバブルドライブ上のファイル暗号化 (FLE) のモードであり、このモードを使用すると社内ネットワーク外にあるデータにアクセスできます。また、ポータブルモードでは、Kaspersky Endpoint Security をインストールしていないコンピューターで暗号化データを操作することもできます。
8. 未使用の新しいリムーバブルドライブを暗号化するときは、 [使用されているディスク領域のみを暗号化] をオンにすることを推奨します。このチェックボックスがオフの場合、過去に削除されたファイルや変更が加えられたファイルの残存している断片も含めたすべてのファイルが Kaspersky Endpoint Security によって暗号化されます。
9. それぞれのリムーバブルドライブに対して個別に暗号化の設定を指定する場合は、 暗号化ルールを設定 します。
10. オフラインモードでリムーバブルドライブ全体の暗号化を使用する場合は、 [オフラインモードでのリムーバブルドライブの暗号化を許可する] をオンにします。

オフラインモードでの暗号化は、Kaspersky Security Center との接続がない状態でのリムーバブルドライブの暗号化 (FDE) です。暗号化を実行中、Kaspersky Endpoint Security はクライアントコンピューター上のみマスター鍵を保存します。Kaspersky Security Center と次に同期したときに、Kaspersky Endpoint Security は Kaspersky Security Center にマスター鍵を送信します。

マスター鍵が保存されているコンピューターでマスター鍵のデータが破損し、なおかつマスター鍵が Kaspersky Security Center に送信されていなかった場合、リムーバブルドライブのデータへのアクセスを復元することはできません。

[オフラインモードでのリムーバブルドライブの暗号化を許可する] がオフの場合、Kaspersky Security Center への接続が確立されていない状況ではリムーバブルドライブの暗号化は実行できません。

## 11. 変更内容を保存します。

ポリシーの適用後、ユーザーがリムーバブルドライブを接続したタイミングで（あるいは既にリムーバブルドライブが接続されている場合はただちに）、暗号化を実行するかどうかの確認メッセージがユーザーに表示されます（以下の図を参照）。

ユーザーは次の操作を実行できます：

- 暗号化を実行することをユーザーが承認した場合、Kaspersky Endpoint Security によってデータが暗号化されます。
- 暗号化の実行をユーザーが拒否した場合、データは変更されませんが、リムーバブルドライブは読み取り専用になります。
- 暗号化を実行するかどうかの確認メッセージにユーザーが応答しない場合、データは変更されませんが、リムーバブルドライブは読み取り専用になります。ポリシーが次に更新されて適用されたとき、あるいはこのリムーバブルドライブが次に接続されたときに、暗号化を実行するかどうかの確認メッセージが再表示されます。

データの暗号化中にユーザーがリムーバブルドライブを安全な手順で取り出そうとすると、Kaspersky Endpoint Security はデータの暗号化プロセスを中断して、暗号化プロセスの完了前にリムーバブルドライブを取り出せるようにします。同じリムーバブルドライブがこのコンピューターに次に接続されたときに、データの暗号化が引き続き実行されます。

リムーバブルドライブの暗号化が失敗した場合、**データ暗号化レポート**を本製品のインターフェイスで参照してください。他のアプリケーションによってファイルアクセスがブロックされている可能性があります。その場合、リムーバブルドライブをコンピューターから取り外してから再度接続してみてください。



リムーバブルドライブの暗号化要求

## リムーバブルドライブの暗号化ルールの追加

リムーバブルドライブの暗号化ルールを追加するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [リムーバブルドライブの暗号化] の順に選択します。
6. [追加] をクリックし、ドロップダウンリストから次のいずれかを選択します：
  - デバイスコントロールの信頼するデバイスのリストにあるリムーバブルドライブの暗号化ルールを追加するには、[このポリシーの信頼するデバイスのリストから指定する] を選択します。
  - Kaspersky Security Center のリストにあるリムーバブルドライブの暗号化ルールを追加するには、[Kaspersky Security Center のデバイスリストから指定する] を選択します。
7. [選択したデバイスの暗号化モード] で、選択したリムーバブルドライブに保存されているファイルに対して Kaspersky Endpoint Security が行う処理を選択します。
8. 暗号化の前に Kaspersky Endpoint Security にリムーバブルドライブの準備をさせて、リムーバブルドライブに保存される暗号化ファイルをポータブルモードで使用できるようにする場合は、[ポータブルモード] をオンにします。

ポータブルモードでは、[暗号化機能を持たない](#)コンピューターに接続されたリムーバブルドライブに保存された暗号化ファイルを使用できます。
9. ファイルによって占められているディスクセクターのみを暗号化する場合、[使用されているディスク領域のみを暗号化] をオンにします。

既に使用されているドライブに暗号化を適用する場合、ドライブ全体を暗号化してください。それにより、削除されているが取り出すことのできる情報を含む可能性があるデータを含め、すべてのデータが保護されます。[使用されているディスク領域のみを暗号化] は、まだ使用されていない新しいドライブに推奨します。

デバイスがすでに [使用されているディスク領域のみを暗号化] をオンにして暗号化されている場合、[リムーバブルドライブ全体の暗号化] をオンにしたポリシーを適用しても、ファイルによって占められていないセクターは暗号化されません。

10. [以前に選択したデバイスの処理] で、リムーバブルドライブに対して以前に定義された暗号化ルールについて Kaspersky Endpoint Security が行う処理を選択します：
  - リムーバブルドライブに対して以前に作成された暗号化ルールを変更しない場合、[スキップ] を選択します。
  - リムーバブルドライブに対して以前に作成された暗号化ルールを新しいルールで置き換える場合、[更新] を選択します。
11. 変更内容を保存します。

リムーバブルドライブに追加された暗号化ルールは、組織内の任意のコンピューターに接続されたリムーバブルドライブに適用されます。

# リムーバブルドライブの暗号化ルールの一覧のエクスポートまたはインポート

リムーバブルドライブの暗号化ルールの一覧を XML ファイルにエクスポートすることができます。これにより、例えば同じ種別のリムーバブルドライブのルールをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ルールの一覧のバックアップをとったり、別のサーバーにルールを移行することができます。

## 管理コンソール (MMC) でリムーバブルドライブの暗号化ルールの一覧をエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [リムーバブルドライブの暗号化] の順に選択します。
6. リムーバブルドライブの暗号化ルールの一覧をエクスポートするには：
  - a. エクスポートするルールを選択します。複数のポートを選択するには、CTRL または SHIFT キーを使用します。  
ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
  - b. [エクスポート] をクリックします。
  - c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
  - d. [保存] をクリックします。  
Kaspersky Endpoint Security は、ルールの一覧全体を XML ファイルにエクスポートします。
7. リムーバブルドライブの暗号化ルールの一覧をインポートするには：
  - a. [インポート] をクリックします。  
表示されたウィンドウで、ルールの一覧をインポートする XML ファイルを選択します。
  - b. [開く] をクリックします。  
コンピューターにルールの一覧が既にある場合、Kaspersky Endpoint Security から、既存の一覧を削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

## Web コンソールでリムーバブルドライブの暗号化ルールの一覧をエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. リムーバブルドライブの暗号化ルールをリストをエクスポートまたはインポートするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[データ暗号化]** → **[リムーバブルドライブの暗号化]** の順に選択します。
5. **[選択したデバイスの暗号化ルール]** ブロックで、**[暗号化ルール]** をクリックします。  
リムーバブルドライブの暗号化ルールがリストが開きます。
6. リムーバブルドライブの暗号化ルールをリストをエクスポートするには：
  - a. エクスポートするルールを選択します。
  - b. **[エクスポート]** をクリックします。
  - c. 選択したルールのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。
  - d. **[エクスポート]** をクリックします。  
Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールを XML ファイルでエクスポートします。
7. ルールのリストをインポートするには：
  - a. **[インポート]** をクリックします。  
表示されたウィンドウで、ルールをインポートする XML ファイルを選択します。
  - b. **[開く]** をクリックします。  
コンピューターにルールが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

## リムーバブルドライブ上の暗号化ファイルにアクセスするためのポータブルモード

[ポータブルモード] は、リムーバブルドライブ上のファイル暗号化 (FLE) のモードであり、このモードを使用すると社内ネットワーク外にあるデータにアクセスできます。また、ポータブルモードでは、Kaspersky Endpoint Security をインストールしていないコンピューターで暗号化データを操作することもできます。

ポータブルモードは、次の場合に使用すると便利です：

- コンピューターと Kaspersky Security Center 管理サーバーとの間に接続がない。



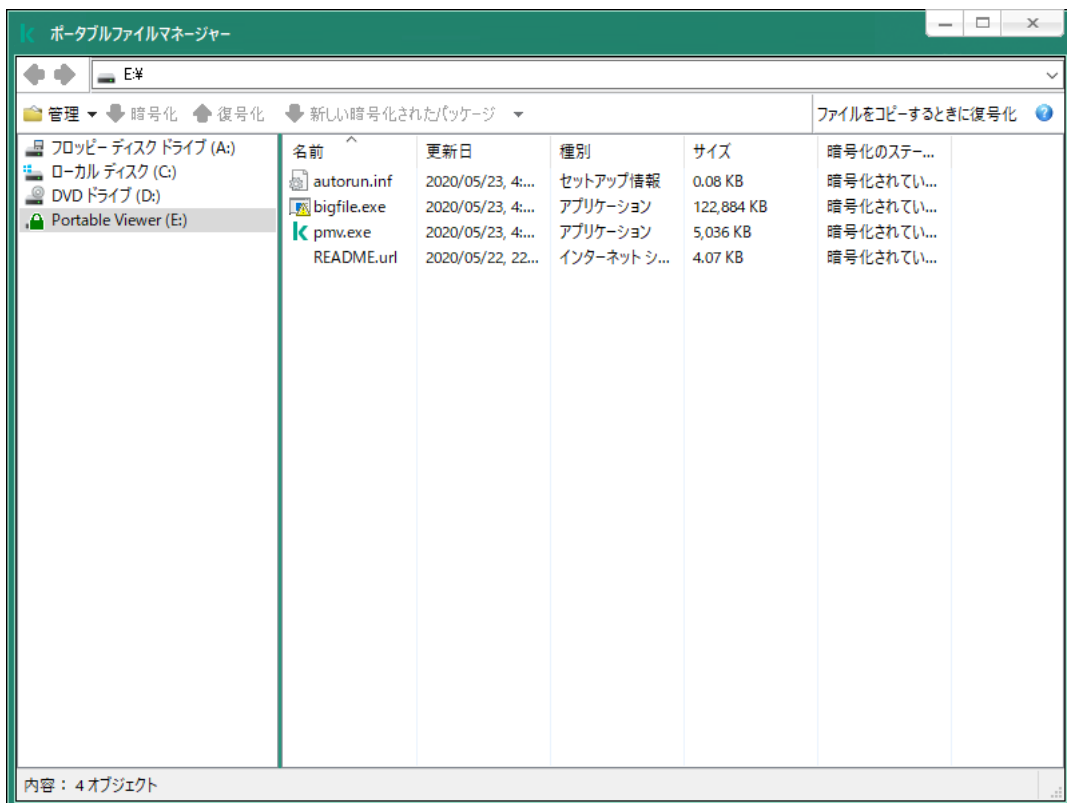
- Kaspersky Security Center 管理サーバーの変更により、インフラストラクチャが変更された。
- Kaspersky Endpoint Security がコンピューターにインストールされていない。

## ポータブルファイルマネージャー

ポータブルモードで作業するために、Kaspersky Endpoint Security は、ポータブルファイルマネージャーという特別な暗号化モジュールをリムーバブルドライブにインストールします。ポータブルファイルマネージャーは、Kaspersky Endpoint Security がコンピューターにインストールされていない場合に暗号化データを操作するためのインターフェイスを提供します（以下の図を参照）。コンピューターに Kaspersky Endpoint Security がインストールされている場合は、通常のファイルマネージャー（エクスプローラーなど）を使用して、暗号化されたリムーバブルドライブを操作できます。

ポータブルファイルマネージャーは、リムーバブルドライブ上のファイルを暗号化するためのキーを保存します。キーは、ユーザーパスワードで暗号化されます。ユーザーは、リムーバブルドライブ上のファイルを暗号化する前に、パスワードを設定します。

Kaspersky Endpoint Security がインストールされていないコンピューターにリムーバブルドライブが接続されると、ポータブルファイルマネージャーが自動的に起動します。コンピューターでアプリケーションの自動起動が無効になっている場合は、ポータブルファイルマネージャーを手動で起動します。これを行うには、リムーバブルドライブに保存されている pmv.exe という名前のファイルを実行します。



ポータブルファイルマネージャー

## 暗号化ファイルを操作するためのポータブルモードのサポート

[管理コンソール（MMC）でリムーバブルドライブ上の暗号化ファイルを操作するためのポータブルモードのサポートを有効にする方法](#)



1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、 [ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、 [データ暗号化] → [リムーバブルドライブの暗号化] の順に選択します。
6. [選択したデバイスの暗号化モード] ドロップダウンリストで、 [すべてのファイルの暗号化] または [新しいファイルのみ暗号化] を選択します。

ポータブルモードは、ファイルレベルの暗号化 (FLE) でのみ使用できます。ディスク全体の暗号化 (FDE) のポータブルモードのサポートを有効にすることはできません。

7. [ポータブルモード] をオンにします。
8. 必要に応じて、 [個々のリムーバブルドライブの暗号化ルールを追加](#)します。
9. 変更内容を保存します。
10. ポリシーを適用後、リムーバブルドライブをコンピューターに接続します。
11. リムーバブルドライブの暗号化操作を確認します。  
ポータブルファイルマネージャーのパスワードを作成するウィンドウが表示されます。
12. 強度の要件を満たすパスワードを指定し、再度入力します。
13. 変更内容を保存します。

Kaspersky Endpoint Security は、リムーバブルドライブ上のファイルを暗号化します。暗号化ファイルの操作に使用されるポータブルファイルマネージャーも、リムーバブルドライブに追加されます。リムーバブルドライブに既に暗号化されたファイルがある場合は、Kaspersky Endpoint Security は独自のキーを使用してそれらを再度暗号化します。これによりユーザーは、ポータブルモードでリムーバブルドライブ上のすべてのファイルにアクセスできます。

[Web コンソールでリムーバブルドライブ上の暗号化ファイルを操作するためのポータブルモードのサポートを有効にする方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. ポータブルモードのサポートを有効にするコンピューターで使用されている Kaspersky Endpoint Security ポリシーをクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[データ暗号化]** → **[リムーバブルドライブの暗号化]** の順に選択します。
5. **[暗号化の管理]** で、**[すべてのファイルの暗号化]** または **[新しいファイルのみ暗号化]** を選択します。

ポータブルモードは、ファイルレベルの暗号化 (FLE) でのみ使用できます。ディスク全体の暗号化 (FDE) のポータブルモードのサポートを有効にすることはできません。

6. **[ポータブルモード]** をオンにします。
7. 必要に応じて、個々のリムーバブルドライブの暗号化ルールを追加します。
8. 変更内容を保存します。
9. ポリシーを適用後、リムーバブルドライブをコンピューターに接続します。
10. リムーバブルドライブの暗号化操作を確認します。  
ポータブルファイルマネージャーのパスワードを作成するウィンドウが表示されます。
11. 強度の要件を満たすパスワードを指定し、再度入力します。
12. 変更内容を保存します。

Kaspersky Endpoint Security は、リムーバブルドライブ上のファイルを暗号化します。暗号化ファイルの操作に使用されるポータブルファイルマネージャーも、リムーバブルドライブに追加されます。リムーバブルドライブに既に暗号化されたファイルがある場合は、Kaspersky Endpoint Security は独自のキーを使用してそれらを再度暗号化します。これによりユーザーは、ポータブルモードでリムーバブルドライブ上のすべてのファイルにアクセスできます。

## リムーバブルドライブ上の暗号化ファイルにアクセスする

ポータブルモードをサポートするリムーバブルドライブ上のファイルを暗号化した後、次のファイルアクセス方法を使用できます：

- Kaspersky Endpoint Security がコンピューターにインストールされていない場合、ポータブルファイルマネージャーにパスワードの入力を要求されます。コンピューターを再起動するたび、またはリムーバブルドライブを再接続するたびに、パスワードを入力する必要があります。
- コンピューターが企業ネットワークの外部にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合は、パスワードの入力を要求されるか、管理者にファイルへのアクセス要求が送信されます。リムーバブルドライブ上のファイルにアクセスすると、Kaspersky Endpoint Security は秘密の鍵

をコンピューターの保管領域に保存します。これにより今後は、パスワードを入力したり、管理者に依頼したりすることなく、ファイルにアクセスできるようになります。

- コンピューターが企業ネットワーク内にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合、パスワードを入力せずにデバイスにアクセスできます。Kaspersky Endpoint Security は、コンピューターが接続されている Kaspersky Security Center 管理サーバーから秘密の鍵を受信します。

## ポータブルモードで作業するためのパスワードの復元

ポータブルモードで作業するためのパスワードを忘れた場合は、企業ネットワーク内の Kaspersky Endpoint Security がインストールされているコンピューターに、リムーバブルドライブを接続する必要があります。秘密の鍵はコンピューターの保管領域または管理サーバーに保存されているため、ファイルにアクセスできます。新しいパスワードでファイルを復号化および再暗号化します。

## リムーバブルドライブを別のネットワークからコンピューターに接続するときのポータブルモードの機能

コンピューターが企業ネットワークの外部にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合は、次の方法でファイルにアクセスできます：

### • パスワードベースでアクセスする

パスワードを入力すると、リムーバブルドライブ上のファイルを表示、変更、保存できるようになります（透過的アクセス権）。リムーバブルドライブの暗号化に関するポリシー設定で、次のパラメータが設定されている場合は、Kaspersky Endpoint Security はリムーバブルドライブの読み取り専用アクセス権を設定できます：

- ポータブルモードのサポートが無効になっている
- **[すべてのファイルの暗号化]** または **[新しいファイルのみ暗号化]** モードが選択されている

それ以外の場合は、リムーバブルドライブへのフルアクセス権（読み取り／書き込み権限）が付与されます。ファイルの追加と削除ができるようになります。

リムーバブルドライブがコンピューターに接続中であっても、リムーバブルドライブへのアクセス権限を変更できます。リムーバブルドライブへのアクセス権限が変更されると、ファイルへのアクセスがブロックされ、パスワードを再度入力するよう要求されます。

パスワードの入力後は、リムーバブルドライブの暗号化ポリシー設定を適用できません。この場合、リムーバブルドライブ上のファイルを復号化または再暗号化することはできません。

### • 管理者にファイルへのアクセス権を依頼する

ポータブルモードで作業するためのパスワードを忘れた場合は、管理者にファイルへのアクセス権を依頼します。ファイルにアクセスするには、ユーザーは管理者にアクセス要求ファイル（拡張子が KESDC のファイル）を送信する必要があります。ユーザーは、メールなどでアクセス要求ファイルを送信できます。管理者は、暗号化されたデータアクセスファイル（拡張子が KESDR のファイル）を送信します。

要求と応答のパスワード復元手順を完了すると、リムーバブルドライブ上のファイルへの透過的アクセス権とリムーバブルドライブへのフルアクセス権（読み取り／書き込み権限）が付与されます。

たとえば、リムーバブルドライブの暗号化ポリシーの適用やファイルの復号化を行えます。パスワードの復元を完了するか、ポリシーが更新されると、変更を確認するよう要求されます。

**[管理コンソール \(MMC\) で暗号化されたデータアクセスファイルを取得する方法](#)**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[デバイス] タブを選択します。
4. [デバイス] タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
5. コンテキストメニューで、[オフラインモードでのアクセスを許可する] を選択します。
6. 表示されたウィンドウで、[データ暗号化] タブを選択します。
7. [データ暗号化] タブで [参照] をクリックします。
8. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。

### Web コンソールで暗号化されたデータのアクセスファイルを取得する方法

1. Web コンソールのメインウィンドウで、[デバイス] → [管理対象デバイス] の順に選択します。
2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。
4. [データ暗号化] セクションを選択します。
5. [ファイルを選択] をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。  
Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。
6. [ライセンスを保存] をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

## リムーバブルドライブの復号化

ポリシーを使用して、リムーバブルドライブを復号化できます。リムーバブルドライブの暗号化の設定が定義されたポリシーが、特定の管理グループに対して生成されます。このため、リムーバブルドライブに対するデータ復号化の結果は、リムーバブルドライブが接続されているコンピューターによって異なります。

リムーバブルドライブを復号化するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[データ暗号化] → [リムーバブルドライブの暗号化] の順に選択します。
6. リムーバブルドライブに保存されている暗号化ファイルをすべて復号化するには、[暗号化モード] で [リムーバブルドライブ全体の復号化] を選択します。
7. 個々のリムーバブルドライブに保存されているデータを復号化するには、復号化の対象にするデータを保存しているリムーバブルドライブの暗号化ルールを編集します。次の手順に従います：
  - a. 暗号化ルールの設定対象にしたリムーバブルドライブのリストで、必要なリムーバブルドライブに対応するエントリを選択します。
  - b. [ルールの設定] をクリックして、選択したリムーバブルドライブの暗号化ルールを編集します。
  - c. [ルールの設定] のコンテキストメニューで、[リムーバブルドライブ全体の復号化] をクリックします。
8. 変更内容を保存します。

その結果、ユーザーがリムーバブルドライブを接続する場合、または既に接続されている場合は、Kaspersky Endpoint Security はリムーバブルドライブを復号化します。復号化プロセスには一定の時間がかかることについての警告も表示されます。データの復号化中にユーザーがリムーバブルドライブを安全な手順で取り出そうとすると、Kaspersky Endpoint Security はデータの復号化プロセスを中断して、復号化操作の完了前にリムーバブルドライブを取り出せるようにします。同じリムーバブルドライブがコンピューターに次に接続されたときに、データの復号化が引き続き実行されます。

リムーバブルドライブの復号化が失敗した場合、**データ暗号化レポート**を本製品のインターフェイスで参照してください。他のアプリケーションによってファイルアクセスがブロックされている可能性があります。その場合、リムーバブルドライブをコンピューターから取り外してから再度接続してみてください。

## データ暗号化の詳細の表示

Kaspersky Endpoint Security は、暗号化または復号化の進行中に、クライアントコンピューターに適用される暗号化パラメータのステータスに関する情報を Kaspersky Security Center にリレーします。

その際、暗号化ステータスとして次の値が使われる可能性があります：

- 暗号化ポリシーが指定されていません：このコンピューターでは Kaspersky Security Center の暗号化ポリシーが定義されていません。
- ポリシーの適用中：このコンピューターで、データの暗号化または復号化あるいはその両方が進行中です。

- エラー：このコンピューターで、データの暗号化または復号化の進行中にエラーが発生しました。
- 再起動が必要です：このコンピューターでは、データの暗号化または復号化を開始または完了するためにオペレーティングシステムを再起動する必要があります。
- ポリシーによって割り当てられました：このコンピューターでは、コンピューターに適用されている Kaspersky Security Center ポリシーで指定された暗号化設定を使用してデータの暗号化が行われ完了しています。
- ユーザーによってキャンセルされました：ユーザーが、リムーバブルドライブでのファイル暗号化操作の確認を拒否しました。

## 暗号化ステータスの表示

コンピューターデータの暗号化ステータスを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[デバイス] タブを選択します。  
[デバイス] タブの作業領域に、選択された管理グループのコンピューターのプロパティが表示されません。
4. [デバイス] タブの作業領域で、スクロールバーを右端までスライドさせます。
5. [暗号化のステータス] 列が表示されていない場合：
  - a. 表のヘッダー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、[表示] の [列の追加と削除] を選択します。
  - c. 表示されたウィンドウで、[暗号化のステータス] タブを選択します。
6. [OK] をクリックします。

[暗号化のステータス] 列に、選択された管理グループに属するコンピューター上のデータの暗号化ステータスが表示されます。このステータスは、コンピューターのローカルドライブでのファイル暗号化とディスク全体の暗号化に関する情報をもとに作成されます。

## Kaspersky Security Center ダッシュボードで暗号化の統計情報の表示

Kaspersky Security Center ダッシュボードで暗号化の統計情報を表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、[管理サーバー - <コンピューター名>] フォルダーを選択します。
3. コンソールツリーの右側の作業領域で、[統計] タブを選択します。
4. データ暗号化の統計情報を含む情報ペインを備えた新しいページを作成します。次の手順に従います：

- a. **【統計】** タブで **【表示のカスタマイズ】** をクリックします。  
統計のプロパティウィンドウが表示されます。
  - b. 統計のプロパティウィンドウで、**【追加】** をクリックします。  
新規ページのプロパティウィンドウが表示されます。
  - c. 新規ページのプロパティウィンドウの **【全般】** セクションで、ページ名を入力します。
  - d. **【情報パネル】** セクションで、**【追加】** をクリックします。  
**【新規情報パネル】** ウィンドウが表示されます。
  - e. **【新規情報パネル】** ウィンドウの **【保護ステータス】** セクションで、**【デバイスの暗号化】** を選択します。
  - f. **【OK】** をクリックします。  
デバイスの暗号化のプロパティウィンドウが表示されます。
  - g. 必要な場合は、情報ペインの設定を編集します。ペインの編集には、デバイスの暗号化のプロパティウィンドウの **【表示】** および **【デバイス】** セクションを使用します。
  - h. **【OK】** をクリックします。
  - i. 手順のステップ d～h を繰り返します。**【新規情報パネル】** ウィンドウの **【保護ステータス】** セクションでは、**【リムーバブルドライブの暗号化】** 項目を選びます。  
追加された情報ペインが、新規ページのプロパティウィンドウの **【情報パネル】** リストに表示されます。
  - j. 新規ページのプロパティウィンドウで、**【OK】** をクリックします。  
ここまでのステップで作成された情報ペインを含むページの名前が、統計のプロパティウィンドウの **【ページ】** リストに表示されます。
  - k. 統計のプロパティウィンドウで、**【閉じる】** をクリックします。
5. **【統計】** タブで、手順のここまでのステップで作成したページを開きます。
- 情報ペインが表示され、コンピューターとリムーバブルドライブの暗号化ステータスが示されます。

## ローカルコンピュータードライブでのファイル暗号化エラーの表示

ローカルコンピュータードライブでのファイル暗号化エラーを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの **【管理対象デバイス】** フォルダーで、表示するファイル暗号化エラーリストの対象になっているクライアントコンピューターが所属する管理グループの名前のフォルダーを開きます。
3. 作業領域で、**【デバイス】** タブを選択します。
4. **【デバイス】** タブで、リスト内のコンピューター名を選択して右クリックしコンテキストメニューを表示します。
5. コンピューターのコンテキストメニューから **【プロパティ】** 項目を選択します。コンピューターのプロパティウィンドウで、**【プロテクション】** セクションを選択します。



6. コンピューターのプロパティウィンドウの [プロテクション] セクションで、 [データ暗号化エラーの表示] をクリックして [データ暗号化エラー] ウィンドウを開きます。

このウィンドウには、ローカルコンピューターのドライブ上でのファイル暗号化エラーの詳細が表示されます。エラーが訂正されると、この詳細情報は [データ暗号化エラー] ウィンドウから削除されます。

## データ暗号化レポートの表示

データ暗号化レポートを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理サーバー] フォルダで、 [レポート] タブを選択します。
3. [新規レポートテンプレート] をクリックします。  
新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。 [レポートテンプレート種別の選択] ウィンドウの [その他] セクションで、次のいずれかの項目を選択します：

- 管理対象デバイスの暗号化ステータスレポート
- 大容量ストレージデバイスの暗号化ステータスレポート
- ファイル暗号化のエラーに関するレポート
- 暗号化されたファイルへのアクセスのブロックに関するレポート

新規レポートテンプレートウィザードが完了すると、 [レポート] タブのテーブルに新しいレポートテンプレートが表示されます。

5. 手順のここまでのステップで作成したレポートテンプレートを選択します。
6. テンプレートのコンテキストメニューから [レポートの表示] を選択します。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

## 暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用

### 暗号化されたデバイスへのアクセスの取得

次の場合、暗号化されたデバイスにアクセスできるようにユーザーから要求しなければならないことがあります：

- ハードディスクの暗号化が別のコンピューターで行われたとき。
- デバイスの暗号鍵がコンピューター上になく（コンピューター上の暗号化されたリムーバブルドライブに最初にアクセスしようとしたとき、など）、さらにコンピューターが Kaspersky Security Center に接続していないとき。

ユーザーが暗号化されたデバイスへのアクセスキーを適用すると、ユーザーのコンピューターに暗号鍵が保存され、Kaspersky Security Center に接続されていない場合でもこのコンピューターで以降にアクセスを試みるたびにこのデバイスへのアクセスが許可されます。

暗号化されたデバイスには、次の方法でアクセスできます：

1. ユーザー側で Kaspersky Endpoint Security のインターフェイスを使用して拡張子が kesdc のアクセス要求ファイルを作成し、企業 LAN の管理者に送信します。
2. 管理者は Kaspersky Security Center の管理コンソールを使用して拡張子が kesdr のアクセスキーファイルを作成し、ユーザーに送信します。
3. ユーザーはアクセスキーを適用します。

## 暗号化されたデバイス上のデータの復元

ユーザーは、[暗号化されたデバイスの復元ツール](#)（以下、「復元ツール」）を使用して、暗号化されたデバイスにアクセスできます。この操作は次の場合に必要になります：

- アクセスキーを使用してアクセスを取得する方法に失敗した。
- デバイスが暗号化されているコンピューターに暗号化機能がインストールされていない。

復元ツールによる暗号化デバイスへのアクセスの復元に必要なデータは、ユーザーのコンピューターのメモリに暗号化されていない形式で一定期間保存されます。そのようなデータに対する不正アクセスのリスクを減らすために、暗号化されたデバイスへのアクセスの復元は信頼できるコンピューター上で行ってください。

暗号化されたデバイス上のデータは次の方法で復元できます：

1. ユーザー側で 復元ツールを使用して拡張子が fdertc のアクセス要求ファイルを作成し、企業 LAN の管理者に送信します。
2. 管理者は Kaspersky Security Center の管理コンソールを使用して拡張子が fdertr のアクセスキーファイルを作成し、ユーザーに送信します。
3. ユーザーはアクセスキーを適用します。

ユーザーは、復元ツールで認証エージェントアカウントの認証情報を指定して、暗号化されたシステムハードディスクのデータを復元することもできます。認証エージェントのメタデータが破損している場合、アクセス要求ファイルによる復元方法を完了させてください。

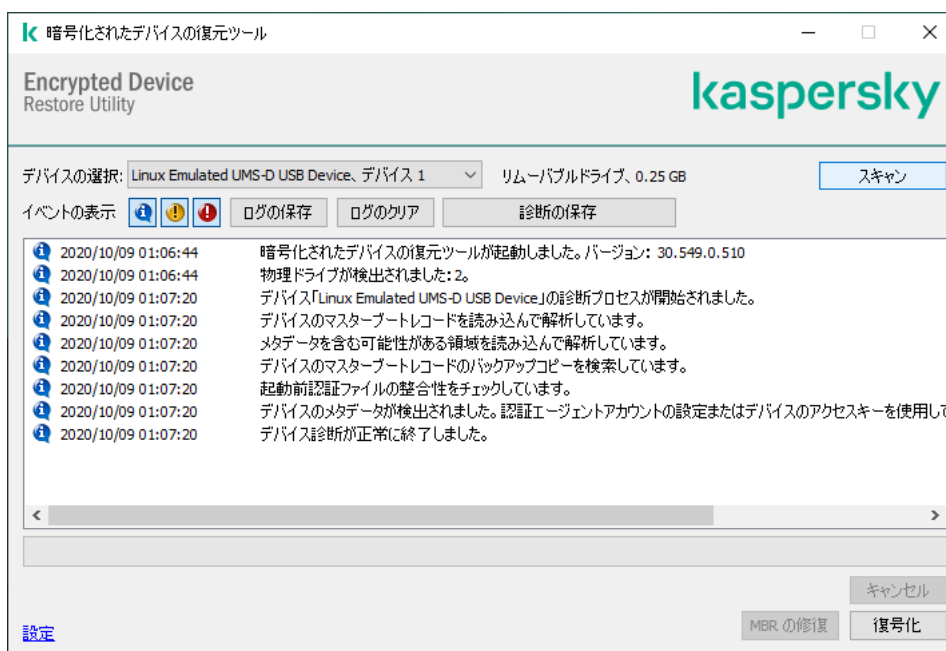
暗号化されたデバイスのデータを復元する前に、この操作を実行するコンピューターで Kaspersky Security Center ポリシーをキャンセルするか、Kaspersky Security Center ポリシー内の暗号化を無効にしてください。これにより、デバイスの再暗号化を防ぐことができます。

## FDERT 復元ツールを使用してデータを復元する

ハードドライブに障害が発生した場合、ファイルシステムが破損している可能性があります。この場合、Kaspersky Disk Encryption 技術で保護されたデータは利用できません。データを復号化し、新しいドライブにデータをコピーできます。

Kaspersky Disk Encryption 技術で保護されたドライブでのデータの復元は、次の手順で構成されます：

1. スタンドアロン復元ツールの作成（下の図を参照）。
2. Kaspersky Endpoint Security 暗号化コンポーネントがインストールされていないコンピューターにドライブを接続します。
3. 復元ツールを実行して、ハードドライブを診断します。
4. ドライブ上のデータにアクセスします。これを行うには、認証エージェントの認証情報を入力するか、復元手順（要求と応答）を開始します。



FDERT 復元ツール

## スタンドアロン復元ツールの作成

復元ツールの実行ファイルを作成するには：

1. メインウィンドウで、**「サポート」** をクリックします。
2. 表示されたウィンドウで、**「暗号化されたデバイスの復元」** をクリックします。  
暗号化されたデバイスの復元ツールが起動します。
3. 復元ツールのウィンドウで **「スタンドアロン復元ツールの作成」** をクリックします。
4. スタンドアロン復元ツールをコンピューターのメモリに保存します。

その結果、復元ツールの実行ファイル (fdert.exe) が、指定したフォルダーに保存されます。Kaspersky Endpoint Security 暗号化コンポーネントを持たないコンピューターに復元ツールをコピーします。これにより、ドライブの再暗号化を防ぐことができます。

復元ツールによる暗号化デバイスへのアクセスの復元に必要なデータは、ユーザーのコンピューターのメモリに暗号化されていない形式で一定期間保存されます。そのようなデータに対する不正アクセスのリスクを減らすために、暗号化されたデバイスへのアクセスの復元は信頼できるコンピューター上で行ってください。

## ハードドライブ上のデータを回復する

復元ツールを使用して、暗号化されたデバイスへのアクセスを復元するには：

1. 復元ツールの実行ファイルである fdert.exe という名前のファイルを実行します。このファイルは、Kaspersky Endpoint Security によって作成されます。
2. 復元ツールのウィンドウで、アクセスを復元する暗号化されたデバイスを選択します。
3. **[スキャン]** をクリックして、デバイスに対して行う処理（ロック解除するか復号化するか）をユーティリティが定義できるようにします。

Kaspersky Endpoint Security の暗号化機能へのアクセス権がコンピューターにある場合、デバイスロックの解除が要求されます。デバイスのロックを解除しても復号化されませんが、ロック解除の結果、このデバイスに直接アクセスできるようになります。Kaspersky Endpoint Security の暗号化機能へのアクセス権がコンピューターにない場合、デバイスの復号化が要求されます。

4. 診断情報をインポートする場合は、**[診断の保存]** をクリックします。  
ユーティリティは、診断情報を含むファイルとともにアーカイブを保存します。
5. 暗号化されたシステムハードディスクの診断からのメッセージで、デバイスのマスターブートレコード（MBR）に関する問題が報告された場合は、**[MBR の修復]** をクリックします。  
デバイスのマスターブートレコードを修正すると、デバイスのロック解除や復号化に必要な情報の取得速度が速くなります。
6. 診断結果に応じて、**[ロック解除]** または **[復号化]** をクリックします。
7. 認証エージェントアカウントを使用してデータを復元する場合は、**認証エージェントアカウント設定の使用 オプション** を選択し、認証エージェントの認証情報を入力します。  
この方法は、システムハードディスク上のデータを復元する場合でのみ可能です。システムハードディスクが破損して認証エージェントのアカウントデータを失ってしまった場合、企業 LAN の管理者からアクセスキーを取得して暗号化されたデバイスにあるデータを復元してください。
8. 復元手順を開始する場合は、次の手順を実行します：
  - a. **[デバイスアクセスキーを手動で指定する]** を選択します。
  - b. **[アクセスキーの取得]** をクリックし、アクセス要求ファイルをコンピューターのメモリ（拡張子が FDERTC のファイル）に保存します。
  - c. アクセス要求ファイルを企業 LAN の管理者に送信します。

アクセスキーを取得するまで **[デバイスアクセスキーの取得]** ウィンドウは閉じないでください。再度このウィンドウを表示しても、管理者が以前に作成したアクセスキーは適用できません。

- d. 企業の LAN 管理者によって作成および送信されたアクセスファイル（拡張子が FDERTR のファイル）を受信して保存します（以下の手順を参照）。

e. **[デバイスアクセスキーの取得]** ウィンドウでアクセスファイルをダウンロードします。

9. デバイスを復号化する場合は、追加の復号化設定を行う必要があります：

- 復号化の範囲を指定します。
  - デバイス全体を復号化する場合は、**[デバイス全体の復号化]** を選択します。
  - デバイスのデータの一部を復号化する場合は、**[特定のデバイス範囲の復号化]** を選択し、復号化の範囲を指定します。
- 復号化データを書き込む場所を選択します：
  - 元のデバイスにあるデータを復号化されたデータに書き換える場合、**[ディスクイメージのファイルに復号化]** をオフにします。
  - 復号化されたデータと元の暗号化データを別に保存する場合、**[ディスクイメージのファイルに復号化]** をオンにし、VHD ファイルの保存先のパスを**[参照]** から指定します。

10. **[OK]** をクリックします。

デバイスのロック解除 / 復号化プロセスが開始されます。

### **管理コンソール (MMC) で暗号化されたデータアクセスファイルを作成する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、**[詳細]** → **[データ暗号化と保護機能]** → **[暗号化されたドライブ]** フォルダの順に選択します。
3. 作業領域で、アクセスキーファイルを作成する暗号化されたデバイスを選択し、デバイスのコンテキストメニューで **[Kaspersky Endpoint Security for Windows のデバイスへのアクセス]** をクリックします。

どのコンピューターに対してアクセス要求ファイルが生成されたのかが不明な場合は、管理コンソールツリーで **[詳細]** → **[データ暗号化と保護機能]** を選択し、作業領域で **[デバイスの暗号化鍵を取得]** をクリックしてください。

4. 表示されたウィンドウで、使用する暗号化アルゴリズムを選択します：**AES256** または **AES56**。  
データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（強度の高い暗号化 (**AES256**) または相対的に強度の低い暗号化 (**AES56**)）。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。
5. **[参照]** をクリックしてウィンドウを開き、ユーザーから受け取った、拡張子が **fdertc** の要求ファイルへのパスを指定します。
6. **[開く]** をクリックします。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。

1. Web コンソールのメインウィンドウで、[操作] → [データ暗号化と保護機能] → [暗号化されたドライブ] の順に選択します。
2. データを回復するコンピューターの名前の横にあるチェックボックスをオンにします。
3. [オフラインモードでのデバイスへのアクセスを許可] をクリックします。  
これにより、デバイスへのアクセスを許可するためのウィザードが開始されます。
4. ウィザードの指示に従って、デバイスへのアクセスを許可します。

a. **Kaspersky Endpoint Security for Windows** のプラグインを選択します。

b. 使用する暗号化アルゴリズムを選択します：**AES256** または **AES56**。

データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（強度の高い暗号化（AES256）または相対的に強度の低い暗号化（AES56））。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。

c. [ファイルの選択] をクリックし、ユーザーから受け取ったアクセス要求ファイル（拡張子が FDERTC のファイル）を選択します。

d. [ライセンスを保存] をクリックし、フォルダーを選択して、暗号化されたデータにアクセスするためのキーファイル（拡張子が FDERTR のファイル）を保存します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

## オペレーティングシステムのレスキューディスクの作成

暗号化されたハードディスクに何らかの理由でアクセスできなくなり、オペレーティングシステムを読み込めなくなったときには、オペレーティングシステムのレスキューディスクが便利です。

レスキューディスクを使用して、Windows オペレーティングシステムのイメージを読み込み、オペレーティングシステムのイメージに用意されている復元ツールを使用して、暗号化されたハードディスクへのアクセスを復元することができます。

オペレーティングシステムのレスキューディスクを作成するには：

1. [暗号化されたデバイスの復元ツールの実行ファイルを作成します](#)。
2. Windows プリブート環境のカスタムイメージを作成します。Windows プリブート環境のカスタムイメージの作成中に、復元ツールの実行ファイルをこのイメージに追加します。
3. Windows プリブート環境のカスタムイメージを、CD やリムーバブルドライブなどのブート可能なドライブに保存します。

Windows プリブート環境のカスタムイメージを作成するための手順については、Microsoft のヘルプファイル ([Microsoft TechNet リソース](#) などにあるもの) を参照してください。



# Detection and Response

## Kaspersky Endpoint Agent

*Kaspersky Endpoint Agent* は、本製品とその他のカスペルスキーのソリューション（Kaspersky Sandbox など）を連携して高度な脅威を検知します。カスペルスキーのソリューションは特定のバージョンの Kaspersky Endpoint Agent と互換性を持ちます。

ご利用中のソフトウェアソリューションに含まれる Kaspersky Endpoint Agent for Windows およびスタンドアロンのソリューションに関する詳細な情報については、関連製品のヘルプを参照してください：

- *Kaspersky Anti Targeted Attack Platform* のヘルプ
- *Kaspersky Sandbox* のヘルプ
- *Kaspersky Endpoint Detection and Response Optimum* のヘルプ
- *Kaspersky Managed Detection and Response* のヘルプ

Kaspersky Endpoint Agent は [Kaspersky Endpoint Security の配信キット](#) に含まれています。Kaspersky Endpoint Security のインストール中に Kaspersky Endpoint Agent をインストールできます。これを行うには、製品のインストール中（たとえば、[インストールパッケージ](#)内）に Endpoint Agent を選択する必要があります。Endpoint Agent と製品をインストールした後、Kaspersky Endpoint Security および Kaspersky Endpoint Agent はインストール済みのアプリケーションのリストに追加されます。Kaspersky Endpoint Security のアンインストール後、Kaspersky Endpoint Agent も自動的にアンインストールされます。

Kaspersky Endpoint Security 11.7.0 に、Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行用のウィザードが実装されました。次のソリューション用のポリシーおよびタスクの設定を移行することができます：

- Kaspersky Sandbox :
- Kaspersky Endpoint Detection and Response (EDR)
- Kaspersky Managed Detection and Response (MDR)

最初に単一のコンピューターで Kaspersky Endpoint Agent から Kaspersky Endpoint Security に移行し、次にコンピューターのグループで移行してから組織のすべてのコンピューターへの移行を完了させてください。

*Kaspersky Endpoint Agent* から *Kaspersky Endpoint Security* にポリシーおよびタスクの設定を移行するには：

Web コンソールのメインウィンドウで、**[操作]** → **[Kaspersky Endpoint Agent からの移行]** の順に選択します。

ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

### ステップ 1. ポリシーの移行



移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Security と設定を統合する Kaspersky Endpoint Agent のポリシーをクリックして選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

## ステップ 2. タスクの移行

移行ウィザードが Kaspersky Endpoint Security 向けの新しいタスクを作成します。タスクのリストで、Kaspersky Endpoint Security のポリシー向けに作成する Kaspersky Endpoint Agent のタスクを選択します。このウィザードでは Kaspersky Endpoint Detection and Response および Kaspersky Sandbox 向けのタスクがサポートされます。次の手順に進みます。

## ステップ 3. ウィザードの完了

ウィザードを終了します。ウィザードは次の操作を行います：

- 新規の Kaspersky Endpoint Security のポリシーを作成する

ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには <Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名> という名前が付けられます。新しいポリシーのステータスは無効になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ無効にして、新しく統合されたポリシーを有効にします。

Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行後、新しいポリシーに [管理サーバーへのデータ転送機能](#)（隔離されたファイルのデータと脅威の活動連鎖のデータ）が設定されていることを確認してください。データ転送のパラメータ値は Kaspersky Endpoint Agent ポリシーからは移行されません。

- 新規の Kaspersky Endpoint Security のタスクを作成する

新規タスクは Kaspersky Endpoint Detection and Response および Kaspersky Sandbox 向けの Kaspersky Endpoint Agent タスクのコピーです。同時に、ウィザードは Kaspersky Endpoint Agent タスクには変更を加えません。

## [KES+KEA] 設定から [KES11.7.0] への移行

Kaspersky Endpoint Security 11.7.0 には Kaspersky Endpoint Detection and Response Optimum 2.0（EDR Optimum）および Kaspersky Sandbox 2.0 向けの組み込みエージェントが含まれています。これらのソリューションと連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Security をバージョン 11.7.0 にアップグレードする際、EDR Optimum および Kaspersky Sandbox ソリューションは Kaspersky Endpoint Security との連携を保持します。さらに、Kaspersky Endpoint Agent はコンピューターから削除されます。

[KES+KEA] 設定から [KES11.7.0] への移行には次の手順が含まれます：

### ① Kaspersky Security Center のアップグレード

ユーザーのコンピューター上にある管理エージェントと Web コンソールを含むすべての Kaspersky Security Center コンポーネントをバージョン 13.2 にアップグレードします。

### ② Kaspersky Endpoint Security Web プラグインのアップグレード

Kaspersky Security Center Web コンソールで、Kaspersky Endpoint Security Web プラグインをバージョン 11.7.0 にアップグレードします。EDR Optimum および Kaspersky Sandbox コンポーネントを管理するには、Web コンソールを使用する必要があります。

### 3 ポリシーおよびタスクの移行

[Kaspersky Endpoint Agent のポリシーおよびタスクの移行ウィザード](#)を使用して Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。

これにより、新規の Kaspersky Endpoint Security のポリシーが作成されます。新しいポリシーのステータスは無効になっています。ポリシーを適用するには、ポリシーのプロパティを開いて Kaspersky Security Network に関する声明に同意して状態を有効にします。

### 4 ライセンス機能

共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Security for Windows および Kaspersky Endpoint Agent をアクティベートした場合は、本製品をバージョン 11.7.0 にアップグレードした後に EDR Optimum 機能は自動的にアクティベートされます。追加で操作する必要はありません。

スタンドアロンの Kaspersky Endpoint Detection and Response Optimum アドオンのライセンスを使用して EDR Optimum 機能をアクティベートした場合は、EDR Optimum のライセンスが Kaspersky Security Center リポジトリに追加されていて、[ライセンスの自動配信機能が有効になっている](#)ことを確認してください。本製品をバージョン 11.7.0 にアップグレードした後に、EDR Optimum 機能が自動的にアクティベートされます。

Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Agent をアクティベートしており、別のライセンスを使用して Kaspersky Endpoint Security for Windows をアクティベートしていた場合、Kaspersky Endpoint Security for Windows のライセンスを共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security のライセンスで置き換える必要があります。ライセンスは [[ライセンスの追加](#)] タスクを使用して置き換えることができます。

Kaspersky Sandbox 機能をアクティベートする必要はありません。Kaspersky Sandbox 機能は Kaspersky Endpoint Security for Windows をアップグレードおよびアクティベートした後すぐに利用可能になります。

### 5 Kaspersky Endpoint Security のアップグレード

本製品のアップグレードと、EDR Optimum および Kaspersky Sandbox 機能を移行するには、[リモートインストールタスク](#)の使用を推奨します。

本製品をリモートインストールタスクを使用してアップグレードするには、次の設定を変更する必要があります：

- インストールパッケージの設定で Endpoint Detection and Response Optimum または Kaspersky Sandbox コンポーネントを選択します。
- インストールパッケージの設定で Kaspersky Endpoint Agent コンポーネントを除外します。

次の方法で本製品をアップグレードすることもできます：

- カスペルスキーのアップデートサービスを使用する（シームレスアップデート - SMU）。
- クライアントデバイスのローカルで、セットアップウィザードを使用する。

この場合、コンピューターにインストールされている Kaspersky Endpoint Agent の設定を確認してください。インストールされている Kaspersky Endpoint Agent に Endpoint Detection and Response Expert (KATA EDR) コンポーネントが含まれている場合、本製品のアップグレード前にコンポーネントを削除してください。Endpoint Detection and Response Expert (KATA EDR) コンポーネントを削除できない場合は、アップグレード時に Kaspersky Endpoint Security は EDR Optimum および Kaspersky Sandbox コンポーネントをスキップします。本製品のアップグレード後に [コンポーネントの変更](#) タスクを使用してこれらのコンポーネントをインストールできます。

## 6 コンピューターの再起動

組み込みエージェントを含む製品へのアップグレードを完了するためにコンピューターを再起動します。本製品のアップグレード中、インストーラーはコンピューターの再起動前に Kaspersky Endpoint Agent を削除します。コンピューターの再起動後、組み込みエージェントが追加されます。つまり、コンピューターが再起動されるまで、Kaspersky Endpoint Security は EDR および Kaspersky Sandbox の機能を実行しません。

## 7 Kaspersky Endpoint Detection and Response Optimum および Kaspersky Sandbox の状態を確認する。

アップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターに管理エージェント 13.2 がインストールされていることを確認します。
- EDR Optimum および Kaspersky Sandbox コンポーネントの動作状態を製品コンポーネントのステータスレポートを表示して確認します。コンポーネントの状態が「インストールされていません」となっている場合は、[コンポーネントの変更](#) タスクを使用してコンポーネントをインストールしてください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

製品コンポーネントのステータスレポートを使用して EDR Optimum 機能がアクティベートされているかどうかを確認してください。コンポーネントの状態が「ライセンスに含まれていません」と表示されている場合は、[EDR Optimum の自動ライセンス配信機能がオンになっている](#)ことを確認してください。

## 本製品を KATA EDR の一部としてアップグレードする

Kaspersky Endpoint Agent を Kaspersky Anti Targeted Attack Platform (Endpoint Detection and Response Expert (KATA EDR) コンポーネント) の一部としてインストールしていた場合、Kaspersky Endpoint Security for Windows を次のいずれの方法でもアップグレードすることができます：

- リモートインストールタスクを使用する。

次の設定を変更する必要があります：

- インストールパッケージの設定で Endpoint Detection and Response Optimum または Kaspersky Sandbox コンポーネントを除外します。
- インストールパッケージの設定で Kaspersky Endpoint Agent コンポーネントを選択します。コンピューターに既に Kaspersky Endpoint Agent がインストールされていた場合は、バージョン 3.11 にアップグレードされます。

- カスペルスキーのアップデートサービス (SMU) を使用する。

製品アップグレードを確認する必要があります。Kaspersky Endpoint Security は Endpoint Detection and Response Optimum および Kaspersky Sandbox をインストールから除外します。Kaspersky Endpoint Agent のアップグレードはサポートされません。Kaspersky Endpoint Agent を手動でアップグレードすることができます。

- クライアントデバイスのローカルで、セットアップウィザードを使用する。

Kaspersky Endpoint Security は Endpoint Detection and Response Optimum および Kaspersky Sandbox をインストールから除外します。コンピューターに既に Kaspersky Endpoint Agent がインストールされていた場合は、バージョン 3.11 にアップグレードされます。

## Managed Detection and Response



Kaspersky Endpoint Security 11.6.0 に、Managed Detection and Response ソリューション向けの組み込みエージェントが導入されました。Kaspersky Managed Detection and Response (MDR) ソリューションはお客様のインフラストラクチャ内のセキュリティインシデントを自動で検知し分析します。MDR はエンドポイントから取得する遠隔測定したデータと機械学習を使用します。MDR はカスペルスキーのエキスパートにインシデントのデータを送信します。エキスパートはインシデントを処理し、新しい項目を定義データベースに追加するなどの対応をします。また、エキスパートたちはインシデントの処理に対して、コンピューターをネットワークから分離するなど、推奨事項を提示することもあります。ソリューションについて詳しくは、[Kaspersky Managed Detection and Response のヘルプ](#) を参照してください。

Kaspersky Managed Detection and Response と連携することで、本製品は次の機能を提供します：

- BLOB 設定ファイルを使用して Managed Detection and Response を有効化する。
- Kaspersky Managed Detection and Response からのコマンドを実行する。
- 脅威検知のため、遠隔測定したデータを Kaspersky Managed Detection and Response に送信する。

### Kaspersky Managed Detection and Response との連携

Kaspersky Managed Detection and Response とは次の手順で連携されます：

#### ① プライベートの Kaspersky Security Network の設定

Kaspersky Security Center Cloud コンソールを使用している場合、この手順は省略してください。Kaspersky Security Center Cloud コンソールは、MDR プラグインのインストール中に自動的にローカルの Kaspersky Security Network を設定します。

プライベート KSN はコンピューターと Kaspersky Security Network 専用のサーバー間でのデータ通信をサポートしますが、グローバル KSN はサポートしません。

Kaspersky Security Network 設定ファイルを管理サーバーのプロパティ内でアップロードします。Kaspersky Security Network 設定ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。プライベートの Kaspersky Security Network の設定について詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。コマンドラインから Kaspersky Security Network 設定ファイルをコンピューターにアップロードすることも可能です（下記の説明を参照してください）。

#### [コマンドラインからプライベートの Kaspersky Security Network を設定する方法](#)

1. 管理者としてコマンドラインインタプリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：  
avp.com KSN /private <ファイル名>  
<ファイル名> にはプライベート KSN の設定を含む設定ファイルの名前を入力します (PKCS7 または PEM ファイル形式)。

例：

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Kaspersky Endpoint Security はプライベート KSN を使用してファイル、アプリケーション、Web サイトの評価を決定します。[**Kaspersky Security Network**] セクションのポリシー設定には、次の動作ステータスが表示されます：*KSN* ネットワーク：プライベート *KSN*

Managed Detection and Response が動作するためには、[拡張 KSN モードを有効にする](#)必要があります。

## ② Managed Detection and Response をアクティベートします。

Kaspersky Endpoint Security のポリシーで BLOB 設定ファイルを読み込みます (下の手順を参照してください)。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、[Kaspersky Managed Detection and Response のヘルプ](#)を参照してください。

### 管理コンソール (MMC) で Managed Detection and Response をアクティベートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの [管理対象デバイス] フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、[ポリシー] タブを選択します。
4. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
5. ポリシーウィンドウで、[Detection and Response] → [Managed Detection and Response] の順に選択します。
6. [Managed Detection and Response] をオンにします。
7. [設定] ブロックで、[インポート] をクリックし、Kaspersky Managed Detection and Response コンソールで受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。
8. 変更内容を保存します。

### Web コンソールおよび Cloud コンソールで Managed Detection and Response をアクティベートする方法



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Managed Detection and Response]** の順に選択します。
5. **[Managed Detection and Response]** をオンにします。
6. **[インポート]** をクリックし、Kaspersky Managed Detection and Response Console で受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。
7. 変更内容を保存します。

### コマンドラインから Managed Detection and Response をアクティベートする方法

1. 管理者としてコマンドラインインタプリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：
  - 製品設定が パスワードによって保護 されていない場合：  
avp.com MDRLICENSE /ADD <ファイル名>  
<ファイル名>には、Managed Detection and Response をアクティベートする BLOB 設定ファイル名を入力します (P7 ファイル形式)。
  - 製品設定が パスワードによって保護 されている場合：  
avp.com MDRLICENSE /ADD <ファイル名> /login=<ユーザー名> /password=<パスワード>

BLOB ファイルが検証されます。BLOB の検証には、デジタル署名およびライセンス期間の確認も含まれます。BLOB ファイルの検証が正常に完了すると、Kaspersky Endpoint Security はファイルをアップロードして、次回の Kaspersky Security Center との同期の際にファイルをコンピューターに送信します。コンポーネントの動作状態は製品機能の状態レポートで表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。

**[Managed Detection and Response]** は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

### ③ Managed Detection and Response のサポート

Managed Detection and Response が動作するためには、次の機能を有効にする必要があります：

- Kaspersky Security Network (拡張モード)
- ふるまい検知

これらの機能は必ず有効にしてください。有効になっていないと、遠隔測定したデータを受け取ることができないため、Kaspersky Managed Detection and Response は機能できません。

また、Kaspersky Managed Detection and Response は別の製品機能から受け取ったデータを使用します。これらの機能は有効にしなくても Kaspersky Managed Detection and Response を使用できます。追加のデータを提供する機能は次の通りです：

- [ウェブ脅威対策](#)
- [メール脅威対策](#)
- [ファイアウォール](#)

Kaspersky Security Center 13 Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、新しい保護された接続であるバックグラウンド接続を確立する必要があります。Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、新しい保護された接続であるバックグラウンド接続を確立する必要があります。ソリューションを配備する際に Kaspersky Managed Detection and Response はバックグラウンド接続を確立するよう求めます。バックグラウンド接続が確立されていることを確認してください。Kaspersky Security Center とその他のカスペルスキーのソリューションとの統合について詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。

## Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行

MDR ソリューションは Kaspersky Endpoint Security バージョン 11 以降でサポートされます。Kaspersky Endpoint Security のバージョン 11 ~ 11.5.0 は、脅威検知を有効にするために Kaspersky Managed Detection and Response に遠隔測定したデータを送信するだけです。Kaspersky Endpoint Security のバージョン 11.6.0 には、組み込みエージェント (Kaspersky Endpoint Agent) のすべての機能が含まれています。

お客様が Kaspersky Endpoint Security 11 ~ 11.5.0 を使用している場合、MDR ソリューションとの連携のためにデータベースを最新版にアップデートする必要があります。また、Kaspersky Endpoint Agent をインストールする必要があります。

お客様が Kaspersky Endpoint Security 11.6.0 以降のバージョンを使用している場合、MDR ソリューションと連携するには、本製品のインストール時に Managed Detection and Response コンポーネントを選択する必要があります。この場合は、Kaspersky Endpoint Agent のインストールは必要ありません。

Kaspersky Endpoint Agent から Kaspersky Endpoint Security に切り替えるには：

1. Kaspersky Endpoint Security のポリシーで Kaspersky Managed Detection and Response との連携を設定します。
2. Kaspersky Endpoint Agent のポリシーで Managed Detection and Response を無効にします。

Kaspersky Endpoint Security 11 ~ 11.5.0 をインストールしていないコンピューターに Kaspersky Endpoint Security のポリシーが適用されている場合、まずこれらのコンピューターに対して別の Kaspersky Endpoint Agent のポリシーを作成する必要があります。新しいポリシーで、Kaspersky Managed Detection and Response との連携を設定してください。

## Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 には、Kaspersky Endpoint Detection and Response Optimum ソリューション (以降「EDR Optimum」とします) の組み込みエージェントが含まれます。Kaspersky Endpoint Detection and Response Optimum は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻



撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

Kaspersky Endpoint Detection and Response Optimum は脅威の活動を調査して分析し、迅速な対応に必要な攻撃の可能性に関する情報をセキュリティの担当者または管理者に提供します。Kaspersky Endpoint Detection and Response は別のウィンドウでアラートの詳細を表示します。アラートの詳細 (Alert details) は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

このソリューションは次の脅威インテリジェンスツールを使用します：

- Kaspersky Security Network (以下、「KSN」とも表記)。クラウドサービスのインフラストラクチャで、カスペルスキーの情報基盤に基づいたリアルタイムのファイル、Web サイト、ソフトウェアの評価情報を提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。
- Kaspersky Private Security Network (以降「KPSN」とも表記) との連携。KSN にコンピューターからデータを送信することなく、その他の統計データや KSN 評価データベースへのアクセスを提供します。
- Kaspersky Threat Intelligence Portal の情報システムとの連携。ファイルや URL の評価に関する情報を蓄積し、表示できます。
- カスペルスキーの脅威データベース。

Kaspersky Endpoint Detection and Response Optimum が正常に動作するには、Kaspersky Security Center バージョン 13.2 が必要です。以前のバージョンの Kaspersky Security Center では、EDR Optimum をアクティベートすることはできません。

この機能は Web コンソールを使用した場合のみ管理できます。管理コンソール (MMC) を使用してこの機能を管理することはできません。

## Kaspersky Endpoint Detection and Response Optimum との連携

Kaspersky Endpoint Detection and Response Optimum とは次の手順で連携されます：

### ① Kaspersky Endpoint Detection and Response Optimum コンポーネントのインストール

Kaspersky Endpoint Detection and Response Optimum コンポーネントは、[インストール中](#)または[アップグレード中](#)、または[コンポーネントの変更](#)タスクを使用して選択できます。

コンポーネントの変更タスクの実行後、タスクのステータスが正しく表示されないことがあります。「正常に完了しました」と表示されるはずの箇所に「スケジュール済み」ステータスが表示されます。しかし、タスクは正常に完了している可能性があります。Kaspersky Security Center コンソール ( [アプリケーション] - [Kaspersky Endpoint Security for Windows] - [コンポーネント] ) の順に選択) または製品のローカルインターフェイスで新しいコンポーネントが正しくインストールされていることを確認してください。

### ② Kaspersky Endpoint Detection and Response Optimum をアクティベートする

次の方法で Kaspersky Endpoint Detection and Response Optimum を使用するライセンスを入手できます：

- EDR Optimum の機能が Kaspersky Endpoint Security for Windows を使用するライセンスに含まれている。機能は [Kaspersky Endpoint Security for Windows のアクティベーション](#)後すぐに使用できます。
- EDR Optimum を使用するためにライセンスを拡張する。  
Kaspersky Endpoint Detection and Response 向けの別のライセンスを追加すると使用できます。結果として、Kaspersky Endpoint Security のライセンスおよび Kaspersky Endpoint Detection and Response Optimum のライセンスの 2 種類のライセンスがコンピューターにインストールされることになります。  
個別の EDR Optimum のライセンスと Kaspersky Endpoint Security のライセンスに違いはありません。

EDR Optimum がライセンスでサポートされており、[本製品のローカルインターフェイス](#)で実行中であることを確認してください。

### 3 Endpoint Detection and Response Optimum コンポーネントの有効化

Kaspersky Endpoint Security for Windows のポリシー設定でこの機能を有効または無効にできます。

この機能を使用するには、次の条件を満たす必要があります：

- 本製品がアクティベートされており、Kaspersky Endpoint Detection and Response Optimum の機能がライセンスでサポートされている。
- Endpoint Detection and Response Optimum コンポーネントがオンになっている。
- Endpoint Detection and Response Optimum が連携する製品機能が有効になっており、動作している。Endpoint Detection and Response Optimum は次の製品機能と連携します：
  - [ファイル脅威対策](#)：
  - [ウェブ脅威対策](#)
  - [メール脅威対策](#)
  - [脆弱性攻撃ブロック](#)：
  - [ふるまい検知](#)
  - [ホスト侵入防止](#)：
  - [修復エンジン](#)：
  - [アダプティブアノマリーコントロール](#)：

[Web コンソールで Endpoint Detection and Response Optimum コンポーネントを有効または無効にする方法](#) 

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Endpoint Detection and Response Optimum]** の順に選択します。
5. **[Endpoint Detection and Response Optimum]** をオンにします。
6. 変更内容を保存します。

Kaspersky Endpoint Detection and Response Optimum コンポーネントが有効になりました。コンポーネントの動作状態は製品機能の状態レポートで表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。

**[Endpoint Detection and Response Optimum]** が Kaspersky Endpoint Security のコンポーネントのリストに追加されました。

#### ④ 管理サーバーへのデータ転送を有効にする

すべての EDR Optimum の機能を有効するには、次の種別のデータの転送を有効にする必要があります。

- 隔離されたファイルのデータ。

このデータは Web コンソール経由でコンピューター上で隔離されたファイルに関する情報を取得するために必要となります。たとえば、Web コンソールで分析用に隔離からファイルをダウンロードすることができます。

- 脅威の活動連鎖のデータ。

このデータは Web コンソールでコンピューター上で検知されたファイルに関する情報を取得するために必要となります。Web コンソールでアラートの詳細を憑依して必要な応答操作を行うことができます。

#### [Web コンソールで管理サーバーへのデータ転送を有効にする方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[全般設定]** → **[レポートと保管領域]** の順に選択します。
5. **[管理サーバーへのデータ転送]** の次のチェックボックスを選択してください：
  - **隔離ファイルの情報**
  - **脅威の活動連鎖の情報**
6. 変更内容を保存します。

## Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行

EDR Optimum コンポーネント（組み込みエージェント）を備えた Kaspersky Endpoint Security 11.7.0 以降がインストールされている場合、Kaspersky Endpoint Detection and Response Optimum ソリューションの動作のために必要な操作はありません。EDR Optimum コンポーネントは Kaspersky Endpoint Agent と互換性はありません。Kaspersky Endpoint Agent がコンピューターにインストールされている場合、Kaspersky Endpoint Security をバージョン 11.7.0 にアップデートするときに Kaspersky Endpoint Detection and Response Optimum は Kaspersky Endpoint Security との連携を継続します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行を完了するには、[移行ウィザード](#)を使用してポリシーとタスクの設定を移す必要があります。

Kaspersky Endpoint Security 11.4.0～11.6.0 を Kaspersky Endpoint Detection and Response Optimum との連携に使用している場合は、製品には Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Security のインストール中に並行して Kaspersky Endpoint Agent をインストールできます。

Kaspersky Endpoint Security の一部としての EDR Optimum コンポーネントは Kaspersky Endpoint Detection and Response Optimum 2.0 ソリューションとの連携をサポートします。Kaspersky Endpoint Detection and Response Optimum バージョン 1.0 との連携はサポートされていません。

## セキュリティ侵害インジケータ（IOC）のスキャン

セキュリティ侵害インジケータ（IOC）とは、コンピューターへの認証されないアクセス（コンピューターの侵害）の痕跡を示すオブジェクトまたは活動に関する一連のデータです。たとえば、システムへのログインを複数回失敗すると、セキュリティ侵害インジケータの構成要素となります。IOC スキャンタスクは、コンピューターのセキュリティ侵害インジケータを検索し、脅威への対応方法を確立するのに役立ちます。

Kaspersky Endpoint Security は IOC ファイルを使用して侵害インジケータを検索します。IOC ファイルとは、本製品が検知の判断時に一致させる一連のインジケータを含むファイルです。IOC ファイルは [OpenIOC 標準](#) に準拠している必要があります。Kaspersky Endpoint Security は IOC ファイルを自動で作成し、また、ユーザーが作成した IOC ファイルを読み込むこともできます。手動で侵害インジケータを追加する場合は、[IOC ファイルの要件](#)を参照してください。

以下のリンクをクリックすることでダウンロードできるファイルには、Kaspersky Endpoint Detection and Response がサポートするすべての OpenIOC 標準の IOC タームの一覧が含まれています。

 [こちらのリンクから IOC TERMS.XLSX ファイルをダウンロードできます](#)

## IOC スキャンタスクの実行モード

Kaspersky Endpoint Security では、次のモードで IOC スキャンが実行されます：

- 標準の IOC スキャンタスクは Web コンソールで手動で作成および設定されたタスクまたはタスクのグループを意味します。タスクは、ユーザーが準備した IOC ファイルを使用して実行されます。
- スタンドアロンの IOC スキャンタスクは、[Kaspersky Sandbox](#) で検知された脅威に到達した際に自動的に作成されるタスクのグループです。Kaspersky Endpoint Security は IOC ファイルを自動で作成します。カスタム IOC ファイルはサポートされていません。タスクは、そのタスクが最後に開始されてから（実行されていない場合は作成日から）7 日が経過すると自動的に削除されます。スタンドアロンの IOC スキャンタスクについて詳しくは、[Kaspersky Sandbox のヘルプ](#) を参照してください。

## IOC スキャンタスクの実行

脅威への対応時に、Kaspersky Sandbox が IOC スキャンタスクを自動で作成することがあります。Kaspersky Endpoint Detection and Response Optimum では、手動で IOC スキャンタスクの作成のみできます。

IOC スキャンタスクを次の方法で手動で作成することができます：

- アラートの詳細で作成する。  
アラートの詳細 (*Alert details*) は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。
- タスクウィザードを使用する。

Web コンソールでのみ設定できます。

脅威に対するスタンドアロンの IOC スキャンタスクを作成するには、Kaspersky Security Center バージョン 13.2 が必要です。

IOC スキャンタスクを作成するには：

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：

- a. **アプリケーション**ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)**を選択します。
  - b. **[タスク種別]** で、 **[IOC スキャン]** を選択します。
  - c. **[タスク名]** に簡潔な内容を入力します。
  - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。 **[次へ]** をクリックします。
  5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。 **[次へ]** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

システムアカウント (SYSTEM) にはネットワークドライブの IOC スキャンタスクを実行する権限がありません。ネットワークドライブに対してタスクを実行する場合に、そのドライブにアクセス権のあるユーザーアカウントを選択してください。

ネットワークドライブのスタンドアロンの IOC スキャンタスクには、タスクのプロパティで、そのドライブにアクセス権のあるユーザーアカウントを手動で選択する必要があります。

6. **[終了]** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
8. **[アプリケーション設定]** タブを選択します。
9. **[IOC スキャン設定]** を選択します。
10. 侵害インジケータを検索するために IOC ファイルを読み込みます。  
IOC ファイルの読み込み後、IOC ファイルのインジケータのリストが表示できます。必要に応じて、タスク範囲から一時的に IOC ファイルを除外することができます。

タスク実行後の IOC ファイルの追加または削除は推奨されません。前回実行された IOC スキャン結果が正しく表示されないことがあります。IOC ファイルの侵害インジケータを検索するには、新しいタスクを追加するようにしてください。

#### 11. IOC 検知時の動作の設定 :

- **コンピューターをネットワークから分離する** : このオプションを選択した場合、Kaspersky Endpoint Security は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。分離時間は [Endpoint Detection and Response コンポーネントの設定](#) で設定できます。
- **コピーを隔離に移動し、オブジェクトを削除する** : このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。



- **簡易スキャンを実行する**：このオプションを選択した場合、Kaspersky Endpoint Security は[簡易スキャン](#)タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。

12. **[詳細]** に移動します

13. タスクの一部として分析される必要のあるデータ種別（IOC ドキュメント）を選択します。

Kaspersky Endpoint Security は、読み込まれた IOC ファイルの内容に従って IOC スキャンタスク用のデータ種別（IOC ドキュメント）を自動で選択します。選択されたデータ種別の選択解除は推奨されません。

次のデータ種別に対してスキャン範囲を追加で設定できます：

- **ファイル - FileItem**：事前定義された範囲を使用してコンピューター上の IOC スキャン範囲を設定します。

既定では、Kaspersky Endpoint Security はコンピューターの重要な領域（ダウンロードフォルダー、デスクトップ、一時的なオペレーティングシステムのファイルがあるフォルダーなど）のみの IOC をスキャンします。スキャン範囲を手動で追加することもできます。

- **Windows イベントログ - EventLogItem**：イベントが記録された際の時間周期を入力します。IOC スキャンにアプリケーションイベントログ、システムイベントログ、セキュリティイベントログなど、Windows イベントログを選択することもできます。

Kaspersky Endpoint Security はデータ種別 **[Windows レジストリ - RegistryItem]** に対しては、[レジストリキー](#)式をスキャンします。

14. **[保存]** をクリックします。

15. タスクの横にあるチェックボックスをオンにします。

16. **[開始]** をクリックします。

Kaspersky Endpoint Security はコンピューター上にある侵害インジケータの検索を実行します。**[結果]** のタスクのプロパティでタスクの結果を確認できます。**[アプリケーション設定]** → **[IOC スキャン結果]** の順に選択して、タスクのプロパティで侵害インジケータに関する情報を表示することができます。

IOC スキャン結果は 30 日間保持されます。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータを自動的に削除します。

## ファイルを隔離する

脅威への対応として、Kaspersky Endpoint Detection and Response Optimum はファイルの隔離タスクを作成します。隔離とは、ウイルスに感染したファイルや駆除できないファイルを移動する特別なローカルの保管領域です。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。

Kaspersky Endpoint Security は Kaspersky Sandbox および Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する際にのみこの隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、[Kaspersky Sandbox](#) および [Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。



次の方法でファイルの隔離タスクを作成できます：

- アラートの詳細で作成する。

アラートの詳細 (*Alert details*) は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれません。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

- タスクウィザードを使用する。

ファイルのパスまたはハッシュ (SHA256 または MD5) 、もしくはファイルのパスとハッシュの両方を入力する必要があります。

ファイルのサイズは 100 MB を超えることはできません。

Web コンソールでのみ設定できます。

ファイルの隔離タスクを作成するには：

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. **[追加]** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **[タスク種別]** で、**[ファイルの隔離]** を選択します。
  - c. **[タスク名]** に簡潔な内容を入力します。
  - d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。**[次へ]** をクリックします。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。**[次へ]** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

6. **[終了]** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
8. **[アプリケーション設定]** タブを選択します。

9. ファイルのリストで、**【追加】** をクリックします。

ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「\\」から開始されるファイルのパスを入力してください。例： \\server\shared\_folder\file.exe ファイルのパスにドライブ文字があると、ファイルが見つかりませんというエラーになります。

11. **【保存】** をクリックします。

12. タスクの横にあるチェックボックスをオンにします。

13. **【開始】** をクリックします。

Kaspersky Endpoint Security はファイルを隔離します。ファイルが別のプロセスでロックされている場合は、タスクは完了として表示されますが、ファイルそのものはコンピューターが再起動されてから隔離されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

実行中のファイルを隔離しようとした場合、ファイルの隔離タスクはエラー「アクセスが拒否されました」で終了することがあります。ファイルに対して[プロセスの終了タスクを作成](#)してから再度実行してください。

サイズが大きいファイルを隔離しようとする場合、ファイルの隔離タスクがエラー「隔離の保管領域に十分な空き容量がありません」で失敗することがあります。隔離の中身を空にするか、[隔離のサイズを拡大](#)してください。再度実行してください。

Web コンソールを使用して隔離からファイルを復元したり、隔離の中身を空にすることができます。[コマンドライン](#)を使用してオブジェクトをローカルコンピューター上に復元できます。

## ファイルを取得する

ユーザーのコンピューターからファイルを取得することができます。たとえば、サードパーティ製品によって作成されたイベントログファイルを取得するよう設定することができます。ファイルを取得するには、専用のタスクを作成する必要があります。そのタスクの実行結果として、ファイルは隔離に保存されます。Web コンソールを使用して隔離に保存されたこのファイルをダウンロードすることができます。ユーザーのコンピューターでは、ファイルは元のフォルダーに残ります。

ファイルのサイズは 100 MB を超えることはできません。

Web コンソールでのみ設定できます。

ファイルの取得タスクを作成するには：

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。

タスクのリストが表示されます。

2. **【追加】** をクリックします。

タスクウィザードが起動します。

3. タスクの設定を指定します：

- a. **アプリケーション**ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)**を選択します。
- b. **[タスク種別]** で、**[ファイルの取得]** を選択します。
- c. **[タスク名]** に簡潔な内容を入力します。
- d. **[タスクを割り当てるデバイスの選択]** で、タスク範囲の指定方法を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。 **[次へ]** をクリックします。

5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。 **[次へ]** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

6. **[終了]** をクリックして、ウィザードを終了します。

タスクのリストに新しいタスクが表示されます。

7. 新しいタスクをクリックします。

タスクのプロパティウィンドウが表示されます。

8. **[アプリケーション設定]** タブを選択します。

9. ファイルのリストで、 **[追加]** をクリックします。

ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「**\\**」から開始されるファイルのパスを入力してください。例： `\\server\shared_folder\file.exe` ファイルのパスにドライブ文字があると、ファイルが見つかりませんというエラーになります。

11. **[保存]** をクリックします。

12. タスクの横にあるチェックボックスをオンにします。

13. **[開始]** をクリックします。

この結果、Kaspersky Endpoint Security はファイルのコピーを作成し、コピーを隔離に移動します。Web コンソールで隔離からファイルをダウンロードします。

## ファイルを削除する

ファイルの削除タスクを使用してリモートからファイルを削除できます。たとえば、脅威への対応としてリモートからファイルを削除する場合などです。

Web コンソールでのみ設定できます。

ファイルの削除タスクを作成するには：

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **【タスク種別】** で、**【ファイルの削除】** を選択します。
  - c. **【タスク名】** に簡潔な内容を入力します。
  - d. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。 **【次へ】** をクリックします。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。 **【次へ】** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

6. **【終了】** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
8. **【アプリケーション設定】** タブを選択します。
9. ファイルのリストで、**【追加】** をクリックします。  
ファイルの追加ウィザードが開始されます。
10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「**\\**」から開始されるファイルのパスを入力してください。例： `\\server\shared_folder\file.exe` ファイルのパスにドライブ文字があると、ファイルが見つかりませんというエラーになります。

11. **【保存】** をクリックします。
12. タスクの横にあるチェックボックスをオンにします。

### 13. **【開始】** をクリックします。

Kaspersky Endpoint Security はコンピューターからファイルを削除します。ファイルが別のプロセスでロックされている場合は、タスクは完了として表示されますが、ファイルそのものはコンピューターが再起動されてから削除されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

実行中のファイルを隔離しようとした場合、ファイルの削除タスクはエラー「アクセスが拒否されました」で終了することがあります。ファイルに対して[プロセスの終了タスクを作成](#)してから再度実行してください。

## プロセスの開始

プロセスの開始タスクを使用してリモートからファイルを実行することができます。たとえば、コンピューターの設定ファイルを作成するユーティリティをリモートから実行したりすることができます。次に、[ファイルの取得タスク](#)を使用して Kaspersky Security Center Web コンソールで作成されたファイルを受け取ります。

Web コンソールでのみ設定できます。

プロセスの開始タスクを作成するには：

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。  
タスクのリストが表示されます。
2. **【追加】** をクリックします。  
タスクウィザードが起動します。
3. タスクの設定を指定します：
  - a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
  - b. **【タスク種別】** で、**【プロセスの開始】** を選択します。
  - c. **【タスク名】** に簡潔な内容を入力します。
  - d. **【タスクを割り当てるデバイスの選択】** で、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。**【次へ】** をクリックします。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。**【次へ】** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

6. **【終了】** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。
8. タスクのプロパティウィンドウが表示されます。

9. **【アプリケーション設定】** タブを選択します。

10. プロセスの開始コマンドを入力します。

たとえば、「conf.txt」というファイルにコンピューターの設定に関する情報を保存する「utility.exe」というユーティリティを使用する場合、次のように値を入力します：

- **実行コマンド** – utility.exe
- **コマンドライン引数** – /R conf.txt
- **作業フォルダーのパス** – C:\Users\admin\Diagnostic\

または、**【実行コマンド】** フィールドに、「C:\Users\admin\Diagnostic\utility.exe /R conf.txt」と入力することもできます。この場合、その他の設定を入力する必要はありません。

11. **【保存】** をクリックします。

12. タスクの横にあるチェックボックスをオンにします。

13. **【開始】** をクリックします。

この結果、Kaspersky Endpoint Security はコマンドをサイレントモードで実行し、プロセスを開始します。**【結果】** のタスクのプロパティでタスクの結果を確認できます。

## プロセスの終了

プロセスの終了タスクを使用してリモートからプロセスを終了することができます。たとえば、[プロセスの開始タスク](#)を使用して開始されたインターネットの速度テストツールをリモートから終了する場合などです。

ファイルの実行をブロックする場合は、[実行防止機能](#)を設定することができます。実行ファイル、スクリプト、Office 形式のファイルの実行を禁止することができます。

プロセスの終了タスクには次の制限事項があります：

- 重要なシステムオブジェクト（SCO）のプロセスは終了できません。SCO とはオペレーティングシステムと Kaspersky Endpoint Security for Windows アプリケーションが実行できる必要のあるファイルです。
- EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

プロセスの終了タスクを作成するには：

1. Web コンソールのメインウィンドウで、**【デバイス】** → **【タスク】** の順に選択します。

タスクのリストが表示されます。

2. **【追加】** をクリックします。

タスクウィザードが起動します。

3. タスクの設定を指定します：

- a. **アプリケーション** ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (11.7.0)** を選択します。
- b. **【タスク種別】** で、**【プロセスの強制終了】** を選択します。

- c. **【タスク名】** に簡潔な内容を入力します。
  - d. **【タスクを割り当てるデバイスの選択】** ブロックで、タスク範囲の指定方法を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。 **【次へ】** をクリックします。
  5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。 **【次へ】** をクリックします。

既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント (SYSTEM) として開始します。

6. **【終了】** をクリックして、ウィザードを終了します。  
タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。  
タスクのプロパティウィンドウが表示されます。
8. **【アプリケーション設定】** タブを選択します。
9. 手順を完了するには、強制終了するファイルを選択する必要があります。次のいずれかの方法でファイルを選択することができます：
  - ファイルの完全名を入力します。
  - ファイルのハッシュとパスを入力します。
  - プロセスの PID を入力します (ローカルタスクのみ) 。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「\\」から開始されるファイルのパスを入力してください。例： \\server\shared\_folder\file.exe ファイルのパスにドライブ文字があると、ファイルが見つかりませんというエラーになります。

10. コンピューターのプロパティウィンドウで、 **【スケジュール】** タブを選択します。
11. タスクのスケジュールを設定します。

このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっている、タスクを実行できることを確認してください。

12. **【保存】** をクリックします。
13. タスクの横にあるチェックボックスをオンにします。
14. **【開始】** をクリックします。

この結果、Kaspersky Endpoint Security はコンピューター上でそのプロセスを終了します。たとえば、アプリケーション「ゲーム」が実行中で、game.exe プロセスを終了すると、データを保存せずにアプリケーションは終了されます。 **【結果】** のタスクのプロパティでタスクの結果を確認できます。

## 実行防止



実行防止を使用して、実行ファイルやスクリプトの実行や Office 形式のファイルを開く動作を管理することができます。こうすることで、安全でないと考えられるアプリケーションの実行をブロックしたりすることができます。実行防止は、[Office ファイルの拡張子のセット](#)および[スクリプトインタープリターのセット](#)をサポートしています。

## 実行防止ルール

実行防止ルールを含むファイルへのユーザーのアクセスを管理することができます。実行防止ルールはブロック時に参照される条件の一式です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。

実行防止ルールは次の方法で作成できます：

- アラートの詳細で作成する。

アラートの詳細 (*Alert details*) は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれません。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

- グループポリシーまたはローカルアプリケーション設定を使用する。

ファイルのパスまたはハッシュ (SHA256 または MD5)、もしくはファイルのパスとハッシュの両方を入力する必要があります。

ローカルで[コマンドライン](#)を使用して実行防止を管理することもできます。

5000 以上の実行防止ルールの作成は、システムが不安定になる可能性があるため推奨されません。

CD や IOS イメージ上のファイルは実行防止の対象外です。これらのファイルの実行はブロックされません。

## 実行防止ルールのモード

実行防止機能は以下の 2 つのモードで動作します：

- **統計の作成のみ：**

このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。

- **アクティブ：**

このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。

## 実行防止の管理

Web コンソールでのみこの機能を設定できます。

実行を防止するには：

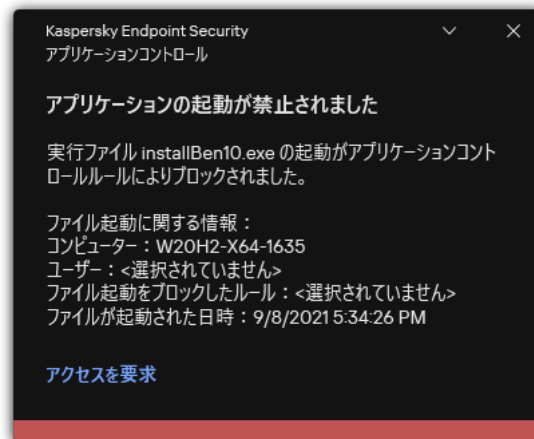
1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [Detection and Response] → [Endpoint Detection and Response] の順に選択します。
5. [実行防止] を使用して機能を有効または無効にします。
6. [禁止されたオブジェクトを実行、または開いたときの処理] で、機能の操作モードを選択します：
  - **ブロックしてレポートに書き込む**：このモードでは、オブジェクトを実行したり、禁止するルールに基づいて一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。
  - **イベントの記録のみ**：このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。
7. 実行防止ルールのリストを作成します：
  - a. [追加] をクリックします。
  - b. 表示されるウィンドウで、「アプリケーション A」のように実行防止ルールの名前を入力します。
  - c. [種別] で、[実行ファイル]、[スクリプト]、[Microsoft Office ドキュメント] からブロックするオブジェクトを選択します。  
オブジェクト種別を誤って選択すると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。
  - d. ファイルを追加するには、ファイルのハッシュ（SHA256 または MD5）、ファイルの完全パス、ハッシュとパスの両方を入力する必要があります。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「\\」から開始されるファイルのパスを入力してください。例： \\server\shared\_folder\file.exe ファイルのパスにネットワークドライブ文字が含まれていると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。

実行防止は、[Office ファイルの拡張子のセット](#)および[スクリプトインタープリターのセット](#)をサポートしています。

- e. [OK] をクリックします。
8. 変更内容を保存します。

この結果、Kaspersky Endpoint Security はオブジェクトの実行（実行ファイルやスクリプトの実行、Office 形式のファイルを開く動作）をブロックします。スクリプトの実行がブロックされていても、例えばスクリプトファイルテキストエディタで開くことなどは可能です。オブジェクトの実行をブロックする際、[製品設定で有効にされている](#)場合は Kaspersky Endpoint Security は標準の通知（下の図を参照）を表示します。



実行防止の通知

## コンピューターのネットワーク分離

コンピューターのネットワーク分離を使用して、セキュリティ侵害インジケータ（IOC）の検知時の対応として、コンピューターを自動的にネットワークから分離できます。

ネットワーク分離がオンになると、本製品はすべてのアクティブな接続を切断し、コンピューターのすべての新規 TCP/IP 接続をブロックしますが、以下の接続は切断されません：

- ネットワーク分離の除外リストに追加されている接続。
- Kaspersky Endpoint Security サービスによって開始された接続。
- Kaspersky Security Center 管理エージェントによって開始された接続。

## ネットワーク分離の管理

Web コンソールでのみこの機能を設定できます。

IOC 検知時の対応として、ネットワーク分離を自動的にオンにするよう設定できます。手動でネットワーク分離をオンまたはオフにすることができます。

ネットワーク分離は次の方法でオンにできます：

- アラートの詳細で作成する。  
アラートの詳細（Alert details）は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれません。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。
- 個別のローカル環境用の製品設定を使用する。

## IOC 検知時の対応として、ネットワーク分離を自動的に有効にするよう設定する方法

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。  
タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **[IOC スキャン]** タスクを選択します。  
タスクのプロパティウィンドウが表示されます。  
必要に応じて、[IOC スキャン](#) タスクを作成します。
3. **[アプリケーション設定]** タブを選択します。
4. **[IOC 検知時の処理]** で、**[IOC が見つかった後に応答処理を実行する]** および **[コンピューターをネットワークから分離する]** を選択します。
5. 変更内容を保存します。

この結果、IOC が検知されると、本製品は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。

## 手動でコンピューターのネットワーク分離を有効にする方法

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[管理対象デバイス]** の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。  
コンピューターのプロパティが表示されます。
3. **[アプリケーション]** タブを選択します。
4. Kaspersky Endpoint Security for Windows をクリックします。  
ローカルアプリケーション設定が表示されます。
5. **[アプリケーション設定]** タブを選択します。
6. **[Detection and Response]** → **[Endpoint Detection and Response]** の順に選択します。
7. **[ネットワーク分離]** で、**[コンピューターをネットワークから分離する]** をクリックします。
8. 変更内容を保存します。

指定した時間が経過した後にネットワーク分離を自動でオフにするよう設定することができます。既定では、ネットワーク分離がオンになってから 5 時間が経過すると、本製品はネットワーク分離をオフにします。手動でネットワーク分離をオフにすることもできます。ネットワーク分離をオフにした後は、コンピューターは制限されることなくネットワークを使用することができます。

## コンピューターのネットワーク分離を自動でオフにする時間の遅延を設定する方法

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Endpoint Detection and Response]** の順に選択します。
5. **[ネットワーク分離]** で、**[コンピューターのロック解除を設定する]** をクリックします。
6. 表示されたウィンドウで、**[分離されたコンピューターのロックを自動的に解除するまでの時間]** を選択して、自動でネットワーク分離をオフにするまでの時間を入力します。
7. 変更内容を保存します。

### 手動でコンピューターのネットワーク分離を無効にする方法

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[管理対象デバイス]** の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。  
コンピューターのプロパティが表示されます。
3. **[アプリケーション]** タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。  
ローカルアプリケーション設定が表示されます。
5. **[アプリケーション設定]** タブを選択します。
6. **[Detection and Response]** → **[Endpoint Detection and Response]** の順に選択します。
7. **[ネットワーク分離]** で、**[ネットワークから分離されたコンピューターをブロック解除する]** をクリックします。
8. 変更内容を保存します。

ローカルで [コマンドライン](#) を使用してネットワーク分離を無効にすることもできます。

## ネットワーク分離の除外リスト

ネットワーク分離の除外リストを設定できます。ネットワーク分離がオンになっても、ルールに一致するネットワーク接続はブロックされません。

標準のネットワークプロファイルのリストを使用してネットワーク分離の除外リストを設定できます。既定では、除外リストには DNS/DHCP サーバーおよび DNS/DHCP クライアントルールを持つデバイスの動作が妨げられないようにするルールを含むネットワークプロファイルが含まれています。標準のネットワークプロファイルまたは除外リストの設定は手動で変更できます（以下の手順を参照してください）。

ポリシーのプロパティで指定された除外リストは、脅威の検知時の対応としてネットワーク分離が自動的にオンになった場合にのみ適用されます。コンピューターのプロパティで指定された除外リストは、Kaspersky Security Center のコンソールのコンピューターのプロパティから手動でネットワーク分離をオンにした場合にのみ適用されます。

これらのパラメータは異なる使用シナリオを持つため、有効なポリシーはコンピューターのプロパティで設定されたネットワーク分離の除外リストの適用をブロックしません。

## ネットワーク分離の除外リストを追加する方法

1. Web コンソールのメインウィンドウで [デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [Detection and Response] → [Endpoint Detection and Response] の順に選択します。
5. [ネットワーク分離の除外リスト] で、[除外リスト] をクリックします。
6. 表示されるウィンドウで、[プロファイルから追加] をクリックして例外を設定する標準ネットワークプロファイルを選択します。  
プロファイルからネットワーク分離の除外リストがネットワーク分離の除外リストのリストに追加されます。ネットワーク接続のプロパティが表示されます。必要に応じて、ネットワーク接続設定を編集できます。
7. 必要に応じて、ネットワーク分離の除外リストを手動で追加してください。ネットワーク分離の除外リストを手動で追加するには、除外リストのウィンドウで [追加] をクリックしてネットワーク接続設定を手動で編集してください。
8. 変更内容を保存します。

ローカルで [コマンドライン](#) を使用してネットワーク分離の除外リストを表示することもできます。

## Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 には Kaspersky Sandbox コンポーネントが含まれています。この機能は Kaspersky Sandbox ソリューションとの連携を有効にします。Kaspersky Sandbox ソリューションはコンピューター上の高度な脅威を検知し、自動的にブロックします。Kaspersky Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Kaspersky Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Kaspersky Sandbox サーバー）上でオブジェクトを分析およびスキャンします。このソリューションについて詳しくは、[Kaspersky Sandbox](#) のヘルプを参照してください。

Kaspersky Sandbox と連携すると、以下の操作が可能になります：



- Kaspersky Sandbox サーバーに安全に接続するための TLS 証明書を追加する。
- Kaspersky Sandbox サーバーを追加する。
- 脅威に対する応答処理を選択する。
- セキュリティ侵害インジケータ (IOC) をスキャンする。

Kaspersky Sandbox が正常に動作するためには Kaspersky Security Center バージョン 13.2 が必要です。Kaspersky Security Center の以前のバージョンでは、脅威応答のスタンドアロンの IOC スキャンタスクの作成は許可されません。

この機能は Web コンソールを使用した場合のみ管理できます。管理コンソール (MMC) を使用してこの機能を管理することはできません。

## Kaspersky Sandbox との連携

Kaspersky Sandbox と連携するためには、次の手順を実行してください：

### ① Kaspersky Sandbox コンポーネントのインストール

Kaspersky Sandbox コンポーネントは、[インストール中](#)または[アップグレード中](#)、または[コンポーネントの変更](#)タスクを使用して選択できます。

コンポーネントの変更タスクの実行後、タスクのステータスが正しく表示されないことがあります。「正常に完了しました」と表示されるはずの箇所に「スケジュール済み」ステータスが表示されます。しかし、タスクは正常に完了している可能性があります。Kaspersky Security Center コンソール（[アプリケーション] - [Kaspersky Endpoint Security for Windows] - [コンポーネント] の順に選択）または製品のローカルインターフェイスで新しいコンポーネントが正しくインストールされていることを確認してください。

### ② TLS 証明書の追加

Kaspersky Sandbox サーバーと信頼済み接続を設定するには、TLS 証明書を準備する必要があります。次にその証明書を Kaspersky Sandbox サーバーおよび Kaspersky Endpoint Security ポリシーに追加します。証明書の準備およびサーバーへの証明書の追加について詳しくは、Kaspersky Sandbox のヘルプを参照してください。

[Web コンソールを使用して TLS 証明書を追加する方法](#) 



1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Kaspersky Sandbox]** の順に選択します。
5. **[サーバーの接続設定]** をクリックします。  
Kaspersky Sandbox サーバーの接続設定ウィンドウが表示されます。
6. **[サーバー TLS 証明書]** で、**[追加]** を選択して TLS 証明書ファイルを選択します。  
Kaspersky Endpoint Security は、1つの Kaspersky Sandbox サーバーに対して1つの TLS 証明書のみ持つことができます。以前に TLS 証明書を追加していた場合、その証明書は取り消されます。一番新しい証明書が使用されます。
7. Kaspersky Sandbox サーバーの詳細な接続設定を行います。
  - **要求のタイムアウト** : Kaspersky Sandbox サーバーの接続タイムアウトです。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、Kaspersky Sandbox の接続タイムアウトの時間を長くすることができます。既定値は5秒です。
  - **Kaspersky Sandbox 要求のキュー** : 要求のキューフォルダーのサイズです。オブジェクトがコンピューター上でアクセス（実行ファイルが開始されたり、DOCX や PDF 形式のドキュメントを開いたり）されると、Kaspersky Endpoint Security はそのオブジェクトを Kaspersky Sandbox に送ります。複数の要求があった場合は、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは100 MB に制限されています。最大サイズに到達すると、Kaspersky Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。
8. 変更内容を保存します。

TLS 証明書が検証されます。証明書の検証が正常に完了すると、Kaspersky Endpoint Security は次回の Kaspersky Security Center との同期の際に証明書をコンピューターに送信します。2つの TLS 証明書を追加した場合、Kaspersky Sandbox は新しいほうの証明書を使用して信頼済み接続を確立します。

[コマンドライン](#)を使用して TLS 証明書をコンピューターに追加することもできます。

### 3 Kaspersky Sandbox コンポーネントの有効化

Kaspersky Endpoint Security for Windows のポリシー設定でこの機能を有効または無効にできます。

この機能を使用するには、次の条件を満たす必要があります :

- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- Kaspersky Sandbox コンポーネントが有効になっている。

[Web コンソールを使用して Kaspersky Sandbox を有効または無効にする方法](#) 

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Kaspersky Sandbox]** の順に選択します。
5. **[Kaspersky Sandbox との統合]** トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

[コマンドライン](#)を使用して Kaspersky Sandbox をローカルで有効または無効にすることもできます。

Kaspersky Sandbox コンポーネントが有効になりました。コンポーネントの動作状態は製品機能の状態レポートで表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。**[Kaspersky Sandbox]** が Kaspersky Endpoint Security のコンポーネントのリストに追加されました。

#### 4 Kaspersky Sandbox サーバーへのコンピューターの接続

オペレーティングシステムの仮想イメージを持つ Kaspersky Sandbox サーバーにコンピューターを接続するには、サーバーのアドレスとポートを入力する必要があります。仮想イメージの配備と Kaspersky Sandbox サーバーの設定について詳しくは、[Kaspersky Sandbox のヘルプ](#) を参照してください。

##### [Web コンソールを使用して Kaspersky Sandbox サーバーにコンピューターを接続する方法](#)

1. Web コンソールのメインウィンドウで **[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Kaspersky Sandbox]** の順に選択します。
5. **[Kaspersky Sandbox のサーバー]** で、**[追加]** をクリックします。
6. 表示されるウィンドウで、Kaspersky Sandbox のサーバーのアドレス (IPv4、IPv6、DNS) およびポートを入力します。
7. 変更内容を保存します。

#### 5 Kaspersky Security Center Web コンソールと管理サーバー間でのバックグラウンド接続の確立

Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Sandbox が連携するためには、新しい保護された接続であるバックグラウンド接続を確立する必要があります。Kaspersky Security Center とその他のカスペルスキーのソリューションとの統合について詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。

##### [Web コンソールとのバックグラウンド接続を確立する](#)

1. Web コンソールのメインウィンドウで、**【コンソールの設定】** → **【タスク】** の順に選択します。
2. **【サービス間連携】** に移動します。
3. **【サービス間連携のためのバックグラウンド接続を確立する】** トグルスイッチを有効にします。
4. 変更内容を保存します。

Kaspersky Security Center Web コンソールと管理サーバー間でバックグラウンド接続が確立されていない場合、脅威への対応の一部としてのスタンドアロンのIOC スキャンタスクは作成されません。

## 6 管理サーバーへのデータ転送を有効にする

Kaspersky Sandbox のすべての機能を使用するには、隔離するファイルのデータ転送が有効になっていることを確認してください。このデータは Web コンソール経由でコンピューター上で隔離されたファイルに関する情報を取得するために必要となります。たとえば、Web コンソールで分析用に隔離からファイルをダウンロードすることができます。

### Web コンソールで管理サーバーへのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで **【デバイス】** → **【ポリシーとプロファイル】** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。  
ポリシーのプロパティウィンドウが表示されます。
3. **【アプリケーション設定】** タブを選択します。
4. **【全般設定】** → **【レポートと保管領域】** の順に選択します。
5. **【管理サーバーへのデータ転送】** で、**【隔離ファイルの情報】** をオンにします。
6. 変更内容を保存します。

## Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行

Kaspersky Sandbox がインストールされた Kaspersky Endpoint Security 11.7.0 以降のバージョンを使用している場合は、Kaspersky Sandbox ソリューションとの連携はインストール直後から利用可能です。Kaspersky Sandbox コンポーネントは Kaspersky Endpoint Agent と互換性はありません。Kaspersky Endpoint Agent がコンピューターにインストールされている場合、Kaspersky Endpoint Security をバージョン 11.7.0 にアップデートするときに Kaspersky Sandbox は Kaspersky Endpoint Security との連携を継続します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行を完了するには、[移行ウィザード](#)を使用してポリシーとタスクの設定を移す必要があります。

Kaspersky Endpoint Security 11.4.0~11.6.0 を Kaspersky Sandbox との連携に使用している場合は、製品には Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Security のインストール中に並行して Kaspersky Endpoint Agent をインストールできます。

Kaspersky Endpoint Security の一部としての Kaspersky Sandbox コンポーネントは Kaspersky Sandbox ソリューション 2.0 との連携をサポートします。Kaspersky Sandbox ソリューション 1.0 はサポートされません。

# コマンドラインを使用しての製品の管理

コマンドラインを使用して Kaspersky Endpoint Security を管理できます。本製品の管理に利用できるコマンドのリストは、「HELP」コマンドを実行して確認できます。特定のコマンドの構文を確認するには、「HELP <コマンド>」コマンドを実行します。

コマンド内の特殊文字はエスケープする必要があります。文字「&」、「|」、「(」、「)」、「<」、「>」、「^」をエスケープするには、「^」を使用します（たとえば、「&」を使用するには「^&」と入力します）。文字「%」をエスケープするには、「%%」と入力します。

## 本製品のインストール

Kaspersky Endpoint Security は次のいずれかのモードでコマンドラインを使用してインストールできます。

- セットアップウィザードを使用したインタラクティブモード
- サイレントモード：サイレントモードでのインストールの開始後は、インストールプロセスでユーザーが操作を行う必要はありません。サイレントモードで本製品をインストールするには、「/s」と「/qn」パラメータを使用します。

サイレントモードで本製品をインストールする前には、使用許諾契約書とプライバシーポリシーをよくお読みください。使用許諾契約書とプライバシーポリシーのテキストは、[Kaspersky Endpoint Security の配信キット](#)に含まれています。使用許諾契約書の条項をすべて確認し、理解した上でこれに同意しており、なおかつプライバシーポリシーの内容をすべて確認し、理解した上で、プライバシーポリシーに従ってデータの処理と送信（第三国への送信を含む）が行われることに同意している場合のみ、本製品のインストールに進むことができます。使用許諾契約書の条項とプライバシーポリシーに同意しない場合、Kaspersky Endpoint Security をインストールまたは使用しないでください。

本製品をインストールまたは以前のバージョンからアップグレードするには：

1. 管理者としてコマンドラインインタープリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<ユーザー名> /pKLPASSWD=<パスワード> /pKLPASSWDAREA=<パスワードを要求する操作>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<トレースレベル>] [/s]
```

または

```
msiexec /i <配信キット名> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1]
[SKIPPRODUCTCHECK=1] [KLLOGIN=<ユーザー名> KLPASSWD=<パスワード> KLPASSWDAREA=<パスワードを要求する操作>] [ENABLETRACES=1|0 TRACESLEVEL=<トレースレベル>] [/qn]
```

EULA=1	使用許諾契約書の条項に同意する。使用許諾契約書のテキストは、 <a href="#">Kaspersky Endpoint Security の配信キット</a> に含まれています。
--------	---

	<p>製品をインストールまたはアップグレードするには、使用許諾契約書に同意する必要があります。</p>
PRIVACYPOLICY=1	<p>プライバシーポリシーに同意する。プライバシーポリシーのテキストは、<a href="#">Kaspersky Endpoint Security の配信キット</a>に含まれています。</p> <p>本製品のインストールおよびバージョンのアップグレードには、プライバシーポリシーに同意する必要があります。</p>
KSN	<p>Kaspersky Security Network への参加に同意するかどうか。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security を最初に起動したときに、KSN への参加に同意するかどうかの確認画面が表示されます。次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1：KSN への参加に同意する</li> <li>• 0：KSN への参加に同意しない（既定値）</li> </ul> <p>Kaspersky Endpoint Security の配布パッケージは、Kaspersky Security Network とともに使用するよう最適化されています。Kaspersky Security Network に参加しない場合、インストール後すぐに Kaspersky Endpoint Security をアップデートしてください。</p>
ALLOWREBOOT=1	<p>製品のインストール後またはアップグレード後にコンピューターの再起動が必要な場合に自動再起動を行うかどうか。このパラメータの値が指定されていない場合、コンピューターの自動再起動はブロックされます。</p> <p>Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。</p>
SKIPPRODUCTCHECK=1	<p>競合する製品のチェックの実行を無効にするかどうか。競合する製品のリストは、<a href="#">配信キット</a>に含まれている incompatible.txt ファイルで参照できます。このパラメータの値が指定されておらず、互換性のない製品が検知された場合、Kaspersky Endpoint Security のインストールは終了します。</p>
SKIPPRODUCTUNINSTALL=1	<p>競合する製品を検知したときに自動的に削除するかどうか。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security は互換性のないソフトウェアの削除を試みます。</p> <p>msiexec インストーラーを使用して Kaspersky Endpoint Security をインストールする場合、競合する製品の自動削除を有効にすることはできません。競合する製品の自動削除を有効にする場合は、setup_kes.exe を使用してください。</p>
KLLOGIN	<p>Kaspersky Endpoint Security の機能と設定にアクセスできるユーザー名の指定（<a href="#">パスワードによる保護機能</a>）。ユーザー名は、「KLPASSWD」および「KLPASSWDAREA」の設定と合わせて指定します。既定では、ユーザー名 KLAdmin が使用されます。</p>
KLPASSWD	<p>Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワード</p>



	<p>ード（パスワードは「KLLOGIN」および「KLPASSWDAREA」パラメータと合わせて指定します）。</p> <p>「KLLOGIN」パラメータでユーザー名を指定せずにパスワードを指定した場合、KAdmin が既定のユーザー名として使用されます。</p>
KLPASSWDAREA	<p>Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワードが必要になる操作の範囲。この範囲内に含まれている操作をユーザーが実行しようとした場合、Kaspersky Endpoint Security でアカウントの認証情報の入力を求められます（「KLLOGIN」と「KLPASSWD」パラメータ）。複数の値を指定するには、区切り文字として「;」を使用してください。次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• SET：製品設定の変更</li> <li>• EXIT：製品の終了</li> <li>• DISPROTECT：保護機能の停止とスキャンタスクの停止</li> <li>• DISPOLICY：Kaspersky Security Center ポリシーの無効化</li> <li>• UNINST：コンピューターからの製品の削除</li> <li>• DISCTRL：管理コンポーネントの停止</li> <li>• REMOVELIC：ライセンスの削除</li> <li>• REPORTS：レポートの表示</li> </ul>
ENABLETRACES	<p>本製品のトレース記録を有効にするかどうか。Kaspersky Endpoint Security は、起動後にトレースファイルを「%ProgramData%\Kaspersky Lab\KES\Traces」フォルダーに保存します。次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1：トレース記録をオンにする</li> <li>• 0：トレース記録をオフにする（既定値）</li> </ul>
TRACESLEVEL	<p>トレース記録の詳細度。次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 100（緊急）：深刻なエラーに関するメッセージのみ。</li> <li>• 200（高）：深刻なエラーを含めたすべてのエラーに関するメッセージ。</li> <li>• 300（診断）：すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。</li> <li>• 400（重要）：すべてのエラーに関するメッセージとすべての警告および詳細情報。</li> <li>• 500（通常）：すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ（既定値）。</li> <li>• 600（低）：すべてのメッセージ。</li> </ul>



AMPPL	<p>AM-PPL 技術（Antimalware Protected Process Light）を使用した Kaspersky Endpoint Security プロセスの保護を有効にするかどうか。AM-PPL 技術について詳しくは、<a href="#">Microsoft の Web サイトの情報</a>を参照してください。</p> <p>AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。</p> <p>次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を有効にする</li> <li>• 0：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を無効にする</li> </ul>
RESTAPI	<p>REST API を使用した製品の管理。REST API を使用して製品を管理するには、ユーザー名（RESTAPI_User パラメータ）を指定する必要があります。</p> <p>次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1 – REST API による管理を許可する</li> <li>• 0 – REST API による管理をブロックする（既定値）</li> </ul> <p>REST API を使用して製品を管理するには、管理システムを使用した管理を許可する必要があります。許可するには、AdminKitConnector=1 パラメータを設定します。REST API を使用して製品を管理する場合、カスペルスキーの管理システムを使用して製品を管理することはできません。</p>
RESTAPI_User	<p>REST API による製品の管理に使用する Windows ドメインアカウントのユーザー名。REST API による製品の管理はこのユーザーのみ実行できます。ユーザー名は、&lt;ドメイン&gt;\&lt;ユーザー名&gt; の形式で入力します（例：RESTAPI_User=COMPANY\Administrator）。REST API を利用するユーザーは1人しか選択できません。</p> <p>REST API を使用して製品を管理するには、ユーザー名の追加は必須です。</p>
RESTAPI_Port	<p>REST API による製品の管理に使用するポート。既定ではポート 6782 が使用されます。</p>
RESTAPI_Certificate	<p>リクエストを識別するための証明書（例：RESTAPI_Certificate=C:\cert.pem）。REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。</p>
ADMINKITCONNECTOR	<p>管理システムを使用した製品管理。管理システムには、Kaspersky Security Center などが含まれます。カスペルスキーの管理システムに加えて、サードパーティ製ソリューションを使用することもできます。Kaspersky Endpoint Security はそのための API を提供します。</p> <p>次の値を設定できます：</p> <ul style="list-style-type: none"> <li>• 1 – 管理システムを利用した製品管理を許可します（既定値）。</li> <li>• 0 – ローカルインターフェイスを利用した製品管理のみを許可します。</li> </ul>

例：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pALLOWREBOOT=1  
  
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1  
KSN=1 KLLLOGIN=Admin KLPASSWD=Password  
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn  
  
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

[setup.ini ファイル](#)でアクティベーションコードを指定していない限り、Kaspersky Endpoint Security のインストール後、試用版ライセンスでアクティベーションが行われます。通常、試用版ライセンスには短い有効期間が設定されています。試用版ライセンスの有効期間が終了すると、すべての Kaspersky Endpoint Security 機能が無効になります。製品を引き続き使用するには、[アクティベーションウィザード](#)または[専用のコマンド](#)を使用して、製品版ライセンスで本製品をアクティベートする必要があります。

サイレントモードで製品をインストールまたはアップグレードする場合、以下のファイルの使用がサポートされています：

- [setup.ini](#)：製品のインストールの全般設定
- [install.cfg](#)：Kaspersky Endpoint Security の動作に関する設定
- setup.reg：レジストリキー

[setup.ini ファイル](#)で SetupReg パラメータの値として setup.reg が設定されている場合にのみ、setup.reg ファイルに含まれるレジストリキーがレジストリに書き込まれます。setup.reg ファイルはカスペルスキーのエキスパートが生成しています。このファイルの内容は変更しないでください。

setup.ini ファイル、install.cfg ファイル、setup.reg ファイルの設定を適用するには、これらのファイルを Kaspersky Endpoint Security の配布パッケージと同じフォルダーに配置します。setup.reg ファイルを別のフォルダーに配置することもできます。この場合、アプリケーションのインストールコマンドで次のようにパスを指定する必要があります：SETUPREG=<setup.reg ファイルのパス>

## 製品のアクティベーション

コマンドラインから製品をアクティベートするには：

コマンドラインに以下のように入力します：

```
avp.com license /add <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> [/login=<ユーザー名> /password=<パスワード>]
```

[パスワードによる保護が有効](#)な場合、ユーザーアカウントの認証情報（「/login=<ユーザー名> /password=<パスワード>」）を入力する必要があります。

## 製品の削除

Kaspersky Endpoint Security は次のいずれかのモードでコマンドラインを使用してアンインストールできます。

- セットアップウィザードを使用したインタラクティブモード。
- サイレントモード：サイレントモードでのアンインストールの開始後は、アンインストールプロセスでユーザーが操作を行う必要はありません。サイレントモードで本製品をアンインストールするには、「/s」と「/qn」パラメータを使用します。

サイレントモードで製品をアンインストールするには：

1. 管理者としてコマンドラインインタプリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

- アンインストール操作がパスワードによって保護されていない場合：

```
setup_kes.exe /s /x
```

または

```
msiexec.exe /x <GUID> /qn
```

<GUID> は、アプリケーションの固有の識別子です。次のコマンドを使用して、アプリケーションの GUID を確認できます：

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
```

- アンインストール操作がパスワードによって保護されている場合：

```
setup_kes.exe /pKLLLOGIN=<ユーザー名> /pKLPASSWD=<パスワード> /s /x
```

または

```
msiexec.exe /x <GUID> KLLLOGIN=<ユーザー名> KLPASSWD=<パスワード> /qn
```

例：

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

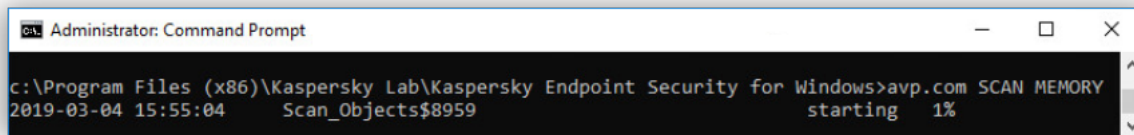
## AVP コマンド

コマンドラインを使用して *Kaspersky Endpoint Security* を管理するには：

1. 管理者としてコマンドラインインタプリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. コマンドを実行するには、次の形式でコマンドとオプションを入力します：

```
avp.com <コマンド> [オプション]
```

Kaspersky Endpoint Security で、次の図のようにコマンドが実行されます。



コマンドラインを使用しての製品の管理

## SCAN : スキャン

スキャンタスクを実行します。

### コマンド構文

SCAN [<スキャン範囲>] [<脅威の検知時の処理>] [<ファイル種別>] [<信頼するオブジェクト (スキャンからの除外対象) >] [/R[A]:<ログファイルの名前>] [<スキャン技術>] [/C:<スキャンタスクの設定ファイル>]

スキャン範囲	
<スキャン対象のファイル>	<p>スペース区切りのファイルとフォルダーのリスト。指定するパスが長くスペースを含むときは引用符 (" ) で囲む必要があります。スペースを含まない短いパス (MS-DOS 短縮形式) は引用符で囲む必要はありません。例：</p> <ul style="list-style-type: none"> <li>• "C:\Program Files (x86)\Example Folder" – 長いパス</li> <li>• C:\PROGRA~2\EXAMPL~1 – スペースを含まない短いパス</li> </ul>
/ALL	<p>完全スキャンタスクを実行します。Kaspersky Endpoint Security が、次のオブジェクトをスキャンします：</p> <ul style="list-style-type: none"> <li>• カーネルメモリ</li> <li>• オペレーティングシステムの起動時に読み込まれるオブジェクト</li> <li>• ディスクブートセクター</li> <li>• システムバックアップ</li> <li>• すべてのハードディスクドライブとリムーバブルドライブ</li> </ul>
/MEMORY	カーネルメモリをスキャンします
/STARTUP	オペレーティングシステムの起動時に読み込まれるオブジェクトをスキャンします
/MAIL	Outlook のメールボックスをスキャンします
/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。
/NETDRIVES	ネットワークドライブをスキャンします。

/QUARANTINE	Kaspersky Endpoint Security のバックアップ保管領域のファイルをスキャンします。
/@:<ファイルとフォルダーのリストを記載したファイルの名前 (拡張子は 1st) >	<p>リストに含まれるファイルとフォルダーをスキャンします。リストに複数のファイルを含める場合は、1行に1つずつ入力して指定するようにします。指定するパスが長くスペースを含むときは引用符 (") で囲む必要があります。スペースを含まない短いパス (MS-DOS 短縮形式) は引用符で囲む必要はありません。例：</p> <ul style="list-style-type: none"> <li>• "C:\Program Files (x86)\Example Folder" – 長いパス</li> <li>• C:\PROGRA~2\EXAMPL~1 – スペースを含まない短いパス</li> </ul>

脅威の検知時の処理	
/i0	通知する：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
/i1	駆除する。駆除できない場合はブロックする：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除ができない場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
/i2	<p>駆除する。駆除できない場合は削除する：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。</p> <p>既定では、この処理が選択されています。</p>
/i3	検知した感染したファイルを駆除します。駆除に失敗した場合、感染したファイルは削除されません。また、複合ファイル (アーカイブなど) の一部に感染したファイルが含まれ、感染したファイルの駆除や削除を実行できない場合、複合ファイル自体を削除します。
/i4	感染したファイルを削除します。また、複合ファイル (アーカイブなど) の一部に感染したファイルが含まれ、感染したファイルを削除できない場合、複合ファイル自体を削除します。
/i8	脅威が検知されたら即座にユーザーに対応を行うように通知します。
/i9	スキャンの完了後に、ユーザーに対応を行うように通知します。

ファイル種別	
/fe	拡張子でファイルをスキャン：この設定を有効にした場合、Kaspersky Endpoint Security は <u>感染する可能性のあるファイルのみ</u> をスキャンします。ファイル形式はファイルの拡張子に基づいて識別されます。
/fi	ファイル形式でファイルをスキャン：この設定を有効にした場合、Kaspersky Endpoint Security は <u>感染する可能性のあるファイルのみ</u> をスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式 (txt、doc、exe など) が識別されます。また、特定の拡張子を持つファイルも検索します。
/fa	<p>すべてのファイルをスキャン：この設定が有効な場合、すべてのファイル (すべての形式と拡張子) が例外なくチェックされます。</p> <p>これは既定の設定です。</p>

信頼するオブジェクト	
-e:a	RAR、ARJ、ZIP、CAB、LHA、JAR、ICE アーカイブはスキャンの対象から除外します。
-e:b	メールデータベース、受信メール、送信メールをスキャンの対象から除外します。
-e:<ファイルのマスク>	ファイルマスクと一致するファイルがスキャンの対象から除外されます。例： <ul style="list-style-type: none"> <li>「*.exe」というマスクには、拡張子が「exe」のファイルへのすべてのパスが含まれます。</li> <li>「example*」というマスクには、名前が「example」のファイルへのすべてのパスが含まれます。</li> </ul>
-e:<秒>	指定した上限時間（秒単位）よりもスキャンに時間がかかるファイルは、スキャンの対象から除外されます。
-es:<MB>	指定したファイルサイズの上限（MB 単位）よりサイズが大きいファイルは、スキャンの対象から除外されます。

ログファイルへのイベント保存方式	
/R:<ログファイルの名前>	緊急イベントのみをログファイルに保存します。
/RA:<ログファイルの名前>	すべてのイベントをログファイルに保存します。

スキャン技術	
/iChecker=on off	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iCheckerには制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。
/iSwift=on off	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

詳細設定	
/C:<スキャンタスクの設定ファイル>	スキャンタスクの設定を指定したファイル。ファイルは手動で作成して TXT 形式で保存する必要があります。ファイルでは次の内容を指定できます： [<スキャン範囲>] [<脅威の検知時の処理>] [<ファイル種別>] [<信頼するオブジェクト（スキャンからの除外対象）>] [/R[A]:<ログファイルの名前>][<スキャン技術>]

例：

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```



## UPDATE : 定義データベースとソフトウェアモジュールのアップデート

アップデートタスクを実行します。

### コマンド構文

```
UPDATE [local] ["<アップデート元>"] [/R[A]:<レポートファイル>] [/C:<アップデートタスクの設定ファイル >]
```

アップデートタスクの設定	
local	<p>アプリケーションがインストールされた後に自動で作成されたアップデートタスクの開始です。Kaspersky Security Center のコンソール内またはローカルのアプリケーションインターフェイス内でアップデートタスクの設定を変更することができます。設定されない場合、Kaspersky Endpoint Security はアップデートタスクを既定の設定またはコマンド内で指定された設定で開始します。アップデートタスクの設定は次のように指定できます：</p> <ul style="list-style-type: none"><li>• UPDATE : 既定の設定でアップデートタスクを開始します：アップデート元はカスペルスキーのアップデートサーバーで、アカウントは「System」、その他既定の設定。</li><li>• UPDATE local : インストール後に自動で作成されたアップデートタスクを開始します（事前定義されたタスク）。</li><li>• UPDATE &lt;アップデート設定&gt; : 手動で定義された設定でアップデートタスクを開始します（以下を参照）。</li></ul>

アップデート元	
"<アップデート元>"	<p>HTTP サーバーまたは FTP サーバーのアドレス、あるいはアップデートパッケージの保存された共有フォルダーのアドレス。アップデート元は1つだけ指定できます。アップデート元が指定されていない場合は、Kaspersky Endpoint Security は既定のアップデート元であるカスペルスキーのアップデートサーバーを使用します。</p>

ログファイルへのイベント保存方式	
/R:<ログファイルの名前>	緊急イベントのみをログファイルに保存します。
/RA:<ログファイルの名前>	すべてのイベントをログファイルに保存します。

詳細設定	
/C:<アップデートタスクの設定ファイル>	アップデートタスクの設定を指定したファイル。ファイルは手動で作成して TXT 形式で保存する必要があります。ファイルでは次の内容を指定できます： ["<アップデート元>"] [/R[A]:<ログファイルの名前>]。



例：

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

## ROLLBACK：前回のアップデータのロールバック

定義データベースを前のバージョンにロールバックします。これにより、必要に応じて、定義データベースとソフトウェアモジュールを前のバージョンにロールバックすることができます。この機能は、たとえば新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。

### コマンド構文

```
ROLLBACK [/R[A]:<ログファイルの名前>]
```

ログファイルへのイベント保存方式	
/R:<ログファイルの名前>	緊急イベントのみをログファイルに保存します。
/RA:<ログファイルの名前>	すべてのイベントをログファイルに保存します。

例：

```
avp.com ROLLBACK /RA:rollback.txt
```

## TRACES：トレース

システムトレースを有効化または無効化します。[トレースファイル](#)は、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。認証エージェントのトレースファイルを除いて、トレースファイルはフォルダー「%ProgramData%\Kaspersky Lab\KES\Traces」に保存されます。既定では、トレースは無効です。

### コマンド構文

```
TRACES on|off [<トレースレベル>] [<詳細設定>]
```

トレースレベル	
<トレースレベル>	トレース記録の詳細度。次の値を設定できます： <ul style="list-style-type: none"><li>100（緊急）：深刻なエラーに関するメッセージのみ。</li><li>200（高）：深刻なエラーを含めたすべてのエラーに関するメッセージ。</li><li>300（診断）：すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。</li><li>400（重要）：すべてのエラーに関するメッセージとすべての警告および詳細情報。</li></ul>

- 500（通常）：すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ（既定値）。
- 600（低）：すべてのメッセージ。

詳細設定	
all	以下の「dbg」、「file」、「mem」パラメータを使用するように指定してコマンドを実行します。
dbg	「OutputDebugString」機能を使用して、トレースファイルを保存します。 「OutputDebugString」は、画面上に表示する文字列を製品のデバッグプログラムに送信します。この機能について詳しくは、 <a href="#">MSDNページ</a> を参照してください。
file	トレースファイルを1つ保存します（容量の上限なし）。
rot	ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。
mem	トレースの記録をダンプファイルに保存します。

例：

- avp.com TRACES on 500
- avp.com TRACES on 500 dbg
- avp.com TRACES off
- avp.com TRACES on 500 dbg mem
- avp.com TRACES off file

## START：指定した機能の起動

機能を指定して起動します（例：定義データベースのアップデート、保護機能の有効化）。

### コマンド構文

```
START <コマンド指定用の機能名> [/R[A]:<ログファイルの名前>]
```

コマンド指定用の機能名	
<コマンド指定	コマンド指定用の機能名。コマンド指定用の機能名で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能な <a href="#">コマンド指定用の機能名</a> のリストは、「HELP START」コマンドを実行して確認できます。

用の機能名>

### ログファイルへのイベント保存方式

/R:<ログファイルの名前>	緊急イベントのみをログファイルに保存します。
/RA:<ログファイルの名前>	すべてのイベントをログファイルに保存します。

例：

avp.com START Scan\_Objects

## STOP：指定した機能の停止

実行中の機能を指定して停止させます（例：スキャンの停止、リムーバブルドライブスキャンの停止、保護機能の無効化）。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーは[**保護機能の停止**] および [**管理コンポーネントの停止**] 権限が必要です。

### コマンド構文

STOP <コマンド指定用の機能名> /login=<ユーザー名> /password=<パスワード>

### コマンド指定用の機能名

<コマンド指定用の機能名> コマンド指定用の機能名。コマンド指定用の機能名で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能な[コマンド指定用の機能名](#)のリストは、「HELP STOP」コマンドを実行して確認できます。

### 認証

/login=<ユーザー名> /password=<パスワード> 必要な[パスワード保護](#)された権限を持つユーザーアカウントの認証情報。

## STATUS：指定した機能のステータス

[指定した機能](#)のステータス情報を表示します（「running」や「completed」など）。利用可能なコマンド指定用の機能名のリストは、「HELP STATUS」コマンドを実行して確認できます。

Kaspersky Endpoint Security は、指定したサービスのステータスも表示できます。カスペルスキーのテクニカルサポートに問い合わせを行って調査が必要になったときに、コマンド指定用のサービス名を使用してサービスのステータス情報を取得する場合があります。

## コマンド構文

STATUS [<コマンド指定用の機能名>]

## STATISTICS : 指定した機能の動作の統計情報

[指定した機能](#)の統計情報を表示します（例：スキャンの所要時間や検知した脅威の数）。利用可能なコマンド指定用の機能名のリストは、「HELP STATISTICS」コマンドを実行して確認できます。

## コマンド構文

STATISTICS <コマンド指定用の機能名>

## RESTORE : バックアップからのファイルの復元

バックアップ保管領域から元のフォルダーにファイルを復元できます。復元先のフォルダーに同じ名前のファイルが既に存在する場合は、そのファイル名の末尾に「-copy」という文字が追加されます。バックアップ保管領域から復元されるファイルの名前は元のまま変更されません。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**バックアップから復元**」操作を実行する権限が付与されている必要があります。

バックアップ保管領域には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。バックアップコピーは、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルのバックアップコピーは、フォルダー C:\ProgramData\Kaspersky Lab\KES\QB に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。

## コマンド構文

RESTORE [/REPLACE] <ファイル名> /login=<ユーザー名> /password=<パスワード>

### 詳細設定

/REPLACE	復元先に同じファイル名のファイルがある場合に、これを上書きします。
<ファイル名>	復元するファイルの名前。

### 認証

/login=<ユーザー名> /password=<パスワード>

必要な[パスワード保護](#)された権限を持つユーザーアカウントの認証情報。

例：

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

## EXPORT：本製品の設定のエクスポート

Kaspersky Endpoint Security の設定をファイルにエクスポートします。ファイルはフォルダー「C:\Windows\SysWOW64」に保存されます。

### コマンド構文

```
EXPORT <コマンド指定用の機能名> <ファイル名>
```

<b>コマンド指定用の機能名</b>	
<コマンド指定用の機能名>	コマンド指定用の機能名。コマンド指定用の機能名で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能な <a href="#">コマンド指定用の機能名</a> のリストは、「HELP EXPORT」コマンドを実行して確認できます。
<b>エクスポートするファイル</b>	
<ファイル名>	本製品の設定をエクスポートするファイルの名前。Kaspersky Endpoint Security の設定を DAT または CFG 設定ファイル、TXT テキストファイル、または XML ドキュメントにエクスポートできます。

例：

- avp.com EXPORT ids ids\_config.dat
- avp.com EXPORT fm fm\_config.txt

## IMPORT：本製品の設定のインポート

「EXPORT」コマンドを使用して Kaspersky Endpoint Security の設定をエクスポートしたファイルから、設定をインポートできます。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**本製品の設定**」操作を実行する権限が付与されている必要があります。

## コマンド構文

```
IMPORT <ファイル名> /login=<ユーザー名> /password=<パスワード>
```

### インポートするファイル

<ファイル名>	本製品の設定をインポートするファイルの名前。Kaspersky Endpoint Security の設定を DAT または CFG 設定ファイル、TXT テキストファイル、または XML ドキュメントからインポートできます。
---------	---

### 認証

/login=<ユーザー名> /password=<パスワード>	必要な <a href="#">パスワード保護</a> された権限を持つユーザーアカウントの認証情報。
----------------------------------	---

例：

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

## ADDKEY：ライセンス情報ファイルの適用

ライセンス情報ファイルを適用して Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。

## コマンド構文

```
ADDKEY <ファイル名> /login=<ユーザー名> /password=<パスワード>
```

### ライセンス情報ファイル

<ファイル名>	ライセンス情報ファイルの名前。
---------	-----------------

### 認証

/login=<ユーザー名> /password=<パスワード>	ユーザーアカウントの認証情報。これらの認証情報は、 <a href="#">パスワードによる保護</a> が有効になっている場合にのみ入力する必要があります。
-------------------------------------	---

例：

```
avp.com ADDKEY file.key
```

## LICENSE：ライセンス管理

Kaspersky Endpoint Security のライセンスに対する操作を実行します。

このコマンドを実行してライセンスを削除するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**ライセンスの削除**」操作を実行する権限が付与されている必要があります。

## コマンド構文

```
LICENSE <実行する操作> [/login=<ユーザー名> /password=<パスワード>]
```

実行する操作	
/ADD <ファイル名>	ライセンス情報ファイルを適用して Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。
/ADD <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 Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。
/REFRESH <ファイル名>	ライセンスの更新で使用するライセンス情報ファイルを指定します。その結果、予備のライセンスが追加されます。このライセンスは、前のライセンスの有効期間が終了した時点から、現在のライセンスとして使用されるようになります。このコマンドを実行しても、現在のライセンスを追加することはできません。
/REFRESH <アクティベーションコード>	ライセンスの更新で使用するアクティベーションコードを指定します。その結果、予備のライセンスが追加されます。このライセンスは、前のライセンスの有効期間が終了した時点から、現在のライセンスとして使用されるようになります。このコマンドを実行しても、現在のライセンスを追加することはできません。
/DEL /login=<ユーザー名> /password=<パスワード>	ライセンスを削除します。予備のライセンスも削除されます。

認証	
/login=<ユーザー名> /password=<パスワード>	必要な <a href="#">パスワード保護</a> された権限を持つユーザーアカウントの認証情報。

例：

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAAA-BBBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

## RENEW：ライセンスの更新または購入

カスペルスキーの製品ページが開きます（日本語版ライセンスを更新または購入するときは、販売代理店に直接ご連絡ください）。



## PBATESTRESET : 暗号化前のディスクチェックの結果のリセット

ディスク全体の暗号化 (FDE) の互換性チェックの結果をリセットします。リセットの対象には、Kaspersky Disk Encryption と BitLocker ドライブ暗号化技術の両方が含まれます。

ディスク全体の暗号化を実行する前に、コンピューターを暗号化できるかどうかのチェックが実行されます。コンピューターが暗号化をサポートしていない場合は、互換性がないという情報が、Kaspersky Endpoint Security により記録されます。その後、暗号化を再び試行した場合は、互換性に関するチェックは実行されず、暗号化を実行できないという警告が表示されます。前回の互換性チェック後に、コンピューターのハードウェア構成が変更された場合、記録されている前回の互換性チェックの結果をリセットし、システムハードディスクと Kaspersky Disk Encryption または BitLocker 暗号化技術との互換性を再チェックする必要があります。

## EXIT : 本製品の終了

Kaspersky Endpoint Security を終了します。本製品の動作が終了し、コンピューターのメモリ領域が解放されます。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**本製品の終了**」操作を実行する権限が付与されている必要があります。

### コマンド構文

```
EXIT /login=<ユーザー名> /password=<パスワード>
```

## EXITPOLICY : ポリシーの無効化

Kaspersky Security Center で設定したポリシーをコンピューター上で無効にします。ポリシーでロックされている設定 (🔒 状態) も含めて、Kaspersky Endpoint Security のすべての設定を編集できるようになります。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**Kaspersky Security Center ポリシーを無効にする**」操作を実行する権限が付与されている必要があります。

### コマンド構文

```
EXITPOLICY /login=<ユーザー名> /password=<パスワード>
```

## STARTPOLICY : ポリシーの有効化

Kaspersky Security Center で設定したポリシーをコンピューター上で有効にします。ポリシーで指定した設定が本製品に適用されます。

## DISABLE : 保護の無効化

Kaspersky Endpoint Security のライセンスの有効期限が切れている場合に、ファイル脅威対策を無効化します。本製品がアクティベーションされていない場合、あるいは有効なライセンスが適用されている場合には、このコマンドは実行できません。

## SPYWARE : スパイウェアの検知の切り替え

スパイウェアの検知を有効または無効にします。既定では、スパイウェアの検知は有効になっています。

### コマンド構文

```
SPYWARE on|off
```

## KSN : グローバル / プライベート KSN の切り替え

ファイルまたは Web サイトの評価の決定に使用する Kaspersky Security Network の選択 Kaspersky Endpoint Security では、次の種別の KSN インフラストラクチャの使用をサポートしています：

- ほとんどのカスペルスキー製品で使用されるのがグローバル KSN です。KSN の参加者は、Kaspersky Security Network から情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、Kaspersky Security Network の評価データベースと統計情報のデータベースに追加されます。
- プライベート KSN は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターから KSN にデータを送信せずに Kaspersky Security Network の評価データベースや統計情報のデータにアクセスできるようにするソリューションです。プライベート KSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：
  - コンピューターがインターネットに接続されていない。
  - 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

### コマンド構文

```
KSN /global | /private <ファイル名>
```

<b>プライベート KSN 設定ファイル</b>	
<ファイル名>	KSN プロキシサーバー設定を含む設定ファイル名です。このファイルの拡張子は PKCS7 または PEM です。
例：	

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

## KESCLI コマンド

KESCLI コマンドを使用すると、OPSWAT コンポーネントを使用してコンピューターの保護の状態に関する情報を受け取ったり、ウイルススキャンや定義データベースのアップデートのような標準的なタスクを実行することができます。

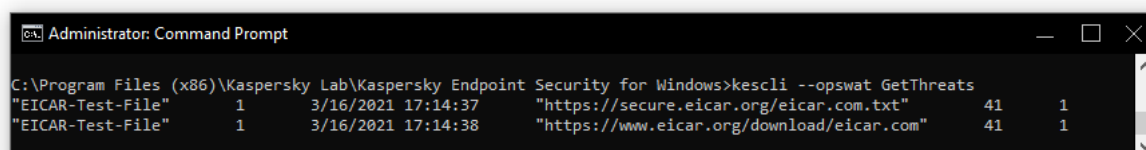
`--help` コマンドまたは省略された `-h` コマンドを使用して KESCLI コマンドのリストを表示できます。

コマンドラインを使用して *Kaspersky Endpoint Security* を管理するには：

1. 管理者としてコマンドラインインタープリタ (cmd.exe) を実行します。
2. *Kaspersky Endpoint Security* の実行ファイルがあるフォルダーに移動します。
3. コマンドを実行するには、次の形式でコマンドとオプションを入力します：

```
kescli <コマンド> [オプション]
```

*Kaspersky Endpoint Security* で、次の図のようにコマンドが実行されます。



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

コマンドラインを使用しての製品の管理

## Scan : スキャン

スキャンタスクを実行します。

### コマンド構文

```
--opswat Scan <スキャン範囲> <脅威の検知時の処理>
```

完全スキャンタスクの完了状況については、[GetScanState](#) コマンドを使用して確認できます。また、前回のスキャン完了日時については、[GetLastScanTime](#) コマンドを使用して表示できます。

スキャン範囲

<スキャン対象のファイル>

「;」で区切られたファイルとフォルダーのリスト。例：C:\Program Files (x86)\Example Folder

脅威の検知時の処理	
0	通知する：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
1	駆除する。駆除できない場合は削除する：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。 既定では、この処理が選択されています。

例：

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

## GetScanState：スキャン完了のステータス

完全スキャンタスクの完了状態についての情報を受け取ります：

- 1 – スキャンが実行中です。
- 0 – スキャンは実行されていません。

### コマンド構文

```
--opswat GetScanState
```

例：

```
kescli --opswat GetScanState
```

## GetLastScanTime：スキャン完了時刻の判断

完全スキャンタスクの完了日時に関する情報を受け取ります。

### コマンド構文

```
--opswat GetLastScanTime
```

例：

```
kescli --opswat GetLastScanTime
```

## GetThreats : 検知した脅威に関するデータの取得

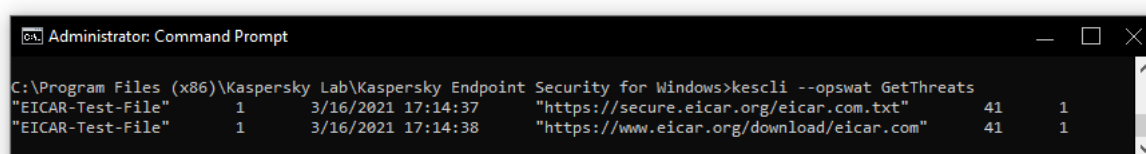
検知した脅威のリストを受け取ります（脅威レポート）。このレポートには、レポート作成時より前の30日間で検知された脅威およびウイルスに関する情報が含まれます。

### コマンド構文

```
--opswat GetThreats
```

コマンドを実行すると、Kaspersky Endpoint Security は次の形式で応答を送信します：

<検知されたオブジェクト名> <オブジェクトの種別> <検知日時> <ファイルのパス> <脅威の検知時の処理> <脅威の危険度>



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

コマンドラインを使用しての製品の管理

オブジェクト種別	
0	不明（Unknown）。
1	ウイルス（Virware）。
2	トロイの木馬（Trojware）。
3	悪意のあるプログラム（Malware）。
4	広告プログラム（Adware）。
5	オートダイヤラープログラム（Pornware）。
6	ユーザーのコンピューターまたはデータに損害を与える目的で犯罪者に悪用される可能性のあるアプリケーション（Riskware）。
7	悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト（Packed）。
20	不明なオブジェクト（Xfiles）。
21	既知のアプリケーション（Software）。
22	隠蔽されたファイル（Hidden）。
23	注意の必要なアプリケーション（Pupware）。
24	異常なふるまい（Anomaly）。
30	決定されていない（Undetect）。
40	広告バナー（Banner）。
50	ネットワーク攻撃（Attack）。
51	レジストリへのアクセス（Registry）。

52	疑わしい動作 (Suspicion)。
60	脆弱性 (Vulnerability)。
70	フィッシング。
80	望ましくないメール添付 (Attachment)。
90	Kaspersky Security Network により検知されたマルウェア (Urgent)。
100	不明なリンク (Suspicious URL)。
110	その他のマルウェア (Behavioral)。

脅威の検知時の処理	
0	不明 (unknown)。
1	脅威が修復されました (ok)。
2	オブジェクトは感染しており、駆除されていません (infected)。
5	オブジェクトはアーカイブ内にあり、駆除されていません (archive)。
9	オブジェクトは駆除されました (disinfected)。
10	オブジェクトは駆除されていません (not disinfected)。
11	オブジェクトは削除されました (deleted)。
13	オブジェクトのバックアップコピーが作成されました (backupped)。
15	オブジェクトはバックアップに移動されました (quarantined)。
23	オブジェクトはコンピューターの再起動時に削除されました (delete on reboot)。
25	オブジェクトはコンピューターの再起動時に駆除されました (disinfect on reboot)。
29	オブジェクトはユーザーによりバックアップに移動されました (added by user)。
30	オブジェクトは除外リストに追加されました (added to exclude)。
31	オブジェクトはコンピューターの再起動時にバックアップに移動されました (quarantine on reboot)。
36	誤検知 (false alarm)。
38	プロセスが中断されました (terminated)。
40	オブジェクトは検出されませんでした (not found)。
41	脅威を解決できませんでした (untreatable)。
42	オブジェクトは復元されました (rolled back)。
43	オブジェクトは脅威の活動の結果作成されました (produced by threat)。
44	オブジェクトはコンピューターの再起動時に復元されました (roll back on reboot)。
0xffffffff	オブジェクトは処理されませんでした (discarded)。

脅威の危険度	
--------	--

0	不明
1	高
2	スキャン(レベル中)
4	低
8	情報(「低」以下)

## UpdateDefinitions : 定義データベースとソフトウェアモジュールのアップデート

アップデートタスクを実行します。Kaspersky Endpoint Security は既定のアップデート元であるカスペルスキーのアップデートサーバーを使用します。

### コマンド構文

```
--opswat UpdateDefinitions
```

前回のアップデートタスクの完了日時については、[GetDefinitionsetState](#) コマンドを使用して表示できます。

例 :

```
kescli --opswat UpdateDefinitions
```

## GetDefinitionState : アップデート完了時刻の判断

アップデートタスクの完了日時に関する情報を受け取ります。

### コマンド構文

```
--opswat GetDefinitionState
```

例 :

```
kescli --opswat GetDefinitionState
```

## EnableRTP : 保護の有効化

次の Kaspersky Endpoint Security の保護機能を有効にします : ファイル脅威対策、ウェブ脅威対策、メール脅威対策、ネットワーク脅威対策、ホスト侵入防止。

### コマンド構文

```
--opswat EnableRTP
```



ファイル脅威対策の動作状態については、[GetRealTimeProtectionState](#) コマンドを使用して確認できます。

```
例 :
kescli --opswat EnableRTP
```

## GetRealTimeProtectionState : ファイル脅威対策のステータス

ファイル脅威対策の動作状態に関する情報を受け取ります。

- 1 – 機能が有効です。
- 0 – 機能が無効です。

### コマンド構文

```
--opswat GetRealTimeProtectionState
```

```
例 :
kescli --opswat GetRealTimeProtectionState
```

## Version : 本製品のバージョンの識別

Kaspersky Endpoint Security for Windows のバージョンを識別します。

### コマンド構文

```
--Version
```

省略したコマンド「`-v`」を使用することもできます。

```
例 :
kescli -v
```

## Detection and Response management commands

You can use the command line to manage built-in functionality of Detection and Response solutions (for example, Kaspersky Sandbox or Kaspersky Endpoint Detection and Response Optimum). You can manage Detection and Response solutions if management using the Kaspersky Security Center console is not possible. You can view the list of commands for managing the application by executing the `HELP` command. To read about the syntax of a specific command, enter `HELP <command>`.

## SANDBOX : Kaspersky Sandbox の管理

Kaspersky Sandbox コンポーネントを管理するコマンド：

- Kaspersky Sandbox コンポーネントを有効または無効にする  
Kaspersky Sandbox コンポーネントは、Kaspersky Sandbox ソリューションとの連携を有効にします。
- Kaspersky Sandbox コンポーネントを設定する
  - Kaspersky Sandbox サーバーにコンピューターを接続する  
サーバーは配備された Microsoft Windows オペレーティングシステムの仮想イメージを使用してスキャンする必要のあるオブジェクトを実行します。IP アドレス (IPv4 または IPv6)、または完全修飾ドメイン名を入力できます。仮想イメージの配備と Kaspersky Sandbox サーバーの設定について詳しくは、[Kaspersky Sandbox のヘルプ](#) を参照してください。
  - Kaspersky Sandbox サーバーの接続タイムアウトを設定する  
オブジェクトのスキャン要求に対して Kaspersky Sandbox サーバーからの応答を受け取るまでのタイムアウトです。設定したタイムアウト期間が経過すると、Kaspersky Sandbox は要求を次のサーバーに送ります。タイムアウトの値は接続のスピードと安定性によって異なります。既定値は 5 秒です。
  - コンピューターと Kaspersky Sandbox サーバーとの間に信頼済み接続を設定する  
Kaspersky Sandbox サーバーと信頼済み接続を設定するには、TLS 証明書を準備する必要があります。次にその証明書を Kaspersky Sandbox サーバーおよび Kaspersky Endpoint Security ポリシーに追加します。証明書の準備およびサーバーへの証明書の追加について詳しくは、[Kaspersky Sandbox のヘルプ](#) を参照してください。
- コンポーネントの現在の設定を表示します。

#### コマンド構文

```
stop sandbox [/login=<ユーザー名> /password=<パスワード>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<サーバーアドレス>:<ポート>] [--timeout=
<Kaspersky Sandbox サーバーの接続タイムアウト (ms)>] [--pinned-certificate=<TLS 証明書の
パス>][/login=<ユーザー名> /password=<パスワード>]
sandbox /show
```

実行する操作	
stop	Kaspersky Sandbox コンポーネントを有効にします。
start	Kaspersky Sandbox コンポーネントを無効にします。
set	Kaspersky Sandbox コンポーネントを設定します。次の設定を変更できます： <ul style="list-style-type: none"><li>• 信頼済み接続を使用する (--tls)</li><li>• TLS 証明書を追加する (--pinned-certificate)</li><li>• Kaspersky Sandbox サーバーの接続タイムアウトを設定する (--timeout)</li><li>• Kaspersky Sandbox サーバーを追加する (--servers)</li></ul>
show	コンポーネントの現在の設定を表示します。次の応答が表示されます： sandbox.timeout=<Kaspersky Sandbox サーバーの接続タイムアウト (ms)> sandbox.tls=<信頼済み接続の状態> sandbox.servers=<Kaspersky Sandbox サーバーのリスト>

<b>認証</b>	
/login=<ユーザー名> /password=<パスワード>	必要な <a href="#">パスワード保護</a> された権限を持つユーザーアカウントの認証情報。

例：

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

## PREVENTION：実行防止の管理

実行防止を無効にするか、実行防止ルールを含む現在のコンポーネントの設定を表示します。

### コマンド構文

```
prevention disable
prevention /show
```

コマンド「`prevention /show`」を実行する値、次の応答が表示されます：

`prevention.enable=true|false`

`prevention.mode=audit|prevent`

`prevention.rules`

`id: <ルール ID>`

`target: script|process|document`

`md5: <ファイルの MD5 ハッシュ>`

`sha256: <ファイルの SHA256 ハッシュ>`

`pattern: <オブジェクトのパス>`

`case-sensitive: true|false`

コマンド戻り値：

- -1：端末にインストールされているバージョンの Kaspersky Endpoint Agent ではコマンドがサポートされていません。
- 0：コマンドが正常に実行されました。
- 1：必要な引数がコマンドに渡されていません。
- 2：一般的なエラーが発生しました。
- 4：構文エラーがあります。
- 9：操作に誤りがあります（すでに機能が無効にされている状態でその機能を無効にしようとするなど）。

## ISOLATION : ネットワーク分離の管理

コンピューターのネットワーク分離を無効にしたり、設定済みのネットワーク除外プロファイルやネットワークプロファイル内で設定されたルールのリストを含む現在のコンポーネントの設定を表示します。

### コマンド構文 :

```
isolation /OFF /login=<ユーザー名> /password=<パスワード>  
isolation /STAT
```

Show コマンドを実行すると、次の応答を受け取ります : `isolation.enable=true|false`

### コマンド戻り値 :

- -1 : 端末にインストールされているバージョンの Kaspersky Endpoint Agent ではコマンドがサポートされていません。
- 0 : コマンドが正常に実行されました。
- 1 : 必要な引数がコマンドに渡されていません。
- 2 : 一般的なエラーが発生しました。
- 4 : 構文エラーがあります。
- 9 : 操作に誤りがあります (すでに機能が無効にされている状態でその機能を無効にしようとするなど)。

## RESTORE : 隔離からのファイルの復元

コンピューター上の特別なフォルダーに隔離からのファイルを復元します。その後、ファイルを手動で移動先のフォルダーに移動する必要があります。隔離とは、ウイルスに感染したファイルや駆除できないファイルを移動する特別なローカルの保管領域です。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は Kaspersky Sandbox および Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する際にのみこの隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、[Kaspersky Sandbox](#) および [Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

このコマンドを実行するには、[パスワードによる保護を有効にする](#)必要があります。ユーザーには「**バックアップから復元**」操作を実行する権限が付与されている必要があります。

オブジェクトはシステムアカウント (SYSTEM) で隔離されます。

### コマンド構文

```
RESTORE [/REPLACE] <ファイル名> /login=<ユーザー名> /password=<パスワード>
```

### 詳細設定

/REPLACE	復元先に同じファイル名のファイルがある場合に、これを上書きします。
<ファイル名>	復元するファイルの名前。

<b>認証</b>	
/login=<ユーザー名> /password=<パスワード>	必要な <a href="#">パスワード保護</a> された権限を持つユーザーアカウントの認証情報。

例：

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

コマンド戻り値：

- -1：端末にインストールされているバージョンの Kaspersky Endpoint Agent ではコマンドがサポートされていません。
- 0：コマンドが正常に実行されました。
- 1：必要な引数がコマンドに渡されていません。
- 2：一般的なエラーが発生しました。
- 4：構文エラーがあります。

## IOCSCAN. Scan for indicators of compromise (IOC)

Run the Scan for indicators of compromise (IOC) task. An *Indicator of Compromise (IOC)* is a set of data about an object or activity that indicates unauthorized access to the computer (compromise of data). For example, many unsuccessful attempts to sign in to the system can constitute an Indicator of Compromise. The *IOC Scan* tasks allows finding Indicators of Compromise on the computer and take threat response measures.

### Command syntax

```
IOCSCAN <full path to the IOC file>[/path=<path to the IOC files folder>
[/process=on|off] [/hint=<full path to executable file of a process|full file path>]
[/registry=on|off] [/dnsentry=on|off] [/arprentry=on|off] [/ports=on|off]
[/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off]
[/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>]
[/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of
exclusions>][/scope=<list of folders to scan>]
```

<b>IOC files</b>	
<full path to the IOC file>	Full path to the IOC file that you want to use for scanning. You can specify multiple IOC files separated by spaces. The full path to the IOC file must be entered without the /path argument. For example, C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<path to the folder with IOC files>	Path to the folder with IOC files that you want to use for scanning. <i>IOC files</i> are files containing the sets of indicators that the application tries to match to count a detection. IOC files must conform to the <a href="#">OpenIOC standard</a> . For example, C:\Users\Admin\Desktop\IOC

Data type for IOC scanning	
/process=on off	<p>Analyze process data when performing the IOC scan (ProcessItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not analyze processes running on the computer when performing the scan. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes process data only if the ProcessItem IOC document is described in the IOC file that is provided for the scan.</p>
/hint=<full path to the executable file of the process full path to the file>	<p>Analyze file data when performing the IOC scan (ProcessItem and FileItem terms).</p> <p>You can select a file in one of the following ways:</p> <ul style="list-style-type: none"> <li>• &lt;full path to the executable file of the process&gt; – ProcessItem;</li> <li>• &lt;full path to the file&gt; – FileItem.</li> </ul>
/registry=on off	<p>Analyze Windows registry data when performing an IOC scan (RegistryItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the Windows registry. If the IOC file contains RegistryItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes the Windows registry only if the RegistryItem IOC document is described in the IOC file that is provided for the scan.</p> <p>For the RegistryItem data type, Kaspersky Endpoint Security scans <a href="#">a set of registry keys</a>.</p>
/dnsentry=on off	<p>Analyze the data about records in the local DNS cache when performing the IOC scan (DnsEntryItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the local DNS cache. If the IOC file contains DnsEntryItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes the local DNS cache only if the DnsEntryItem IOC document is described in the IOC file that is provided for the scan.</p>
/arpentry=on off	<p>Analyze the data about records in the ARP table when performing the IOC scan (ArpEntryItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the ARP table. If the IOC file contains ArpEntryItem IOC document terms, they are ignored (detected as no match).</p>

	<p>If the argument is not specified, Kaspersky Endpoint Security analyzes the ARP table only if the ArpEntryItem IOC document is described in the IOC file that is provided for the scan.</p>
/ports=on off	<p>Analyze data about ports open for listening when performing the IOC scan (PortItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the table of active connections on the device. If the IOC file contains PortItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes the table of active connections only if the PortItem IOC document is described in the IOC file that is provided for the scan.</p>
/services=on off	<p>Analyze data about services installed on the device when performing the IOC scan (ServiceItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the data about services installed on the device. If the IOC file contains ServiceItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes service data only if the ServiceItem IOC document is described in the IOC file that is provided for the scan.</p>
/system=on off	<p>Analyze environment data when performing the IOC scan (SystemInfoItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not analyze environment data. If the IOC file contains SystemInfoItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes environment data only if the SystemInfoItem IOC document is described in the IOC file that is provided for the scan.</p>
/users=on off	<p>Analyze data about users when performing the IOC scan (UserItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not analyze data about users created in the system. If the IOC file contains UserItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes data about users created in the system only if the UserItem IOC document is described in the IOC file that is provided for the scan.</p>
/volumes=on off	<p>Analyze data about volumes when performing the IOC scan (VolumeItem term).</p> <p>If the value of the argument is off, Kaspersky Endpoint Security does not scan the data about volumes on the device. If the IOC file contains VolumeItem IOC document terms, they are ignored (detected as no match).</p>



	<p>If the argument is not specified, Kaspersky Endpoint Security analyzes volume data only if the Volumeltem IOC document is described in the IOC file that is provided for the scan.</p>
<p><code>/eventlog=on off</code></p>	<p>Analyze the data about records in the Windows event log when performing the IOC scan (EventLogItem term).</p> <p>If the value of the argument is <code>off</code>, Kaspersky Endpoint Security does not scan the records in the Windows event log. If the IOC file contains EventLogItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes the Windows event log if the EventLogItem IOC document is described in the IOC file that is provided for the scan.</p>
<p><code>/datetime=&lt;event publication date&gt;</code></p>	<p>Take into consideration the date when the event was published in the Windows event log when determining the IOC scan scope for the corresponding IOC document.</p> <p>When performing an IOC scan, Kaspersky Endpoint Security scans Windows event log entries published during the period from the specified time and date to the moment when the task is run.</p> <p>Kaspersky Endpoint Security allows specifying the event publication date as the value of the argument. The scan is performed only for events published in the Windows event log after the specified date and before the scan is run.</p> <p>If the argument is not specified, Kaspersky Endpoint Security scans events with any publication date. The TaskSettings::BaseSettings::EventLogItem::datetime setting cannot be edited.</p> <p>The setting is used only if the EventLogItem IOC document is described in the IOC file provided for the scan.</p>
<p><code>/channel=&lt;list of channels&gt;</code></p>	<p>List of channel (log) names for which you want to perform an IOC scan.</p> <p>If the argument is specified, Kaspersky Endpoint Security scans records published in the specified logs. The IOC document must have the EventLogItem term described.</p> <p>The name of the log is specified as a string in accordance with the name of the log (channel) specified in the properties of the log (the Full Name parameter) or in the event properties (the &lt;Channel&gt; &lt;/Channel&gt; parameter in the xml schema of the event). You can specify multiple channels separated by spaces.</p> <p>If the argument is not specified, Kaspersky Endpoint Security scans records for channels <code>Application</code>, <code>System</code>, <code>Security</code>.</p>
<p><code>/files=on off</code></p>	<p>Analyze file data when performing the IOC scan (FileItem term).</p> <p>If the value of the argument is <code>off</code>, Kaspersky Endpoint Security does not analyze file data. If the IOC file contains FileItem IOC document terms, they are ignored (detected as no match).</p> <p>If the argument is not specified, Kaspersky Endpoint Security analyzes file data only if the FileItem IOC document is described in the IOC file that is provided for the scan.</p>
<p><code>/drives=&lt;all system critical custom&gt;</code></p>	<p>Set IOC scan scope when analyzing data for the FileItem IOC document.</p> <p>You can set the following values for the scan scope:</p> <ul style="list-style-type: none"> <li>• <code>&lt;all&gt;</code> for all available file scopes.</li> </ul>

	<ul style="list-style-type: none"> <li>• &lt;system&gt; for files in folders where the operating system is installed.</li> <li>• &lt;critical&gt; for temporary files in user and system folders.</li> <li>• &lt;custom&gt; for files in user-defined scopes (/scope=&lt;list of folders to scan&gt;).</li> </ul> <p>If the argument is not specified, the scan is performed for critical areas.</p>
/excludes=<list of exclusions>	Set exclusion scope when analyzing data for the FileItem IOC document. You can specify multiple paths separated by spaces.
/scope=<list of folders to scan>	User-defined IOC scan scope when analyzing data for the FileItem IOC document (/drives=custom). You can specify multiple paths separated by spaces.

Command return values:

- -1 means the command is not supported by the version of Kaspersky Endpoint Agent that is installed on the device.
- 0 means the command was executed successfully.
- 1 means a mandatory argument was not passed to the command.
- 2 means a general error occurred.
- 4 means there was a syntax error.

If the command was executed successfully (return value 0) and indicators of compromise were detected along the way, Kaspersky Endpoint Security outputs the following task result information to the command line:

Uuid	ID of the IOC file from the header of the IOC file structure (the <ioc id=""> tag)
Name	Description of the IOC file from the header of the IOC file structure (the <description></description> tag)
Matched Indicator Items	List of IDs of all matched indicators.
Matched objects	Data for each IOC document for which there was a match.

## MDRLICENSE : MDR のアクティベーション

BLOB 設定ファイルを使用して Managed Detection and Response をアクティベートします。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、[Kaspersky Managed Detection and Response のヘルプ](#) を参照してください。

BLOB ファイルを使用した操作を実行するには、管理者権限が必要です。ポリシーの Managed Detection and Response の設定は編集可能である必要があります (🔑)。

## コマンド構文

MDRLICENSE <実行する操作> [/login=<ユーザー名> /password=<パスワード>]

実行する操作	
/ADD <ファイル名>	Kaspersky Managed Detection and Response との連携用の BLOB 設定ファイルを適用します (P7 形式)。BLOB ファイルは 1 ファイルのみ適用可能です。BLOB ファイルがコンピューター上で適用済みの場合は、ファイルが置き換えられます。
/DEL	BLOB 設定ファイルを削除します。

認証	
/login=<ユーザー名> /password=<パスワード>	必要な <a href="#">パスワード保護</a> された権限を持つユーザーアカウントの認証情報。

例：

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

## エラーコード

コマンドラインを使用して本製品を使用しているときに、エラーが発生することがあります。エラーが発生すると、Kaspersky Endpoint Security は「Error: Cannot start task 'EntAppControl1」のようなエラーメッセージを表示します。さらに、より詳細な状況を確認するためのエラーコード（例：error=8947906D）が表示される場合もあります（詳しくは、下記の表を参照してください）。

エラーコード

エラーコード	説明
09479001	操作中のコンピューターで、Kaspersky Endpoint Security のライセンスが既に使用されています。
0947901D	ライセンスの有効期間が終了しています。定義データベースのアップデートが利用できません。
89479002	ライセンスが見つかりませんでした。
89479003	デジタル署名がないか、破損しています。
89479004	データが破損しています。
89479005	ライセンス情報ファイルが破損しています。
89479006	ライセンスの有効期間が終了しています。
89479007	ライセンス情報ファイルが指定されていません。

89479008	ライセンス情報ファイルを適用できません。
89479009	データを保存できませんでした。
8947900A	データを読み取れませんでした。
8947900B	入出力エラー。
8947900C	定義データベースが見つかりませんでした。
8947900E	ライセンスライブラリが読み込まれていません。
8947900F	定義データベースが破損しているか、手動で更新されています。
89479010	定義データベースが破損しています。
89479011	無効なライセンスを使用して予備のライセンスを追加することはできません。
89479012	システムエラー。
89479013	ライセンスの拒否リストが破損しています。
89479014	ファイルのデジタル署名がカスペルスキーのデジタル署名と一致しません。
89479015	非製品版ライセンスを製品版のライセンスとして使用できません。
89479016	本製品のベータ版を使用するには、ベータ版のライセンスが必要です。
89479017	ライセンス情報ファイルが本製品に対応していません。
89479018	ライセンスがカスペルスキーによってブロックされています。
89479019	本製品は既に試用版ライセンスで使用されています。試用版のライセンスを再度追加することはできません。
8947901A	ライセンス情報ファイルが破損しています。
8947901B	デジタル署名がないか、破損しているか、カスペルスキーのデジタル署名と一致しません。
8947901C	有効期間が終了している非製品版ライセンスは追加できません。
8947901E	ライセンスファイルの作成日または使用日が無効です。システムの日付を確認してください。
8947901F	試用版のライセンスを追加できません。試用版の他のライセンスが既に有効になっています。
89479020	ライセンスの拒否リストが破損しているか、見つかりません。
89479021	アップデートの説明がないか、破損しています。
89479022	ライセンスサービスデータにエラーがあります。
89479023	無効なライセンスを使用して予備のライセンスを追加することはできません。
89479025	アクティベーションサーバーへの要求の送信でエラーが発生しました。考えられる原因は、インターネット接続エラーまたはアクティベーションサーバーでの一時的な問題です。しばらく時間が経過してから（約1~2時間）、アクティベーションコードを使用して本製品のアクティベーションを行ってください。このエラーが再発する場合、インターネットプロバイダーに連絡してください。
89479026	アクティベーションサーバーからの応答でエラーが発生しました。
89479027	応答ステータスを取得できません。
89479028	一時ファイルの保存時にエラーが発生しました。
89479029	無効なアクティベーションコードが入力されたか、システム日付が無効です。コンピュー

	ターのシステム日付を確認してください。
8947902A	ライセンス情報ファイルが本製品に対応していないか、ライセンスの有効期間が終了しています。他の製品のライセンス情報ファイルを使用して Kaspersky Endpoint Security をアクティベートすることはできません。
8947902B	ライセンス情報ファイルの取得に失敗しました。無効なアクティベーションコードが入力されました。
8947902C	アクティベーションサーバーがエラー 400 を返しました。
8947902D	アクティベーションサーバーがエラー 401 を返しました。
8947902E	アクティベーションサーバーがエラー 403 を返しました。
8947902F	アクティベーションサーバーがエラー 404 を返しました。
89479030	アクティベーションサーバーがエラー 405 を返しました。
89479031	アクティベーションサーバーがエラー 406 を返しました。
89479032	プロキシサーバーの認証が必要です。ネットワーク設定を確認してください。
89479033	要求はタイムアウトになりました。
89479034	アクティベーションサーバーがエラー 409 を返しました。
89479035	アクティベーションサーバーがエラー 410 を返しました。
89479036	アクティベーションサーバーがエラー 411 を返しました。
89479037	アクティベーションサーバーがエラー 412 を返しました。
89479038	アクティベーションサーバーがエラー 413 を返しました。
89479039	アクティベーションサーバーがエラー 414 を返しました。
8947903A	アクティベーションサーバーがエラー 415 を返しました。
8947903C	内部サーバーのエラーです。
8947903D	機能がサポートされていません。
8947903E	無効なゲートウェイ応答です。ネットワーク設定を確認してください。
8947903F	サービスを利用できません (HTTP エラー 503) 。
89479040	ゲートウェイ応答はタイムアウトになりました。ネットワーク設定を確認してください。
89479041	このプロトコルはこのサーバーでサポートされていません。
89479043	不明な HTTP エラーです。
89479044	無効なリソース ID です。
89479046	無効な URL です。
89479047	無効な出力先フォルダーです。
89479048	メモリ割り当てエラーです。
89479049	パラメータの ANSI 文字列への変換時にエラーが発生しました (URL、フォルダー、エージェント) 。
8947904A	ワーカースレッドの作成時にエラーが発生しました。
8947904B	ワーカースレッドは既に実行中です。
8947904C	ワーカースレッドが実行されていません。

8947904D	ライセンス情報ファイルがアクティベーションサーバーで見つかりません。
8947904E	ライセンスがブロックされています。
8947904F	アクティベーションサーバーの内部エラーです。
89479050	アクティベーション要求のデータに不足があります。
89479053	ライセンスの有効期間が終了しています。
89479054	コンピューター上のシステム日付が無効です。
89479055	試用版のライセンスの有効期間が終了しています。
89479056	ライセンスの有効期間が終了しています。
89479057	指定したコードでの本製品のアクティベーション数の上限を超えています。
89479058	アクティベーションのプロセスがシステムエラーで終了しました。
89479059	非製品版ライセンスを製品版のライセンスとして使用できません。
8947905C	アクティベーションコードが必要です。
89479062	アクティベーションサーバーに接続できません。
89479064	アクティベーションサーバーが利用できません。インターネット接続を確認して、アクティベーションを再試行してください。
89479065	定義データベースの公開日が、ライセンスの有効期限よりも後の日付です。
89479066	現在のライセンスを有効期間が終了したライセンスで置き換えることはできません。
89479067	現在のライセンスより前に期限が切れる場合は、予備のライセンスを追加できません。
89479068	更新後の定額制サービスのライセンスが見つかりません。
8947906A	無効なアクティベーションコードです（チェックサムが一致しません）。
8947906B	ライセンスがアクティベーション済みです。
8947906C	現在のライセンスと予備のライセンスに対応するライセンス種別が一致しません。
8947906D	ライセンスでサポートされていない機能コンポーネントです。
8947906E	定額制サービスのライセンスを予備のライセンスとして追加することはできません。
89479213	ネットワークのトランスポート層でのエラー。
89479214	アクティベーションサーバーに接続できませんでした。
89479215	無効な URL 形式。
89479216	プロキシサーバーアドレスを変換できません。
89479217	サーバーアドレスを変換できませんでした。インターネット接続の設定を確認してください。
89479218	アクティベーションサーバーまたはプロキシサーバーに接続できませんでした。
89479219	リモートアクセスが拒否されました。
8947921A	応答はタイムアウトになりました。
8947921B	HTTP 要求の送信でエラーが発生しました。
8947921C	SSL 接続エラー。
8947921D	コールバックにより処理が中断されました。



8947921E	転送を試行可能な回数を超過しました。
8947921F	受信者を確認できません。
89479220	アクティベーションサーバーからの応答が空です。
89479221	データの送信でエラーが発生しました。
89479222	データの受信でエラーが発生しました。
89479223	ローカルの SSL 証明書のエラー。
89479224	SSL 暗号化のエラー。
89479225	サーバーの SSL 証明書のエラー。
89479226	ネットワークパケットの無効なコンテンツ。
89479227	ユーザーアクセスが拒否されました。
89479228	無効な SSL 証明書ファイル。
89479229	SSL 接続を確立できませんでした。
8947922A	ネットワークパケットの送受信を行えませんでした。しばらく時間が経過してから再試行してください。
8947922B	失効した証明書が含まれる無効なファイル。
8947922C	SSL 証明書の要求エラー。
89479401	不明なサーバーエラー。
89479402	内部サーバーのエラーです。
89479403	入力したアクティベーションコードで利用できるライセンスがありません。
89479404	現在のライセンスがブロックされました。
89479405	本製品のアクティベーション要求に必要なパラメータがありません。
89479406	無効なユーザー名またはパスワード。
89479407	サーバーに無効なアクティベーションコードが送信されました。
89479408	アクティベーションコードが Kaspersky Endpoint Security に対応していないため無効です。不明な製品のライセンス情報ファイルを使用して Kaspersky Endpoint Security をアクティベートすることはできません。
89479409	要求にアクティベーションコードがありません。
8947940B	ライセンスの有効期間が終了しています（アクティベーションサーバーからのデータの情報）。
8947940C	このコードを使用したアクティベーション数が上限を超えました。
8947940D	無効な形式の要求 ID です。
8947940E	アクティベーションコードが Kaspersky Endpoint Security に対応していないため無効です。その他のカスペルスキー製品のためのアクティベーションコードです。
8947940F	ライセンスを更新できません。
89479410	アクティベーションコードはこの地域で無効です。
89479411	このアクティベーションコードは使用中の言語バージョンには適用できません。
89479412	アクティベーションサーバーへの追加のアクセスが必要です。
89479413	アクティベーションサーバーがエラー 643 を返しました。



89479414	アクティベーションサーバーがエラー 644 を返しました。
89479415	アクティベーションサーバーがエラー 645 を返しました。
89479416	アクティベーションサーバーがエラー 646 を返しました。
89479417	アクティベーションコードの形式がアクティベーションサーバーではサポートされていません。
89479418	無効なアクティベーションコード形式。
89479419	コンピューター上のシステム時刻が無効です。
8947941A	アクティベーションコードはこのバージョンの Kaspersky Endpoint Security に対応していません。
8947941B	定額制サービスの有効期間が終了しました。
8947941C	このライセンスでのアクティベーション数の上限を超過しました。
8947941D	ライセンスのデジタル署名が無効です。
8947941E	追加のデータが必要です。
8947941F	ユーザーデータの検証に失敗しました。
89479420	定額制サービスを利用できません。
89479421	アクティベーションサーバーがメンテナンス中です。
89479501	Kaspersky Endpoint Security の不明なエラー。
89479502	無効なパラメータが転送されました（例：アクティベーションサーバーのアドレスが空のリスト）。
89479503	無効なアクティベーションコード。
89479504	無効なユーザー名。
89479505	無効なユーザーパスワード。
89479506	アクティベーションサーバーからの無効な応答。
89479507	アクティベーション要求が中断されました。
89479509	アクティベーションサーバーが空の転送リストを返しました。

## 補足資料：コマンド指定用の機能名

コマンド指定用の機能名で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。コマンドラインから製品を管理するときに、コマンド指定用の機能名を使用します。「START」、「STOP」、「STATUS」、「STATISTICS」、「EXPORT」、「IMPORT」コマンドで、コマンド指定用の機能名を使用できます。コマンド指定用の機能名を使用することで、本製品の設定（例：STOP DeviceControl）やタスクの実行（例：START Scan\_My\_Computer）を行うことができます。

コマンド指定用に次の機能名を利用できます：

- AdaptiveAnomaliesControl - アダプティブアノマリーコントロール。
- AMSI : AMSI 保護。
- BehaviorDetection : ふるまい検知。

- DeviceControl : デバイスコントロール。
- EntAppControl : アプリケーションコントロール。
- File\_Monitoring または FM : ファイル脅威対策。
- Firewall または FW : ファイアウォール。
- HIPS : ホスト侵入防止。
- IDS : ネットワーク脅威対策。
- IntegrityCheck : 整合性チェック。
- Mail\_Monitoring または EM : メール脅威対策。
- Rollback : アップデートのロールバック。
- Scan\_ContextScan : コンテキストメニューからのスキャン。
- Scan\_IdleScan : バックグラウンドスキャン。
- Scan\_Memory : カーネルメモリのスキャン。
- Scan\_My\_Computer : 完全スキャン。
- Scan\_Objects : オブジェクトスキャン。
- Scan\_Qscan : オペレーティングシステムの起動時に読み込まれるオブジェクトのスキャン。
- Scan\_Removable\_Drive : リムーバブルドライブのスキャン。
- Scan\_Startup または STARTUP : 簡易スキャン。
- Updater : アップデート。
- Web\_Monitoring または WM : ウェブ脅威対策。
- WebControl - ウェブコントロール。

Kaspersky Endpoint Security では、コマンド指定用のサービス名もサポートされています。カスペルスキーのテクニカルサポートに問い合わせを行って調査が必要になったときに、コマンド指定用のサービス名を使用する場合があります。

## REST API を使用した製品の管理

Kaspersky Endpoint Security では、サードパーティ製ソリューションを使用して、製品設定の編集、スキャンの実行、定義データベースのアップデートなどのタスクを実行できます。Kaspersky Endpoint Security はそのための API を提供します。Kaspersky Endpoint Security の REST API は HTTP を介して操作でき、要求と応答の一連のメソッドで構成されています。これにより、製品のローカルインターフェイスまたは Kaspersky Security Center 管理コンソールではなく、サードパーティ製ソリューションを使用して Kaspersky Endpoint Security を管理できます。

REST API を使用するには、[REST API のサポートを有効にして Kaspersky Endpoint Security をインストールする](#)必要があります。REST クライアントと Kaspersky Endpoint Security は同じコンピューターにインストールしてください。

Kaspersky Endpoint Security および REST クライアントが安全に相互動作するためには：

- 認証されていないアクセスに対する REST クライアントの保護を REST クライアントの開発者の推奨に従って設定します。任意アクセス制御リスト (DACL) を使用して REST クライアントを書き込みから保護します。
- REST クライアントを実行するには、管理者権限を持つ別のアカウントを使用します。このアカウントのシステムへの対話的なサインインをオフにします。

REST API を使用すると、`http://127.0.0.1` または `http://localhost` を経由して製品が管理されます。REST API を使用してリモートで Kaspersky Endpoint Security を管理することはできません。



[REST API のドキュメントを開く](#)

## REST API の使用を有効にしての本製品のインストール

REST API を使用して製品を管理するには、REST API のサポートを有効にして Kaspersky Endpoint Security をインストールする必要があります。REST API を使用して Kaspersky Endpoint Security を管理する場合、Kaspersky Security Center を使用して製品を管理できなくなります。

### REST API のサポートを有効にした製品のインストールの準備

REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。

証明書の作成には、OpenSSL などを使用することができます。

例：

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

鍵長が 2048 ビット以上の RSA 暗号化アルゴリズムを使用してください。

この結果、証明書「cert.pem」と秘密鍵「key.pem」を入手できます。

### REST API のサポートを有効にした本製品のインストール

REST API のサポートを有効にして Kaspersky Endpoint Security をインストールするには：

1. 管理者としてコマンドラインインタープリタ (cmd.exe) を実行します。
2. Kaspersky Endpoint Security のバージョン 11.2.0 以降の配布パッケージを含むフォルダーに移動します。
3. 次の設定で Kaspersky Endpoint Security をインストールします :

- RESTAPI=1

- RESTAPI\_User=<ユーザー名>

REST API による本製品の管理に使用するユーザー名。ユーザー名は、<ドメイン>\<ユーザー名> の形式で入力します (例: RESTAPI\_User=COMPANY\Administrator)。このアカウントでのみ、REST API を使用して製品を管理できます。REST API を利用するユーザーは1人しか選択できません。

- RESTAPI\_Port=<ポート>

データ交換に使用するポート。省略可能なパラメータです。既定ではポート 6782 が選択されています。

- RESTAPI\_Certificate=<証明書のパス>

リクエストを識別するための証明書 (例: RESTAPI\_Certificate=C:\cert.pem)。

本製品のインストール後または証明書の有効期間が終了した後に証明書をインストールできます。

#### [REST API リクエストの識別用の証明書をインストールする方法](#)

1. [Kaspersky Endpoint Security セルフディフェンス](#) を無効にします。

セルフディフェンスは、ハードディスクのアプリケーションファイル、メモリプロセス、およびシステムレジストリのエントリの改竄や削除を防止します。

2. REST API 設定を含むレジストリキー

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest に移動します。

3. 「Certificate = C:\Folder\cert.pem」のように、証明書のパスを入力します。

4. [Kaspersky Endpoint Security セルフディフェンス](#) を有効にします。

5. [本製品を再起動](#) します。

- AdminKitConnector=1

管理システムを使用した製品管理。既定では管理が許可されています。

[setup.ini ファイル](#) を使用して REST API を使用するための設定を指定することもできます。

例 :

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator  
/pRESTAPI_Certificate=C:\cert.pem /s
```

これにより、REST API を使用して製品を管理できます。REST API が動作していることを確認するには、GET 要求を使用して REST API のドキュメントを開きます。

例 :

```
GET http://localhost:6782/kes/v1/api-docs
```

REST API のサポートを有効にした本製品がインストールされている場合、Kaspersky Endpoint Security はウェブコントロールの設定内で Web リソースへのアクセスの許可ルール（REST API 用のサービスルール）を自動的に作成します。REST API のサポートを有効にした本製品がインストールされている場合、Kaspersky Endpoint Security はウェブコントロールの設定内で Web リソースへのアクセスの許可ルール（REST API 用のサービスルール）を自動的に作成します。このルールは REST クライアントの Kaspersky Endpoint Security へのアクセスを常時許可するために必要です。たとえば、ユーザーの Web リソースへのアクセスを制限した場合、REST API 経由でのアプリケーションの管理には影響しません。REST API 用のサービスルールの設定の削除や変更は推奨されません。ルールを削除した場合、Kaspersky Endpoint Security は本製品を再起動した際に復元します。

## API の使用

パスワードによる保護を使用して、REST API から製品へのアクセスを制限することはできません。たとえば、ユーザーが REST API を使用して保護を無効にしようとした場合、この操作をブロックすることはできません。一方で、REST API を使用してパスワードによる保護を設定し、ローカルインターフェイスを介した製品へのユーザーアクセスを制限することはできます。

REST API を使用して製品を管理するには、REST API のサポートを有効にして製品をインストールし、なおかつそのときに指定したアカウントで REST クライアントを実行する必要があります。REST API を利用するユーザーは 1 人しか選択できません。



### [REST API のドキュメントを開く](#)

REST API による製品の管理には次の手順があります：

1. 製品設定の現在の値を取得します。これを行うには GET 要求を送信します。

例：

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. 製品が設定の構文と値を含む応答を送信します。Kaspersky Endpoint Security は XML 形式と JSON 形式をサポートします。

例：

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": true,
  "enabled": true
}
```

3. 製品設定を編集します。GET 要求に対する応答で受信した設定の構文を使用します。

例：

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. 製品設定（ペイロード）を JSON（payload.json）に保存します。
5. PKCS7 形式で JSON に署名します。

例：

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -  
binary -outform pem -out signed_payload.pem
```

その結果、要求のペイロードを持つ署名済みファイルを手に入れます（signed\_payload.pem）。

6. 製品設定を編集します。これを行うには、POST 要求を送信し、要求のペイロードを持つ署名済みファイル（signed\_payload.pem）を添付します。

本製品は新しい設定を適用し、製品の設定結果を含む応答を送ります（応答は空白にできます）。設定が更新されたかどうかを GET 要求を送信して確認することができます。

## 製品の情報源

### カスペルスキーの Web サイトの Kaspersky Endpoint Security のページ

カスペルスキーの[製品ページ](#)で、製品とその機能に関する一般的情報を見ることができます。

### ナレッジベースの Kaspersky Endpoint Security 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 Endpoint Security のページ](#)に、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、Kaspersky Endpoint Security 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。ナレッジベースの記事には、テクニカルサポートからのお知らせが含まれることもあります。

### カスペルスキー製品のユーザーコミュニティ

特に緊急の対応が必要ではない場合は、[カスペルスキー製品のユーザーコミュニティ](#)をご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、さまざまなトピックで意見交換しています。

このコミュニティでは、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。



# Contacting Technical Support

If you cannot find a solution to your problem in the documentation or in other [sources of information about Kaspersky Endpoint Security](#), we recommend that you contact Technical Support. Technical Support will answer your questions about installing and using Kaspersky Endpoint Security.

Kaspersky provides support for Kaspersky Endpoint Security during the application's life cycle (refer to the [application life cycle page](#)). Before contacting Technical Support, please read the [support rules](#).

You can contact Technical Support in one of the following ways:

- By [visiting the Technical Support website](#)
- By sending a request to Kaspersky Technical Support through the [Kaspersky CompanyAccount portal](#)

After you inform Kaspersky Technical Support specialists about your issue, they may ask you to create a *trace file*. The trace file allows you to trace the process of performing application commands step by step and determine the stage of application operation at which an error occurs.

Technical Support specialists may also require additional information about the operating system, processes that are running on the computer, detailed reports on the operation of application components.

While running diagnostics, Technical Support experts may ask you to change application settings by:

- Activating the functionality for receiving extended diagnostic information.
- Fine-tuning the settings of individual application components, which are not available via standard user interface elements.
- Changing the settings for storage of diagnostic information.
- Configuring the interception and logging of network traffic.

Technical Support experts will provide all the information needed to perform these operations (description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc.) and inform you about the scope of data used for purposes of debugging. The extended diagnostic information is saved on the user's computer. The data is not automatically transmitted to Kaspersky.

The operations listed above should be performed only under the supervision of Technical Support specialists by following their instructions. Unsupervised changes to application settings performed in ways other than those described in the Administrator's Guide or instructions of Technical Support specialists can slow down or crash the operating system, affect computer security, or compromise the availability and integrity of data being processed.

## トレースファイルの内容と保存場所

お客様は、コンピューターに保存されているデータのセキュリティ、特にカスペルスキーに送信されるまでのデータへのアクセス監視および制限の責任を個人的に負います。

トレースファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。

認証エージェントのトレースファイルを除いて、トレースファイルはフォルダー「%ProgramData%\Kaspersky Lab\KES\Traces」に保存されます。

トレースファイルの命名規則は「KES<サービスのバージョン番号\_日付XX.XX\_時刻XX.XX\_pidXXX.><トレースファイル種別>.log」となります。

トレースファイルに保存されたデータを確認できます。

すべてのトレースファイルには、次の共通データが含まれます：

- イベントの日時
- 実行された脅威の数

認証エージェントのトレースファイルには、この情報は含まれません。

- イベントを発生させたコンポーネント
- イベントの重大度（情報イベント、警告、緊急イベント、エラー）
- コンポーネントによるコマンド実行およびそのコマンドの実行結果を含むイベントの説明

Kaspersky Endpoint Security は、ユーザーパスワードについて、暗号化したかたちでのみトレースファイルに保存します。

## SRV.log、GUI.log、ALL.log トレースファイルの内容

SRV.log、GUI.log、ALL.log トレースファイルは、共通データの他に次の情報を保存する場合があります：

- ローカルコンピューターのファイルのパスに含まれている、姓名を含む個人情報。
- コンピューターにインストールされているハードウェアのデータ（BIOS / UEFI ファームウェアデータなど）。このデータは、Kaspersky Disk Encryption の実行時にトレースファイルに書き込まれます。
- 平文で転送されたユーザー名とパスワード。このデータは、インターネットトラフィックのスキャン中にトレースファイルに記録されることがあります。
- HTTP ヘッダーに含まれているユーザー名とパスワード。
- ファイル名に含まれている Windows アカウント名。
- 検知されたオブジェクトの名前に含まれている、アカウント名およびパスワードを含むメールアドレスまたは Web アドレス。
- アクセスした Web サイトおよびその Web サイトからのリダイレクト。このデータは、Web サイトがスキャンされる際にトレースファイルに書き込まれます。

- プロキシサーバーにサインインするために使用したプロキシサーバーのアドレス、コンピューター名、ポート、IP アドレス、ユーザー名。このデータは、プロキシサーバーを使用する場合にトレースファイルに書き込まれます。
- コンピューターが接続を確立したリモート IP アドレス。
- ソーシャルネットワークにおけるメッセージの件名、ID、送信者名、メッセージを送信した Web サイトのアドレス。このデータは、ウェブコントロールが有効になっている場合にトレースファイルに書き込まれます。
- ネットワークトラフィックデータトラフィック監視コンポーネントが有効になっている場合（Web Control など）、このデータはトレースファイルに書き込まれます。
- Kaspersky サーバーから受信したデータ（ウイルス対策データベースのバージョンなど）。
- Kaspersky Endpoint Security コンポーネントとその動作データのステータス。
- アプリケーションのユーザーの活動に関するデータ。
- オペレーティングシステムのイベント

## HST.log、BL.log、Dumpwriter.log、WD.log、AVPCon.dll.log トレースファイルの内容

HST.log トレースファイルには、共通データの他に、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の実行に関する情報が含まれます。

BL.log トレースファイルには、共通データの他に、本製品の動作中に発生したイベントの情報と、本製品のエラーを解決するために必要なデータが含まれます。このファイルは、本製品が `avp.exe -bl` パラメータで開始された場合に作成されます。

Dumpwriter.log トレースファイルには、共通データの他に、ダンプファイルが書き込まれる際に発生するエラーの解決に必要なサービス情報が含まれます。

WD.log トレースファイルには、共通データの他に、ソフトウェアモジュールのアップデートイベントを含め、avpsus サービスの操作中に発生したイベントに関する情報が含まれます。

AVPCon.dll.log トレースファイルには、共通データの他に、Kaspersky Security Center 接続モジュールの動作中に発生したイベントに関する情報が含まれます。

## パフォーマンスのトレースファイルの内容

パフォーマンスのトレースファイルの命名規則は「`KES<バージョン番号>_日付XX.XX_時刻XX.XX_pidXXX.>PERF.HAND.et1`」となります。

パフォーマンスのトレースファイルには、共通データの他に、プロセッサでの負荷、オペレーティングシステムとアプリケーションの読み込み時間、実行されていたプロセスに関する情報が含まれます。

## AMSI 保護機能のトレースファイルの内容

AMSI.log トレースファイルには、共通データの他に、サードパーティ製品の要求に基づいて実行したスキャン結果に関する情報が含まれます。

## メール脅威対策のトレースファイルの内容

mcou.OUTLOOK.EXE.log トレースファイルには、共通データの他に、メールアドレスなど、メールメッセージの一部が含まれます。

## コンテキストメニューからのスキャンのトレースファイルの内容

shellex.dll.log トレースファイルには、共通データの他に、スキャンタスクの完了に関する情報と、本製品のデバッグに必要なデータが含まれています。

## Web プラグインのトレースファイルの内容

本製品の Web プラグインのトレースファイルは、Kaspersky Security Center Web コンソールサーバーを配備しているコンピューターの「Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs」に保存されます。

本製品の Web プラグインのトレースファイルの命名規則は「 logs-kes\_windows-<トレースファイル種別>.DESKTOP-<ファイルの更新日>.log」となります。Web コンソールをインストールするとデータの書き込みが始まり、Web コンソールをアンインストールするとトレースファイルも削除されます。

Web プラグインのトレースファイルには、共通データの他に次の情報が含まれます：

- Kaspersky Endpoint Security のインターフェイスのロックを解除するための KAdmin ユーザーパスワード ([パスワードによる保護](#))。
- Kaspersky Endpoint Security のインターフェイスのロックを解除するための一時パスワード ([パスワードによる保護](#))。
- SMTP メールサーバーのユーザー名とパスワード ([メール通知](#))。
- 内部プロキシサーバーのユーザー名とパスワード ([プロキシサーバー](#))。
- [[アプリケーション機能の変更](#)] タスクのユーザー名とパスワード。
- Kaspersky Endpoint Security のタスクとポリシーのプロパティで指定されているアカウント認証情報とフォルダーやファイルのパス。

## 認証エージェントのトレースファイルの内容

認証エージェントのトレースファイルは、次の名前ですべてシステムボリューム情報フォルダーに保存されます：  
KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin


認証エージェントのトレースファイルには、共通データの他に、認証エージェントの動作および認証エージェントを使用してユーザーにより実行された動作に関する情報が含まれます。

## アプリケーションの動作のトレース

アプリケーションのトレースとは、製品が実行する処理の詳細な記録と製品の動作中に発生したイベントに関するメッセージです。

アプリケーションのトレースは、カスペルスキーのテクニカルサポート担当者の協力のもと、その指示に従いながら実行してください。

アプリケーションのトレースファイルを作成するには：

1. メインウィンドウで、 をクリックします。  
[サポート] ウィンドウが開きます。
2. [サポート] ウィンドウで、[サポートツール] をクリックします。
3. [アプリケーショントレースを有効にする] トグルスイッチを使用してアプリケーションの操作の追跡を有効または無効にします。
4. [トレース] で、アプリケーションのトレースモードを選択します：
  - **ローテーション**：ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。このモードが選択されている場合、ローテーションするファイルの最大数と各ファイルの最大サイズを定義することができます。
  - **単一のファイルに書き込む**：トレースファイルを1つ保存します（容量の上限なし）。
5. [レベル] で、トレースレベルを選択します。  
テクニカルサポートのスペシャリストに、必要なトレースレベルを確認してください。テクニカルサポートのガイダンスを受けることができない場合は、トレースレベルを[通常(500)]に設定します。
6. Kaspersky Endpoint Security を再起動します。
7. トレースのプロセスを停止するには、[サポート] ウィンドウに戻ってトレースを無効にします。

[コマンドライン](#)から本製品をインストールする場合も、[setup.ini ファイル](#)を使用して設定することで、トレースファイルを作成できます。

パフォーマンスのトレースファイルがフォルダー「%ProgramData%\Kaspersky Lab\KES\Traces」に作成されます。トレースファイルが作成されたら、カスペルスキーのテクニカルサポートに送信してください。


Kaspersky Endpoint Security は本製品が削除される際に自動でトレースファイルを削除します。手動でファイルを削除することもできます。手動でファイルを削除するには、トレースを無効にして[本製品を停止](#)する必要があります。

## 製品のパフォーマンスのトレース

Kaspersky Endpoint Security では、本製品の使用中にコンピューター上で発生した動作エラーや問題に関する情報を取得できます。たとえば、本製品のインストール後にオペレーティングシステムの読み込みが遅くなったなどの問題に関する情報を取得できます。こうした目的のために、Kaspersky Endpoint Security では[パフォーマンスのトレースファイル](#)を作成できます。パフォーマンスのトレースでは、Kaspersky Endpoint Security のパフォーマンスに関する問題を診断するために、本製品によって実行される処理に関する情報が記録されます。情報の取得には、Windows イベントトレーシングサービス (ETW) が使用されます。Kaspersky Endpoint Security の問題に関する診断と問題の発生原因の特定は、カスペルスキーのテクニカルサポートが担当します。

アプリケーションのトレースは、カスペルスキーのテクニカルサポート担当者の協力のもと、その指示に従いながら実行してください。

パフォーマンスのトレースファイルを作成するには：

1. メインウィンドウで、 をクリックします。  
[サポート] ウィンドウが開きます。
2. [サポート] ウィンドウで、[サポートツール] をクリックします。
3. [パフォーマンストレースを有効にする] トグルスイッチを使用してアプリケーションのパフォーマンスの追跡を有効または無効にします。
4. [トレース] で、アプリケーションのトレースモードを選択します：
  - **ローテーション**：ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。このモードが選択されている場合、各ファイルの最大サイズを設定できます。
  - **単一のファイルに書き込む**：トレースファイルを1つ保存します（容量の上限なし）。
5. [レベル] で、トレースレベルを選択します。
  - **低**：Kaspersky Endpoint Security は、パフォーマンスに関連するオペレーティングシステムの最も重要なプロセスを分析します。
  - **詳細**：Kaspersky Endpoint Security は、パフォーマンスに関連するオペレーティングシステムのすべてのプロセスを分析します。
6. [トレース種別] で、いずれかのトレース種別を選択します：
  - **基本情報**：Kaspersky Endpoint Security は、オペレーティングシステムの実行中にプロセスを分析します。このトレース種別は、オペレーティングシステムの読み込み後に問題が継続して発生する場合（ブラウザを使用してインターネットにアクセスするときに問題が発生するなど）に使用してください。
  - **再起動時**：Kaspersky Endpoint Security は、オペレーティングシステムの読み込み中のみプロセスを分析します。オペレーティングシステムの読み込みが完了すると、Kaspersky Endpoint Security はトレースの実行を停止します。オペレーティングシステムの読み込み時の遅延に関する問題が発生している場合は、このトレース種別を使用してください。
7. コンピューターを再起動して、問題の再現を試行してください。
8. トレースのプロセスを停止するには、[サポート] ウィンドウに戻ってトレースを無効にします。

パフォーマンスのトレースファイルがフォルダー「%ProgramData%\Kaspersky Lab\KES\Traces」に作成されます。トレースファイルが作成されたら、カスペルスキーのテクニカルサポートに送信してください。


## ダンプ書き込み

ダンプファイルには、ダンプファイルの作成時点で Kaspersky Endpoint Security のプロセスが作業していたメモリについてのすべての情報が含まれます。

保存されたダンプファイルには、機密情報が含まれる可能性があります。データへのアクセスを制御するには、ダンプファイルのセキュリティを個別に確保する必要があります。

ダンプファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。ダンプファイルは、フォルダー「%ProgramData%\Kaspersky Lab\KES\Traces」に保存されます。

ダンプの書き込みを有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【全般設定】** の順に選択します。
3. **【デバッグ情報】** ブロックで、**【ダンプへの書き込みを有効にする】** を使用してアプリケーションのダンプ書き込みを有効または無効にします。
4. 変更内容を保存します。


## ダンプファイルとトレースファイルの保護

ダンプファイルとトレースファイルには、オペレーティングシステムに関する情報が含まれます。また、[ユーザーの個人情報](#)が含まれる場合があります。そのデータに対する不正アクセスを防ぐため、ダンプファイルとトレースファイルの保護を有効にできます。

ダンプファイルとトレースファイルの保護が有効な場合、これらのファイルには次のユーザーがアクセスできます：

- ダンプファイルには、システム管理者と LAN 管理者、およびダンプファイルとトレースファイルの書き出しを有効にしたユーザーがアクセスできます。
- トレースファイルには、システム管理者と LAN 管理者がアクセスできます。

ダンプファイルとトレースファイルの保護を有効または無効にするには：

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、**【詳細設定】** → **【全般設定】** の順に選択します。
3. **【デバッグ情報】** ブロックで、**【ダンプおよびトレースファイルの保護を有効にする】** を使用してファイルの保護を有効または無効にします。
4. 変更内容を保存します。

保護が有効なときに書き出されたダンプファイルとトレースファイルは、この機能を無効にしても引き続き保護されます。



## 制限と警告

Kaspersky Endpoint Security には、製品の操作上是重大ではないですがいくつかの制限があります。

[本製品のインストール](#) 

- Microsoft Windows 10、Microsoft Windows Server 2016 および Microsoft Windows Server 2019 サポートについては、[テクニカルサポートサイトのナレッジベースの記事](#)を参照してください。
- Microsoft Windows 11 および Microsoft Windows Server 2022 のサポートについては、[テクニカルサポートサイトのナレッジベースの記事](#)を参照してください。
- 感染したコンピューターにインストールされた後、本製品はコンピューターのスキャンを実行する必要があることをユーザーに通知しません。[製品のアクティベーション](#)で問題が発生する可能性があります。これらの問題を解決するには、[簡易スキャン](#)を実行する必要があります。
- setup.ini および setup.reg ファイルで非 ASCII 文字（例えばロシア文字など）が使用されていた場合、notepad.exe を使用して編集し、UTF-16LE エンコードで保存する必要があります。その他のエンコーディングはサポートされません。
- [インストールパッケージの設定](#)で本製品のインストールパスを指定する際には非 ASCII 文字の使用はサポートされません。
- [製品設定が CFG ファイルからインポート](#)された場合、Kaspersky Security Network への参加を定義する設定値は適用されません。設定のインポート後、Kaspersky Security Network に関する声明を読み、Kaspersky Security Network への参加の設定に同意してください。製品のインターフェイス、または製品の配信キットに含まれるフォルダーにある ksn\_\*.txt ファイルで声明の内容を確認できます。
- 暗号化（FLE または FDE）またはデバイスコントロール機能を削除して再インストールする場合は、再インストール前にシステムを再起動する必要があります。
- Microsoft Windows 10 オペレーティングシステムを実行している場合は、ファイルレベルの暗号化（FLE）機能を削除した後にシステムの再起動が必要になります。
- Kaspersky Endpoint Security for Windows 11.7.0 がインストールされていて暗号化機能がインストールされていないコンピューターに AES 暗号化モジュールをインストールする場合、暗号化モジュールのインストールは新しいバージョンの製品が既にインストールされているというエラーが発生して終了します。Kaspersky Endpoint Security 10 for Windows Service Pack 2（バージョン 10.3.0.6294）から開始すれば、暗号化モジュールの個別のインストールファイルはありません。暗号化ライブラリは製品の配信パッケージに含まれています。Kaspersky Endpoint Security 11.7.0 は AES 暗号化モジュールと互換性はありません。暗号化に必要なライブラリは、ディスク全体の暗号化（FDE）またはファイルレベルの暗号化（FLE）コンポーネントが選択されている場合は自動的にインストールされます。
- 本製品のインストールが名前がないまたは読み込めないアプリケーションがインストールされているというエラーにより終了することがあります。これは、お使いのコンピューターに互換性のないアプリケーションがあるか、その一部が残っているということを意味します。互換性のない製品の影響を取り除くには、状況の詳細な説明を入力して[カスペルスキーのカンパニーアカウント](#)からカスペルスキーのテクニカルサポートにリクエストを送信してください。
- 本製品のアンインストールをキャンセルした場合、コンピューターを再起動した後に復元を開始してください。
- Windows 10 バージョン 1903 および 1909 では、Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3（ビルド 10.3.3.275）、Service Pack 2 Maintenance Release 4（ビルド 10.3.3.304）、ファイルレベルの暗号化（FLE）機能付きの 11.0.0 および 11.0.1 からのアップグレードはエラーで終了することがあります。これは、Windows 10 バージョン 1903 および 1909 でこれらのバージョンの Kaspersky Endpoint Security for Windows がファイルの暗号化をサポートしていないためです。このアップグレードをインストールする前に、[ファイル暗号化機能を削除](#)してください。
- 本製品の動作には Microsoft .NET Framework 4.0 以降が必要です。Microsoft .NET Framework 4.6.1 には脆弱性があります。Microsoft .NET Framework 4.6.1 を使用している場合は、セキュリティアップデート

をインストールする必要があります。Microsoft .NET Framework のセキュリティアップデートに関して詳しくは、[Microsoft のテクニカルサポートサイト](#) を参照してください。

- Kaspersky Endpoint Agent をインストールするために本製品の以前のバージョンからバージョン 11.7.0 にアップグレードする場合は、コンピューターを再起動してローカル管理者権限のあるアカウントを使用してシステムにサインインしてください。そうしないと、Kaspersky Endpoint Agent はアップグレード中にインストールされません。
- サーバーオペレーティングシステムで選択された Kaspersky Endpoint Agent 機能との本製品のインストールが正常に終了せず、*Windows Installer Coordinator Error* ウィンドウが表示された場合は、Microsoft サポート Web サイトの内容を参照してください。
- 本製品がローカルで対話モードでなくインストールされた場合は、提供された [setup.ini ファイル](#) を使用してインストールされたコンポーネントを置き換えてください。
- Windows 7 の構成に Kaspersky Endpoint Security for Windows がインストールされた後、Windows Defender は動作を続行します。この場合、システムのパフォーマンスの低下を避けるため、Windows Defender を手動で無効にしてください。

## [本製品のアップグレード](#)

- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (ビルド 10.3.0.6294) からアップグレードする場合、[ホスト侵入防止機能は有効になっています](#)。
- Kaspersky Endpoint Security 10 for Windows Service Pack 2 (ビルド 10.3.0.6294) をアップデートする場合、以前のバージョンの製品で [バックアップ] または [隔離] に置かれていたファイルは、新しいバージョンの製品の [バックアップ] に移動されます。これらのファイルは Kaspersky Endpoint Security 10 for Windows Service Pack 2 (ビルド 10.3.0.6294) 以前のバージョンでは移動されません。これらを保存するには、アップグレードする前に [バックアップ] または [隔離] からファイルを復元する必要があります。アップグレードの完了後、復元されたファイルを再度スキャンしてください。
- 本製品のバージョン 11.0.0 から、Kaspersky Endpoint Security for Windows MMC プラグインは、以前のバージョンのプラグインに上書きインストールされるようになりました。以前のバージョンのプラグインに戻すには、現在のプラグインを削除してから以前のバージョンのプラグインをインストールしてください。
- Kaspersky Endpoint Security 11.0.0 または 11.0.1 for Windows をアップグレードする際、アップデート、簡易スキャン、カスタムスキャン、整合性チェックの[ローカルタスクのスケジュールの設定](#)は保存されません。
- Windows 10 バージョン 1903 および 1909 では、Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (ビルド 10.3.3.275)、Service Pack 2 Maintenance Release 4 (ビルド 10.3.3.304)、ファイルレベルの暗号化 (FLE) 機能付きの 11.0.0 および 11.0.1 からのアップグレードはエラーで終了することがあります。これは、Windows 10 バージョン 1903 および 1909 でこれらのバージョンの Kaspersky Endpoint Security for Windows がファイルの暗号化をサポートしていないためです。このアップグレードをインストールする前に、[ファイル暗号化機能を削除](#)してください。
- 本製品の動作には Microsoft .NET Framework 4.0 以降が必要です。Microsoft .NET Framework 4.6.1 には脆弱性があります。Microsoft .NET Framework 4.6.1 を使用している場合は、セキュリティアップデートをインストールする必要があります。Microsoft .NET Framework のセキュリティアップデートに関して詳しくは、[Microsoft のテクニカルサポートサイト](#) を参照してください。
- Kaspersky Endpoint Agent をインストールするために本製品の以前のバージョンからバージョン 11.7.0 にアップグレードする場合は、コンピューターを再起動してローカル管理者権限のあるアカウントを使用してシステムにサインインしてください。そうしないと、Kaspersky Endpoint Agent はアップグレード中にインストールされません。
- Windows 10 バージョン 1809、1903 および 1909 を実行しているコンピューター上でファイルレベルの暗号化機能 (FLE) 付きの Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 をアップグレードする場合、FDE ドライバーは WinRE イメージにはインストールされません。
- Kaspersky Endpoint Security のアップグレード時、本製品は Kaspersky Security Network に関する声明が同意されるまで、KSN の使用を無効にします。さらに、KSN サーバーが使用できないイベントが受け取られるため、Kaspersky Security Center でコンピューターのステータスが緊急に変更されることがあります。[Kaspersky Managed Detection and Response](#) を使用している場合、ソリューションの動作で違反に関するイベントを受け取ります。KSN の使用は Kaspersky Managed Detection and Response の操作に必要です。Kaspersky Endpoint Security は、管理者が KSN 利用規約に同意したポリシーの適用後 [KSN の使用を有効](#) にします。Kaspersky Security Network に関する声明に同意すると、Kaspersky Endpoint Security は動作を再開します。
- Kaspersky Endpoint Security 11 for Windows より以前のバージョンから本製品がアップグレードされた場合、コンピューターを再起動する必要があります。

- ReFS ファイルシステムは次の制限付きでサポートされます：
  - Kaspersky Endpoint Security が脅威の駆除イベントを正しく処理しないことがあります。たとえば、本製品が悪意のあるファイルを削除した際に、レポートにはオブジェクトが処理されていないと記載されることがあります。一方、Kaspersky Endpoint Security は製品の設定に従って脅威を駆除します。また、Kaspersky Endpoint Security は同じオブジェクトに対してオブジェクトが再起動時に駆除されるイベントを重複して作成することがあります。
  - ファイル脅威対策は一部の脅威をスキップする可能性があります。一方、スキャンは正常に作動します。
  - サーバーのウイルスチェックが開始された後、iChecker で追加されたスキャンの除外リストはサーバーの再起動時にリセットされます。
  - iSwift はサポートされません。iSwift を使用して追加されたスキャンの除外リストは認識されません。
  - Kaspersky Endpoint Security がインストールされるより前にコンピューター上に meicar.exe ファイルが存在した場合は、eicar.com および susp-eicar.com ファイルは検出されません。
  - 脅威の駆除に関する通知を誤って表示することがあります。たとえば、以前に駆除した脅威に関する通知を表示することがあります。
- Server Core およびクラスター構成はサポートされません。
- ファイルレベルの暗号化 (FLE) と Kaspersky Disk Encryption (FDE) 技術は、サーバープラットフォームではサポートされません。また、Kaspersky Endpoint Security はデータ暗号化イベントを誤って処理することがあります。
- サーバープラットフォーム上ではデバイスコントロールはサポートされません。
- サーバーオペレーティングシステムでは、特別な駆除の必要性についての警告は表示されません。
- Microsoft Windows Server 2008 はサポート対象外となりました。 - Microsoft Windows Server 2008 オペレーティングシステムを実行するコンピューターへの本製品のインストールはサポートされません。

## [仮想プラットフォームのサポート](#)

- Hyper-V 仮想マシンでのディスク全体の暗号化（FDE）はサポートされていません。
- Citrix 仮想プラットフォームでのディスク全体の暗号化（FDE）はサポートされていません。
- Windows 10 Enterprise のマルチセッションは次の制限付きでサポートされます：
  - Kaspersky Endpoint Security は Windows 10 Enterprise のマルチセッションをサーバーオペレーティングシステムと認識します。そのため、Windows 10 Enterprise のマルチセッションはサーバープラットフォーム特有の制限付きでサポートされます。たとえば、サーバーでは Kaspersky Endpoint Security の機能の一部が使用できません。また、ワークステーション用のライセンスではなく、サーバー用のライセンスが使用されます。
  - ディスク全体の暗号化（FDE）はサポートされません。
  - BitLocker の管理はサポートされません。
  - リムーバブルドライブでの Kaspersky Endpoint Security の使用はサポートされません。Microsoft Azure インフラストラクチャはリムーバブルドライブをネットワークドライブとして定義します。
- Citrix 仮想プラットフォームでのファイルレベルの暗号化（FLE）のインストールおよび使用はサポートされていません。
- Kaspersky Endpoint Security for Windows と Citrix PVS の互換性をサポートするには、[\[Citrix Provisioning Services との互換性を確保する\]](#) を有効にしてください。このオプションは[セットアップウィザード](#)または[コマンドラインのパラメータ](#)「/pCITRIXCOMPATIBILITY=1.」を使用して有効にすることが可能です。リモートインストールの場合は、[KUD ファイル](#)を編集して次のパラメータを追加する必要があります。： /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop：vDisk を使用する仮想マシンを複製するため、複製の開始前に、[セルフディフェンス](#)を無効にする必要があります。
- Citrix XenDesktop で Kaspersky Endpoint Security for Windows および Kaspersky Security Center Network Agent がプリインストールされたマスターイメージのテンプレートを準備する際、設定ファイルに次の種別の除外リストを追加してください：
 

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

 Citrix XenDesktop の詳細については、[Citrix のサポートサイト](#)を参照してください。
- VMware ESXi ハイパーバイザー上で配備された仮想マシン上で、リムーバブルドライブの安全な接続解除が正常に完了しないことがあります。再度安全な接続解除を実行してください。

## [Kaspersky Security Center との互換性](#)



- アダプティブアノマリーコントロールは Kaspersky Security Center のバージョン 11 以降でのみ管理できます。
- Kaspersky Security Center 11 の脅威レポートには AMSI 保護により検知された脅威に対して行った操作についての情報は表示されません。
- AMSI 保護およびアダプティブアノマリーコントロールの動作ステータスは Kaspersky Security Center のバージョン 11 以降でのみ利用できます。【タスク】セクション内のコンピューターのプロパティで Kaspersky Security Center コンソール内の動作ステータスを表示できます。これらの機能のレポートは Kaspersky Security Center のバージョン 11 以降でのみ利用可能です。

## ライセンス管理

- 「データの受信でエラーが発生しました」というシステムメッセージが表示された場合、アクティベーションを実行しているコンピューターがネットワークに接続されているかどうかを確認するか、また Kaspersky Security Center Activation Proxy 経由でのアクティベーション設定を設定してください。
- ライセンスの有効期間が終了しているか、試用版のライセンスがコンピューターで有効になっている場合、Kaspersky Security Center 経由での定額制サービスによるアクティベートはできません。試用版のライセンスや、有効期間がまもなく切れるライセンスを定額制サービスに置き換えるには、[ライセンスの配信タスクを使用](#)してください。
- 製品のインターフェイスで、ライセンスの有効期間はコンピューターのローカル時刻で表示されません。
- インターネットアクセスが安定していない状況にあるコンピューターに埋め込みライセンスで本製品をインストールしようとする、本製品がアクティベートされていない、またはライセンスで機能の動作が制限されているというイベントが一時的に表示されることがあります。これは、本製品が初回インストール中にアクティベーションのためインターネット接続が必要な埋め込みの試用版ライセンスをインストールしてアクティベートするためです。
- 試用期間中は、インターネット接続が不安定な環境でアップグレードまたはパッチをインストールしようとする、本製品がアクティベートされていないというイベントが一時的に表示されることがあります。これは、本製品がアップグレード中にアクティベーションのためインターネット接続が必要な埋め込みの試用版ライセンスを再度インストールしてアクティベートするためです。
- 試用版のライセンスが本製品のインストール中に自動的にアクティベートされて、それからライセンス情報を保存せずに本製品をアンインストールすると、本製品の再インストール時には試用版のライセンスが自動で適用されることはありません。この場合は手動で本製品をアクティベートしてください。
- Kaspersky Security Center のバージョン 11 と Kaspersky Endpoint Security のバージョン 11.7.0 を使用している場合、機能のパフォーマンスレポートは誤動作する可能性があります。お使いのライセンスに含まれない Kaspersky Endpoint Security をインストールしている場合、ネットワークエージェントは Windows イベントログにコンポーネントのステータスエラーを書き込むことがあります。このようなエラーを避けるには、ライセンスに含まれない機能を削除してください。

## 修復エンジン



- 本製品では、NTFS ファイルシステムまたは FAT32 ファイルシステムを使用しているデバイス上のファイルのみを修復できます。
- 本製品を使用して次の拡張子のファイルを修復できます : ods、odp、odm、odc、odb、doc、docx、docm、wps、xls、xlsx、xlsm、xlsb、xll、ppt、pptx、pptm、mdb、accdb、pst、dwg、dxf、dxg、wpd、rtf、wb2、pdf、mdf、dbf、psd、pdd、eps、ai、indd、cdr、jpg、jpe、dng、3fr、arw、srf、sr2、bay、crw、cr2、dcr、kdc、erf、mef、mrw、nef、nrw、orf、raf、raw、rwl、rw2、r3d、ptx、pef、srw、x3f、der、cer、crt、pem、pfx、p12、p7b、p7c、1cd
- ネットワークドライブまたは再書き込み可能な CD / DVD 上に保存されているファイルは修復できません。
- 暗号化ファイルシステム (EFS) を使用して暗号化されたファイルは修復できません。EFS の動作について詳しくは、[Microsoft の Web サイトの情報](#) を参照してください。
- 本製品では、オペレーティングシステムのカーネルレベルのプロセスで実行されたファイル変更は監視されません。
- 本製品では、ネットワークインターフェイスを経由して行われたファイル変更は監視されません (例 : ファイルが共有フォルダーに保存されていて、プロセスが別のコンピューターからリモートで起動された場合など)

## ファイアウォール

- ローカルアドレス、物理インターフェイスおよびパケットの最大生存時間（TTL）によるパケットまたは接続のフィルタリングは次のケースでサポートされます：
  - 送信パケットまたはアプリケーションルール内の TCP および UDP、パケットルールの接続のローカルアドレス
  - 受信パケットまたはブロックアプリケーションルールまたはパケットルール内の接続（UDPを除く）のローカルアドレス
  - 受信および送信パケットのブロックパケットルール内のパケットの最大生存時間（TTL）
  - 受信および送信パケットまたはパケットルール内の接続のネットワークインターフェイス
- 本製品のバージョン 11.0.0 および 11.0.1 では、定義された MAC アドレスは誤って適用されます。11.0.0、11.0.1 および 11.1.0 以降のバージョンの MAC アドレスの設定は互換性がありません。本製品のこれらのバージョンのプラグインを 11.1.0 以降のバージョンにアップグレードした後、ファイアウォールルールで定義された MAC アドレスを確認して再度設定する必要があります。
- バージョン 11.1.1 および 11.2.0 から 11.7.0 へのアップグレードを行う際に、次のファイアウォールルールの権限のステータスは移行されません。
  - TCP 経由の DNS サーバーへの要求
  - UDP 経由の DNS サーバーへの要求
  - ネットワークの動作
  - ICMP「宛先到達不可能」応答の受信
  - ICMP ストリームの受信
- 許可するパケットルールにネットワークアダプターまたはパケットの最大生存時間（TTL）を設定していた場合は、このルールの優先度はブロックするアプリケーションルールより低くなります。たとえば、アプリケーションが強い制限付きの信頼グループに入っていてネットワーク動作がブロックされていた場合、これらの設定をしたパケットルールを使用してアプリケーションのネットワークの動作を許可することはできません。その他の場合は、パケットルールの優先度はアプリケーションネットワークルールより高くなります。
- [ファイアウォールのパケットルールをインポート](#)する際、Kaspersky Endpoint Security がルール名を変更することがあります。本製品は主要なパラメータ（プロトコル、方向、リモートおよびローカルポート、パケット最大生存時間（TTL））のセットでルールを決定します。この主要なパラメータのセットが複数のルール間で同一である場合、本製品は同じ名前を割り当てるか、名前にパラメータのタグを追加します。このように、Kaspersky Endpoint Security はすべてのパケットルールをインポートしますが、主要なパラメータが同一であるルールの名前が変更されることがあります。
- アプリケーションを別の信頼グループに移動する際の[ネットワークルール内で製品イベントのレポートを有効にしている](#)場合、この信頼グループの制限は適用されません。このため、アプリケーションが信頼済みのグループに属している場合、ネットワークの制限はありません。次に、イベントのレポートを有効にしてブロックグループに移動したとします。ファイアウォールはこのアプリケーションに対してネットワーク制限を適用しません。最初にアプリケーションを適切な信頼グループに移動してからイベントのレポートを有効にしてください。この方法が適切でない場合は、ネットワークルール内でアプリケーションの制限を手動で設定してください。制限はアプリケーションのローカルインターフェイスに対してのみ適用されます。ポリシー内でのアプリケーションの信頼グループ間の移動は正常に動作します。

- ファイアウォールと侵入防止機能には、アプリケーション権限と保護対象のリソースという共通の設定があります。ファイアウォールのこれらの設定を変更した場合、Kaspersky Endpoint Security は自動的に侵入防止に新しい設定を適応します。たとえば、ファイアウォールポリシーの全般設定の変更が許可した場合（鍵が開いた状態）、侵入防止も同様に編集可能となります。
- Kaspersky Endpoint Security 11.6.0 以前のバージョンでネットワークパケットルールが適用された時、ファイアウォールのレポートの [アプリケーション名] 列に *Kaspersky Endpoint Security* の値が常に表示されます。また、すべてのアプリケーションの接続をパケットレベルでブロックします。この動作は Kaspersky Endpoint Security 11.7.0 以降のバージョンでは修正されています。[ルール種別] 列がファイアウォールのレポートに追加されました。ネットワークパケットルールが適用されると、[アプリケーション名] 列の値は空白のままになります。

## 有害 USB 攻撃ブロック

- Kaspersky Endpoint Security はコンピューターがロック（時間が経過して画面がロックされるなど）されると、USB デバイスのタイムアウトをリセットします。USB デバイスの認証コードを複数回誤って入力し、本製品によって USB デバイスがロックされた場合、コンピューターのロック解除後に再度認証コードを入力することができるようになります。この場合、Kaspersky Endpoint Security は [有害 USB 攻撃ブロックの設定](#) で指定された時間 USB をロックしないこととなります。
- Kaspersky Endpoint Security は [コンピューターの保護機能が一時停止した場合](#) に USB デバイスのロックをリセットします。USB デバイスの認証コードを複数回誤って入力し、本製品によって USB デバイスがロックされた場合、[コンピューターの保護機能の再開後](#) に再度認証コードを入力することができるようになります。この場合、Kaspersky Endpoint Security は [有害 USB 攻撃ブロックの設定](#) で指定された時間 USB をロックしないこととなります。

## アプリケーションコントロール

- Microsoft Windows 10 でアプリケーションの拒否リストモードでの動作中に、ブロックルールが誤って適用されてしまい、ルールで指定されていないアプリケーションがブロックされてしまうことがあります。
- プログレッシブウェブアプリ (PWA) がアプリケーションコントロール機能でブロックされた際に、appManifest.xml がレポート内でブロックされたアプリとして表示されます。
- 標準のメモ帳 (Notepad) を Windows 11 のアプリケーションコントロールルールに追加する場合は、アプリケーションのパスを指定しないでください。Windows 11 を実行しているコンピューターではオペレーティングシステムは C:\Program Files\WindowsApps\Microsoft.WindowsNotepad\*\Notepad\Notepad.exe にある Metro のメモ帳を使用しています。オペレーティングシステムの以前のバージョンでは、メモ帳は次のフォルダーにありました：
  - C:\Windows\notepad.exe
  - C:\Windows\System32\notepad.exe
  - C:\Windows\SysWOW64\notepad.exe

アプリケーションコントロールルールにメモ帳を追加する場合は、製品名や実行中のファイルのプロパティからのファイルのハッシュなどから指定します。

## デバイスコントロール

- 信頼するリストに追加されたプリンタデバイスへのアクセスが、デバイスおよびバスブロックルールによりブロックされます。
- MTP デバイスでは、オペレーティングシステムの組み込み Microsoft ドライバーを使用している場合は読み取り、書き込み、および接続のコントロールがサポートされます。ユーザーがデバイスで作業するために (iTunes または Android Debug Bridge の一部としてなど) カスタムドライバーをインストールする場合、読み取りおよび書き込み操作は機能しないことがあります。
- MTP デバイスで作業する際、デバイスへ再接続したあとにアクセスルールが変更されます。
- デバイスを、ID に含まれるが機種名に含まれない文字を使用した機種のマスクで信頼リストに追加しようとすると、追加されません。ワークステーションでは、デバイスは ID のマスクに基づいた信頼リストに追加されます。

## ウェブコントロール

- OGV および WEBM 形式はサポートされません。
- RTMP プロトコルはサポートされません。

## アダプティブアノマリーコントロール

- イベントに基づいて自動で除外リストを作成することをお勧めします。[手動で除外リストを追加する際](#)、対象オブジェクトの指定時に「\*」をパスの先頭に追加してください。
- サンプルの名前が1つでも 260 文字を超える場合は[アダプティブアノマリーコントロールルールのレポートは作成できません](#)。
- 対象のオブジェクトのパスなど、オブジェクトやプロセスのプロパティに 256 文字以上の値を持つ場合は、アダプティブアノマリーコントロールルール適用条件リポジトリからの除外の追加はサポートされません。[ポリシーの設定で手動で除外を追加](#)できます。また、適用された[アダプティブアノマリーコントロールルールのレポート](#)で除外を追加することもできます。

## ドライブの暗号化 (FDE)


- 本製品のインストール後、ハードドライブの暗号化が正常に動作するためにオペレーティングシステムの再起動を吸う必要があります。
- 認証エージェントでは記号や特殊文字、| および \ はサポートされません。
- 暗号化後のコンピューターのパフォーマンスを最適に保つため、プロセッサは AES-NI (Intel Advanced Encryption Standard New Instructions) 命令セットをサポートする必要があります。プロセッサが AES-NI をサポートしていない場合、コンピューターのパフォーマンスが低下することがあります。
- 暗号化されたデバイスに本製品がアクセス権を付与する前にプロセスがアクセスしようとする、本製品はこのようなプロセスを中断するよう警告を表示します。プロセスが中断されない場合、暗号化デバイスを再接続してください。
- ハードドライブの一意な ID はデバイス暗号化の統計では倒置形式で表示されます。
- 暗号化されているデバイスのフォーマットは推奨されません。
- 複数のリムーバブルデバイスが同時にコンピューターに接続されている場合、暗号化ポリシーは1つのリムーバブルドライブにのみ適用されます。リムーバブルデバイスが再度接続された際に、暗号化ポリシーは正常に適用されます。
- 過度に断片化されたハードドライブでは暗号化が開始できないことがあります。ハードドライブをデフラグしてください。
- ハードドライブが暗号化されると、Microsoft Windows 7、8、8.1 がインストールされたコンピューターでは暗号化タスクが実行されたときから再起動するまで、また、Microsoft Windows 8、8.1、10 ではハードドライブの暗号化のインストール後から再起動するまで休止状態がブロックされます。ハードドライブが復号化されると、ブートドライブが完全に復号化されたときからオペレーティングシステムが最初に再起動されるまでの間、休眠状態はブロックされます。Microsoft Windows 8、8.1、10 の **クイックスタート** が有効にされていると、休眠状態がブロックされることでオペレーティングシステムのシャットダウンができなくなることがあります。
- Windows 7 搭載のコンピューターでは、BitLocker でディスクが暗号化された場合、回復中にパスワードの変更が許可されません。回復キーが入力され、オペレーティングシステムが読み込まれた後は、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促しません。このため、新しいパスワードまたは PIN コードを設定することはできません。この問題はオペレーティングシステムの実行によるものです。続行するには、ハードドライブを再度暗号化する必要があります。
- 追加のプロバイダーが有効な状態での xbootmgr.exe ツールの使用はお勧めできません。例えばディスクパッチャ、ネットワーク、またはドライブなどです。
- Kaspersky Endpoint Security for Windows がインストールされているコンピューターでの暗号化されたリムーバブルドライブのフォーマットはサポートされません。
- FAT32 ファイルシステムでの暗号化されたリムーバブルドライブのフォーマットはサポートされません（ドライブは暗号化されていると表示されます）。ドライブをフォーマットするには、NTFS ファイルシステムでフォーマットしなおしてください。
- バックアップコピーから暗号化された GPT デバイスにオペレーティングシステムを復元する詳細については、[テクニカルサポートのナレッジベースの記事](#) を参照してください。
- 1台の暗号化されたコンピューター上で複数のダウンロードエージェントは共存できません。
- 以下の条件を同時に満たす場合は、別のコンピューターで以前暗号化されたリムーバブルドライブにアクセスできません：
  -



- Kaspersky Security Center のサーバーに接続されていない
- ユーザーが新しいトークンまたはパスワードで認証しようとしている

同様の状況が発生する場合は、コンピューターを再起動してください。コンピューターが再起動した後、暗号化されたリムーバブルドライブへのアクセス権が付与されます。

- BIOS 設定で US b の xHCI モードが有効になっている場合、認証エージェントの USB デバイスの検出はサポートされないことがあります。
- 頻繁に使用されているデータをキャッシュするために使用されるデバイスの SSD パーツの Kaspersky Disk Encryption (FDE) 技術は SSHD デバイスではサポートされません。
- UEFI モードで実行されている 32 ビットの Microsoft Windows 8、8.1、10 オペレーティングシステムはサポートされていません。
- 復号化されたハードドライブを再度暗号化するには、コンピューターを再起動してください。
- ハードドライブの暗号化は Kaspersky Anti-Virus for UEFI と互換性がありません。Kaspersky Anti-Virus for UEFI がインストールされているコンピューターでハードドライブの暗号化を使用してください。
- Microsoft アカウントに基づいた[認証エージェントアカウントの作成](#)は次の制限付きでサポートされません：
  - [シングルサインオン](#)技術はサポートされません。
  - 直近で特定の日数システムにログインしたユーザーにアカウントを作成するオプションを有効にしている場合、認証エージェントの自動アカウント作成はサポートされません。
- 認証エージェントのアカウント名が「<ドメイン>/<Windows アカウント名>」の形式である場合、コンピューター名を変更した後にそのコンピューターのローカルユーザー用に作成されたアカウント名も変更する必要があります。例えば、コンピューター「Ivanov」のローカルユーザー「Ivanov」があるとして、このユーザーに認証エージェントのアカウント名が「Ivanov/Ivanov」として作成された場合などです。コンピューター名「Ivanov」が「Ivanov-PC」に変更されると、ユーザー名「Ivanov」の認証エージェントのアカウント名 w p 「Ivanov/Ivanov」から「Ivanov-PC/Ivanov」に変更する必要があります。認証エージェントのローカルアカウント管理タスクを使用してアカウント名を変更することができます。アカウント名の変更前に、起動前環境の認証は古い名前（例「Ivanov/Ivanov」）を使用して認証することが可能です。
- Kaspersky Disk Encryption 技術を使用して暗号化されたコンピューターに、ユーザーがトークンを使用するのみアクセスが許可されており、このユーザーはアクセスの復元手順を完了する必要がある場合、このユーザーに、暗号化されたコンピューターへのアクセスが復元された後にコンピューターへのパスワードベースでのアクセスが許可されていることを確認してください。アクセスの復元時に設定されたパスワードは保存されない可能性があります。この場合、暗号化されたコンピューターが次回再起動された場合にこのコンピューターへのアクセスの復元手順を完了する必要があります。
- [FDE 復元ツール](#)を使用してハードドライブを復号化した場合、元のデバイスのデータが復号化されたデータで上書きされるとエラーが発生する可能性があります。ハードドライブのデータの一部は暗号化されたままになります。FDE 復元ツールを使用する際には、デバイス復号化設定で復号化されたデータを保存するオプションを選択してください。
- 認証エージェントのパスワードが変更された場合、パスワードは正常に変更されたことを示す文章を含むメッセージが表示されます。OK をクリックというメッセージが表示されてユーザーがコンピューターを再起動した場合、新しいパスワードは保存されません。起動前環境において続く認証では古いパスワードを使用する必要があります。
- ディスクの暗号化は Intel Rapid Start 技術とは互換性がありません。

- ディスクの暗号化は ExpressCache 技術とは互換性がありません。
- いくつかのケースでは、[FDE 復元ツール](#)を使用して暗号化されたドライブを復号化しようとする、「応答要求」手順が完了した後にツールが誤ってデバイスのステータスを「暗号化されていない」と検知することがあります。ツールのログには、デバイスは正常に復号化されたことを記載するイベントが表示されます。この場合、デバイスの復号化のためにデータ復元手順を再度開始する必要があります。
- Kaspersky Endpoint Security for Windows のプラグインが Web コンソールでアップデートされた後、Web コンソールが再開されるまではクライアントコンピューターのプロパティに BitLocker 回復キーが表示されません。
- ディスク全体の暗号化のサポートの制限事項および制限付きでサポートされるハードドライブの暗号化のデバイスのリストを確認するには、[テクニカルサポートのナレッジベースの記事](#)  を参照してください。

## [ファイルレベルの暗号化 \(FLE\)](#)



- ファイルおよびフォルダーの暗号化は Microsoft Windows Embedded ファミリーのオペレーティングシステムで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後、ファイルおよびフォルダーの暗号化が正常に動作するためにオペレーティングシステムを再起動する必要があります。
- 暗号化されたファイルが利用可能な暗号化機能のあるコンピューターに保存されており、暗号化機能の利用できないコンピューターからそのファイルにアクセスする場合、このファイルへの直接アクセスが提供されます。利用可能な暗号化機能を持つコンピューターのネットワークフォルダーに保存された暗号化されたファイルは、利用可能な暗号化機能を持たないコンピューターにコピーされる場合は復号化された形式でコピーされます。
- Kaspersky Endpoint Security for Windows でファイルを暗号化する前に、暗号化ファイルシステムで暗号化されたファイルを復号化してください。
- ファイルが暗号化されると、ファイルのサイズは 4 KB に増えます。
- ファイルの暗号化後、ファイルのプロパティにはアーカイブ属性が設定されます。
- 暗号化されたアーカイブから解凍されたファイルの名前がコンピューター上に既に存在するファイルと同じ名前だった場合、コンピューター上のファイルは暗号化されたアーカイブから解凍された新しいファイルで上書きされます。ユーザーには上書き操作について通知されません。
- 暗号化されたアーカイブを解凍する前に、解凍されたファイルを保管する空き容量が十分にあるかどうか確認してください。空き容量がない場合、アーカイブの解凍は完了しますが、ファイルが破損することがあります。この場合、Kaspersky Endpoint Security でエラーメッセージが表示されない可能性があります。
- [ポータブルファイルマネージャー](#) インターフェイスでは、その操作中に発生したエラーに関するメッセージは表示されません。
- Kaspersky Endpoint Security for Windows は、ファイルレベルの暗号化機能がインストールされたコンピューター上で [ポータブルファイルマネージャー](#) を開始しません。
- 次の条件を同時に満たす場合、[ポータブルファイルマネージャー](#) を使ってリムーバブルドライブにアクセスすることはできません：
  - Kaspersky Security Center に接続されていない。
  - Kaspersky Endpoint Security for Windows がコンピューターにインストールされている。
  - コンピューターでデータ暗号化（FDE または FLE）が実行されていない。

ポータブルファイルマネージャーのパスワードが分かってもアクセスできません。

- 暗号化が使用されると、アプリケーションは Sylphed メールクライアントとの互換性がなくなります。
- Kaspersky Endpoint Security for Windows では、特定のアプリケーションに対して [暗号化されたファイルへのアクセスを制限するルール](#) はサポートされません。これは、一部のファイル操作がサードパーティ製品によって実行されるためです。たとえば、ファイルのコピーは、アプリケーション自体ではなく、ファイルマネージャーによって実行されます。このようにして、暗号化されたファイルへのアクセスが Outlook メールクライアントに対し拒否された場合、ユーザーがクリップボードまたはドラッグアンドドロップ機能を使用してメールメッセージにファイルをコピーした際、Kaspersky Endpoint Security は、メールクライアントが暗号化されたファイルにアクセスできるようにします。コピー操作

は、暗号化されたファイルへのアクセス制限ルールが指定されていない、つまりアクセスが許可されているファイルマネージャーによって実行されました。

- リムーバブルドライブが[ポータブルモードのサポート](#)で暗号化された場合、パスワードの有効期間の制御は無効にできません。
- ページファイルの設定の変更はサポートされません。オペレーティングシステムはパラメータの値で指定されたものの代わりに既定値を使用します。
- 暗号化されたリムーバブルドライブの操作には安全な取り外しを使用してください。安全に取り外されていないリムーバブルドライブのデータ整合性は保証できません。
- ファイルが暗号化された後、暗号化されていない元のファイルは安全に削除されます。
- クライアントサイド キャッシュ (CSC) を使用したオフラインファイルの同期はサポートされません。共有リソースのオフライン管理はグループポリシーのレベルで禁止することを推奨します。オフラインモードのファイルは編集可能です。同期後、オフラインファイルへの変更は失われます。暗号化の使用時のクライアントサイドキャッシュ (CSC) のサポートに関する詳細については、[テクニカルサポートのナレッジベースの記事](#)を参照してください。
- システムハードドライブのルートでの[暗号化されたアーカイブの作成](#)はサポートされません。
- ネットワーク越しでの暗号化されたファイルへのアクセスでは問題が発生する可能性があります。このようなファイルは別の場所に移動するか、ファイルサーバーとして使用されているコンピューターが同じ Kaspersky Security Center 管理サーバーで管理されているか確認してください。
- キーボードのレイアウトの変更は自己解凍アーカイブのパスワード入力画面のフリーズの原因になる可能性があります。問題を解決するには、パスワード入力画面を閉じて、オペレーティングシステムのキーボードレイアウトに切り替え、再度暗号化されたアーカイブのパスワードを入力します。
- 1つのディスク上に複数のパーティションを持つシステムでファイルの暗号化が使用された際には、pagefile.sys ファイルのサイズを自動的に決定されるオプションを使用してください。コンピューターの再起動後、pagefile.sys ファイルはディスクパーティション間で移動される可能性があります。
- マイドキュメントフォルダー内のファイルを含むファイルの暗号化ルールの適用後、暗号化が適用されたユーザーが問題なく暗号化されたファイルにアクセスできることを確認してください。Kaspersky Security Center への接続が利用可能な時に、各ユーザーにシステムへのサインインを依頼してください。Kaspersky Security Center への接続がない状態で暗号化されたファイルにアクセスした場合、システムがフリーズすることがあります。
- ファイルレベルの暗号化の範囲にシステムファイルが含まれていた場合、これらのファイルの暗号化の際のエラーについてのイベントがレポートに表示されることがあります。これらのイベント内で指定されたファイルは実際には暗号化されていません。
- ピコプロセスはサポートされません。
- パスの大文字小文字の区別はサポートされません。暗号化ルールまたは復号化ルールが適用された際、製品イベントのパスはすべて小文字で表示されます。
- スタートアップ時にシステムが使用するファイルの暗号化はお勧めしません。これらのファイルが暗号化されると、Kaspersky Security Center への接続がないときに暗号化されたファイルにアクセスすると、システムのフリーズが起きたり、暗号化されていないファイルへのアクセスを促されたりします。
- ユーザーが WordPad または FAR のようなメモリマップファイル方式を使用したアプリケーションまたは Notepad ++ などの大きなファイルで作業するために設計されたアプリケーションを介して FLE ルールが適用されたネットワークを介してファイルで作業する場合、暗号化されていない形式のファイルはファイルのあるコンピューターからのアクセスが無制限にブロックされる可能性があります。

- OneDrive 同期フォルダーのファイル暗号化はサポートされていません。暗号化済みのファイルを含むフォルダーを OneDrive 同期リストに追加すると、暗号化されたファイル内のデータの損失につながる可能性があります。
- ファイルレベルの暗号化機能がインストールされていると、WSL (Windows Subsystem for Linux) モードではユーザーおよびグループの管理は機能しません。
- ファイルレベルの暗号化機能がインストールされている際にはファイルの名前変更および削除の POSIX (Portable Operating System Interface) はサポートされません。
- データが消失する可能性があるため、一時ファイルの暗号化は推奨されません。たとえば、Microsoft Word は文書の処理中に一時ファイルを作成します。一時ファイルが暗号化されて、元のファイルが暗号化されていない場合、文書を保存する際に「アクセスが拒否されました」というエラーが表示される可能性があります。さらに、Microsoft Word がファイルを保存することはできても、データが消失して次回文書を開くことができなくなる問題が発生する可能性があります。このようなデータの消失を防ぐには、暗号化ルールから一時ファイルフォルダーを除外する必要があります。
- Kaspersky Endpoint Security for Windows のバージョン 11.0.1 以前のバージョンからのアップデート後、コンピューターの再起動後に暗号化されたファイルにアクセスするため、ネットワークエージェントが実行されていることを確認してください。ネットワークエージェントの開始は遅延されるため、オペレーティングシステムの読み込み直後には暗号化されたファイルにアクセスすることはできません。次回のコンピューターの開始以降はネットワークエージェントの開始を待つ必要はありません。

## その他の制限事項

- [信頼リストに追加された](#) Wen アドレスが誤って処理されることがあります。
- システムウォッチャー。プロセスに関する完全な情報は表示されません。
- Kaspersky Endpoint Security for Windows のh疎開起動時、デジタル署名されたアプリケーションは一時的に正しくないグループに配置されることがあります。デジタル署名されたアプリケーションはのちに正しいグループに配置されます。
- [メール脅威対策のMicrosoft Outlook のアドイン](#)でメールをスキャンする際、Exchange キャッシュモードの使用オプションで Exchange キャッシュモードを使用してください。
- [スキャンタスク](#)は 64 ビットの Microsoft Outlook をサポートしません。つまり、[スキャン範囲にメールが含まれている](#)場合でも、Kaspersky Endpoint Security は Outlook x64 のファイル（PST および OST ファイル）をチェックしません。
- Kaspersky Security Center 10 では、グローバル Kaspersky Security Network からプライベート Kaspersky Security Network の使用に切り替えたりその逆に切り替えたりする際に、特定の製品のポリシー内の[Kaspersky Security Network への参加設定のオプションが無効](#)になります。切り替え後、Kaspersky Security Network に関する声明を読み、KSN への参加の設定に同意してください。声明の内容については、製品のインターフェイスから、または製品ポリシーの編集時に確認することができます。
- サードパーティのソフトウェアによりブロックされた悪意のあるオブジェクトの再スキャン中に、その脅威が再度検知されたことはユーザーには通知されません。脅威の再検知イベントは製品レポートおよび Kaspersky Security Center 10 のレポートに表示されます。
- [Endpoint Sensor](#) 機能は Microsoft Windows Server 2008 にインストールできません。
- デバイスの暗号化に関する Kaspersky Security Center 10 レポートには、デバイスコントロール機能がインストールされていないサーバープラットフォームまたはワークステーション上にある Microsoft BitLocker を使用して暗号化されたデバイスに関する情報は含まれません。
- Kaspersky Security Center Web コンソールでは、すべてのレポート項目の表示を有効にすることはできません。Web コンソールでは、レポート内で表示される項目の数のみ変更できます。既定では、Kaspersky Security Center Web コンソールは 1000 個のレポート項目を表示します。管理コンソール（MMC）ではすべてのレポート項目の表示を有効にできます。
- Kaspersky Security Center コンソールでは、1000 以上のレポート項目の表示を設定することはできません。1000 以上の値を設定すると、Kaspersky Security Center コンソールは 1000 項目のみ表示します。
- ポリシー階層を使用している際、親ポリシーがこれらの設定を禁止している場合に、子ポリシーのリムーバブルドライブの暗号化セクションの設定は、編集のためのアクセスが可能です。
- [外部からの暗号化の試みに対して共有フォルダーを保護するための除外設定](#)が正常に動作するためにオペレーティングシステムの設定内で監査ログオンを有効にする必要があります。
- [共有フォルダーの保護が有効になっていると](#)、Kaspersky Endpoint Security for Windows は、リモートアクセスセッションが開始されたコンピューターが除外リストに追加されている場合も含め、Kaspersky Endpoint Security for Windows の開始前に開始されたリモートアクセスセッションが共有フォルダーを暗号化しようとする動作を監視します。Kaspersky Endpoint Security for Windows の開始より前に開始された、除外リストに追加されたコンピューターから開始されたリモートアクセスセッションからの共有フォルダーの暗号化の操作の監視を有効にしない場合はリモートアクセスセッションを遮断して再度確立するか、Kaspersky Endpoint Security for Windows がインストールされたコンピューターを再起動してください。



- アップデートタスクが特定のユーザーアカウントの権限で実行されている場合、認証が必要なダウンロード元からアップデートする場合製品パッチはダウンロードされません。
- システムのパフォーマンスが十分でない場合アプリケーションの開始が失敗することがあります。この問題を解決するには、Ready Boot オプションを使用するか、サービスの開始のためのオペレーティングシステムのタイムアウトを増やしてください。
- 本製品はセーフモードでは動作しません。
- Kaspersky Endpoint Security for Windows のバージョン 11.5.0 および 11.6.0 が Cisco AnyConnect ソフトウェアと正常に連携するには、コンプライアンス モジュールのバージョン 4.3.183.2048 以降がインストールされている必要があります。Cisco Identity Services Engine との互換性については、[Cisco のマニュアル](#)を参照してください。
- 本製品のインストール後、初回の再起動までオーディオコントロールの正常な動作は保証しません。
- 管理コンソール (MMC) では、アプリケーションの権限の設定ウィンドウの侵入防止設定の [削除] ボタンは使用できません。本製品のコンテキストメニューを使用してアプリケーションを信頼グループから削除することができます。
- コンピューターがポリシーによって管理されている場合、本製品のローカルインターフェイスでは侵入防止設定のアプリケーションと保護対象のリソースは表示できません。スクロール、検索、フィルターおよびその他のウィンドウコントロールは利用できません。アプリケーションの権限は Kaspersky Security Center コンソールのポリシーのプロパティで表示できます。
- トレースのローテーションが有効になっていると、AMSI コンポーネントおよび Outlook アドインにはトレースファイルは作成されません。
- パフォーマンスのトレースは Windows Server 2008 では手動で収集できません。
- 「再起動」トレース種別のパフォーマンスのトレースはサポートされていません。
- ピコプロセスについてログのダンプはサポートされていません。
- KSN の利用状況のチェックタスクはサポートされなくなりました。
- システムサービスの外部管理の無効化のオプションをオフにすると、パラメータ「AMPPL=1」（既定ではパラメータの値は 1 に設定されており、Windows 10RS2 オペレーティングシステムバージョンから開始されます）でインストールされた本製品のサービスの停止ができなくなります。パラメータ「AMPPL」の値を 1 にすると、保護プロセス技術を製品サービスに対して使用できるようになります。
- フォルダーに対してオブジェクトスキャンを実行するには、スキャンを実行するユーザーがそのフォルダーの読み取り権限を持っている必要があります。そうでない場合はスキャンは実行できず、エラーで終了します。
- ポリシーで定義されるスキャンルールに、行末に文字「\」がついていないパスが含まれる場合、例えば「C:\folder1\folder2」のように記載されている場合は、スキャンは C:\folder1\ に対して実行されます。
- 製品のバージョン 11.1.0 から 11.7.0 にアップグレードする場合、AMSI 保護の設定は既定値にリセットされます。
- ソフトウェアの制限のポリシー (SRP) を使用している場合、コンピューターが読み込みに失敗することがあります (真っ黒な画面)。ソフトウェアの制限のポリシーを次の通り変更してください：[ソフトウェアの制限のポリシーの適用ユーザー] に、[DLL などのライブラリを除くソフトウェアのファイルすべて] を選択し、本製品のパス (C:\Program Files\Common Files\Kaspersky Lab およ

び C:\Program Files\Kaspersky Lab) にセキュリティレベル [制限しない] を追加してください。SRP の使用について詳しくは、[Microsoft 社の資料](#) を参照してください。

- Rest API 経由での Outlook プラグインの管理はサポートされません。
- 特定のユーザーのタスク実行設定は、設定ファイルを介してデバイス間で転送することはできません。設定ファイルから設定を適用した後、ユーザー名およびパスワードを手動で指定してください。
- アップデートのインストール後、整合性チェックタスクはシステムが再起動してアップデートが適用されるまで動作しません。
- リモート診断ユーティリティを介してトレースのローテーションレベルが変更された場合、Kaspersky Endpoint Security for Windows はトレースレベルに空白の値を表示します。しかし、トレースファイルは正しいトレースレベルに基づいて書き込まれます。トレースレベルが本製品音ローカルインターフェイスを介して変更された場合、トレースレベルは正しく編集されますが、リモート診断ユーティリティは、ユーティリティが最後に定義した正しくないトレースレベルを表示します。これにより、ユーザーがローカルの製品インターフェイスでトレースレベルを手動で編集すると、管理者が現在のトレースレベルに関する最新情報が把握できず、関連する情報が欠如することがあります。
- ローカルのインターフェイスでは、パスワードによる保護の設定で、管理者アカウント（既定では KLAdmin）の名前の変更は許可されていません。管理者アカウントの名前を変更するには、パスワードによる保護を一度無効にしてから有効にし、管理者アカウントの新しい名前を指定してください。
- Kaspersky Endpoint Security は RFC 2616、RFC 7540、RFC 7541、RFC 7301 に適合する HTTP トラフィックを監視します。HTTP トラフィックに別のデータ交換形式を検知すると、Kaspersky Endpoint Security はインターネットからの悪意のあるファイルのダウンロードを防止するため、接続をブロックします。
- 暗号化された接続をスキャンする際、Kaspersky Endpoint Security は強制的に HTTP/1 を使用します。
- [ファイルを隔離する](#) タスクの結果として隔離されたオブジェクトをスキャンすることはできません。
- Kaspersky Endpoint Security はタスクのプロパティ内のフォルダーのパスがドライブ文字から始まるネットワークドライブに対して [IOC スキャン](#) タスクを実行しません。Kaspersky Endpoint Security はネットワークドライブの IOC スキャンタスクでは UNC パスのみサポートしています。例：  
\\server\shared\_folder
- [Kaspersky Sandbox との連携](#) 設定が設定ファイルで有効になっている場合、[製品設定ファイルのインポート](#) はエラーが発生して終了します。製品設定をエクスポートする前に、Kaspersky Sandbox を無効にしてください。それからエクスポートまたはインポートの手順を実行してください。設定ファイルのインポート後に、Kaspersky Sandbox を有効にします。
- [IOC スキャン](#) タスクの実行中に侵害インジケーターが検知された場合、本製品は Fileitem タームでのみファイルを隠します。その他のタームでの隔離はサポートされません。
- 4 MB より大きい代替データストリーム (ADS) を隔離することはできません。Kaspersky Endpoint Security はこのような ADS をユーザーに通知せずスキップします。
- アラートの詳細を管理するには、Kaspersky Endpoint Security for Windows 11.7.0 以降向けの Web プラグインが必要です。アラートの詳細は [Endpoint Detection and Response](#) ソリューション (EDR Optimum および EDR Expert) で必要になります。アラートの詳細は Kaspersky Security Center Web コンソール および Kaspersky Security Center Cloud コンソールでのみ使用可能です。
- Windows Server 2019 サーバー上に Kaspersky Endpoint Security をインストールした場合、Docker とは互換性がありません。Kaspersky Endpoint Security がインストールされたコンピューターに Docker コンテナを導入するとクラッシュ (BSOD) が発生します。

# 用語解説

## IOC

侵害インジケーター。悪意のあるオブジェクトまたは活動に関するデータ一式。

## IOC ファイル

侵害インジケーター (IOC) を含むファイルで、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。スキャンの結果として複数の IOC ファイル内の項目と一致した場合は、検知の可能性がより高くなります。

## OLE オブジェクト

別のファイルに埋め込まれた添付ファイルまたはファイル。カスペルスキー製品は、OLE オブジェクトにウイルスがあるかどうかスキャンします。たとえば、Microsoft Office Excel® のテーブルを Microsoft Office Word 文書に挿入する場合、テーブルは OLE オブジェクトとしてスキャンされます。

## OpenIOC

公開されている侵害インジケーター (IOC) の規格で、XML に基づいて記述されており、500 を超える侵害インジケーターが含まれています。

## Trusted Platform Module

セキュリティに関連する基本的な機能（暗号鍵の保存など）を提供するために開発されたマイクロチップ。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。

## Web リソースアドレスの正規化された形式

Web リソースの正規化された形式のアドレスは Web リソースアドレスのテキスト表記で、正規化によって取得されます。正規化は、Web リソースアドレスのテキスト表記を特定のルール（ユーザーログインの除外、パスワード、Web リソースアドレスのテキスト表記の接続ポート、Web リソースアドレスを大文字から小文字に変更するかなど）に従って変更するプロセスです。

保護機能では、Web リソースアドレスの正規化は、物理的には同じでも構文上は異なる可能性がある Web サイトのアドレスが何度もスキャンされるのを回避することを目的としています。

例：

正規化されていない形式のアドレス：www.Example.com\  
正規化された形式のアドレス：www.example.com



## アーカイブ

1つの圧縮ファイルにまとめられた1つまたは複数のファイル。データの圧縮および回答には、アーカイバと呼ばれる専用のアプリケーションが必要です。

## 悪意のある URL のデータベース

危険とみなされるコンテンツを含む Web アドレスのリスト。このリストは、カスペルスキーによって作成されます。このリストは定期的にアップデートされ、カスペルスキー製品の配信キットに含まれます。

## 感染可能なファイル

ファイルの構造または形式により、侵入者が悪意のあるコードを保存して拡散させるための「入れ物」として使用できるファイル。一般的には、com、exe、dll などの拡張子を持つ実行ファイルです。このようなファイルには、悪意のあるコードが含まれるリスクが非常に高いです。

## 感染したファイル

悪意のあるコードを含むファイル（ファイルのスキャンにより、既知のマルウェアのコードが検知された）。このようなファイルは、コンピューターを感染させる可能性があるため、使用しないでください。

## 管理グループ

共通の機能を共有し、インストールされている一連のカスペルスキー製品を共有する一連のデバイス。デバイスは、便宜上1つのユニットとして管理できるようにグループ化されます。グループには他のグループを含めることができます。グループポリシーを作成したり、グループにインストールされている各アプリケーションに対してグループタスクを作成したりすることができます。

## 駆除

感染しているオブジェクトの処理方法の1つ。駆除の結果、データが完全に復元するかまたは部分的に復元します。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。

## 現在のライセンス

製品によって現在使用されているライセンス。

## 誤検知

ファイルの署名がウイルスの署名に似ているため、カスペルスキー製品が未感染のファイルを感染していると報告すると、誤報が発生します。

## 証明書の発行元

証明書を発行した認証局。

## スキャン範囲

スキャンタスクの実行時に、Kaspersky Endpoint Security によってスキャンされるオブジェクト。

## タスク

カスペルスキー製品によってタスクとして実行される機能：たとえば、リアルタイムファイル保護、フルデバイススキャン、データベースのアップデート。

## 定義データベース

カスペルスキーが把握しているコンピューターセキュリティ上の脅威の情報が含まれるデータベース。データベースの公開時点までの情報が含まれています。定義データベースの署名は、スキャン対象のオブジェクト内の悪意のあるコードの検知に役立ちます。定義データベースは、カスペルスキーのエキスパートによって作成され、1時間ごとにアップデートされます。

## 認証エージェント

起動可能なハードディスクが暗号化された後で、暗号化されたハードディスクにアクセスしオペレーティングシステムを読み込むための認証を実行するインターフェイス。

## ネットワークエージェント

特定のネットワークノード（ワークステーションまたはサーバー）にインストールされている管理サーバーとカスペルスキー製品の相互作用を可能にする Kaspersky Security Center のコンポーネント。このコンポーネントは、Windows で実行されるすべてのカスペルスキー製品に標準装備されています。その他のオペレーティングシステムで実行される製品については、専用バージョンのネットワークエージェントを用意しています。

## フィッシングサイトの URL のデータベース

カスペルスキーがフィッシング関連であると判断した Web アドレスのリスト。定義データベースは定期的なアップデートされ、カスペルスキー製品の配信キットの一部となっています。

## ポータブルファイルマネージャー

リムーバブルドライブ上の暗号化ファイルを使用するためのインターフェイスを提供するアプリケーション。暗号化機能がコンピューターにない場合に使用できます。

## 保護範囲

脅威対策の実行中に常にスキャンされているオブジェクト。各コンポーネントの保護範囲には、それぞれ異なる特性があります。

## マスク

ワイルドカードを使用したファイル名および拡張子の表示。

ファイルマスクには、ワイルドカードを含む、ファイル名に使用可能な文字をすべて含めることができます：

- 「\*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C:ドライブ上のフォルダーにある拡張子がtxtのすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
- 2つの連続した「\*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子がtxtのすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。「\*\*」というマスクは、スキャンからの除外リストの作成でのみ使用できます。
- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子がtxtでファイル名が3文字のすべてのファイルのパスを含みます。

## 予備のライセンス

製品を使用する権限を認定する、現在使用されていないライセンス。

## ライセンス証明書

カスペルスキーが、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と合わせてユーザーに転送するドキュメント。ユーザーに許諾されたライセンスに関する情報が記載されています。

## 補足資料

このセクションには、本ドキュメントの内容を補足する内容が含まれています。

### 補足資料 1：製品設定

[ポリシー](#)、[タスク](#)、[製品インターフェイス](#)を使用して Kaspersky Endpoint Security を設定します。製品の各機能に関して詳しくは、それぞれの機能の該当セクションを参照してください。

## File Threat Protection

The File Threat Protection component lets you prevent infection of the file system of the computer. By default, the File Threat Protection component permanently resides in the computer's RAM. The component scans files on all drives of the computer, as well as on connected drives. The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

The component scans the files accessed by the user or application. If a malicious file is detected, Kaspersky Endpoint Security blocks the file operation. The application then disinfects or deletes the malicious file, depending on the settings of the File Threat Protection component.

When attempting to access a file whose contents are stored in the OneDrive cloud, Kaspersky Endpoint Security downloads and scans the file contents.

File Threat Protection component settings

Parameter	Description
<b>Security level</b> <i>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</i>	<p>For File Threat Protection, Kaspersky Endpoint Security can apply different groups of settings. These groups of settings that are stored in the application are called <i>security levels</i>:</p> <ul style="list-style-type: none"><li>• <b>High.</b> When this file security level is selected, the File Threat Protection component takes the strictest control of all files that are opened, saved, and started. The File Threat Protection component scans all file types on all hard drives, removable drives, and network drives of the computer. It also scans archives, installation packages, and embedded OLE objects.</li><li>• <b>Recommended.</b> This file security level is recommended by Kaspersky Lab experts. The File Threat Protection component scans only the specified file formats on all hard drives, removable drives, and network drives of the computer, and embedded OLE objects. The File Threat Protection component does not scan archives or installation packages.</li><li>• <b>Low.</b> The settings of this file security level ensure maximum scanning speed. The File Threat Protection component scans only files with specified extensions on all hard drives, removable drives, and network drives of the computer. The File Threat Protection component does not scan compound files.</li></ul>
<b>File types</b>	<b>All files.</b> If this setting is enabled, Kaspersky Endpoint Security checks all files without exception (all formats and extensions).

<p><i>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</i></p>	<p><b>Files scanned by format.</b> If this setting is enabled, Kaspersky Endpoint Security scans <a href="#">infectable files only</a> [?]. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). The scan also looks for files with particular file extensions.</p> <p><b>Files scanned by extension.</b> If this setting is enabled, Kaspersky Endpoint Security scans <a href="#">infectable files only</a> [?]. The file format is then determined based on the file's extension.</p>
<p><b>File Threat Protection scope</b></p>	<p>Contains objects that are scanned by the File Threat Protection component. A scan object may be a hard drive, removable drive, network drive, folder, file, or multiple files defined by a mask.</p> <p>By default, the File Threat Protection component scans files that are started on any hard drives, removable drives, or network drives. The protection scope for these objects cannot be changed or deleted. You can also exclude an object (such as removable drives) from scans.</p>
<p><b>Machine learning and signature analysis</b> <i>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</i></p>	<p>The machine learning and signature analysis method uses the Kaspersky Endpoint Security databases that contain descriptions of known threats and ways to neutralize them. Protection that uses this method provides the minimum acceptable security level.</p> <p>Based on the recommendations of Kaspersky experts, machine learning and signature analysis is always enabled.</p>
<p><b>Heuristic Analysis</b> <i>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</i></p>	<p>The technology was developed for detecting threats that cannot be detected by using the current version of Kaspersky application databases. It detects files that may be infected with an unknown virus or a new variety of a known virus.</p> <p>When scanning files for malicious code, the heuristic analyzer executes instructions in the executable files. The number of instructions that are executed by the heuristic analyzer depends on the level that is specified for the heuristic analyzer. The heuristic analysis level ensures a balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.</p>
<p><b>Action on threat detection</b></p>	<p><b>Disinfect; delete if disinfection fails.</b> If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.</p> <p><b>Disinfect; block if disinfection fails.</b> If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.</p> <p><b>Block.</b> If this option is selected, the File Threat Protection component automatically blocks all infected files without attempting to disinfect them.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Before attempting to disinfect or delete an infected file, Kaspersky Endpoint Security creates a backup copy of the file in case you need to <a href="#">restore the file or if it can be disinfected in the future</a>.</p> </div>

<b>Scan only new and changed files</b>	<p>Scans only new files and those files that have been modified since the last time they were scanned. This helps reduce the duration of a scan. This mode applies both to simple and to compound files.</p>
<b>Scan archives</b>	<p>Scans archives in the following formats: RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE. Kaspersky Endpoint Security scans archives not only by file extension, but also by format.</p>
<b>Scan distribution packages</b>	<p>This check box enables/disables scanning of third-party distribution packages.</p>
<b>Scan files in Microsoft Office formats</b>	<p>Scans Microsoft Office files (DOC, DOCX, XLS, PPT and other Microsoft extensions). Office format files include OLE objects as well.</p>
<b>Do not unpack large compound files</b>	<p>If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the specified value.</p> <p>If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.</p> <div data-bbox="376 797 1493 920" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security scans large files that are extracted from archives regardless of whether the check box is ticked or not.</p> </div>
<b>Unpack compound files in the background</b>	<p>If the check box is selected, Kaspersky Endpoint Security provides access to compound files that are larger than the specified value before these files are scanned. In this case, Kaspersky Endpoint Security unpacks and scans compound files in the background.</p> <p>Kaspersky Endpoint Security provides access to compound files that are smaller than this value only after unpacking and scanning these files.</p> <p>If the check box is not selected, Kaspersky Endpoint Security provides access to compound files only after unpacking and scanning files of any size.</p>
<b>Scan mode</b> <i>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</i>	<div data-bbox="376 1330 1493 1453" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security scans files accessed by the user, operating system, or an application running under the user's account.</p> </div> <p><b>Smart mode.</b> In this mode, File Threat Protection scans an object based on an analysis of actions taken on the object. For example, when working with a Microsoft Office document, Kaspersky Endpoint Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.</p> <p><b>On access and modification.</b> In this mode, File Threat Protection scans objects whenever there is an attempt to open or modify them.</p> <p><b>On access.</b> In this mode, File Threat Protection scans objects only upon an attempt to open them.</p> <p><b>On execution.</b> In this mode, File Threat Protection only scans objects upon an attempt to run them.</p>
<b>iSwift Technology</b>	<p>This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings. The iSwift technology is an advancement of the iChecker technology for the NTFS file system.</p>

<p>(available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</p>	
<p><b>iChecker Technology</b> (available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</p>	<p>This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scans by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date when the file was last scanned, and any modifications to the scan settings. There are limitations to iChecker Technology: it does not work with large files and applies only to files with a structure that the application recognizes (for example, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, and RAR).</p>
<p><b>Pause File Threat Protection</b> (available only in the Administration Console (MMC) and in the Kaspersky Endpoint Security interface)</p>	<p>This temporarily and automatically pauses operation of File Threat Protection at the specified time or when working with the specified applications.</p>

## ウェブ脅威対策

ウェブ脅威対策は、インターネットからの悪意のあるファイルのダウンロードを防ぎ、悪意のある Web サイトやフィッシングサイトをブロックします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

Kaspersky Endpoint Security では、HTTP、HTTPS、FTP のトラフィック、URL、IP アドレスがスキャンされます。[Kaspersky Endpoint Security で監視するポートを指定する](#)か、すべてのポートを監視対象として選択できます。

HTTPS トラフィックをスキャンするには、[暗号化された接続のスキャンを有効にする](#)必要があります。

ユーザーが、悪意のある Web サイトやフィッシングサイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックし、警告を表示します（下の図を参照）。





Web サイトへのアクセスが拒否されたことを示すメッセージ

ウェブ脅威対策の設定

パラメータ	説明
<p><b>セキュリティレベル</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>ウェブ脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループはセキュリティレベルと呼ばれます：</p> <ul style="list-style-type: none"> <li> <b>高</b>：HTTP や FTP 経由でコンピューターが受信する Web トラフィックをウェブ脅威対策が最大限にスキャンするときのセキュリティレベル。ウェブ脅威対策は、あらゆる定義データベースを使用してすべての Web トラフィックオブジェクトを詳細にスキャンし、最も徹底的な <a href="#">ヒューリスティック分析</a> を実行します。         </li> <li> <b>推奨</b>：Kaspersky Endpoint Security のパフォーマンスと Web トラフィックのセキュリティの間で最適なバランスが取れたセキュリティレベル。ウェブ脅威対策は <b>中</b> スキャンレベルでヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、この Web トラフィックセキュリティレベルを推奨しています。         </li> <li> <b>低</b>：この Web トラフィックセキュリティレベルの設定により、Web トラフィックのスキャンの速度が最大になります。ウェブ脅威対策は <b>低</b> スキャンレベルでヒューリスティック分析を実行します。         </li> </ul>
<p><b>脅威の検知時の処理</b></p>	<p><b>ダウンロードのブロック</b>：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザ上に表示します。</p> <p><b>通知する</b>：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。</p>
<p><b>悪意のある Web アドレスのデータベースで Web アドレスをチェックする</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。</p>

<p><b>ヒューリスティック分析を使用する</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
<p><b>フィッシングサイトのデータベースで Web アドレスをチェックする</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。</p>
<p><b>信頼する URL の Web トラフィックをスキャンしない</b></p>	<p>このチェックボックスをオンにすると、ウェブ脅威対策は、信頼する Web サイトにアドレスが含まれている Web ページ / Web サイトのコンテンツをスキャンしません。信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。</p>

## メール脅威対策

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、悪意のあるリンクやフィッシングリンクのメッセージもスキャンします。既定では、メール脅威対策はコンピューターの RAM に常駐し、POP3、SMTP、IMAP、NNTP プロトコル、または Microsoft Office Outlook メールクライアント (MAPI) を使用して送受信されるすべてのメッセージをスキャンします。このコンポーネントは、定義データベース、[Kaspersky Security Network クラウドサービス](#)、およびヒューリスティック分析を使用してコンピューターを保護します。

メールクライアントがブラウザで開いている場合、メール脅威対策はメッセージをスキャンしません。

添付ファイルで悪意のあるファイルが検知されると、Kaspersky Endpoint Security はメッセージの件名を「[Message infected] <メッセージの元の件名>」または「[Infected object deleted] <メッセージの元の件名>」に変更します。

このコンポーネントは、コンピューターにインストールされているメールクライアントと連携します。Microsoft Office Outlook メールクライアントの場合、[追加のパラメータを持つ拡張機能](#)が提供されます。メール脅威対策の機能拡張は、Kaspersky Endpoint Security のインストール中に Microsoft Office Outlook メールクライアントに組み込まれます。

#### メール脅威対策の設定

パラメータ	説明
<b>セキュリティレベル</b> (管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)	<p>メール脅威対策では、異なる設定の組み合わせを適用します。本製品に保存されているこれらの設定のグループはセキュリティレベルと呼ばれます：</p> <ul style="list-style-type: none"> <li> <b>高</b>：このメールセキュリティレベルを選択すると、メール脅威対策は最も厳格にメールをスキャンします。メール脅威対策は送受信されたメールメッセージをスキャンし、徹底的なヒューリスティック分析を実行します。リスクの高い環境で作業している場合には [高] メールセキュリティレベルが推奨されます。このような環境の例としては、一元化されたメールアンチウイルスで守られていない家庭用ネットワークからのフリーメールサービスへの接続などがあります。         </li> <li> <b>推奨</b>：Kaspersky Endpoint Security のパフォーマンスとメールのセキュリティの間で最適なバランスが取れたメールセキュリティレベル。メール脅威対策は送受信メールをスキャンし、中レベルのヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、このメールセキュリティレベルを推奨しています。         </li> <li> <b>低</b>：このメールセキュリティレベルを選択すると、メール脅威対策は受信メールのみをスキャンし、簡易ヒューリスティック分析を実行します。メールに添付されている圧縮ファイルはスキャンしません。このメールセキュリティレベルでは、オペレーティングシステムのリソースの使用を最小限に抑えながら、メールのスキャン速度が最大化します。「低」メールセキュリティレベルは、十分に保護された環境で作業している場合に推奨されます。このような環境の例としては、一元化されたメールセキュリティが適用された企業 LAN などがあります。         </li> </ul>
<b>脅威の検知時の処理</b>	<p><b>駆除する。駆除できない場合は削除する</b>：感染したオブジェクトが送受信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security は感染したオブジェクトを削除します。Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「[Infected object was deleted] &lt;メッセージの元の件名&gt;」に変更します。</p> <p><b>駆除する。駆除できない場合はブロックする</b>：感染したオブジェクトが受信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security はメッセージの件名に警告を追加して、件名を「[Message infected] &lt;メッセージの元の件名&gt;」に変更します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、Kaspersky Endpoint Security は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、Kaspersky Endpoint Security はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。</p> <p><b>ブロック</b>：感染したオブジェクトが受信メッセージで検知された場合、Kaspersky Endpoint Security はメッセージの件名に警告を追加して、件名を「[Message infected] &lt;メッセージの元の件名&gt;」に変更します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、Kaspersky Endpoint Security はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。</p>
<b>保護範囲</b>	<p>保護範囲には、機能の実行中にチェックするオブジェクトが含まれます：<b>送受信メッセージ</b>または<b>受信メッセージ</b>。</p>

<p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。</p>
<p><b>POP3、SMTP、NNTP、IMAP トラフィックのスキャン</b></p>	<p>このチェックボックスでは、POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメールをメール脅威対策でスキャンするかどうかを選択します。</p>
<p><b>Microsoft Outlook アドインに接続</b></p>	<p>このチェックボックスをオンにすると、POP3、SMTP、NNTP、IMAP プロトコルで送信されるメールのスキャンは、Microsoft Outlook に組み込まれた拡張機能側で有効になります。</p> <p>メールのスキャンに Microsoft Outlook 用機能拡張を使用している場合は、Exchange キャッシュモードを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、<a href="#">マイクロソフトサポート技術情報</a>を参照してください。</p>
<p><b>ヒューリスティック分析</b></p> <p>(管理コンソール (MMC) および Kaspersky Endpoint Security のインターフェイスでのみ利用可能)</p>	<p>この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。</p> <p>悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。</p>
<p><b>添付のアーカイブのスキャン</b></p>	<p>次の形式のアーカイブのファイルのスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR および ICE。</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>スキャン中に Kaspersky Endpoint Security がメッセージ本文に圧縮ファイルのパスワードを検出した場合は、このパスワードを使用して圧縮ファイルの内容に対して悪意のあるアプリケーションのスキャンを実行します。この場合、パスワードは保存されません。圧縮ファイルはスキャン中に解凍されます。圧縮ファイルの解凍中にアプリケーションでエラーが発生した場合、次のパスに保存されたファイルを手動で削除できます：%systemroot%\temp。このファイルには接頭辞 PR が付いています。</p> </div>
<p><b>添付の Office 形式ファイル</b></p>	<p>Microsoft Office 形式のファイルのスキャンします (DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル)。Office 形式のファイルには OLE オブジェクトが含まれます。</p>



ルをスキャン	
次のサイズを超えるアーカイブをスキャンしない	このチェックボックスをオンにすると、メール脅威対策が指定したサイズを超える、メールメッセージに添付されたアーカイブをスキャンしません。このチェックボックスをオフにすると、添付オブジェクトのサイズに関係なく、メール脅威対策がメール添付のアーカイブをスキャンします。
アーカイブのスキャンの時間を制限する	このチェックボックスを選択すると、メールメッセージに添付されたアーカイブのスキャンに割り当てられる時間が指定の時間に制限されます。
添付ファイルのフィルター	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;">           添付ファイルのフィルター機能は、送信されるメールには適用されません。         </div> <p><b>フィルタリングを無効にする</b>：このオプションをオンにした場合、メール脅威対策は、メールに添付されているファイルをフィルター処理しません。</p> <p><b>選択した種別の添付ファイルの名前を変更する</b>：このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。</p> <p><b>選択した種別の添付ファイルを削除する</b>：このオプションをオンにした場合、メール脅威対策は特定の種類の添付ファイルをメールから削除します。</p> <p>ファイルマスクのリストを使用して、メール上で名前を変更あるいはファイル自体を削除する添付ファイル種別を指定できます。</p>

## ネットワーク脅威対策

ネットワーク脅威対策は、受信ネットワークトラフィックをスキャンし、典型的なネットワーク攻撃の活動をチェックします。Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、Kaspersky Endpoint Security データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、[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](#)時にアップデートされます。

ネットワーク脅威対策の設定

パラメータ	説明
ポートのスキャンおよびネットワークフラッシングを攻撃として扱う	<p>ネットワークフラッシングとは、Web サーバーなど、企業のネットワークリソースに対する攻撃を意味します。これは、大量のリクエストを送信し、ネットワークリソースの帯域幅をオーバーロードさせる攻撃です。攻撃されると、ユーザーは企業のネットワークリソースにアクセスできなくなります。</p> <p>ポートのスキャンとは、コンピューターの UDP ポート、TCP ポート、ネットワークサービスをスキャンする攻撃を意味します。これにより、攻撃者がコンピューターの脆弱性を把握して、より悪質な攻撃を仕掛けることができるようになります。また、コンピューターのオペレーティングシステムを識別し、そのオペレーティングシステムに適したネットワーク攻撃を行うためにポートがスキャンされることもあります。</p>

	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security はこれらの攻撃を検知するためネットワークトラフィックを監視します。攻撃が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。また、脅威の対応処理を迅速に行うために必要な、攻撃元のコンピューターに関する情報が提供されます。</p> <p>一部の許可されるアプリケーションがこのような攻撃と似た動作を行う場合は、これらの検知機能を無効にすることができます。これにより誤検知を減らすことができます。</p>
<b>攻撃元コンピューターをブロックする時間</b>	<p>このチェックボックスをオンにすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は1分です。最大値は32768分です。</p> <p>ブロックのリストは<a href="#">ネットワークモニターツール</a>ウィンドウで表示できます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。</p> </div>
<b>除外リスト</b>	<p>IP アドレスのリストです。ネットワーク脅威対策は、このリストに掲載される IP アドレスからのネットワーク攻撃をブロックしません。</p> <p>除外リストに含まれる IP アドレスからのネットワーク攻撃に関する情報は、ログに記録されません。</p>
<b>MAC スプーフィング対策</b>	<p>MAC スプーフィング攻撃では、ネットワークデバイス（ネットワークカード）の MAC アドレスを変更します。その結果、攻撃者はデバイスに送信されたデータを別のデバイスにリダイレクトし、このデータにアクセスすることができます。Kaspersky Endpoint Security で MAC スプーフィング攻撃をブロックし、攻撃に関する通知を管理者に送信できます。</p>

## ファイアウォール

ファイアウォールは、インターネットまたはローカルネットワークでの作業中に、コンピューターへの不正な接続をブロックします。ファイアウォールは、コンピューター上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義されたネットワークルールを使用してコンピューターを保護します。

ネットワークエージェントは Kaspersky Security Center との連携に使用されます。ファイアウォールは本製品とネットワークエージェントが正常に動作するために、自動でネットワークルールを作成します。その結果、ファイアウォールはコンピューターのいくつかのポートを開きます。どのポートが開かれるかは、ディストリビューションポイントなど、コンピューターの役割により異なります。コンピューターで開かれるポートについて詳しくは、[Kaspersky Security Center のヘルプ](#) を参照してください。

## ネットワークルール

次の情報に基づいてネットワークルールを構成できます：

- **ネットワークパケットルール**：ネットワークパケットルールでは、アプリケーションに関係なく、ネットワークパケットに制限が適用されます。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。Kaspersky

Endpoint Security には、カスペルスキーのエキスパートが推奨する権限を持つネットワークパケットルールが事前に定義されています。

- アプリケーションネットワークルール：アプリケーションネットワークルールでは、特定のアプリケーションのネットワークアクティビティに制限が適用されます。このルールでは、ネットワークパケットの特徴だけでなく、このネットワークパケットの宛先またはネットワークパケットを発行する特定のアプリケーションも考慮されます。

オペレーティングシステムのリソース、プロセス、および個人データへのアプリケーションの制御されたアクセスは、アプリケーション権限を使用することにより、[ホスト侵入防止](#)によって提供されます。

アプリケーションの最初の起動時に、ファイアウォールは次の動作を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティの確認。  
ファイアウォールがより効果的に機能するように、[Kaspersky Security Network に参加](#)することを推奨します。
3. 信頼グループのいずれかにアプリケーションを配置します：信頼、弱い制限付き、強い制限付き、ブロック。

[許可グループ](#)は、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は [ホスト侵入防止の設定](#)に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じて、アプリケーションのネットワーク動作をブロックします。たとえば、強い制限付きの信頼グループのアプリケーションは、ネットワーク接続を使用できません。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のネットワークルールをそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

## ネットワークルールの優先度

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ネットワーク動作が複数のルールに追加された場合、ファイアウォールは最も優先度の高いルールに従ってネットワーク動作を制限します。

ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。同じ種類のネットワークアクティビティに、ネットワークパケットルールとアプリケーションのネットワークルールの両方が指定されている場合、そのネットワークアクティビティはネットワークパケットルールに従って処理されます。



アプリケーションのネットワークルールは次のように動作します：アプリケーションのネットワークルールには、パブリック、ローカル、または許可するなど、ネットワークのステータスに基づいたアクセスルールが含まれます。例えば、強い制限付きの信頼グループのアプリケーションは、既定ではすべてのステータスのネットワーク内でネットワークアクティビティが許可されません。個別のアプリケーション（親アプリケーション）にネットワークルールが指定されている場合、他のアプリケーションの子プロセスは、親アプリケーションのネットワークルールに基づいて実行されます。アプリケーションにネットワークルールが指定されていない場合は、子プロセスはアプリケーションの信頼グループのネットワークアクセスルールに基づいて実行されます。

例えば、ブラウザ X 以外のすべてのアプリケーションのすべてのステータスのネットワークアクティビティを禁止したとします。その後ブラウザ X（親アプリケーション）からブラウザ Y（子プロセス）のインストールを開始した場合、ブラウザ Y のインストーラはネットワークにアクセスし、必要なファイルをダウンロードします。インストール後、ブラウザ Y はファイアウォールの設定により、すべてのネットワーク接続を拒否します。子プロセスとしてのブラウザ Y のネットワークアクティビティを禁止するには、ブラウザ Y のインストーラに対してネットワークルールを設定する必要があります。

## ネットワーク接続のステータス

ファイアウォールを使用すると、ネットワーク接続の状態に応じてネットワーク動作を制御できます。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムからネットワーク接続のステータスを受け取ります。オペレーティングシステムでのネットワーク接続のステータスは、接続のセットアップ時にユーザーが設定します。[Kaspersky Endpoint Security の設定でネットワーク接続のステータスを変更](#)できます。ファイアウォールは、オペレーティングシステムではなく、Kaspersky Endpoint Security の設定のネットワークステータスに応じてネットワーク動作を監視します。

ネットワーク接続種別は、次のいずれかの種類になります：

- パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。

既定では、ファイアウォールは、[パブリックネットワーク] ステータスをインターネットに割り当てます。インターネットのステータスは変更できません。

- プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。
- 許可するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。

ファイアウォールの設定

パラメータ	説明
ネットワークパケットルール	<p>ネットワークパケットルールのリストのテーブル。ネットワークパケットルールはアプリケーションに関係なく、ネットワークパケットに制限を加えるために使用します。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。</p> <p>このテーブルには、Microsoft Windows オペレーティングシステムで動作しているコンピューターのネットワークトラフィックを最適に保護するために、カスペルスキーが推奨する設定済みのネットワークパケットルールがリスト表示されます。</p>

	<p>ファイアウォールでは、各ネットワークパケットルールに実行優先度が設定されます。ファイアウォールは、ネットワークパケットルールのリストに表示されているネットワークパケットルールを、上から下に順番に処理します。ネットワーク接続ごとに適用可能な最上位のネットワークパケットルールが検出され、ネットワークの動作を許可またはブロックすることによって、そのルールが適用されます。それぞれのネットワーク接続に対して、適用されたルールよりも優先度が低いネットワークパケットルールはすべてファイアウォールによって無視されます。</p> <p>ネットワークパケットルールの優先度は、アプリケーションのネットワークルールよりも高くなります。</p>
<b>ネットワーク接続</b>	<p>このテーブルには、ファイアウォールによって検知されるコンピューターのネットワーク接続に関する情報が表示されます。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>既定では、[パブリックネットワーク] ステータスがインターネットに割り当てられます。インターネットのステータスは変更できません。</p> </div>
<b>ネットワークルール</b>	<p><b>アプリケーション</b></p> <p>ファイアウォールコンポーネントによって制御されるアプリケーションのテーブル。アプリケーションは許可グループに割り当てられます。信頼グループは、アプリケーションのネットワーク動作を制御するときに Kaspersky Endpoint Security が使用する権限を定義します。ポリシーの影響下でコンピューターにインストールされているすべてのアプリケーションの1つのリストからアプリケーションを選択し、そのアプリケーションを信頼グループに追加できます。</p> <p><b>ネットワークルール</b></p> <p>信頼グループの一部であるアプリケーションのネットワークルールの表。これらのルールに従って、ファイアウォールは、アプリケーションのネットワークの動作を制限します。</p> <p>この表には、カスペルスキーの専門家が推奨する定義済みネットワークルールが表示されます。これらのネットワークルールは、Windows オペレーティングシステムを実行しているコンピューターのネットワークトラフィックを最適に保護するために追加されました。定義済みネットワークルールを削除することはできません。</p>

## 有害 USB 攻撃ブロック

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します（下の図を参照）。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID および PID、キーボードが接続されたポート番号）が、認証されたキーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターのUSBポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、新しいコードが生成されます。[数値コードの入力試行回数は指定](#)できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合（下の図を参照）、本製品はキーボードからの入力をブロックします。USBデバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックは、既定ではインストールされません。有害 USB 攻撃ブロックが必要な場合は、製品のインストール前に[インストールパッケージ](#)のプロパティにコンポーネントを追加するか、製品のインストール後に[利用可能なコンポーネントを変更](#)できます。



キーボード承認

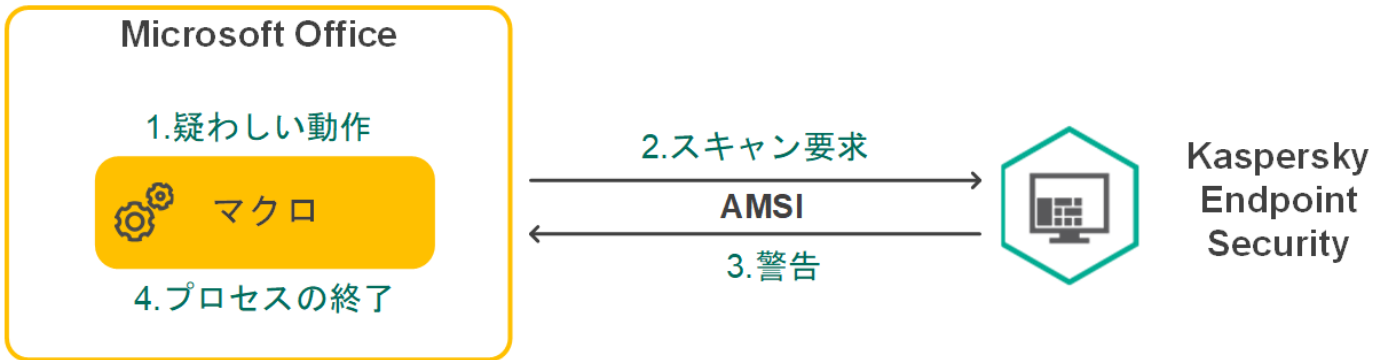
#### 有害 USB 攻撃ブロックの設定

パラメータ	説明
USB デバイスの認証時にセキュリティキーボードの使用を禁止する	このチェックボックスをオンにすると、認証用のコードが入力できない USB デバイスの認証時に、セキュリティキーボードの使用をブロックします。
デバイスの最大認証試行回数	認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は 1～10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗したあとに USB デバイスがブロックされます。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。
最大試行回数を超えた場合のタイムアウト (分) :	認証コードの入力の失敗回数が指定した回数を超えた後に USB デバイスをブロックする時間です。有効な値は 1～180 (分) です。

# AMSI 保護

AMSI 保護機能は Microsoft 社の AMSI (Antimalware Scan Interface) をサポートすることを目的とした機能です。AMSI (Antimalware Scan Interface) により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト (たとえば、PowerShell スクリプトなど) のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。対象となるサードパーティ製品としては、たとえば Microsoft Office 製品があります。AMSI について詳しくは、[Microsoft 社の資料](#) を参照してください。

AMSI 保護機能では、脅威の検知とサードパーティ製品への検知された脅威に関する通知のみを実行できます。脅威に関する通知を受信したサードパーティ製品側では、脅威による悪意のあるふるまいを許可しません (たとえば、プロセスを終了します)。



AMSI の動作例

また、一定間隔の間に特定のサードパーティ製品から上限を超えてスキャン要求を受信した場合などにも、AMSI 保護機能でそのサードパーティ製品からのスキャン要求を拒否する場合があります。Kaspersky Endpoint Security は、拒否したサードパーティ製品のスキャン要求に関する情報を管理サーバーに送信します。[\[AMSI 保護機能との相互作用をブロックしない\]](#) がオンになっているサードパーティ製品からのスキャン要求は拒否されません。

AMSI 保護機能は、ワークステーションおよびサーバー用の次のオペレーティングシステムで使用できます：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2022

## AMSI 保護の設定

パラメータ	説明
アーカイブをスキャン	次の形式のアーカイブのファイルをスキャンします：RAR、ARJ、ZIP、CAB、LHA、JAR および ICE。
配布パッケージをスキャン	このチェックボックスでは、サードパーティの配布パッケージのスキャンを有効または無効にします。
Microsoft Office 形式のファイル	Microsoft Office 形式のファイルをスキャンします (DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル)。Office 形式のファイルには OLE オブ

をスキャン	ジェクトが含まれます。
大きな複合ファイルのスキャンしない	<p>このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。</p> <p>このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。</p> <p>圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。</p>

## 脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとする、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。

### 脆弱性攻撃ブロックの設定

パラメータ	説明
攻撃を検知したとき	<p><b>操作をブロックする</b>：このオプションを選択した場合、脆弱性を利用した攻撃が検知されると、攻撃によって試行されたすべての処理をブロックします。</p> <p><b>通知する</b>：このオプションを選択した場合、脆弱性を利用した攻撃が検知されると、攻撃によって試行された処理はブロックされませんが、攻撃に関する情報がアクティブな脅威のリストに追加されます。</p>
システムプロセスのメモリ保護を有効にする	このオプションをオンにすると、システムプロセスメモリへアクセスしようとする外部プロセスをブロックします。

## ふるまい検知

ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures (BSS) を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

### ふるまい検知の設定

パラメータ	説明
マルウェアの動作を検知したとき	<ul style="list-style-type: none"> <li><b>ファイルを削除する</b>：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。</li> <li><b>アプリケーションを終了する</b>：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。</li> </ul>



	<ul style="list-style-type: none"> <li>• <b>通知する</b>：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、アプリケーションは終了されませんが、悪意のある活動に関する情報がアクティブな脅威のリストに追加されます。</li> </ul>
<b>外部からの暗号化に対する共有フォルダーの保護を有効にする</b>	<p>このオプションをオンにすると、共有フォルダー上で実行される操作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。</p> <div data-bbox="352 398 1493 524" style="border: 1px solid gray; padding: 5px;"> <p>NTFS ファイルシステムで、EFS システムで暗号化されていないメディア上にあるファイルのみ外部からの暗号化をブロックします。</p> </div> <ul style="list-style-type: none"> <li>• <b>通知する</b>：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、共有フォルダーにあるファイルを変更する試みに関する情報がアクティブな脅威のリストに追加されます。</li> <li>• <b>接続をブロックする時間</b>：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、ファイルの変更を試みたコンピューターからのネットワーク動作がブロックされ、変更されたファイルのバックアップコピーが作成されます。</li> </ul> <div data-bbox="352 887 1493 1012" style="border: 1px solid gray; padding: 5px;"> <p>修復エンジンが有効になっていて <b>[接続をブロックする]</b> が選択されている場合、変更されたファイルがバックアップコピーから復元されます。</p> </div>
<b>除外リスト</b>	<p>このリストにある、共有フォルダーの暗号化を試行したコンピューターは監視されません。</p> <div data-bbox="352 1182 1493 1413" style="border: 1px solid gray; padding: 5px;"> <p>共有フォルダーの外部からの暗号化からの保護で、暗号化を行う側のコンピューターの除外リストを有効にするには、Windows セキュリティポリシーでログオンの監査を有効にする必要があります。既定では、ログオンの監査は無効です。Windows の監査ポリシーを使用したセキュリティ設定の詳細については、<a href="#">Microsoft 社の Web サイト</a> を参照してください。</p> </div>

## ホスト侵入防止

ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。

コンポーネントは、アプリケーション権限を使用してアプリケーションの動作を制御します。アプリケーション権限には、次のアクセスパラメータが含まれます：

- オペレーティングシステムリソースへのアクセス（自動起動オプション、レジストリキーなど）
- 個人データ（ファイルやアプリケーションなど）へのアクセス

アプリケーションのネットワーク動作は、ネットワークルールを使用して[ファイアウォール](#)によって制御されます。

アプリケーションの最初の起動時に、ホスト侵入防止は次の処理を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティの確認。

ホスト侵入防止がより効果的に機能するように、[Kaspersky Security Network に参加](#)することを推奨します。

3. 信頼グループのいずれかにアプリケーションを配置します：信頼、弱い制限付き、強い制限付き、ブロック。

[許可グループ](#)は、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は [ホスト侵入防止の設定](#) に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じてアプリケーション動作をブロックします。たとえば、高い制限付きの信頼グループのアプリケーションは、オペレーティングシステムモジュールへのアクセスを拒否されます。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のアプリケーション権限をそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

#### ホスト侵入防止の設定

パラメータ	説明
アプリケーション権限	<p><b>アプリケーション</b></p> <p>ホスト侵入防止によって監視されるアプリケーションのテーブル。アプリケーションは許可グループに割り当てられます。許可グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。</p> <p>ポリシーの影響下でコンピューターにインストールされているすべてのアプリケーションの1つのリストからアプリケーションを選択し、そのアプリケーションを信頼グループに追加できます。</p> <p>次の表に、アプリケーションのアクセス権を示します：</p> <ul style="list-style-type: none"><li>• <b>ファイルとシステムレジストリ</b>：このテーブルには、オペレーティングシステムリソースおよび個人データにアクセスするための、信頼グループ内のアプリケーションの権利</li></ul>



	<p>が含まれています。</p> <ul style="list-style-type: none"> <li>• <b>権限</b>：このテーブルには、オペレーティングシステムのプロセスとリソースにアクセスするための、信頼グループのアプリケーションの権限が含まれています。</li> <li>• <b>ネットワークルール</b>：信頼グループの一部であるアプリケーションのネットワークルールの表。これらのルールに従って、<a href="#">ファイアウォール</a>は、アプリケーションのネットワークの動作を制限します。この表には、カスペルスキーの専門家が推奨する定義済みネットワークルールが表示されます。これらのネットワークルールは、Windows オペレーティングシステムを実行しているコンピューターのネットワークトラフィックを最適に保護するために追加されました。定義済みネットワークルールを削除することはできません。</li> </ul>
<b>保護対象のリソース</b>	<p><b>Name</b></p> <p>このテーブルには、コンピューターのリソースがカテゴリ別に表示されます。ホスト侵入防止は、他のアプリケーションがテーブル内のリソースにアクセスしようとする動作を監視します。</p> <p>リソースにはレジストリカテゴリ、ファイル、フォルダー、レジストリキーがあります。</p> <p><b>アプリケーション</b></p> <p>選択したリソースのホスト侵入防止によって監視されるアプリケーションのテーブル。アプリケーションは許可グループに割り当てられます。許可グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。</p>
<b>本製品より前に起動したアプリケーションの信頼グループ</b>	<p>Kaspersky Endpoint Security が Kaspersky Endpoint Security より前に起動されるアプリケーションを配置する信頼グループ。</p>
<b>未知のアプリケーションの権限を KSN データベースからアップデートする</b>	<p>このチェックボックスをオンにすると、ホスト侵入防止は Kaspersky Security Network データベースを使用して以前に不明であったアプリケーションの権限をアップデートします。</p>
<b>デジタル署名があるアプリケーションを信頼する</b>	<p>このチェックボックスをオンにすると、ホスト侵入防止は信頼済みの製造元のデジタル署名付きのアプリケーションを「許可」グループに割り当てます。</p> <p>信頼済みの製造元とは、カスペルスキーによる信頼済みのソフトウェアベンダーです。<a href="#">手動で信頼済みの証明書ストアに製造元のデジタル署名を追加</a>することも可能です。</p> <p>このチェックボックスをオフにすると、ホスト侵入防止はこのようなアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して許可グループを決定します。</p>
<b>次の期間以上使用されなかったアプリケーションのル</b>	<p>このチェックボックスをオンにすると、次の条件が満たす場合、Kaspersky Endpoint Security はアプリケーションに関する情報（許可グループとアクセス権）を自動的に削除します：</p> <ul style="list-style-type: none"> <li>• アプリケーションを手動で許可グループに配置したか、またはそのアクセス権を設定した</li> </ul>

<p><b>ールを削除する</b></p>	<ul style="list-style-type: none"> <li>• 定義された期間内にアプリケーションが開始されていない</li> </ul> <p>アプリケーションの許可グループと権限が自動的に決定された場合は、Kaspersky Endpoint Security は 30 日後にこのアプリケーションに関する情報を削除します。アプリケーション情報の保管期間を変更したり、自動削除をオフにしたりすることはできません。</p> <p>次回、このアプリケーションを起動すると、Kaspersky Endpoint Security は初めて起動した場合と同様に、アプリケーションを検証します。</p>
<p><b>既存のグループに追加できないアプリケーションの信頼グループ</b></p>	<p>このドロップダウンリストの項目は、Kaspersky Endpoint Security が不明なアプリケーションを割り当てる許可グループを決定します。</p> <p>次の項目のいずれかを選択できます：</p> <ul style="list-style-type: none"> <li>• <b>弱い制限付き：</b></li> <li>• <b>強い制限付き：</b></li> <li>• <b>ブロック：</b></li> </ul>

## 修復エンジン

修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックするとき、次の種別のマルウェアの動作に対して処理を実行します：

### • ファイルの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
- マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
- マルウェアによって変更または削除されたファイルを復元します。

ファイルの修復機能には[いくつかの制限事項](#)があります。

### • レジストリの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成されたレジストリキーを削除します。
- マルウェアによって変更または削除されたレジストリキーは復元されません。

### • システムの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって開始されたプロセスを終了します。
- 悪意のあるアプリケーションによって侵入されたプロセスを終了します。

- マルウェアによって停止されたプロセスは再開しません。

## • ネットワークの動作

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによるネットワーク動作をブロックします。
- マルウェアが侵入したプロセスによるネットワーク動作をブロックします。

マルウェアの動作のロールバックは、[ファイル脅威対策](#)または[ふるまい検知](#)から開始するか、[ウイルススキャン](#)中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピューターデータの整合性に悪影響を与えません。

## Kaspersky Security Network

コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

KSN (*Kaspersky Security Network*) はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。

Kaspersky Security Network の使用は任意です。本製品の初期設定中に、KSN を使用するかどうか尋ねられます。KSN への参加はいつでも開始または中止できます。

KSN に参加している間に生成されたカスペルスキー統計情報の送信や、そのような情報の保存と破棄について詳しくは、KSN 声明および[カスペルスキーの Web サイト](#)を参照してください。Kaspersky Security Network 声明のテキストが含まれたファイル ksn\_<言語 ID>.txt は製品[配信キット](#)に含まれています。

KSN サーバーの負荷を低減するため、Kaspersky Security Network に対するリクエストを一時的に無効にしたり部分的に制限したりする定義データベースのアップデートを、カスペルスキーのエキスパートが公開することがあります。この場合、製品のローカルインターフェイスでの KSN への接続ステータスは「制限付きで有効」になります。

## KSN インフラストラクチャの種別

Kaspersky Endpoint Security では、次の種別の KSN インフラストラクチャの使用をサポートしています：

- ほとんどのカスペルスキー製品で使用されるのがグローバル KSN です。KSN の参加者は、Kaspersky Security Network から情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、Kaspersky Security Network の評価データベースと統計情報のデータベースに追加されます。
- プライベート KSN は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターから KSN にデータを送信せずに Kaspersky Security Network の評価データベースや統計情報のデータにアクセスできるようにするソリューションです。プラ

プライベート KSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：

- コンピューターがインターネットに接続されていない。
- 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

既定では、Kaspersky Security Center はグローバル KSN を使用します。管理コンソール (MMC)、Kaspersky Security Center Web コンソール、および [コマンドライン](#) からプライベート KSN の使用を設定できます。Kaspersky Security Center Cloud コンソールでは、プライベート KSN の使用を設定できません。

プライベート KSN について詳しくは、管理者向けに提供されている *Kaspersky Private Security Network* のガイドを参照してください。

## KSN プロキシ

Kaspersky Security Center 管理サーバーによって管理されるクライアントコンピューターは、KSN プロキシサービス経由で KSN と連携できます。

KSN プロキシサービスは次の機能を提供します：

- クライアントコンピューターはインターネットに直接アクセスしなくても、KSN にクエリを実行し、情報を送信できます。
- KSN プロキシは処理データをキャッシュすることにより、外部ネットワークとの通信チャネルの負荷を軽減し、クライアントコンピューターによって要求される情報の受信を高速化します。

KSN プロキシサービスについて詳しくは、[Kaspersky Security Center のオンラインヘルプ](#) を参照してください。

Kaspersky Security Network の設定

パラメータ	説明
拡張 KSN モードを有効にする	拡張 KSN モードは、カスペルスキーに <a href="#">詳細なデータ</a> を送信するモードです。Kaspersky Endpoint Security は、オプションの設定にかかわらず KSN を使用して脅威を検知します。
クラウドモードを有効にする	クラウドモードで動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用しての本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。  このオプションをオンにすると、Kaspersky Endpoint Security では軽量なバージョンの定義データベースを使用し、オペレーティングシステムのリソースの負荷を減少させます。  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">このチェックボックスをオンにした次のアップデートでは、Kaspersky Endpoint Security は軽量なバージョンの定義データベースをダウンロードします。</div>

	<p>このオプションをオフにすると、定義データベースの完全版を使用します。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>このチェックボックスをオフにした次のアップデートでは、Kaspersky Endpoint Security は定義データベースの全体をダウンロードします。</p> </div>
<p><b>KSN サーバーが使用できないときのコンピューターのステータス</b></p> <p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>このドロップダウンリストでは、KSN サーバーが使用できない場合に Kaspersky Security Center に表示するコンピューターのステータスを指定できます。</p>
<p><b>KSN プロキシを使用する</b></p> <p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security は KSN プロキシサービスを使用します。KSN プロキシサービスの設定は管理サーバーのプロパティで編集できます。</p>
<p><b>KSN プロキシを使用できない場合は、KSN サーバーを使用する</b></p> <p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合（グローバル KSN の使用時）とサードパーティ側に配置されている場合（プライベート KSN の使用時）があります。</p>

## ウェブコントロール

ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します（下図を参照）。

Kaspersky Endpoint Security では、HTTP プロトコルと HTTPS プロトコルのトラフィックのみが監視されません。



HTTPS トラフィックをスキャンするには、[暗号化された接続のスキャンを有効にする](#)必要があります。

## Web サイトへのアクセスの管理方法

ウェブコントロールでは、次の設定を使用して Web サイトへのアクセスを管理できます：

- **Web サイトのカテゴリ**：Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。例えば、「SNS」カテゴリまたは[その他のカテゴリ](#)のサイトに対してユーザーのアクセスを制限することができます。
- **データ種別**：Web サイトのデータへのユーザーのアクセスを制限して、画像を表示できないようにするなどの使い方ができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。

圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「圧縮ファイル」として識別し、「画像ファイル」とは識別しません。

- **個別のアドレス**：URL を入力したり、[マスクを使用](#)して Web アドレスを指定できます。

Web サイトへのアクセスを管理するために、複数の設定を同時に組み合わせて使用できます。たとえば、Web サイトのカテゴリが「Web メール」の場合にのみ「Office のファイル」へのアクセスを制限するような使い方ができます。

## Web サイトへのアクセスルール

ウェブコントロールは、アクセスルールを使用して Web サイトへのユーザーアクセスを管理します。Web サイトへのアクセスルールでは、次のような詳細設定を指定できます。

- **ルールを適用するユーザー**：  
ブラウザによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。
- **ルールスケジュール**：  
ブラウザによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

## アクセスルールの優先順位：

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。適用例として、たとえば、Kaspersky Endpoint Security によって企業ポータルが「ソーシャルネットワーク」サイトと判定されているケースを考えます。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「ソーシャルネットワーク」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 2 つのルールを作成します。この場合、企業ポータルへのアクセスルールには、ソーシャルネットワークカテゴリへのアクセスルールよりも高い優先順位を割り当てる必要があります。



要求された Web ページを表示できません。

アドレス：<http://kaspersky.ru/>

この Web ページはルール「block」によってブロックされました。

理由：Web リソースがコンテンツカテゴリ「不明」とデータ種別カテゴリ「未定義」に属しています。

この Web リソースは社内での使用がブロックされています。誤ってブロックされたと思われる場合やこの Web リソースにアクセスする必要がある場合は、社内のネットワーク管理者([アクセスを要求](#))にお問い合わせください。

メッセージの作成時刻：29.10.2020 13:42:28



要求された Web ページは安全でないか、社内のポリシーによってブロックされている可能性があります。

アドレス：<http://kaspersky.com/>

この Web ページはルール「warn」によってブロックされています。

理由：Web リソースがコンテンツカテゴリ「不明」とデータ種別カテゴリ「未定義」に属しています。

要求した Web ページを開くには、リンク「<http://kaspersky.com/>」をクリックしてください。

要求した Web ページが存在する Web サイトのコンテンツ全体にアクセスするには、リンク「[http://kaspersky.com/\\*](http://kaspersky.com/*)」をクリックしてください。

「\*」で示されたレベル以下の既存のドメインすべてにアクセスするには、リンク「[\\*/\\*.kaspersky.com/\\*](*/*.kaspersky.com/*)」をクリックしてください。

本製品の現在のセッションが終了するまでは、上記の Web リソースへのアクセスが許可されます。誤って警告が表示されている場合は、社内のネットワーク管理者([アクセスを要求](#))に連絡してください。

メッセージの作成時刻：29.10.2020 13:42:12

ウェブコントロールによって表示されるメッセージ

#### ウェブコントロールの設定

パラメータ	説明
Web リソースへのアクセスルール	Web リソースアクセスルールのリストです。それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。
既定のルール	<p>〔既定のルール〕は、他のルールの対象範囲に含まれない Web リソースへのアクセスルールです。次の設定方法があります：</p> <ul style="list-style-type: none"> <li>● <b>ルールリスト以外をすべて許可する</b>：禁止された Web サイトへの拒否リストモードと同様です。</li> <li>● <b>ルールリスト以外をすべて拒否する</b>：許可された Web サイトへの許可リストモードと同様です。</li> </ul>



<p>メッセージのテンプレート</p>	<ul style="list-style-type: none"> <li>• <b>警告</b>この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。</li> <li>• <b>ブロックに関するメッセージ</b>：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。</li> <li>• <b>管理者に送信するメッセージ</b>：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security (は Kaspersky Security Center にイベントを送信します)：<b>Web ページへのアクセスブロックに関するメッセージが管理者に送信されました</b>。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [<b>ユーザー要求</b>] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。</li> </ul>
<p>許可対象のページの閲覧を記録する</p>	<p>Kaspersky Endpoint Security は、許可されている Web サイトも含めて、すべての Web サイトへのアクセスに関するデータをログに記録します。Kaspersky Endpoint Security は、Kaspersky Security Center、<a href="#">Kaspersky Endpoint Security のローカルログ</a>、Windows イベントログのそれぞれに、イベント情報を送信できます。ユーザーが行うインターネット上での活動を監視するには、<a href="#">イベントの保存に関する設定を指定する</a>必要があります。</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>ユーザーが行うインターネット上での活動を監視すると、HTTPS トラフィックの復号のためにより多くのコンピューターリソースを消費する可能性があります。</p> </div>

## デバイスコントロール

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します (例：ハードディスク、カメラ、Wi-Fi モジュール)。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。



### デバイスへのアクセスの判定基準

デバイスコントロールは、次の情報に基づいてアクセスをコントロールできます。

- **デバイス種別**：プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。

次のようにデバイスアクセスを設定できます：

- 許可：
- ブロック：

- バスの種類に依存（Wi-Fiを除く）：
- 例外を除きブロック（Wi-Fiのみ）：
- **接続バス**：接続バスとは、コンピューターへのデバイスの接続に使用されるインターフェイスです（例：USB、FireWire）。これにより、たとえばUSBなど特定の接続バスを使用して接続されるすべてのデバイスの接続を制限できます。


次のようにデバイスアクセスを設定できます：

- 許可：
- ブロック：
- **信頼するデバイス**：「信頼するデバイス」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

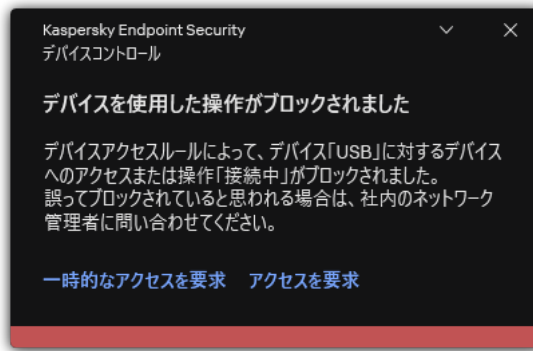
次のデータに基づいて信頼するデバイスを追加できます。

- **IDによるデバイス**：各デバイスには固有の識別子があります（ハードウェアID、またはHWID）。これらのIDは、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイスIDの例：SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000特定のデバイスを複数追加する場合は、IDでデバイスを追加すると便利です。
- **モデルによるデバイス**：各デバイスには製造元ID（VID）および製品ID（PID）があります。これらのIDは、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VIDおよびPIDの入力用テンプレート：VID\_1234&PID\_5678組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。
- **IDマスクによるデバイス**：IDが類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。\*文字は、任意の文字列を置き換えます。Kaspersky Endpoint Securityでは、マスクでの「?」記号の使用をサポートしていません。例：WDC\_C\*
- **モデルマスクによるデバイス**：同一のVIDまたはPIDを持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。\*文字は、任意の文字列を置き換えます。Kaspersky Endpoint Securityでは、マスクでの「?」記号の使用をサポートしていません。例：「VID\_05AC & PID\_\*」。

デバイスコントロールは、[アクセスルール](#)を使用してデバイスへのユーザーアクセスを管理します。デバイスコントロールでは、デバイスの接続や切断のイベントを保存することもできます。イベントを保存するには、ポリシー内でイベントの記録を設定する必要があります。

デバイスへのアクセスが接続バスに依存する場合（ステータスの場合）、Kaspersky Endpoint Securityではデバイスの接続イベントと切断イベントが保存されません。Kaspersky Endpoint Securityでデバイスの接続イベントと切断イベントを保存するには、デバイスへのアクセスを許可する（ステータス）か、デバイスを信頼リストに追加します。

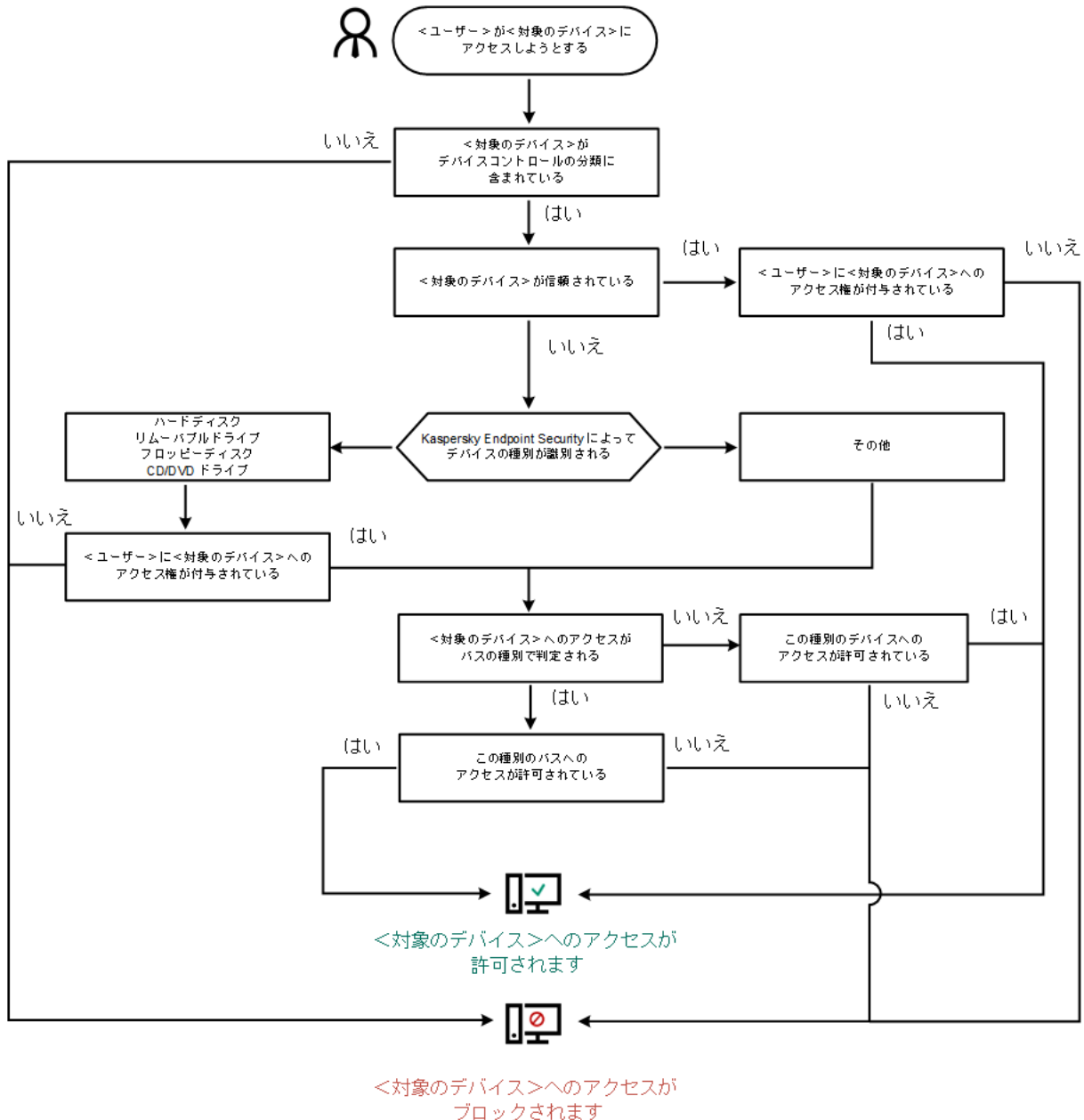
デバイスコントロールでブロックされているデバイスがコンピューターに接続された場合、Kaspersky Endpoint Securityはアクセスをブロックし通知を表示します（以下の図を参照）。



デバイスコントロールの通知

## デバイスコントロールの動作アルゴリズム

ユーザーがデバイスをコンピューターに接続すると、Kaspersky Endpoint Security はデバイスへのアクセスを許可するかどうかを決定します（以下の図を参照）。



デバイスコントロールの動作アルゴリズム

デバイスが接続されてアクセスが許可されている状態で、アクセスをブロックするようにアクセスルールを編集できます。この場合、（フォルダーの内容の表示や、読み取りまたは書き込みの実行など）次にデバイスへのアクセスが試行されたときに、Kaspersky Endpoint Security はアクセスをブロックします。ファイルシステムのないデバイスは、次回デバイスが接続されたときにのみブロックされます。

Kaspersky Endpoint Security がインストールされているコンピューターのユーザーが、誤ってブロックされたと考えられるデバイスへのアクセスを要求できるようにするには、[アクセス要求の手順](#)を伝えます。

#### デバイスコントロールの設定

パラメータ	説明
<b>一時アクセスの要求を許可する</b> (Kaspersky Security Center コンソール内でのみ利用可能)	このチェックボックスをオンにすると、Kaspersky Endpoint Security のローカルインターフェイスで <b>[アクセスを要求する]</b> が有効になります。このボタンをクリックすると、 <b>[デバイスへのアクセス要求]</b> ウィンドウが表示されます。このウィンドウでは、ユーザーがブロックデバイスへの一時アクセスを要求できます。
<b>デバイスと Wi-Fi ネットワーク</b>	このテーブルには、各アクセスステータスなど、デバイスコントロールの分類に従って、考えられるすべてのデバイスの種類が表示されます。
<b>接続バス</b>	それぞれのアクセスルールのステータスなど、デバイスコントロールの分類に従って、すべての使用可能な接続バスのリストが表示されます。
<b>信頼するデバイス</b>	信頼するデバイスと、それぞれのデバイスに対してアクセス権が付与されているユーザーのリストです。
<b>アンチブリッジ</b>	<p>アンチブリッジは、ネットワークブリッジの作成をブロックし、コンピューターで複数のネットワーク接続が同時に確立することを防止します。この機能を使用することで、セキュリティ保護が不十分で接続が許可されていないネットワークから社内ネットワークを保護できます。</p> <p>アンチブリッジは、デバイスの優先度を参照することで、複数のネットワーク接続の確立をブロックします。デバイスのリスト上の位置が高くなるほど、優先度が高くなります。</p> <p>現在有効な接続と新しい接続の種別が同じ場合（たとえば、両方とも Wi-Fi など）、Kaspersky Endpoint Security は現在有効な接続をブロックし、新しい接続の確立を許可します。</p> <p>現在有効な接続と新しい接続の種別が異なる場合（たとえば、1つはネットワークアダプターでもう1つは Wi-Fi など）、Kaspersky Endpoint Security は優先度が低い方の接続をブロックし、優先度が高い方の接続を許可します。</p> <p>アンチブリッジの使用がサポートされるのは、次の種別のデバイスです：ネットワークアダプター、Wi-Fi、モデム。</p>
<b>メッセージのテンプレート</b>	<ul style="list-style-type: none"> <li> <b>ブロックに関するメッセージ</b>：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。         </li> <li> <b>管理者に送信するメッセージ</b>：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが         </li> </ul>

LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**デバイスへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [**ユーザー要求**] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

## アプリケーションコントロール

アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。

アプリケーションコントロールの設定では、次のステップが必要です：

### 1. アプリケーションカテゴリの作成

管理者は、自身が管理するアプリケーションのカテゴリを作成します。アプリケーションのカテゴリは、管理グループに関係なく、企業ネットワーク内のすべてのコンピューターを対象としています。カテゴリを作成するには、KL カテゴリ（ブラウザーなど）、ファイルのハッシュ、アプリケーションの開発元、およびその他の条件を使用できます。

### 2. アプリケーションコントロールルールの作成

管理者は、管理グループのポリシーにアプリケーションコントロールルールを作成します。ルールには、アプリケーションのカテゴリと、「ブロック」または「許可」のカテゴリからのアプリケーションの起動ステータスが含まれます。

### 3. アプリケーションコントロールモードの選択

管理者は、拒否リストまたは許可リストのいずれのルールにも含まれていないアプリケーションを操作するモードを選択します。

ユーザーが禁止されたアプリケーションを起動しようとするすると、Kaspersky Endpoint Security はアプリケーションの起動をブロックし、通知を表示します（下の図を参照）。

Application Control の構成を確認するためのテストモードが用意されています。このモードでは、Kaspersky Endpoint Security は次のことを行います：

- 禁止されているものも含めて、アプリケーションの起動を許可します。
- 禁止されているアプリケーションの起動に関する通知を表示し、ユーザーのコンピューターのレポートに情報を追加します。
- 禁止されたアプリケーションの起動に関するデータを Kaspersky Security Center に送信します。



アプリケーションコントロールの通知

## アプリケーションコントロールの操作モード

アプリケーションコントロールは2つのモードで動作します。

- **拒否リスト** このモードでは、アプリケーションコントロールルールで禁止されているアプリケーションを除くすべてのアプリケーションを、ユーザーが起動できます。

アプリケーションコントロールのこのモードは、規定では有効になっています。

- **許可リスト** このモードでは、アプリケーションコントロールルールで許可および禁止されていないアプリケーション以外のアプリケーションを、ユーザーが起動できないようにします。

必要なアプリケーションコントロールの許可ルールをすべて設定すると、LAN 管理者が検証していない新しいアプリケーションの起動はブロックされますが、オペレーティングシステムとユーザーが業務で使用している信頼するアプリケーションの動作は許可されます。

許可リストモードでは、[アプリケーションコントロールルールの設定における推奨事項](#)を確認できます。

アプリケーションコントロールは、Kaspersky Endpoint Security のローカルインターフェイスと Kaspersky Security Center の両方で、これらのモードで動作するように設定できます。

Kaspersky Security Center が提供するツールには、Kaspersky Endpoint Security のローカルインターフェイスで使用できないものもあります。これらは次の用途で必要となります：

- [アプリケーションカテゴリの作成](#)

Kaspersky Security Center の管理コンソールで作成するアプリケーションコントロールルールは、カスタマイズされたアプリケーションカテゴリに基づき、Kaspersky Endpoint Security のローカルインターフェイスでの対象条件や除外条件には基づきません。

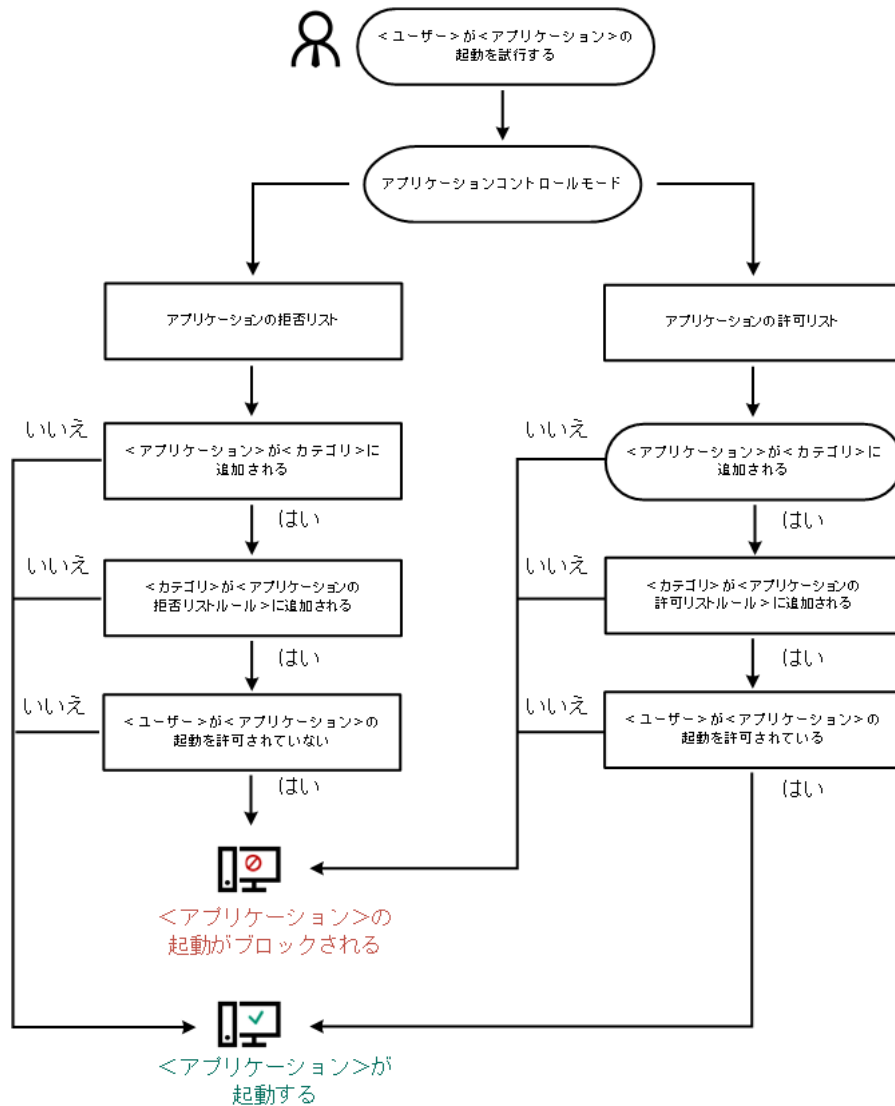
- [企業の LAN コンピューターにインストールされたアプリケーションについての情報の取得](#)

そのため、アプリケーションコントロールの動作設定には Kaspersky Security Center の使用を推奨します。

## アプリケーションコントロールの動作アルゴリズム

Kaspersky Endpoint Security は、アルゴリズムを使用して、アプリケーションの起動に関する決定を下します（下の図を参照）。





アプリケーションコントロールの動作アルゴリズム

アプリケーションコントロールの設定

パラメータ	説明
テストモード	このオプションをオンにすると、アプリケーションコントロールの現在のモードでブロックされているアプリケーションの起動は許可されますが、起動に関する情報がレポートに記録されません。
アプリケーション起動コントロールモード	<p>次のいずれかのオプションを選択できます：</p> <ul style="list-style-type: none"> <li>• <b>拒否リスト</b> このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールの条件を満たす場合は除きます。</li> <li>• <b>許可リスト</b> このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールの条件を満たす場合は除きます。</li> </ul> <p>許可リストモードを選択すると、次の2つのアプリケーションコントロールルールが自動で作成されます：</p> <ul style="list-style-type: none"> <li>• <b>ゴールデンイメージ</b></li> <li>• <b>信頼するアップデーター</b></li> </ul>



自動的に作成されたルールは、削除または編集することはできません。ルールを有効または無効にすることができます。

## DLL モジ ュール の 読み 込み を 管 理

このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。

どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、[アプリケーションコントロール] で、既定の [ゴールデンイメージ] ルールまたは「信頼する証明書」KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。[ゴールデンイメージ] ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。

Kaspersky Endpoint Security は、[DLL とドライバーを管理] をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。

## メッ セー ジの テン プレ ート

**ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。

**管理者に送信するメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの起動ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [ユーザー要求] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

## アダプティブアノマリーコントロール

この機能は Kaspersky Endpoint Security for Business Advanced および Kaspersky Total Security for Business でのみ使用可能です。Kaspersky Endpoint Security for Business の詳細については、[カスペルスキーの Web サイト](#) を参照してください。

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「Office アプリケーションによる Microsoft PowerShell の起動」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートするのと同様に、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。ルールのアップデートの適用は[手動で承認](#)する必要があります。

## アダプティブアノマリーコントロールの設定

アダプティブアノマリーコントロールの設定では、次のステップが必要です：

### 1. アダプティブアノマリーコントロールのトレーニング

アダプティブアノマリーコントロールを有効にすると、アダプティブアノマリーコントロールルールがトレーニングモードで動作します。トレーニング期間中、アダプティブアノマリーコントロールはルールを適用可能な動作が発生するかどうかを監視し、ルールを適用可能な動作が発生したらそのイベントを Kaspersky Security Center に送信します。ルールごとに、設定されているトレーニング期間は異なります。トレーニングモードの継続期間はカスペルスキーのエキスパートが設定しています。通常は、トレーニングモードの継続期間は 2 週間です。

特定のルールを適用可能な動作がトレーニング期間中に 1 回も発生しなかった場合、アダプティブアノマリーコントロールは、そのルールの対象となる動作は平常時には発生しない動作だと判断します。そのため、トレーニング終了後、該当するルールの適用対象となる動作はすべて Kaspersky Endpoint Security でブロックされるようになります。

特定のルールを適用可能な動作がトレーニング期間中に発生した場合、Kaspersky Endpoint Security は「[ルールの適用のレポート](#)」と「[スマートトレーニングでのルールの適用状況](#)」リポジトリにイベントのログ記録を保存します。

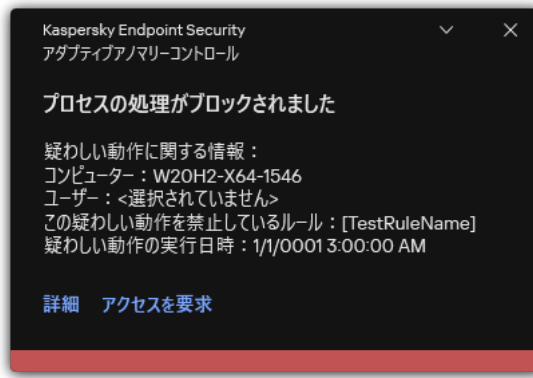
### 2. 「ルールの適用のレポート」の分析

管理者は「[ルールの適用のレポート](#)」または「[スマートトレーニングでのルールの適用状況](#)」リポジトリの内容を分析する必要があります。分析結果に基づき、管理者はそれぞれのルールが適用されたときのアダプティブアノマリーコントロールによる処理を、「ブロック」または「許可」から選択します。管理者は、ルールの適用状況に関する情報をさらに収集した上で判断を行うために、トレーニングモードの期間を延長することもできます。また、管理者がルールの適用状況のレポートに対する対応を行わなかった場合も、アダプティブアノマリーコントロールは引き続きトレーニングモードで動作します。トレーニングモードの残り期間もリセットされます。

アダプティブアノマリーコントロールの設定内容は、即座に動作に反映されます。アダプティブアノマリーコントロールの設定は、自動的に設定される場合と手動で設定する場合を合わせて、次の方法で設定されます：

- トレーニングモードの期間中に 1 回も適用可能な動作が発生しなかったルールについては、該当するルールが適用可能な動作をすべてブロックする設定が自動的に行われる。
- 新しいルールの追加や古くなったルールの削除が Kaspersky Endpoint Security によって行われる。
- 管理者がルール適用のレポートまたは[スマートトレーニングでのルールの適用状況](#)リポジトリの内容を確認した後、アダプティブアノマリーコントロールによる処理を設定します。ルール適用のレポートおよび[スマートトレーニングでのルールの適用状況](#)リポジトリの内容を確認することを推奨します。

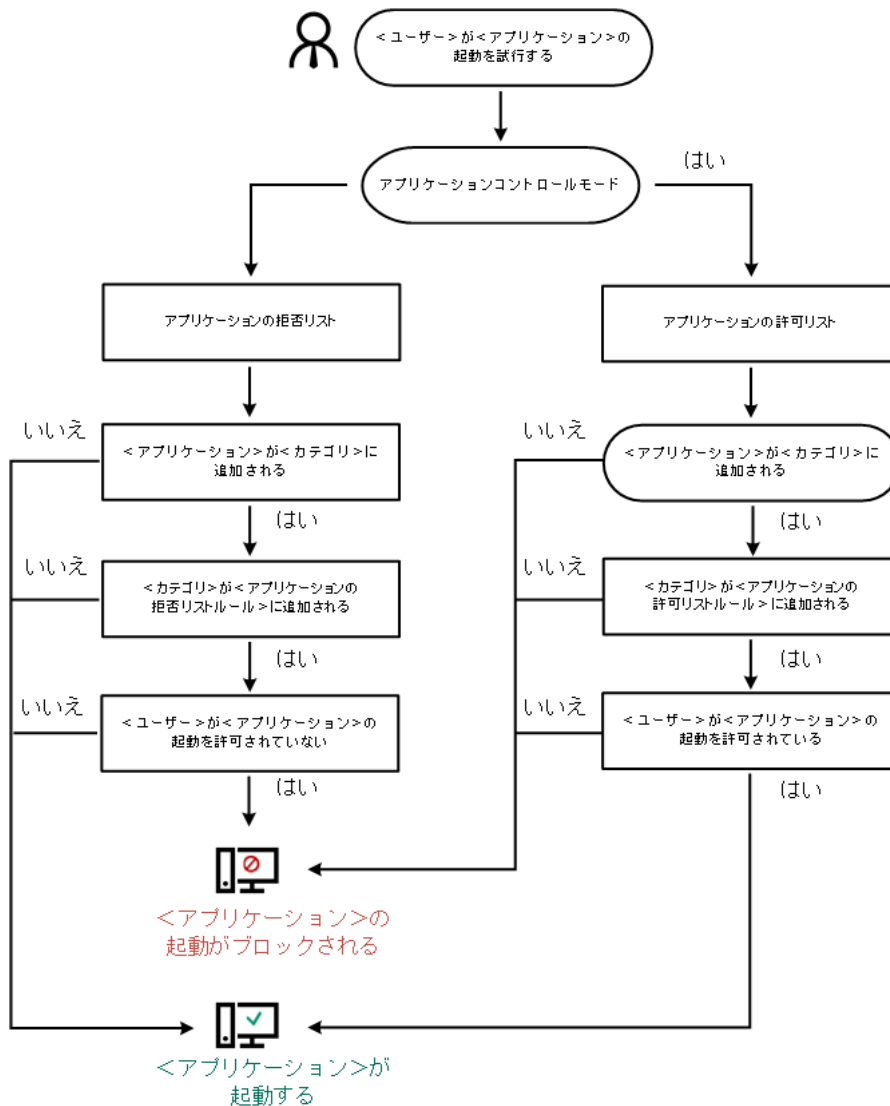
悪意のあるアプリケーションによる動作が検知された場合、Kaspersky Endpoint Security はその動作をブロックし通知を表示します（以下の図を参照）。



アダプティブアノマリーコントロールの通知

## アダプティブアノマリーコントロールの動作アルゴリズム

Kaspersky Endpoint Security は次の図のアルゴリズムに従って、ルールの適用対象となる動作の実行を許可するかブロックするかを判定します。



アダプティブアノマリーコントロールの動作アルゴリズム

### アダプティブアノマリーコントロールの設定

パラメータ	説明

<p><b>アダプティブアノマリールールステータスに関するレポート</b></p> <p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>このレポートにはアダプティブアノマリールールの検知ルールに関する情報が表示されます (ルールの状態が「オフ」または「ブロック」など)。このレポートはすべての管理グループを対象に生成されます。</p>
<p><b>アダプティブアノマリールールレポート</b></p> <p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>このレポートには、アダプティブアノマリールールを使用して検知された典型的でない動作に関する情報が含まれています。このレポートはすべての管理グループを対象に生成されます。</p>
<p><b>ルール</b></p>	<p>アダプティブアノマリールールのルールのリスト。これらのルールは、カスペルスキーのスペシャリストによって、マルウェアの可能性のあるプログラムが示す典型的な動作に基づいて作成されています。</p>
<p><b>テンプレート</b></p>	<ul style="list-style-type: none"> <li>• <b>ブロックに関するメッセージ</b>：典型的でない動作をブロックするアダプティブアノマリールールが適用された際に表示されるメッセージのテンプレート。</li> <li>• <b>管理者に送信するメッセージ</b>：ブロックが誤検知だと考えられる場合に、社内のローカルネットワークの管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：<b>アプリケーションの動作ブロックに関するメッセージが管理者に送信されました</b>。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出 [ユーザー要求] を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。</li> </ul>

## Endpoint Sensor

Kaspersky Endpoint Security 11.4.0 には Endpoint Sensor は含まれていません。

Kaspersky Security Center Web コンソールおよび Kaspersky Security Center 管理コンソールで Endpoint Sensor を管理できます。Kaspersky Security Center Cloud コンソールでは Endpoint Sensor を管理できません。

Endpoint Sensor は、Kaspersky Anti Targeted Attack Platform と連携するよう設計されています。Kaspersky Anti Targeted Attack Platform は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、Kaspersky Anti Targeted Attack（以下、「KATA」とも表記）および Kaspersky Endpoint Detection and Response（以下「KEDR」とも表記）の2つの機能ブロックがあります。KEDR 個別で購入することも可能です。ソリューションについて詳しくは、[Kaspersky Anti Targeted Attack Platform のヘルプ](#) を参照してください。

Endpoint Sensor の管理には次の制限事項があります：

- Kaspersky Endpoint Security のバージョン 11.0.0 から 11.3.0 がコンピューターにインストールされている場合は Endpoint Sensor の設定をポリシー内で設定できます。ポリシーを使用した Endpoint Sensor の設定について詳しくは、[以前のバージョンの Kaspersky Endpoint Security のヘルプの記事](#) を参照してください。
- Kaspersky Endpoint Security のバージョン 11.4.0 以降のバージョンがインストールされていると、ポリシー内で Endpoint Sensor を設定することはできません。

Endpoint Sensor は、クライアントコンピューターにインストールされます。これらのコンピューターで、コンポーネントはプロセス、有効なネットワーク接続、変更されたファイルを継続的に監視し、その情報を KATA サーバーに渡します。

このコンポーネントは、以下のオペレーティングシステムで動作します：

- Windows 7 Service Pack 1 Home / Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 RS3 Home / Professional / Education / Enterprise
- Windows 10 RS4 Home / Professional / Education / Enterprise
- Windows 10 RS5 Home / Professional / Education / Enterprise
- Windows 10 RS6 Home / Professional / Education / Enterprise
- Windows Server 2008 R2 Foundation / Standard / Enterprise（64 ビット）
- Windows Server 2012 Foundation / Standard / Enterprise（64 ビット）
- Windows Server 2012 R2 Foundation / Standard / Enterprise（64 ビット）
- Windows Server 2016 Essentials / Standard（64 ビット）

KATA の動作について詳しくは、[Kaspersky Anti Targeted Attack Platform のヘルプ](#) を参照してください。

## Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 には Kaspersky Sandbox コンポーネントが含まれています。この機能は Kaspersky Sandbox ソリューションとの連携を有効にします。Kaspersky Sandbox ソリューションはコンピューター上の高度な脅威を検知し、自動的にブロックします。Kaspersky Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Kaspersky Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Kaspersky Sandbox サーバー）上でオブジェクトを分析およびスキャンします。このソリューションについて詳しくは、[Kaspersky Sandbox](#) のヘルプを参照してください。

この機能は Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。

#### Kaspersky Sandbox コンポーネントの設定

パラメータ	説明
サーバー TLS 証明書	Kaspersky Sandbox サーバーと信頼済み接続を設定するには、TLS 証明書を準備する必要があります。次にその証明書を Kaspersky Sandbox サーバーおよび Kaspersky Endpoint Security ポリシーに追加します。証明書の準備およびサーバーへの証明書の追加について詳しくは、 <a href="#">Kaspersky Sandbox</a> のヘルプを参照してください。
Kaspersky Sandbox の接続タイムアウト	Kaspersky Sandbox サーバーの接続タイムアウトです。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、Kaspersky Sandbox の接続タイムアウトの時間を長くすることができます。既定値は 5 秒です。
Kaspersky Sandbox 要求のキュー	要求のキューフォルダーのサイズです。オブジェクトがコンピューター上でアクセス（実行ファイルが開始されたり、DOCX や PDF 形式のドキュメントを開いたり）されると、Kaspersky Endpoint Security はそのオブジェクトを Kaspersky Sandbox に送ります。複数の要求があった場合は、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは 100 MB に制限されています。最大サイズに到達すると、Kaspersky Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。
Kaspersky Sandbox サーバー	Kaspersky Sandbox サーバーの接続設定です。サーバーは配備された Microsoft Windows オペレーティングシステムの仮想イメージを使用してスキャンする必要があるオブジェクトを実行します。IP アドレス（IPv4 または IPv6）、または完全修飾ドメイン名を入力できます。
脅威の検知時の処理	<p><b>コピーを隔離に移動し、オブジェクトを削除する：</b>このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。</p> <p><b>簡易スキャンを実行する：</b>このオプションを選択した場合、Kaspersky Endpoint Security は <a href="#">簡易スキャン</a> タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。</p> <p><b>IOC スキャンを実行する：</b>このオプションを選択した場合、Kaspersky Endpoint Security は自動的に <a href="#">IOC スキャン</a> タスク（自動 IOC スキャンタスク）を作成します。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、簡易スキャンタスクの実行）を設定できます。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、簡易スキャンタスクの実行）を設定できます。その他の IOC スキャンタスクの設定を変更するには、タスクの設定に移動してください。</p>
IOC スキャン範囲	<b>重要なファイル領域：</b> このオプションを選択した場合、Kaspersky Endpoint Security はカーネルメモリやブートセクターのような、コンピューター上の重要なファイル領域にのみ IOC スキャンを実行します。

	<b>端末のシステムドライブのファイル領域</b> ：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターのシステムドライブで IOC スキャンを実行します。
<b>IOC スキャンを実行する</b>	<p><b>手動開始</b>：選択した時間に手動で IOC スキャンタスクを開始できる実行モードです。</p> <p><b>脅威の検知後</b>：脅威が検知されたときに自動で Kaspersky Endpoint Security が IOC スキャンタスクを実行する実行モードです。</p> <p><b>コンピューターを使用していないときにのみ実行する</b>：スクリーンセーバーが動作しているまたは画面がロックされているときに Kaspersky Endpoint Security が IOC スキャンタスクを実行する実行モードです。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はタスクを一時停止します。このため、タスクの完了まで数日かかることがあります。</p>

## Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 には、Kaspersky Endpoint Detection and Response Optimum ソリューション（以降「EDR Optimum」とします）の組み込みエージェントが含まれます。Kaspersky Endpoint Detection and Response Optimum は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

Kaspersky Endpoint Detection and Response Optimum は脅威の活動を調査して分析し、迅速な対応に必要な攻撃の可能性に関する情報をセキュリティの担当者または管理者に提供します。Kaspersky Endpoint Detection and Response は別のウィンドウでアラートの詳細を表示します。アラートの詳細（Alert details）は、収集済みの検知した脅威および応答操作の管理に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、[Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

この機能は Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。

### Endpoint Detection and Response Optimum の設定

パラメータ	説明
<b>ネットワーク分離</b>	<p>検知された脅威への対応として、ネットワークからコンピューターを自動的に分離します。</p> <p>ネットワーク分離がオンになると、本製品はすべてのアクティブな接続を切断し、コンピューターのすべての新規 TCP/IP 接続をブロックします。次の接続のみ有効にします：</p> <ul style="list-style-type: none"> <li>ネットワーク分離の除外リストに追加されている接続。</li> <li>Kaspersky Endpoint Security サービスによって開始された接続。</li> <li>Kaspersky Security Center 管理エージェントによって開始された接続。</li> </ul>
<b>分離されたコンピューターのロックを自動的に解除するまでの時間</b>	<p>ネットワーク分離は、指定した時間の経過後に自動で、または手動で解除することができます。既定では、Kaspersky Endpoint Security は分離の開始から 5 時間が経過するとネットワーク分離を解除します。</p>
<b>ネットワーク分離の除</b>	<p>ネットワーク分離から除外されるルールの一覧です。ネットワーク分離がオンになっても、ルールに一致するネットワーク接続はブロックされません。</p>



<b>除外リスト</b>	<p>標準のネットワークプロファイルのリストを使用してネットワーク分離の除外リストを設定できます。既定では、除外リストには DNS/DHCP サーバーおよび DNS/DHCP クライアントロールを持つデバイスの動作が妨げられないようにするルールを含むネットワークプロファイルが含まれています。標準のネットワークプロファイルまたは除外リストの設定は手動で変更できます。</p> <div style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p>ポリシーのプロパティで指定された除外リストは、脅威の検知時の対応としてネットワーク分離が自動的にオンになった場合にのみ適用されます。コンピューターのプロパティで指定された除外リストは、Kaspersky Security Center のコンソールのコンピューターのプロパティから手動でネットワーク分離をオンにした場合にのみ適用されます。</p> </div>
<b>実行防止</b>	<p>実行ファイルやスクリプトを実行したり、Office 形式のファイルを開いたりする動作をコントロールします。たとえば、選択したコンピューター上で安全でないと判断されたアプリケーションの実行を防止することができます。実行防止は、<a href="#">Office ファイルの拡張子のセット</a>および<a href="#">スクリプトインタープリターのセット</a>をサポートしています。</p>
<b>禁止されたオブジェクトを実行、または開いたときの処理</b>	<p><b>ブロックしてレポートに書き込む：</b>このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。</p> <p><b>イベントの記録のみ：</b>このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。</p>
<b>実行防止ルール</b>	<p>オブジェクトの実行防止ルールのリストです。実行防止ルールはブロック時に参照される条件の一式です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。</p>

## ディスク全体の暗号化

次の暗号化技術を選択できます：Kaspersky Disk Encryption、BitLocker ドライブ暗号化（単に BitLocker とも）。

### Kaspersky Disk Encryption

システムハードディスクが暗号化されると、次回のコンピューターの起動時、ユーザーはハードディスクにアクセスしてオペレーティングシステムを読み込む前に[認証エージェント](#)による認証を完了する必要があります。それには、コンピューターに接続されているトークンまたはスマートカードのパスワードを入力するか、[認証エージェントアカウントの管理](#)タスクを使用して LAN 管理者により作成される認証エージェントアカウントのユーザー名とパスワードを入力します。これらのアカウントは、ユーザーがオペレーティングシステムにログインする際にログインアカウントとして使用する Microsoft Windows アカウントに基づいています。また、認証エージェントアカウントのユーザー名とパスワードを使用してオペレーティングシステムに自動的にログインできる[シングルサインオン \(SSO\) 技術を使用](#)することもできます。

認証エージェントでのユーザー認証は 2 通りの方法で実行できます：

- LAN 管理者が Kaspersky Security Center ツールを使用して作成した認証エージェントアカウントの名前とパスワードを入力する。
- コンピューターに接続されたトークンまたはスマートカードのパスワードを入力する。

トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合にのみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

## BitLocker ドライブ暗号化

BitLocker は、Windows オペレーティングシステムに組み込まれた暗号化技術です。Kaspersky Endpoint Security を使用して、Kaspersky Security Center で BitLocker を制御および管理できます。BitLocker は論理ボリュームを暗号化します。BitLocker はリムーバブルドライブの暗号化には使用できません。BitLocker について詳しくは、[Microsoft 社の資料](#) を参照してください。

BitLocker 信頼済みプラットフォームモジュールを使用して、安全なアクセスキーの保管領域を提供します。Trusted Platform Module (TPM) は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。TPM は起動前のシステム整合性検証を行うため、TPM を使用すると最も安全に BitLocker アクセスキーを保管できます。TPM なしでもコンピューター上のドライブを暗号化することは可能です。この場合は、アクセスキーはパスワードで暗号化されます。BitLocker は次の暗号化の方法を使用します：

- TPM。
- TPM と PIN。
- パスワード。

ドライブを暗号化した後、BitLocker はマスター鍵を作成します。Kaspersky Endpoint Security はこのマスター鍵を Kaspersky Security Center に送るため、ユーザーがパスワードを忘れた場合などに[ディスクへのアクセスを復元](#)することができます。

ユーザーが BitLocker を使用してディスクを暗号化すると、Kaspersky Endpoint Security は [Kaspersky Security Center にディスク暗号化に関する情報](#) を送ります。一方、Kaspersky Endpoint Security はマスター鍵を Kaspersky Security Center に送らないため、Kaspersky Security Center を使用してディスクへのアクセスを復元することはできません。Kaspersky Security Center と BitLocker が正しく動作するために、[ドライブの復号化および再暗号化](#)にはポリシーを使用してください。ローカルで、またはポリシーを使用してドライブを復号化できます。

システムの暗号化後、ユーザーはオペレーティングシステムを起動するために BitLocker 認証の手順を完了する必要があります。認証手順完了後、BitLocker はユーザーのログインを許可します。BitLocker はシングルサインオン (SSO) をサポートしていません。

Windows のグループポリシーを使用している場合、ポリシーで BitLocker の管理をオフにしてください。Windows のポリシー設定は Kaspersky Endpoint Security のポリシー設定と競合する可能性があります。ドライブの暗号化の際にエラーが発生する可能性があります。

### Kaspersky Disk Encryption の設定

パラメータ	説明
暗号化モード	<b>すべてのハードディスクを暗号化する</b> ：このオプションを選択すると、ポリシーが適用された時点ですべてのハードディスクが暗号化されます。

コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。

**すべてのハードディスクを復号化する**：このオプションを選択すると、ポリシーの適用時、それ以前に暗号化されていたすべてのハードディスクが復号化されます。

**変更しない**：このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。

暗号化中に Windows ユーザー向けの認証エージェントアカウントを自動的に作成する

このチェックボックスをオンにすると、コンピューター上の Windows ユーザーアカウントのリストに基づいて認証エージェントアカウントを作成します。既定では、Kaspersky Endpoint Security は、過去 30 日間にユーザーがオペレーティングシステムにログインしたすべてのローカルアカウントとドメインアカウントを使用します。

認証エージェントアカウント作成の設定

**コンピューター上のすべてのアカウント**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、アクティブになったことのあるすべてのコンピューターのアカウントを対象に認証エージェントアカウントが作成されます。

**コンピューター上のすべてのドメインアカウント**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、アクティブになったことのある特定のドメインに属するすべてのコンピューターのアカウントを対象に認証エージェントアカウントが作成されます。

**コンピューター上のすべてのローカルアカウント**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、アクティブになったことのあるすべてのローカルコンピューターのアカウントを対象に認証エージェントアカウントが作成されます。

**ローカル管理者**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、ローカルの管理者アカウントが作成されます。

**コンピューター管理者**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、Active Directory の管理者アカウントであることがプロパティに表示されているアカウントを対象に認証エージェントアカウントが作成されます。

**アクティブなアカウント**：このチェックボックスをオンにすると、ディスク全体の暗号化タスクの実行時に、その時点でアクティブなコンピューターのアカウントを対象に認証エージェントアカウントが自動で作成されます。

このコンピューター上のすべてのユーザーの初回ログイン時に認証エージェントアカウントを自動で作成する

このチェックボックスをオンにすると、認証エージェントの開始前にコンピューター上の Windows ユーザーアカウントに関する情報をチェックします。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。認証エージェントアカウントには次の既定の設定（パスワードで保護されているログインのみ、初回認証時のパスワード変更を要求）が適用されています。そのため、すでに暗号化されたドライブを持つコンピューター用に認証エージェントアカウントの管理タスクを使用して [認証エージェントを手動で追加](#) する必要はありません。

認証エージェントに入力したユーザー名を保存する

チェックボックスをオンにすると、認証エージェントアカウントの名前が保存されます。次回、認証エージェントで同じアカウントを使用して認証を完了しようとした場合、アカウント名の入力はありません。

**使用されているディスク領域のみを暗号化**

このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。

暗号化の開始後に **「使用されているディスク領域のみを暗号化（暗号化時間を短縮）」** を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン/オフは、暗号化が開始する前に選択してください。

このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。

チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。

データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。すでに使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。

既定では、このチェックボックスはオフです。

**レガシー USB サポートを使用する**

このチェックボックスでは、レガシー USB サポートを有効または無効にします。レガシー USB サポートは BIOS / UEFI 機能であり、オペレーティングシステム (BIOS モード) を起動する前のコンピューターのブートフェーズ中に USB デバイス (セキュリティトークンなど) を使用することができます。レガシー USB サポートは、オペレーティングシステムが起動した後の USB デバイスのサポートには影響しません。

このチェックボックスをオンにすると、コンピューター起動中の USB デバイスのサポートが有効になります。

レガシー USB サポートが有効になっている場合、BIOS モードの認証エージェントでは USB を介してトークンを操作することはできません。ハードウェアの互換性の問題が発生しているコンピューターでのみ、このオプションをオンにしてください。

**パスワードの設定**

認証エージェントアカウントのパスワード強度設定。シングルサインオン (SSO) 技術の使用も有効にできます。

SSO 技術を使用すると、暗号化されたハードディスクにアクセスする際やオペレーティングシステムにサインインする際に、同一のアカウント認証情報を使用できます。

このチェックボックスをオンにすると、アカウントの資格情報を入力してから暗号化されたハードディスクにアクセスすればオペレーティングシステムに自動的にログインできます。

このチェックボックスをオフにすると、暗号化されたハードディスクにアクセスしてからオペレーティングシステムにログインする場合に、暗号化されたハードディスクへのアクセスに必要な資格情報と、オペレーティングシステムのユーザーアカウントの資格情報を個別に入力する必要があります。

**ヘルプテキスト**

**認証**：アカウントの認証情報を入力するときに認証エージェントウィンドウに表示されるヘルプテキスト。

**パスワードの変更**：認証エージェントアカウントのパスワードを変更するときに、認証エージェントウィンドウに表示されるヘルプテキスト。

**パスワードの復元**：認証エージェントアカウントのパスワードを復元するときに、認証エージェントウィンドウに表示されるヘルプテキスト。



パラメータ	説明
暗号化モード	<p><b>すべてのハードディスクを暗号化する</b>：このオプションを選択すると、ポリシーが適用された時点ですべてのハードディスクが暗号化されます。</p> <div data-bbox="416 331 1493 495" style="border: 1px solid #f08080; padding: 5px; margin: 10px 0;"> <p>コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。</p> </div> <p><b>すべてのハードディスクを復号化する</b>：このオプションを選択すると、ポリシーの適用時、それ以前に暗号化されていたすべてのハードディスクが復号化されます。</p> <p><b>変更しない</b>：このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。</p>
タブレットでブリーフキーボード入力が必要な BitLocker 認証を使用できるようにする	<p>このチェックボックスでは、起動前の環境でデータ入力を必要とする認証を使用するかしないかを選択します。この設定は、起動前に入力できる機能がないプラットフォームに対しても適用されます（例：タブレットのタッチスクリーンキーボード）。</p> <div data-bbox="416 969 1493 1133" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>タブレットコンピューターのタッチスクリーンは起動前環境では利用できません。タブレットコンピューターで BitLocker 認証を完了するには、ユーザーは USB キーボードなどを接続する必要があります。</p> </div> <p>このチェックボックスをオンにすると、起動前の入力を必要とする認証の使用が許可されます。この設定は、起動前の環境でデータ入力ができるツールがあるデバイスに対してのみ使用してください（例：タッチスクリーンキーボードだけでなく USB キーボードも付いているデバイスなど）。</p> <p>チェックボックスをオフにすると、タブレットコンピューターで BitLocker ドライブ暗号化が使用できなくなります。</p>
ハードウェア暗号化を使用	<p>このチェックボックスをオンにすると、ハードウェア暗号化が適用されます。ハードウェア暗号化を使用すると、より少ないコンピューターリソースで、より速く暗号化することができます。</p>
使用されているディスク領域のみを暗号化 (Windows 8 以降)	<p>このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。</p> <div data-bbox="416 1697 1493 1890" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>暗号化の開始後に [使用されているディスク領域のみを暗号化 (暗号化時間を短縮)] を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン/オフは、暗号化が開始する前に選択してください。</p> </div> <p>このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。</p> <p>チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。</p>

データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。すでに使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。

既定では、このチェックボックスはオフです。

## 認証設定

### パスワードを使用 (Windows 8 以降)

このオプションを選択すると、暗号化されたドライブにアクセスしようとした際に、パスワードの入力が要求されます。

このオプションは、Trusted Platform Module (TPM) が使用されていない場合に選択できます。

### Trusted Platform Module (TPM) を使用

このオプションを選択すると、BitLocker は Trusted Platform Module (TPM) を使用します。

*Trusted Platform Module (TPM)* は、セキュリティ関連の基本機能 (暗号化鍵の保存など) を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。

Windows 7 と Windows 2008 R2 では、TPM モジュールを使用した暗号化のみを利用できます。TPM モジュールがインストールされていない場合、BitLocker 暗号化は実行できません。これらのオペレーティングシステムを使用しているコンピューターでは、パスワードを使用した暗号化はサポートされません。

Trusted Platform Module を搭載したデバイスで作成された暗号鍵は、そのデバイスでしか復号化できません。Trusted Platform Module は、各 TPM が保持するストレージルートキーを使って暗号鍵を暗号化します。ストレージルートキーは Trusted Platform Module 内部に格納されています。そのため、暗号鍵を盗もうとする試みに対して、より強固な保護を提供することができます。

既定では、この処理が選択されています。

暗号化鍵およびパスワードまたは PIN で保護された暗号化鍵へのアクセスに、より強固な保護を提供することが可能です。

- **TPM の PIN を使用する**：このチェックボックスをオンにすると、Trusted Platform Module (TPM) 内に格納されている暗号鍵にアクセスする際に暗証番号を使用できます。  
このチェックボックスをオフにすると、PIN コードの使用が禁止されます。暗号鍵へのアクセスには、パスワードの入力が必要となります。  
ユーザーに拡張 PIN の使用を許可することができます。拡張 PIN を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります。

- **Trusted Platform Module (TPM) を使用する。使用できない場合はパスワードを使用する**：このチェックボックスをオンにすると、Trusted Platform Module (TPM) が使用できない場合、パスワードを使用して暗号鍵にアクセスできます。

チェックボックスがオフの場合は TPM は使用できず、ディスク全体の暗号化は開始されません。



## ファイルレベルの暗号化

拡張子や拡張子グループ、ローカルコンピューターのドライブに保存されているフォルダーのリストに基づいて、[ファイルのリストを作成](#)できます。また、[特定のアプリケーションで作成されたファイルを暗号化するルール](#)を作成できます。ポリシーが適用されると、Kaspersky Endpoint Security は以下のファイルを暗号化および復号化します：

- 暗号化および復号化のリストに追加されたファイル
- 暗号化および復号化のリストに追加されたフォルダーにあるファイル
- 別々のアプリケーションによって作成されたファイル

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ファイル暗号化には、次の特別な機能があります：

- Kaspersky Endpoint Security は、オペレーティングシステムのローカルユーザープロファイルについてのみ定義済みフォルダーのファイルの暗号化や復号化を行います。Kaspersky Endpoint Security は、移動ユーザープロファイル、固定ユーザープロファイル、一時ユーザープロファイル、またはリダイレクトされたフォルダーの、定義済みフォルダー内のファイルを暗号化または復号化しません。
- Kaspersky Endpoint Security は、暗号化が原因でオペレーティングシステムやインストールされたアプリケーションに損害を与える可能性がある場合は、ファイルを暗号化しません。たとえば、次のファイルおよびフォルダーは、入れ子になっているすべてのフォルダーとともに、暗号化しないファイルまたはフォルダーのリストに含まれます：
  - %WINDIR%;
  - %PROGRAMFILES% and %PROGRAMFILES(X86)%;
  - Windows のレジストリファイル

暗号化しないファイルまたはフォルダーのリストは、表示することも編集することもできません。暗号化除外リストにあるファイルとフォルダーは暗号化リストに追加できますが、ファイルの暗号化中は暗号化されません。

ファイルレベルの暗号化の設定

パラメータ	説明
暗号化の管理	<p><b>変更しない</b>：このオプションを選択すると、ファイルやフォルダーの状態は維持され暗号化や復号化は行われません。</p> <p><b>ルールに従い暗号化する</b>：このオプションを選択すると、暗号化ルールに従ってファイルとフォルダーが暗号化され、復号化ルールに従ってファイルとフォルダーが復号化されます。また、アプリケーションのルールに従って暗号化されたファイルへのアクセスが規制されます。</p> <p><b>デバイス全体の復号化</b>：このオプションを選択すると、暗号化されたすべてのファイルとフォルダーが復号化されます。</p>
暗号化ル	このタブには、ローカルドライブに保存されているファイルの暗号化ルールが表示され

<p>ール</p>	<p>ます。次のようにファイルを追加できます：</p> <ul style="list-style-type: none"> <li> <b>定義済みフォルダー</b>：Kaspersky Endpoint Security では、次の領域を追加できます： <ul style="list-style-type: none"> <li><b>ドキュメント</b>：オペレーティングシステムの標準の [ドキュメント] フォルダー内のファイルとそのサブフォルダー。</li> <li><b>お気に入り</b>：オペレーティングシステムの標準の [お気に入り] フォルダー内のファイルとそのサブフォルダー。</li> <li><b>デスクトップ</b>：オペレーティングシステムの標準の [デスクトップ] フォルダー内のファイルとそのサブフォルダー。</li> <li><b>一時ファイル</b>：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の動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。</li> <li><b>Outlook ファイル</b>：Outlook メールクライアントの動作に関連するファイル (データファイル (PST)、オフラインデータファイル (OST)、オフラインアドレス帳ファイル (OAB)、および個人のアドレス帳ファイル (PAB))。</li> </ul> </li> <li> <b>フォルダー</b>：フォルダーのパスを入力できます。フォルダーのパスを追加するときは、次のルールに従います： <ul style="list-style-type: none"> <li>環境変数を使用します (たとえば、%FOLDER%\UserFolder\ )。環境変数は、パスの先頭で一度だけ使用できます。</li> <li>相対パスは使用しないでください。 \..\ のセットを使用できます (例：C:\Users\..\UserFolder\ )。 \..\ のセットは、親フォルダーへの移動を意味します。</li> <li>*および?の文字は使用しないでください。</li> <li>UNC パスは使用しないでください。</li> <li>区切り文字として、 ; または , を使用してください。</li> </ul> </li> <li> <b>ファイルの拡張子による指定</b>：拡張グループのアーカイブなど、拡張グループをリストから選択できます。ファイルの拡張子を手動で追加することもできます。 </li> </ul>
<p>復号化ルール</p>	<p>このタブには、ローカルドライブに保存されているファイルの復号化ルールが表示されます。</p>
<p>アプリケーションのルール</p>	<p>このタブには、暗号化されたファイルに対するアプリケーションのアクセスルールおよび、個別のアプリケーションによって作成または変更されたファイルの暗号化ルールのテーブルが表示されます。</p>
<p>暗号化されたパッケージのパスワード設定</p>	<p>暗号化されたパッケージの作成時に必要なパスワードの強度。</p>

## リムーバブルドライブの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムのファイルの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、このリムーバブルドライブの暗号化タスクはエラーにより失敗し、リムーバブルドライブが読み取り専用になります。

リムーバブルドライブ上のデータを保護するには、次の暗号化種別を使用できます：

- ディスク全体の暗号化（FDE）  
ファイルシステムを含むリムーバブルドライブ全体の暗号化。

企業ネットワークの外部で暗号化されたデータにアクセスすることはできません。Kaspersky Security Center へ接続されていないコンピューターの場合（ゲストコンピューターなど）も、企業ネットワーク内の暗号化されたデータへアクセスできません。

- ファイルレベルの暗号化（FLE）  
リムーバブルドライブ上のファイルのみの暗号化。ファイルシステムは変更されません。

リムーバブルドライブ上のファイルの暗号化は、[ポータブルモード](#)と呼ばれる特別なモードを使用して、企業ネットワークの外部のデータにアクセスする機能を提供します。

暗号化中に、Kaspersky Endpoint Security はマスター鍵を作成します。Kaspersky Endpoint Security は、マスター鍵を次のリポジトリに保存します：

- Kaspersky Security Center
- ユーザーのコンピューター  
マスター鍵はユーザーの秘密鍵で暗号化されます。
- リムーバブルドライブ  
マスター鍵は、Kaspersky Security Center の公開鍵で暗号化されています。

暗号化が完了すると、従来のリムーバブルドライブを暗号化せずに使用しているかのように、企業ネットワーク内でリムーバブルドライブ上のデータにアクセスできます。

## 暗号化されたデータへのアクセス

暗号化されたデータのリムーバブルドライブが接続されると、Kaspersky Endpoint Security は次のアクションを実行します：

1. ユーザーのコンピューターのローカル保管領域でマスター鍵を確認します。  
マスター鍵が見つかった場合、ユーザーはリムーバブルドライブ上のデータにアクセスできます。  
マスター鍵が見つからない場合、Kaspersky Endpoint Security は次のアクションを実行します：
  - a. Kaspersky Security Center に要求を送信します。  
要求を受け取った後、Kaspersky Security Center はマスター鍵を含む応答を送信します。
  - b. Kaspersky Endpoint Security は、暗号化されたリムーバブルドライブを使用した、それ以降の操作のために、ユーザーのコンピューターのローカル保管領域にマスター鍵を保存します。

2. データを復号化します。

## リムーバブルドライブ暗号化の特別な機能

リムーバブルドライブの暗号化には、次の特別な機能があります：

- リムーバブルドライブの暗号化に関する事前設定はポリシーに含まれます。このポリシーは、管理対象コンピューターの特定のグループに対して作成されています。このため、リムーバブルドライブの暗号化または復号化の設定を含む Kaspersky Security Center ポリシーの適用結果は、そのリムーバブルドライブがどのコンピューターに接続しているかによって異なります。
- Kaspersky Endpoint Security は、リムーバブルドライブに保存されている読み取り専用ステータスのファイルの暗号化や復号化は行いません。
- リムーバブルドライブとして、次のデバイス種別がサポートされています：
  - USB バス経由で接続されているリムーバブルドライブ
  - USB および FireWire バス経由で接続されているハードディスク
  - USB および FireWire バス経由で接続されている SSD ドライブ

### リムーバブルドライブの暗号化機能の設定

パラメータ	説明
暗号化の管理	<p><b>リムーバブルドライブ全体の暗号化：</b>このオプションを選択した場合、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、ファイルシステムも含めて、リムーバブルドライブをセクター単位で暗号化します。</p> <p><b>すべてのファイルの暗号化：</b>このオプションをオンにすると、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、リムーバブルドライブに保存されているすべてのファイルを暗号化します。既に暗号化されたファイルの再暗号化は実行しません。暗号化されるフォルダー構造やファイルの名前を含む、リムーバブルドライブのファイルシステムの内容は暗号化されないため、引き続きアクセスできます。</p> <p><b>新しいファイルのみ暗号化：</b>このオプションをオンにすると、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、Kaspersky Security Center ポリシーが前回適用された後でリムーバブルドライブに追加されたファイル、またはポリシーの適用後にリムーバブルドライブ上で変更されたファイルのみを暗号化します。この暗号化モードは、リムーバブルドライブをプライベートと仕事の両方で使う場合に便利です。この暗号化モードでは、既存のファイルをすべて変更しないまま残し、Kaspersky Endpoint Security がインストールされ暗号化機能が有効になっている作業用コンピューター上でユーザーが作成したファイルだけを暗号化できます。このため、Kaspersky Endpoint Security がインストールされているコンピューターで暗号化機能が有効になっているかいないかにかかわらず、個人用のファイルには常にアクセスすることができます。</p> <p><b>リムーバブルドライブ全体の復号化：</b>このオプションを選択した場合、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、リムーバブルドライブに保存されている暗号化ファイルをすべて復号化すると共に、リムーバブルドライブのファイルシステムも以前に暗号化されている場合は復号化します。</p> <p><b>変更しない：</b>このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。</p>
ポータブ	このチェックボックスを使用して、社内ネットワーク外にあるコンピューターのリムーバブルドライブ上に保存されたファイルにアクセスできるようにするためのリムーバブルドライ

<p><b>ルモード</b></p>	<p>ブの準備を有効または無効にすることができます。</p> <p>このチェックボックスをオンにした場合、ポリシーを適用すると、リムーバブルドライブにあるファイルを暗号化する前にパスワードを指定するよう要求されます。社内ネットワーク外にあるコンピューターのリムーバブルドライブ上の暗号化ファイルにアクセスするにはパスワードが必要です。パスワードの強度を設定できます。</p> <p>ポータブルモードは、<b>すべてのファイルの暗号化モードまたは新しいファイルのみ暗号化モード</b>で使用できます。</p>
<p><b>使用されているディスク領域のみを暗号化</b></p>	<p>このチェックボックスでは、ディスクの使用されている領域のみを暗号化する暗号化モードを有効または無効にできます。データが変更されたり削除されていない新しいドライブでは、このモードを使用してください。</p> <p>このチェックボックスをオンにすると、ドライブ内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。</p> <p>チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ディスク全体が暗号化されます。</p> <p>占有領域のみを暗号化する機能は、<b>リムーバブルドライブ全体の暗号化モード</b>でのみ使用できます。</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>暗号化の開始後に [使用されているディスク領域のみを暗号化] の有効または無効を切り替えても、設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。</p> </div>
<p><b>選択したデバイスの暗号化ルール</b></p>	<p>このテーブルには、カスタムの暗号化ルールが定義されているデバイスが表示されます。次の方法で、個々のリムーバブルドライブの暗号化ルールを作成できます：</p> <ul style="list-style-type: none"> <li>• デバイスコントロール用の信頼するデバイスのリストからリムーバブルドライブを追加します。</li> <li>• リムーバブルドライブを手動で追加します： <ul style="list-style-type: none"> <li>• デバイス ID を使用：ハードウェア ID、または HWID</li> <li>• デバイスモデルを使用：製造元 ID (VID) および製品 ID (PID)</li> </ul> </li> </ul>
<p><b>オフラインモードでのリムーバブルドライブの暗号化を許可する</b></p>	<p>このチェックボックスがオンになっている場合、Kaspersky Endpoint Security は、Kaspersky Security Center との接続がない場合でもリムーバブルドライブを暗号化します。この場合、リムーバブルドライブの復号化に必要なデータはリムーバブルドライブが接続されているコンピューターのハードディスク上に保存され、Kaspersky Security Center には配信されません。</p> <p>このチェックボックスをオフにすると、Kaspersky Security Center への接続がない場合、Kaspersky Endpoint Security はリムーバブルドライブを暗号化しません。</p>
<p><b>ポータブルモード</b></p>	<p>ポータブルファイルマネージャーのパスワードの強度設定。</p>



## テンプレート（データの暗号化）

データの暗号化後、Kaspersky Endpoint Security は、たとえば組織のインフラストラクチャの変更や Kaspersky Security Center 管理サーバーの変更により、データへのアクセスを制限する場合があります。ユーザーが暗号化されたデータにアクセスできない場合、ユーザーは管理者にデータへのアクセスを依頼できます。つまり、ユーザーはアクセス要求ファイルを管理者に送信する必要があります。ユーザーは、管理者から受け取った応答ファイルを Kaspersky Endpoint Security にアップロードする必要があります。Kaspersky Endpoint Security では、管理者からのデータへのアクセスをメールで要求できます（下の図を参照）。



暗号化されたデータへのアクセス要求

暗号化されたデータへのアクセスができないことを報告するためのテンプレートが提供されます。ユーザーの利便性のため、次のフィールドに入力できます：

- **宛先**：データ暗号化機能に対する権限を持つ管理者グループのメールアドレスを入力します。
- **発行先**：暗号化されたファイルへのアクセス権をリクエストするメールの件名を入力します。たとえば、タグを追加してメッセージをフィルタリングできます。
- **メッセージ**必要に応じて、メッセージの内容を変更します。変数を使用して、必要なデータを取得できます（たとえば、%USER\_NAME%変数）。

## 除外リスト

信頼ゾーンは Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。



管理者は処理されるオブジェクトとコンピューターにインストールされるアプリケーションの特徴を考慮しながら、信頼ゾーンを個別に定義します。Kaspersky Endpoint Security がアクセスをブロックする特定のオブジェクトやアプリケーションが無害であることが確実なときには、オブジェクトやアプリケーションを信頼ゾーンに含めなければならない場合があります。管理者が、ユーザーが特定のコンピューターに対してローカルの信頼するゾーンを作成するよう許可することも可能です。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。

## 信頼するオブジェクト

信頼するオブジェクトとは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。

信頼するオブジェクトにより、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアを安全に使用できるようになります。悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアについて詳しくは、カスペルスキーの[ウイルス百科事典](#)を参照してください。

このようなアプリケーションは Kaspersky Endpoint Security によってブロックされる場合があります。ブロックしないようにするには、使用している製品を信頼するオブジェクトに設定できます。これを行うには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクを信頼ゾーンに追加します。たとえば、ユーザーがコンピューターのリモート管理用に Radmin アプリケーションを使用しているとします。Kaspersky Endpoint Security はこの処理を疑わしいものとみなして、ブロックする可能性があります。アプリケーションがブロックされないようにするには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクによって信頼するオブジェクトを作成します。

情報を収集し、それを処理するために送信するアプリケーションがコンピューターにインストールされていると、Kaspersky Endpoint Security がそのアプリケーションをマルウェアに分類する可能性があります。それを防ぐために、ヘルプ内で説明する方法で Kaspersky Endpoint Security を設定することで、そのアプリケーションをスキャン対象から除外できます。

システム管理者が設定した以下のコンポーネントとタスクによって信頼するオブジェクトを使用できます：

- [ふるまい検知](#)
- [脆弱性攻撃ブロック](#)：
- [ホスト侵入防止](#)：
- [ファイル脅威対策](#)：
- [ウェブ脅威対策](#)
- [メール脅威対策](#)
- [スキャンタスク](#)：

## 信頼するアプリケーションのリスト

信頼するアプリケーションのリストは、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Endpoint Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Endpoint Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトをスキャンし、すべてのアプリケーションとこのようなオブジェクトが生成するネットワークトラフィックの処理を管理します。しかし、信頼するアプリケーションのリストに追加されたアプリケーションは Kaspersky Endpoint Security のスキャンからは除外されます。


たとえば、Microsoft Windows 標準のメモ帳アプリケーションで使用するオブジェクトはスキャンしなくても安全であると考えられる場合は、Microsoft Windows メモ帳を信頼するアプリケーションのリストに追加できます。これにより、スキャン処理では、このアプリケーションが使用するオブジェクトがスキップされます。

また、特定の処理が Kaspersky Endpoint Security によって疑わしい処理に分類されたとしても、多数のアプリケーションの機能を考慮すると安全な場合があります。たとえば、キーボードで入力したテキストの取得は、自動キーボードレイアウト切り替えプログラム (Punto Switcher など) では通常の処理です。このようなアプリケーションの特性を考慮して、アプリケーション処理を監視対象から除外するために、このようなアプリケーションを信頼するアプリケーションのリストに追加してください。

信頼するアプリケーションをスキャン対象から除外することで、Kaspersky Endpoint Security とその他のプログラムとの競合 (Kaspersky Endpoint Security と他のアンチウイルス製品による、サードパーティ製コンピューターのネットワークトラフィックの二重スキャンの問題など) を回避し、コンピューターのパフォーマンスを高めることができます。この点は、サーバーアプリケーションを使用する上では特に重要です。

ただし、信頼するアプリケーションの実行ファイルとプロセスのウイルスおよびその他のマルウェアスキャンは実行されます。アプリケーションを Kaspersky Endpoint Security のスキャンから完全に除外するには、信頼するオブジェクトを設定します。

#### 除外リストの設定

パラメータ	説明
検知するオブジェクトの種別	<p>製品設定にかかわらず、Kaspersky Endpoint Security は常にウイルスやワーム、トロイの木馬を検知してブロックします。これらのプログラムはコンピューターに重大な損害を与える可能性があります。</p> <ul style="list-style-type: none"><li>• <a href="#">ウイルス、ワーム</a> </li></ul>

## サブカテゴリ：ウイルスやワーム (Viruses\_and\_Worms)

### 危険性：高

古典的なウイルスやワームは、ユーザーが許可していない処理を実行します。このようなウイルスやワームは、自己複製が可能な自身のコピーを作成することができます。

### 古典的ウイルス

古典的ウイルスがコンピューターに侵入すると、ファイルに感染して活動を開始し、悪意のある処理を実行し、それ自体のコピーを他のファイルに追加します。

古典的ウイルスは、コンピューターのローカルリソースでしか増殖しないため、自力で他のコンピューターに侵入できません。このウイルスが別のコンピューターに感染するのは、ウイルス自身のコピーを共有フォルダーに保管されているファイルまたは挿入されたCDに追加したときや、ユーザーが感染したファイルを添付したメールを転送したときです。

古典的ウイルスのコードはコンピューター、オペレーティングシステム、アプリケーションの各種領域に侵入する可能性があります。環境により、ウイルスは、ファイルウイルス、ブートウイルス、スクリプトウイルス、およびマクロウイルスに分けられます。

ウイルスはさまざまな技法を駆使してファイルを感染させます。上書きウイルスは、そのコードを、感染したファイルのコードに上書きして、そのファイルの内容を消去します。感染したファイルは機能しなくなり、復元できません。寄生ウイルスは、ファイルを変更しますが、ファイルが完全にまたは部分的に機能する状態を維持します。コンパニオンウイルスは、ファイルを変更しませんが、代わりに複製を作成します。感染したファイルが開かれると、ウイルスの複製（実際にはこれがウイルス）が起動します。他にも、次のような種別のウイルスが見つかっています：リンクウイルス、OBJウイルス、LIBウイルス、ソースコードウイルスなど多数。

### ワーム

古典的ウイルスのコードと同様に、ワームのコードは、コンピューターに侵入してから活動を開始し、悪意のある処理を実行します。ワームは、コンピューターから別のコンピューターに「這うように移動」し、ユーザーの許可なく多数のデータチャネルを経由してコピーを拡散させることから、この名が付けられました。

さまざまなワームの種類を区別する主な特徴は、その拡散方法です。次のテーブルに、拡散方法によって分類される各種ワームの概要を示します：

ワームの拡散方法

種別	Name	説明
メールワーム	メールワーム	これらのワームはメールを介して広がります。

		<p>感染したメールには、ワームのコピーを含んだ添付ファイル、あるいは感染した Web サイトまたは感染させる目的で作成された Web サイトにアップロードされるファイルへのリンクが含まれています。添付ファイルを開くと、ワームが起動します。リンクをクリックし、ファイルをダウンロードして開くと、ワームも悪意のある処理を実行し始めます。その後、ワームは他のメールアドレスを検索して、これらのアドレスに感染メールを送信しながら、自身のコピーを拡散し続けます。</p>
<b>IM ワーム</b>	IM クライアントワーム	<p>インスタントメッセージ (IM) クライアント経由で拡散します。</p> <p>通常、このようなワームは、ユーザーの連絡先リストを使用して、ワームのコピーに感染した Web サイト上のファイルへのリンクを含んだメールを送信します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。</p>
<b>IRC ワーム</b>	インターネットチャットワーム	<p>このワームはインターネットリレーチャット (インターネット上の別のユーザーとリアルタイムで通信できるサービスシステム) を介して拡散します。</p> <p>この種のワームは、インターネットチャットで自身のコピーを含むファイルまたはそのファイルへのリンクを公開します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。</p>
<b>インターネットワーム (Net-Worm)</b>	ネットワークワーム	<p>これらのワームは、コンピューターネットワークを介して広がります。</p> <p>通常のネットワークワームは、他の種類のワームと異なり、ユーザーが参加していなくても拡散します。このワームはプライベートネットワークに、脆弱性のあるプログラムがインストールされたコンピューターがないか探します。この操作を行うために、このワームはワームコードまたはその一部を含む特別に形成されたネットワークパケット (エクスプロイト) を送信します。ネットワーク上に「脆弱な」コンピューターが存在すると、そのコンピューターはこのようなネットワークパケットを受信します。ワームが完全にコンピューターに侵入すると、ワームが起動します。</p>
<b>P2P ワーム</b>	ファイル共有ネットワークワーム	<p>peer-to-peer のファイル共有ネットワーク経由で拡散します。</p> <p>P2P ネットワークに潜入するために、ワームはそれ自身をファイル共有フォルダーにコピーします。このフォルダーは通常、ユーザーのコンピューター上にあります。P2P ネットワークでは、ネットワーク上の感染したファイルをユーザーが他のファイルと同様に「見つけ」、このファイルをダウンロードして開くように、このファイルに関する情報が表示されます。</p> <p>さらに巧妙なワームは特定の P2P ネットワークのネットワークプロトコルを装って検索クエリに肯定応答を返し、自身のコピーをダウンロードさせます。</p>
<b>ワーム</b>	他の種類のワーム	<p>他の種類のワームには、以下のものがあります：</p> <ul style="list-style-type: none"> <li>自身のコピーをネットワークリソースを介して拡散するワーム。このようなワームは、オペレーティングシステムの機能を使って使用可能なネットワークフォルダーを検索し、インターネット上のコンピューターへ</li> </ul>

接続し、このコンピューターのディスクドライブへのフルアクセス権を取得しようと試みます。他の種類のワームは上記種類のワームとは異なり、自力で起動するのではなく、ユーザーがワームのコピーを含むファイルを開いたときに起動します。

- 上記のどの拡散方法も使用しないワーム（携帯電話を通じて拡散するワームなど）。

- [トロイの木馬（ランサムウェアを含む）](#) 

## サブカテゴリ：トロイの木馬

### 危険性：高

ワームやウイルスとは異なり、トロイの木馬は自己複製しません。たとえば、ユーザーが感染している Web サイトにアクセスすると、トロイの木馬はメールやブラウザからコンピューターに侵入します。トロイの木馬は、ユーザーの関与によって起動します。起動直後に、悪意のある処理を実行し始めます。

トロイの木馬は多種多様で、感染コンピューター上でのふるまいも多岐にわたります。トロイの木馬の主な機能は、情報のブロック、改変、破壊、およびコンピューターまたはネットワークの無効化です。また、トロイの木馬はファイルの送受信、ファイルの実行、画面上へのメッセージの表示、Web サイトの要求、プログラムのダウンロードとインストール、コンピューターの再起動を行うこともできます。

多くの場合、ハッカーはトロイの木馬の「セット」を使用します。

次のテーブルでは、トロイの木馬における動作の種類について説明します。

感染コンピューターにおけるトロイの木馬の動作種類

種別	Name	説明
Trojan-ArcBomb	トロイの木馬 - 「圧縮爆弾」	このアーカイブは、解凍するとコンピューターの動作に影響を与える程度のサイズにまで膨張します。 ユーザーがこのようなアーカイブを解凍しようとする、コンピューターは処理速度が低下したりフリーズしたりすることがあります。また、ハードディスクが「空の」データで満杯になることがあります。「圧縮爆弾」は、特にファイルサーバーやメールサーバーにとって危険です。サーバーが自動システムを使用して受信情報を処理すると、「圧縮爆弾」によってサーバーが停止することがあります。
バックドア	リモート管理用のトロイの木馬	このプログラムは、トロイの木馬の中でも最も危険なものと考えられます。機能面で、コンピューターにインストールされるリモート管理アプリケーションに似ています。 これらのプログラムは、ユーザーに気付かれずにコンピューターにインストールされるので、侵入者はコンピューターを遠隔管理できます。
トロイの木馬	トロイの木馬	トロイの木馬には、次のような悪意のあるアプリケーションがあります： <ul style="list-style-type: none"><li>• <b>古典的なトロイの木馬</b>：これらのプログラムはトロイの木馬の主な機能（情報のブロック、改変または破壊、およびコンピューターまたはネットワークの無効化）のみを実行し、テーブルに示す他の種類のトロイの木馬とは異なり、高度な機能を持っていません。</li><li>• <b>多目的なトロイの木馬</b>：これらのプログラムは、数種類のトロイの木馬に特徴的な先進機能を備えています。</li></ul>
Trojan-	トロ	このプログラムは、ユーザーの情報を「人質」にと



Ransom	イの木馬型ランサムウェア	って改変したり、ブロックしたりします。また、ユーザーが情報を使用する能力を喪失するように、コンピューターの動作に影響を与えます。侵入者は、コンピューターのパフォーマンスと保存されていたデータを復元するアプリケーションを送るという約束と引き替えに、ユーザーから身代金を要求します。
Trojan-Clicker	トロイの木馬クリッカー	このプログラムは、ブラウザーにコマンドを送信するか、オペレーティングシステムファイルで指定されている Web アドレスを変更することによって、ユーザーのコンピューターから Web サイトにアクセスします。  侵入者はこのようなプログラムを使用することによって、ネットワーク攻撃を行って Web サイトのアクセス数を増やし、バナー広告の表示回数を増やします。
Trojan-Downloader	トロイの木馬ダウンロード	これは侵入者の Web サイトにアクセスして、そこから他の悪意のあるアプリケーションをダウンロードし、ユーザーのコンピューターにインストールします。このプログラムには、悪意のあるアプリケーションをダウンロードまたは受信するためにアクセスした Web サイトのファイル名が含まれていることがあります。
Trojan-Dropper	トロイの木馬ドロッパー	このプログラムは他のトロイの木馬を内包しており、この内包されたプログラムがハードディスクにインストールされ、実行されます。  侵入者は、トロイの木馬ドロッパー型プログラムを次のような目的で使用することがあります： <ul style="list-style-type: none"> <li>• ユーザーに気付かれずに悪意のあるプログラムをインストールする：トロイの木馬ドロッパー型プログラムは、メッセージを表示しないか、たとえば、アーカイブ中にエラーが発生したことやオペレーティングシステムが互換性のないバージョンであることを示すといった偽のメッセージを表示します。</li> <li>• 既知の悪意のある別のアプリケーションが検知されないようにする：すべてのアンチウイルスのソフトウェアがトロイの木馬ドロッパー型アプリケーション内の悪意のあるアプリケーションを検知できるわけではありません。</li> </ul>
Trojan-Notifier	トロイの木馬型ノーティファイア	このプログラムは、感染したコンピューターにアクセスできることを侵入者に教えるため、コンピューターの次のような情報を侵入者に送信します：IP アドレス、開いているポートの番号、メールアドレスなど。このプログラムはこれらの情報をメール、FTP、侵入者の Web サイトへのアクセス、あるいはこれら以外の方法で侵入者に送ります。  トロイの木馬型ノーティファイアプログラムは、多くの場合、複数のトロイの木馬からなるセットとして使用されます。また、このプログラムはトロイの木馬がユーザーのコンピューターにインストールされたことを侵入者に知らせます。
Trojan-	トロイ	これらのトロイの木馬により、侵入者は、ユーザー

Proxy	イの木馬型プロキシ	のコンピューターを使って匿名で Web サイトにアクセスします。このトロイの木馬はスパムの送信によく利用されます。
Trojan-PSW	パスワード窃盗ソフトウェア	<p>パスワード窃盗ソフトウェアは、ソフトウェア登録データなどのユーザーアカウントを盗むトロイの木馬の一種です。このトロイの木馬はシステムファイルおよびレジストリ内の機密データを見つけ、そのデータを「攻撃者」にメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって送信します。</p> <p>これらのトロイの木馬のうち、いくつかがこのテーブルに示す種類に分類されます。これらは、銀行のアカウント情報 (Trojan-Banker)、メッセージクライアントのユーザーのデータ (Trojan-IM)、およびオンラインゲームのユーザーの情報 (Trojan-GameThief) を盗むトロイの木馬です。</p>
Trojan-Spy	スパイウェア型トロイの木馬	このトロイの木馬はコンピューター上で動作しながら、ユーザーが行う処理に関する情報を収集して、ユーザーの行動を秘密裏に監視します。このトロイの木馬は、ユーザーがキーボードで入力するデータの傍受、スクリーンショットの撮影、あるいはアクティブなアプリケーションのリストの収集などを行うことがあります。このプログラムが情報を入手すると、その情報をメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。
Trojan-DDoS	トロイの木馬ネットワークアタッカー	<p>このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します (サービス妨害攻撃、または DoS 攻撃)。ハッカーは、1台のサーバーを多数のコンピューターから同時に攻撃できるように、このプログラムを利用して多数のコンピューターを感染させることがあります。</p> <p>DoS プログラムは1台のコンピューターから、ユーザーに気付かれることなく攻撃を実行します。DDoS (分散 DoS) プログラムは、感染したコンピューターのユーザーに気付かれずに、複数のコンピューターから分散して攻撃を行います。</p>
Trojan-IM	メッセージクライアントのユーザーから情報を盗むトロイ	このトロイの木馬は、メッセージクライアントのユーザーのアカウント番号とパスワードを盗みます。このプログラムは、データをメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。

	の木馬	
<b>ルートキット</b>	ルートキット	ルートキットは、他の悪意のあるアプリケーションやその活動を隠蔽します。そのため、このアプリケーションはオペレーティングシステムに長期間潜入します。また、ルートキットはファイル、感染しているコンピューターのメモリ内のプロセス、または悪意のあるアプリケーションを実行するレジストリキーを隠蔽することもできます。さらにルートキットは、ユーザー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とネットワーク上の他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間で行われるデータ交換を隠蔽できます。
<b>Trojan-SMS</b>	SMSメッセージ形式のトロイの木馬	このトロイの木馬は携帯電話を感染させ、高額の通話料が発生する電話番号にSMSメッセージを送信します。
<b>Trojan-GameThief</b>	オンラインゲームのユーザーから情報を盗むトロイの木馬	このトロイの木馬は、オンラインゲームのユーザーのアカウント情報を盗み、このデータを侵入者にメールやFTPで送信するか、侵入者のWebサイトにアクセスするなどによって送信します。
<b>Trojan-Banker</b>	銀行のアカウント情報を盗むトロイの木馬	このトロイの木馬は、銀行のアカウント情報や電子マネーシステムのデータを盗み、このデータをメールやFTPを使用して侵入者に送信するか、侵入者のWebサイトにアクセスするなどして送信します。
<b>Trojan-Mailfinder</b>	メールアドレスを収集するトロイの木馬	このトロイの木馬は、コンピューターに保存されているメールアドレスを収集し、侵入者にメールやFTPで送信するか、侵入者のWebサイトにアクセスするなどによって送信します。侵入者が収集したアドレスにスパムを送信することがあります。

- 悪意のあるツール 

## サブカテゴリ：悪意のあるツール

危険度：中

悪意のあるツールは、他の種類のマルウェアとは異なり、起動した直後に処理を実行しません。このプログラムはユーザーのコンピューターに安全に侵入し、そこで起動することができます。侵入者は、多くの場合、悪意のあるツールの機能を悪用して、ウイルス、ワーム、トロイの木馬を作成したり、リモートサーバーに対してネットワーク攻撃を仕掛けたりします。

悪意のあるツールのさまざまな機能を、次のテーブルに示す種類別に分類しています：

悪意のあるツールの機能

種別	Name	説明
コンストラクター	コンストラクター	このツールを使用して、新しいウイルス、ワームおよびトロイの木馬を作成します。一部のコンストラクターは標準的なウィンドウベースのインターフェイスを備えています。このインターフェイスでは、悪意のあるアプリケーションの種類を選択して、デバッグを無効にする手段やその他の機能を作成できます。
Dos	ネットワーク攻撃	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、またはDoS攻撃）。
エクスプロイト	エクスプロイト	<p>エクスプロイトは、処理されるアプリケーションの脆弱性を利用する一連のデータまたはプログラムコードで、コンピューター上で悪意のある処理を実行します。たとえば、エクスプロイトは、ファイルの書き込みまたは読み取り、あるいは「感染している」Webサイトの要求を行うことができます。</p> <p>それぞれのエクスプロイトは、さまざまなアプリケーションまたはネットワークサービスの脆弱性を利用します。ネットワークパケットに偽装したエクスプロイトは、ネットワーク経由で多数のコンピューターに送信され、脆弱なネットワークサービスを備えるコンピューターを探します。DOCファイルのエクスプロイトは、テキストエディターの脆弱性を利用します。このエクスプロイトは、ユーザーが感染したファイルを開いたときに、ハッカーが事前にプログラミングした処理を開始することがあります。メールに組み込まれたエクスプロイトは、メールクライアントの脆弱性を探します。このエクスプロイトは、ユーザーがメールクライアントの感染メールを開くとすぐに悪意のある処理を実行します。</p> <p>エクスプロイトを使用してネットワーク上に拡散するのがネットワームです。ヌーカー型エクスプロイトは、コンピューターを無効にするネットワークパケットです。</p>
FileCryptor	エンクリ	このプログラムは、他の悪意のあるアプリケーションを暗号化してアンチウイルス製品から隠蔽します。

	プ タ ー	
<b>Flooder</b>	ネ ッ ト ワ ー ク を 「汚 染 す る」 た め の プ ロ グ ラ ム	このプログラムは大量のメールをネットワークチャネル上に送信します。この種のツールには、インターネットリレーチャットなどを汚染するプログラムがあります。  Flooder 型ツールには、メール、IM クライアントおよびモバイル通信システムで使用されるチャネルを「汚染する」プログラムは含まれません。これらのプログラムは、テーブルに示す別種（Email-Flooder、IM-Flooder および SMS-Flooder）として区別されます。
<b>HackTool</b>	ハ ッ キ ン グ ツ ー ル	このプログラムは、たとえば、ユーザーの許可なしに新しいシステムアカウントを追加したり、システムログを消去してオペレーティングシステムにおける存在の痕跡を隠蔽したりすることによって、このプログラムがインストールされたコンピューターをハッキングすることや別のコンピューターを攻撃することを可能にします。この種のツールには、パスワードの傍受などの悪意のある機能の特徴とする一部のスニファーが含まれます。スニファーは、ネットワークトラフィックの監視を可能にするプログラムです。
<b>Hoax</b>	デ マ ウ ィ ル ス	このプログラムはウイルスメッセージに似たメッセージでユーザーに注意を喚起します。具体的には、感染していないファイルで「ウイルスを検知した」というメッセージや、実際にはディスクのフォーマットが発生しなかったのに、ディスクがフォーマットされたというメッセージを表示します。
<b>スプーファ</b>	ス プ ー フ ィ ン グ ツ ー ル	このツールは、メッセージ要求やネットワーク要求を送信者の偽装アドレスで送信します。たとえば、侵入者はスプーファ型のツールを使用して、ツール本体をメールの実際の送信者として渡します。
<b>VirTool</b>	悪 意 の あ る ア プ リ ケー ション を 改 変 す る ツ ー ル	このツールを使用すると、他のマルウェアを改変して、アンチウイルス製品から隠蔽することができます。
<b>Email-Flooder</b>	メ ー ル ア ド レ ス を 「汚 染 す る」 プ ロ グ ラ ム	このプログラムはさまざまなメールアドレスに大量のメールを送信して、これらのメールアドレスを「汚染」します。大量の受信メールによって、ユーザーは必要なメールを受信ボックスで表示できなくなります。



IM-Flooder	メッセージクライアントのトラフィックを「汚染する」プログラム	IM クライアントのユーザーをメッセージであふれさせます。大量のメールが送られてくるため、ユーザーは必要な受信メールを表示できなくなります。
SMS-Flooder	トラフィックを SMS メッセージで「汚染する」プログラム	このプログラムは携帯電話に大量の SMS メッセージを送信します。

- [アドウェア](#)<sup>②</sup>

**サブカテゴリ：** 広告ソフトウェア（アドウェア）

**危険性：** 中

アドウェアはユーザーに対して広告情報を表示します。アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。このようなプログラムには、ユーザーに関するマーケティング情報を収集し、それを開発者に送信するものがあります。この情報には、ユーザーが表示した Web サイトの名前や、ユーザーの検索の内容などが含まれます。スパイウェア型のトロイの木馬とは異なり、アドウェアは、このような情報をユーザーの同意を得てから開発者に送ります。

- [オートダイヤラー](#)<sup>②</sup>

**サブカテゴリ** : ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェア。

**危険度** : 中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します :

種別	Name	説明
Client-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダイヤラー	オートダイヤラー	これらのプログラムは、モデムを介してひそかに電話接続を確立できます。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します (どのアプリケーションがアクティブであるか、他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とどのようにデータをやり取りしているかを監視する)。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアク

	プログラム	<p>セスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。</p> <p>合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。</p>
Server-FTP	FTPサーバー	このプログラムはFTPサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP経由でコンピューターへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnetサーバー	このプログラムはTelnetサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet経由でコンピューターへのリモートアクセスを開きます。
Server-Web	Webサーバー	このプログラムはWebサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP経由でコンピューターへのリモートアクセスを開きます。
RiskTool	ローカルコンピューターで動作するツール	このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、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を起動することができます。
Client-P2P	P2Pネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
Client-SMTP	SMTPクライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムを

	イ ア ン ト	ユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Web ツ ー ル バ ー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬 似 プ ロ グ ラ ム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

- ユーザーに損害を与える目的で悪用される可能性があるその他のソフトウェアを検出する

**サブカテゴリ** : ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェア。

**危険度** : 中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します :

種別	Name	説明
Client-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダイヤラー	オートダイヤラー	これらのプログラムは、モデムを介してひそかに電話接続を確立できます。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します (どのアプリケーションがアクティブであるか、他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とどのようにデータをやり取りしているかを監視する)。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアク

	プログラム	<p>セスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。</p> <p>合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。</p>
Server-FTP	FTPサーバー	このプログラムはFTPサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP経由でコンピューターへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnetサーバー	このプログラムはTelnetサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet経由でコンピューターへのリモートアクセスを開きます。
Server-Web	Webサーバー	このプログラムはWebサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP経由でコンピューターへのリモートアクセスを開きます。
RiskTool	ローカルコンピューターで動作するツール	このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、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を起動することができます。
Client-P2P	P2Pネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
Client-SMTP	SMTPクライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムを



	イアント	ユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Webツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

• **悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト** 

Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に圧縮オブジェクトやアンパッカーモジュールがないかスキャンします。

侵入者は、危険なプログラムをアンチウイルス製品から隠蔽するために、特殊なパッカーを使用して危険なプログラムを保存するか、多重圧縮したファイルを作成します。

カスペルスキーのウイルスアナリストは、ハッカーの中で最も使用されているパッカーを識別しています。

Kaspersky Endpoint Security によってそのようなパッカーがファイル内に検知された場合、そのファイルには非常に高い確率で、悪意のあるアプリケーションやユーザーに損害を与える目的で悪用される可能性があるアプリケーションが含まれています。

Kaspersky Endpoint Security は、次のようなプログラムを検知します：

- 損害を与える可能性がある圧縮ファイル – マルウェア（ウイルス、ワーム、トロイの木馬など）を圧縮するために使用されます。
- 多重圧縮ファイル（危険性「中」） – 1個以上のパッカーによって3回圧縮されたオブジェクト。

• **多重圧縮オブジェクト** 

Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に圧縮オブジェクトやアンパッカーモジュールがないかスキャンします。

侵入者は、危険なプログラムをアンチウイルス製品から隠蔽するために、特殊なパッカーを使用して危険なプログラムを保存するか、多重圧縮したファイルを作成します。

カスペルスキーのウイルスアナリストは、ハッカーの中で最も使用されているパッカーを識別しています。

Kaspersky Endpoint Security によってそのようなパッカーがファイル内に検知された場合、そのファイルには非常に高い確率で、悪意のあるアプリケーションやユーザーに損害を与える目的で悪用される可能性があるアプリケーションが含まれています。

Kaspersky Endpoint Security は、次のようなプログラムを検知します：

- 損害を与える可能性がある圧縮ファイル - マルウェア（ウイルス、ワーム、トロイの木馬など）を圧縮するために使用されます。
- 多重圧縮ファイル（危険性「中」） - 1個以上のパッカーによって3回圧縮されたオブジェクト。

## 除外リスト

このテーブルには、信頼するオブジェクトに関する情報が示されます。

次の方法を使用して、スキャンからオブジェクトを除外できます：

- ファイルまたはフォルダーへのパスを指定する
  - オブジェクトハッシュを入力する
  - マスクを使用する
- 「\*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:\\*\\*.txt」は、C:ドライブ上のフォルダーにある拡張子がtxtのすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
  - 2つの連続した「\*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder\\*\*\\*.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子がtxtのすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:\\*\*\\*.txt」というマスクの指定は無効です。
  - 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子がtxtでファイル名が3文字のすべてのファイルのパスを含みます。
  - 「[ウイルス百科事典](#)」の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、「Rootkit」、「RemoteAdmin」）。任意の1文字を置き換える「?」と複数の文字を置き換える「\*」を使用してマスクを使用することができます。たとえ

	<p>ば、マスク「Client*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。</p>
<p><b>信頼するアプリケーション</b></p>	<p>このテーブルには、Kaspersky Endpoint Security の動作中にアクティビティが監視されない信頼するアプリケーションのリストが表示されます。</p> <p>アプリケーションコントロールは、それぞれのアプリケーションが信頼するアプリケーションの表に含まれているかどうかに関係なく、アプリケーションの起動を制限します。</p>
<p><b>継承時に値を統合する</b> (Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>Kaspersky Security Center の親ポリシーと子ポリシーのスキャンの除外リストと信頼するアプリケーションのリストを結合します。リストを結合するには、子ポリシーは Kaspersky Security Center の親ポリシーの設定を継承するよう設定されている必要があります。</p> <p>チェックボックスがオンの場合、Kaspersky Security Center の親ポリシーのリスト項目は子ポリシー内で表示されます。このようにすることで、組織全体の信頼するアプリケーションのリストを作成することが可能です。</p> <p>継承された子ポリシー内のリスト項目は削除または編集できません。継承時に結合されたスキャンの除外リストと信頼するアプリケーションのリストの項目は親ポリシー内でのみ削除および編集可能です。リストの項目は、下位のポリシーで追加、編集、削除が可能です。</p> <p>子ポリシーと親ポリシーのリスト項目が一致する場合、これらの項目は親ポリシー内の同じ項目として表示されます。</p> <p>このチェックボックスをオフにすると、リストの項目は Kaspersky Security Center ポリシーの設定の継承時に結合されません。</p>
<p><b>ローカルの除外リストの使用を許可する / ローカルの信頼するアプリケーションの使用を許可する</b> (Kaspersky Security Center コンソール内でのみ利用可能)</p>	<p>ローカルの除外リストとローカルの信頼するアプリケーションのリスト（ローカルの信頼ゾーン）とは、Kaspersky Endpoint Security で特定のコンピューターに向けてユーザーが定義したオブジェクトのリストです。Kaspersky Endpoint Security はローカルの信頼ゾーンのオブジェクトとアプリケーションを監視しません。ユーザーはポリシー内の一般的な信頼ゾーンに加えて、<a href="#">ローカルで除外リストと信頼するアプリケーションのリストを作成</a>することができます。</p> <p>チェックボックスがオンの場合、ユーザーはスキャンの除外リストと信頼するアプリケーションのリストをローカルに作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。</p> <p>チェックボックスがオフの場合、ユーザーはポリシー内で作成されたスキャンの除外リストと信頼するアプリケーションの全体的なリストのみにアクセスできます。ローカルのリストが作成された場合、この機能を無効にした後でも Kaspersky Endpoint Security は除外リストのオブジェクトをスキャンから除外し続けます。</p>
<p><b>信頼するシステム証明書ストア</b></p>	<p>信頼するシステム証明書ストアの1つが選択されている場合、Kaspersky Endpoint Security は信頼するデジタル署名を持つアプリケーションをスキャンから除外します。Kaspersky Endpoint Security はこのようなアプリケーションを信頼済みグループに割り当てます。</p> <p>[<b>使用しない</b>] が選択されている場合、Kaspersky Endpoint Security はアプリケーションが署名されているかどうかにかかわらずスキャンします。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。</p>

製品の全般設定について次の設定を指定できます：

- ブロックモード
- セルフディフェンス
- パフォーマンス
- デバッグ情報
- 設定が適用された際のコンピューターの状態

製品設定

パラメータ	説明
<p><b>コンピューターの開始時に Kaspersky Endpoint Security for Windows を開始する</b></p>	<p>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の読み込み後に Kaspersky Endpoint Security が起動し、セッション中にコンピューターを保護します。</p> <p>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の読み込み後、ユーザーが手動で起動するまでは Kaspersky Endpoint Security が起動しません。コンピューター保護が無効になるため、ユーザーデータが脅威にさらされる可能性があります。</p>
<p><b>特別な駆除技術を使用する（システムリソースを大量に消費します）</b></p>	<p>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悪意のある活動の検知時に、ポップアップ通知が画面に表示されます。この通知で、Kaspersky Endpoint Security は特別な駆除を実行するようユーザーに通知します。ユーザーがこの方法に同意すると、Kaspersky Endpoint Security はこれらの脅威を無効にします。特別な駆除手順が完了すると、Kaspersky Endpoint Security はコンピューターを再起動します。特別な駆除には大量のコンピューターリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。</p> <p>本製品がアクティブな感染の検知を処理している際、オペレーティングシステムの一部が利用できなくなることがあります。特別な駆除が完了し、コンピューターが再起動すると復元されます。</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>サーバー向けの Windows を実行しているコンピューターに Kaspersky Endpoint Security がインストールされている場合、Kaspersky Endpoint Security は通知を表示しません。そのため、ユーザーはアクティブな脅威を駆除する操作を選択することができません。脅威を駆除するには、製品設定で<b>特別な駆除を有効</b>にして、ウイルススキャンのタスク設定で<b>すぐに特別な駆除を実行する</b>よう設定する必要があります。その後ウイルススキャンタスクを開始します。</p> </div>
<p><b>アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する</b></p>	<p>このオプションをオンにすると、アプリケーションのアクティベーション時に Kaspersky Security Center 管理サーバーがプロキシサーバーとして使用されます。</p>

<p>(Kaspersky Security Center コンソール内でのみ利用可能)</p>	
<p><b>セルフディフェンスを有効にする</b></p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security によってハードディスクのアプリケーションファイル、メモリプロセス、システムレジストリエントリの改竄や削除が防止されます。</p>
<p><b>遠隔操作アプリケーションを利用した Kaspersky Endpoint Security の設定の変更を許可する</b></p>	<p>この設定がオンになっている場合、信頼済みの遠隔管理用のアプリケーション (TeamViewer、LogMeIn Pro、Remotely Anywhere など) で、Kaspersky Endpoint Security の設定を変更できます。</p> <p>チェックボックスがオンの場合でも、信頼済みでないリモート管理アプリケーションは Kaspersky Endpoint Security の設定を変更することはできません。</p>
<p><b>外部からの管理を有効にする</b></p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security はアプリケーションサービスのリモートコンピューターからの管理を許可します。リモートでアプリケーションサービスを管理しようとする、Microsoft Windows タスクバーのアプリケーションアイコン上に通知が表示されます (通知サービスが無効になっている場合を除く)。</p>
<p><b>バッテリー使用中はスケジュールタスクを延期する</b></p>	<p>このチェックボックスをオンにすると、省エネモードが有効になります。Kaspersky Endpoint Security がスケジュールされているタスクを延期します。必要に応じて、スキャンタスクとアップデートタスクを手動で実行できます。</p>
<p><b>他のアプリケーションにシステムリソースを優先的に割り当てる</b></p>	<p>Kaspersky Endpoint Security でスケジュールされたタスクが実行される際には、CPU とディスクサブシステムへの負荷が高くなり、他のアプリケーションのパフォーマンスが低下します。</p> <p>チェックボックスをオンにすると、Kaspersky Endpoint Security が負荷が増大したことを検知した場合、スケジュールされたタスクを一時的に停止し、ユーザーアプリケーションのためにオペレーティングシステムリソースを解放します。</p>
<p><b>ダンプへの書き込みを有効にする</b></p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security はクラッシュ時にダンプを書き出します。</p> <p>このチェックボックスをオフにすると、Kaspersky Endpoint Security はダンプを書き出しません。また、コンピューターのハードディスクから既存のダンプファイルを削除します。</p>
<p><b>ダンプおよびトレースファイルの保護を有効にする</b></p>	<p>このチェックボックスをオンにすると、ダンプファイルまたはトレースファイルの書き込みを有効にしたユーザーの他に、システム管理者およびローカル管理者にもダンプファイルへのアクセス権が付与されます。トレースファイルには、システムおよびローカルの管理者のみがアクセスできます。</p> <p>このチェックボックスをオフにすると、すべてのユーザーがダンプファイルとトレースファイルにアクセスできるようになります。</p>
<p><b>設定が適用された際のコンピューターの状態</b></p>	<p>Kaspersky Endpoint Security がインストールされたクライアントコンピューターについて、ポリシーの適用またはタスクの実行時にエラーが発生した場合に、Web コンソールで表示されるステータスの設定です。OK、警告、緊急というステータスがあります。</p>



(Kaspersky Security Center コンソール内でのみ利用可能)

## レポートと保管領域

### レポート

レポートには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

レポートは、フォルダー「C:\ProgramData\Kaspersky Lab\KES\Report」に保存されます。

### バックアップ

バックアップ保管領域には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。バックアップコピーは、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルのバックアップコピーは、フォルダー C:\ProgramData\Kaspersky Lab\KES\QB に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。

### 隔離

隔離とは、ウイルスに感染したファイルや駆除できないファイルを移動する特別なローカルの保管領域です。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は Kaspersky Sandbox および Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する際にのみこの隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、[Kaspersky Sandbox](#) および [Kaspersky Endpoint Detection and Response Optimum](#) のヘルプを参照してください。

隔離は Web コンソールを使用しないと設定できません。Web コンソールを使用して、隔離されたオブジェクトを管理（復元、削除、追加など）できます。[コマンドライン](#)を使用してオブジェクトをローカルコンピューター上に復元できます。

Kaspersky Endpoint Security はシステムアカウント (SYSTEM) を使用してファイルを隔離します。



パラメータ	説明
<b>保存期間</b>	このチェックボックスをオンにすると、レポートの最長保管期間は指定した期間に制限されます。既定の最長レポート保管期間は30日です。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
<b>レポートファイルの最大サイズ</b>	このチェックボックスをオンにすると、最大レポートファイルサイズは指定した値に制限されます。既定では、最大ファイルサイズは1024 MB です。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
<b>保存期間</b>	このチェックボックスをオンにすると、ファイルの最長保管期間は指定した期間に制限されます。既定の最長ファイル保管期間は30日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。
<b>バックアップのサイズを制限する</b>	このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。既定では、最大サイズは100 MB です。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Endpoint Security は最も古いファイルを保管領域から自動的に削除します。
<b>隔離のサイズを制限する</b> (Web コンソールでのみ利用可能)	隔離の最大サイズを MB で指定します。たとえば、隔離の最大サイズを 200 MB のように指定します。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security は対応するイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を継続します。
<b>隔離の容量が次の割合に到達した際に通知する</b> (Web コンソールでのみ利用可能)	隔離のしきい値です。たとえば、「50%」のように隔離のしきい値を設定できます。  隔離のサイズのしきい値に到達すると、Kaspersky Endpoint Security は対応するイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を継続します。
<b>管理サーバーへのデータ転送</b> (Kaspersky Security Center でのみ利用可能)	管理サーバーへ情報を転送する必要があるイベントのカテゴリです。

## ネットワークの設定

インターネットへの接続と定義データベースのアップデートで使用するプロキシサーバーの設定、ネットワークポートの監視モードの選択、暗号化された接続のスキャンの設定を行えます。

ネットワークのオプション

パラメータ	説明
<b>従量制接続</b>	このチェックボックスをオンにすると、インターネット接続が制限されているときに本製

<p><b>時に本製品によるデータ通信量を抑制する</b></p>	<p>品のネットワークトラフィックを制限します。高速モバイルインターネット接続は制限するネットワークとして、Wi-Fi 接続は無制限のネットワークとして判断されます。</p> <p>ネットワークにかかる費用の対策は、Windows 8 以降を実行中のコンピューターで動作します。</p>
<p><b>Web ページと連携するため Web トラフィック内にスクリプトを埋め込む</b></p>	<p>このチェックボックスをオンにすると、Kaspersky Endpoint Security は Web ページと連携するためのスクリプトを Web トラフィック内に埋め込みます。このスクリプトはウェブコントロール機能が正常に動作するために必要です。スクリプトはウェブコントロールのイベントの登録を有効にします。このスクリプトがない場合は、<a href="#">ユーザーのインターネット上の活動の監視</a>を有効にできません。</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Web ページと連携するスクリプトのトラフィックへの埋め込みは、ウェブコントロールの正常な動作のためカスペルスキーにより推奨されています。</p> </div>
<p><b>プロキシサーバー</b></p>	<p>クライアントコンピューターのユーザーによるインターネット接続で使用されるプロキシサーバーの設定です。Kaspersky Endpoint Security では、定義データベースやソフトウェアモジュールのアップデートに使用するものを含む、特定の保護機能にこの設定が使用されます。</p> <p>プロキシサーバーの自動設定のために、Kaspersky Endpoint Security では WPAD プロトコル (Web Proxy Auto-Discovery Protocol) が使用されます。このプロトコルを使用してプロキシサーバーの IP アドレスを判別できない場合、Kaspersky Endpoint Security は、Microsoft Internet Explorer のブラウザー設定で指定されているプロキシサーバーアドレスを使用します。</p>
<p><b>ローカルアドレスにはプロキシサーバーを使用しない</b></p>	<p>このチェックボックスをオンにすると、共有フォルダーからアップデートを行う際に、プロキシサーバーは使用されません。</p>
<p><b>監視対象のポート</b></p>	<p><b>すべてのネットワークポートを監視する</b>：このネットワークポート監視モードでは、保護機能 (ファイル脅威対策、ウェブ脅威対策、メール脅威対策) はコンピューターで開いているすべてのネットワークポート経由で送信されるデータストリームを監視します。</p> <p><b>選択されたネットワークポートのみを監視する</b>：このネットワークポートの監視モードでは、コンピューターの選択したポートおよび選択したアプリケーションのネットワークの動作を監視します。メールの送信とネットワークトラフィックで通常使用されるネットワークポートのリストは、カスペルスキーの専門家の推奨に従って構成されます。</p> <p><b>カスペルスキーが推奨するリストに含まれるアプリケーションのすべてのポートを監視する</b>：Kaspersky Endpoint Security によってポートが監視されるアプリケーションの事前定義済みのリストを使用します。このリストには例えば、Google Chrome、Adobe Reader、Java やその他のアプリケーションが含まれます。</p> <p><b>選択したアプリケーションのすべてのポートを監視する</b>：Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストを使用します。</p>
<p><b>暗号化された接続のスキャン</b></p>	<p>Kaspersky Endpoint Security は次のプロトコルを介して通信される暗号化されたネットワークトラフィックをスキャンします：</p> <ul style="list-style-type: none"> <li>• SSL 3.0</li> <li>• TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。</li> </ul> <p>Kaspersky Endpoint Security は次の暗号化された接続のスキャンモードをサポートします：</p>

- **〔暗号化された接続をスキャンしない〕**。Kaspersky Endpoint Security は「https://」で始まるアドレスの Web サイトのコンテンツにアクセスしません。
- **〔保護機能の要求時に暗号化された接続をスキャンする〕**。Kaspersky Endpoint Security はファイル脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。
- **〔常に暗号化された接続をスキャンする〕**。Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。

トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。

信頼されない証明書を持つドメインにアクセスするとき

- **許可**：このオプションを選択した場合、信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続を許可します。

信頼されていない証明書を持つドメインをブラウザで開こうとすると、Kaspersky Endpoint Security は、警告とそのドメインにアクセスすることが推奨されない理由が記載された HTML ページを表示します。ユーザーは HTML 警告ページのリンクをクリックすることで、要求された Web リソースにアクセスできます。このリンクを使用して対象の Web リソースにアクセスした後1時間の間は、同じドメインの他のリソースへのアクセス時に、信頼されない証明書に関する警告は表示されません。

- **接続をブロックする**：このオプションを選択した場合、信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続をブロックします。

信頼されていない証明書を持つドメインをブラウザで開こうとすると、Kaspersky Endpoint Security は、そのドメインがブロックされる理由が記載された HTML ページを表示します。

暗号化された接続のスキャンでエラーが発生するとき

- **接続をブロックする**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はネットワーク接続をブロックします。
- **除外リストにドメインを追加**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はエラーが発生したドメインを [スキャンエラーの発生したドメイン] リストに追加し、このドメインへのアクセスでの暗号化されたネットワークトラフィックを監視しません。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。リストに含まれる内容を消去して空にするには、**〔接続をブロックする〕** を選択する必要があります。

SSL 2.0 接続をブロック (推奨)

このチェックボックスをオンにすると、Kaspersky Endpoint Security は SSL 2.0 プロトコルで確立されたネットワーク接続をブロックします。

このチェックボックスをオフにすると、Kaspersky Endpoint Security は SSL 2.0 プロトコルで確立されたネットワーク接続をブロックせず、これらの接続経由で送受信されるネットワークトラフィックを監視しません。

EV 証明書

EV (Extended Validation) 証明書は、Web サイトの信頼性を示すためのもので、接続のセ

を使用した  
Web サイト  
への暗号化  
接続を復号  
化する

セキュリティを向上させます。Web サイトで EV 証明書が使用されている場合、ブラウザのアドレスバーの鍵アイコンでそのことが示されます。また、アドレスバーの全体や一部の色が緑色に変わるブラウザもあります。

このチェックボックスをオンにすると、Kaspersky Endpoint Security は EV 証明書を使用している Web サイトの暗号化された接続を復号化して監視します。

このチェックボックスをオフにすると、HTTPS トラフィックの通信内容に Kaspersky Endpoint Security はアクセスできません。そのため、HTTPS トラフィックは「https://google.com」などの URL のみに基づいて監視されます。

EV 証明書を使用している Web サイトに最初にアクセスするときには、チェックボックスがオンかオフかにかかわらず、接続が復号されます。

信頼するア  
ドレス

Kaspersky Endpoint Security でネットワーク接続をスキャンしない Web アドレスのリストを使用します。ドメイン名または IP アドレスを入力できます。Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「\*」をサポートします。

Kaspersky Endpoint Security は IP アドレスのマスクをサポートしません。本製品のローカルインターフェイスで IP アドレス範囲を入力することができます（例：198.51.100.0/24）。Kaspersky Security Center コンソールでは IP アドレス範囲を入力することはできません。

例：

- 「domain.com」と入力すると次のアドレスが含まれます：https://domain.com、https://www.domain.com、https://domain.com/page123。サブドメイン（例：subdomain.domain.com）は含まれません。
- 「subdomain.domain.com」と入力すると次のアドレスが含まれます：https://subdomain.domain.com、https://subdomain.domain.com/page123。「domain.com」ドメインは含まれません。
- 「\*.domain.com」と入力すると次のアドレスが含まれます：https://movies.domain.com、https://images.domain.com/page123。「domain.com」ドメインは含まれません。

信頼するア  
プリーケー  
ション

Kaspersky Endpoint Security の動作中にアクティビティが監視されない信頼するアプリケーションのリストが表示されます。アプリケーションによるどの種別のアクティビティを監視しないかを選択できます（例：ネットワークトラフィックはスキャンしない、など）。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「\*」および「?」をサポートします。

Mozilla 製品  
で保護され  
たトラフィ  
ックをスキ  
ャンする

このチェックボックスがオンの場合、Kaspersky Endpoint Security は Mozilla Firefox ブラウザーおよび Thunderbird メールクライアントでの暗号化されたトラフィックをスキャンします。Web サイトによっては、HTTPS プロトコルでアクセスする際にブロックされる可能性があります。

(Kaspersky  
Endpoint  
Security の  
インターフ  
ェイス内で  
のみ利用可  
能)

Mozilla Firefox のブラウザおよび Thunderbird メールクライアントでトラフィックをスキャンするには、暗号化された接続のスキャンを有効にするの必要があります。暗号化された接続のスキャンが無効になっている場合、Kaspersky Endpoint Security は Mozilla Firefox ブラウザーおよび Thunderbird メールクライアントでのトラフィックをスキャンしません。





Kaspersky Endpoint Security はカスペルスキーのルート証明書を使用して復号化したり暗号化したトラフィックを分析します。カスペルスキーのルート証明書を含む証明書ストアを選択することができます。

- **Windows の証明書ストアを使用する**カスペルスキーのルート証明書は Kaspersky Endpoint Security のインストール中にこのストアに追加されます。
- **Mozilla 証明書ストアを使用する**Mozilla Firefox および Thunderbird は独自の証明書ストアを使用します。Mozilla 証明書ストアが選択されている場合、カスペルスキーのルート証明書をブラウザのプロパティを使用してこのストアに手動で追加する必要があります。

## インターフェイス

製品インターフェイスの設定を編集できます。

インターフェイスの設定

パラメータ	説明
<b>ユーザーインターフェイス</b> (Kaspersky Security Center コンソール内でのみ利用可能)	<p><b>簡略化して表示：</b>クライアントコンピューター上で、本製品のメインウィンドウにアクセスできなくなり、<a href="#">Windows の通知領域のアイコン</a>だけが利用できます。アイコンのコンテキストメニューから <a href="#">Kaspersky Endpoint Security の一定範囲に限定された操作を実行</a>できます。製品アイコンの上の通知も表示されます。</p> <p><b>通常が表示：</b>クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウと <a href="#">Windows の通知領域のアイコン</a>が利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。</p> <p><b>アプリケーション動作モニターセクションを非表示：</b>クライアントコンピューターの Kaspersky Endpoint Security のメインウィンドウで <b>[アプリケーション動作モニター]</b> を使用できなくなります。アプリケーション動作モニターは、ユーザーのコンピューターのアプリケーションの動作に関する情報をリアルタイムで表示するように設計されたツールです。</p> <p><b>表示しない：</b>クライアントコンピューター上で、Kaspersky Endpoint Security の動作に関するメニューなどが表示されません。<a href="#">Windows の通知領域のアイコン</a>と通知も表示されません。</p>
<b>通知の設定</b>	<p>コンポーネントやタスク、アプリケーション全体の動作中に発生する可能性がある、さまざまな重要度のイベントに関する通知の設定を含むテーブル。Kaspersky Endpoint Security では、これらのイベントに関する通知を画面に表示したり、メールで送信したり、ログを取ったりします。</p>
<b>メール通知の設定</b>	<p>本製品の動作中に登録されたイベントに関する通知を配信するための SMTP サーバー設定。</p>
<b>通知エリアに製品のステータスを表示する</b>	<p>該当するカテゴリのイベントが発生した場合、Windows タスクバーの通知領域の <a href="#">Kaspersky Endpoint Security アイコン</a>が変化し (  または  )、ポップアップ通知が表示されます。</p>
<b>ローカルの定義データベースのステータスに関する通知</b>	<p>製品で使用されている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の通知設定です。</p>
<b>パスワード</b>	<p>切り替えスイッチがオンの場合、パスワードによって保護された操作をユーザーが実行</p>

<p><b>による保護</b></p>	<p>しようとしたときに Kaspersky Endpoint Security によってパスワードの入力が要求されま す。パスワードによる保護の対象範囲は、ブロックされる操作（例：保護機能の停止） とパスワードによる保護が適用されるユーザーアカウントとを組み合わせで指定されま す。</p> <p>パスワードによる保護を有効にすると、Kaspersky Endpoint Security では操作を実行する ためのパスワードの設定が要求されます。</p>
<p><b>テクニカル サポートの Web リソー ス</b></p> <p>(Kaspersky Security Center コン ソール内で のみ利用可 能)</p>	<p>このウィンドウでは、Kaspersky Endpoint Security のサポート関連情報が記載されている Web リソースへのリンクです。標準のリンクに代わって、追加されたリンクが Kaspersky Endpoint Security のローカルインターフェイスの <b>【サポート】</b> ウィンドウに表示されま す。</p>
<p><b>ユーザーへ のメッセー ジ</b></p> <p>(Kaspersky Security Center コン ソール内で のみ利用可 能)</p>	<p>Kaspersky Endpoint Security のローカルインターフェイスの <b>【サポート】</b> ウィンドウに表 示されるメッセージ。</p>

## 設定の管理

現在の Kaspersky Endpoint Security の設定をファイルに保存して、これを使用して別のコンピューターにアプ  
リケーションを簡単にインストールすることができます。また Kaspersky Security Center 12 を介して [インスト  
ールパッケージ](#)を使用したアプリケーションの配布時にこの設定ファイルを使用することができます。既定の  
設定をいつでも復元することができます。

製品設定の管理設定は Kaspersky Endpoint Security のインターフェイス内でのみ利用可能です。

### 製品設定の管理設定

設定	説明
<p><b>イン ポー ト</b></p>	<p>CFG 形式のファイルから設定を抽出し、適用します。</p>
<p><b>エク スポ ート</b></p>	<p>CFG 形式のファイルに現在の設定を保存します。</p>
<p><b>復元</b></p>	<p>Kaspersky Endpoint Security の設定は、カスペルスキーが推奨する設定にいつでも戻ることがで きます。この設定が復元されると、すべての保護機能のセキュリティレベルが <b>【推奨】</b> に設定さ れます。</p>



## 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

Kaspersky Endpoint Security の定義データベースとソフトウェアモジュールをアップデートすることにより、コンピューターを最新の方法で保護することができます。世界では、毎日、新しいウイルスと他の種類のマルウェアが出現しています。Kaspersky Endpoint Security データベースには、脅威に関する情報と脅威を無効化する方法が格納されています。脅威をすばやく検知するため、定義データベースとソフトウェアモジュールを定期的にアップデートしてください。

定期的なアップデートには、現在のライセンスが必要です。現在のライセンスがない場合、アップデートは一度だけ実行することができます。

Kaspersky Endpoint Security の主なアップデート元は、カスペルスキーのアップデートサーバーです。

カスペルスキーのアップデートサーバーからアップデートパッケージを正常にダウンロードするには、コンピューターをインターネットに接続する必要があります。既定では、インターネットの接続設定は自動的に行われます。プロキシサーバーを使用する場合は、設定を調整する必要があります。

アップデートは HTTPS プロトコルを経由してダウンロードされます。HTTPS プロトコル経由でダウンロードできない場合は、HTTP プロトコル経由でダウンロードすることもできます。

アップデートの実行中、次のオブジェクトがコンピューターにダウンロードされインストールされます：

- Kaspersky Endpoint Security の定義データベース：コンピューターの保護は、ウイルスおよびその他の脅威のシグネチャとそれらを無効化する方法についての情報を含む定義データベースを使用して実現されます。保護機能はこの情報を使用して、コンピューター上で感染したファイルを検索して無効化します。定義データベースには、定期的に、新しい脅威とそれに対処する方法のレコードが追加されます。このため、定義データベースを定期的にアップデートしてください。

Kaspersky Endpoint Security の定義データベースに加えて、アプリケーションのコンポーネントでネットワークトラフィックのインターセプトを可能にするネットワークドライバがアップデートされます。

- ソフトウェアモジュール：Kaspersky Endpoint Security の定義データベースに加えて、ソフトウェアモジュールもアップデートできます。ソフトウェアモジュールをアップデートすることにより、Kaspersky Endpoint Security の脆弱性が修正されるとともに新しい機能が追加され、さらに既存の機能が強化されます。

アップデート中、コンピューター上のソフトウェアモジュールと定義データベースがアップデート元にある最新のバージョンと比較されます。現在の定義データベースとソフトウェアモジュールがそれぞれの最新バージョンと異なる場合、アップデート内の不足している部分がコンピューターにインストールされます。

コンテキストヘルプファイルは、ソフトウェアモジュールのアップデートとともにアップデートできます。

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、アップデートパッケージのサイズが大きくなり、インターネットトラフィックが最大で数十 MB まで増加することがあります。

Kaspersky Endpoint Security の定義データベースに関する情報は、メインウィンドウまたは通知領域の本製品のアイコンの上にカーソルを置いた際に表示されるツールチップに表示されます。

アップデート結果、およびアップデートタスクの実行中に発生するイベントに関する情報が [Kaspersky Endpoint Security のレポートに記録](#)されます。

パラメータ	説明
<b>実行方法</b>	<p><b>自動開始：</b>このモードでは、新しいアップデートパッケージが使用可能であるかどうかアップデート元に特定の頻度で確認されます。アップデートパッケージを確認する頻度は、ウイルスの発生中には高くなり、ウイルスがないときは低くなります。新しいアップデートパッケージが検知されると、Kaspersky Endpoint Security によってそのパッケージがコンピューターにダウンロードされアップデートがインストールされます。</p> <p><b>手動開始：</b>このアップデートタスク実行方法を使用して、アップデートタスクを手動で開始することができます。</p> <p><b>スケジュールで指定：</b>このアップデートタスク実行方法では、アップデートタスクは指定したスケジュールに従って実行されます。このアップデートタスク実行方法を選択した場合でも、Kaspersky Endpoint Security のアップデートタスクを手動で開始することができます。</p>
<b>未実行のタスクを実行する</b>	<p>このチェックボックスをオンにすると、スキップされたアップデートタスクは実行可能になると同時に開始されます。アップデートタスクの開始時間にコンピューターの電源がオフになっていた場合などに、アップデートタスクがスキップされることがあります。</p> <p>このチェックボックスをオフにすると、スキップされたアップデートタスクは開始されません。代わりに、現在のスケジュールに従って、次のアップデートタスクが実行されます。</p>
<b>アップデート元</b>	<p>「アップデート元」は、Kaspersky Endpoint Security 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含むリソースです。</p> <p>アップデート元には、Kaspersky Security Center サーバーやカスペルスキーのアップデートサーバー、ネットワークフォルダーまたはローカルフォルダーが含まれます。</p> <p>アップデート元の既定のリストには Kaspersky Security Center とカスペルスキーのアップデートサーバーが含まれています。リストに他のアップデート元を追加できます。アップデート元には、HTTP/FTP サーバーと共有フォルダーを指定できます。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security は、カスペルスキーのアップデートサーバーである場合を除き、HTTPS サーバーからのアップデートをサポートしません。</p> </div> <p>複数のリソースがアップデート元として選択されている場合は、リスト上位のリソースから徐々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。</p>
<b>他のユーザーでタスクを実行する</b>	<p>既定では、Kaspersky Endpoint Security のアップデートタスクは、オペレーティングシステムへのログインに使用したアカウントを持つユーザーの代わりに開始されます。ただし、Kaspersky Endpoint Security は、必要な権利がないことが原因でユーザーがアクセスできないアップデート元（アップデートパッケージを含む共有フォルダーからアップデートを実行する場合など）やプロキシサーバーの認証が設定されていないアップデート元からアップデートされる場合があります。Kaspersky Endpoint Security の設定でアップデートの権限を持つユーザーを指定して、そのユーザーアカウントで Kaspersky Endpoint Security のアップデートタスクを開始できます。</p>
<b>製品機能のアップデートをダウンロード</b>	<p>このチェックボックスでは、製品のアップデートを定義データベースのアップデートとともにダウンロードするかどうかを切り替えます。</p> <p>このチェックボックスをオンにすると、Kaspersky Endpoint Security によって適用可能な製品モジュールのアップデートについてユーザーに通知され、アップデートタスクの実行中に、アップデートパッケージに製品モジュールのアップデートが含まれます。製品モジュールのアップデートを適用する方法は次の設定によって決定されます：</p>

- **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、ソフトウェアモジュールのアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべてのソフトウェアモジュールは、インストールがアプリケーションインターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。
- **承認済みのアップデートのみをインストール**：このオプションをオンにすると、ソフトウェアモジュールのアップデートが利用できるようになると、インストールがアプリケーションインターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。

このチェックボックスをオフにすると、Kaspersky Endpoint Security から適用可能なソフトウェアモジュールのアップデートについてユーザーに通知されず、アップデートタスクの実行中に、アップデートパッケージにソフトウェアモジュールのアップデートは含まれません。

ソフトウェアモジュールのアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。

既定では、このチェックボックスはオンです。

<b>アップデートをフォルダーにコピー</b>	<p>このチェックボックスをオンにすると、チェックボックス下部で指定されている共有フォルダーにアップデートパッケージをコピーします。これで、LAN 上のその他のコンピューターは、アップデートパッケージを共有フォルダーから受け取ることができます。この設定を行うと、アップデートパッケージのダウンロードは一度だけ実行されるようになります。このため、インターネットトラフィックが減少します。既定では、次のフォルダーが指定されます：C:\ProgramData\Kaspersky Lab\KES\Update distribution\。</p>
<b>アップデート対象のプロキシサーバー</b> <small>(Kaspersky Endpoint Security のインターフェイス内でのみ利用可能)</small>	<p>製品モジュールと定義データベースのアップデート用のクライアントコンピューターのユーザーのインターネットアクセスのプロキシサーバー設定です。</p> <p>プロキシサーバーの自動設定のために、Kaspersky Endpoint Security では WPAD プロトコル (Web Proxy Auto-Discovery Protocol) が使用されます。このプロトコルを使用してプロキシサーバーの IP アドレスを判別できない場合、Kaspersky Endpoint Security は、Microsoft Internet Explorer のブラウザー設定で指定されているプロキシサーバーアドレスを使用します。</p>
<b>ローカルアドレスにはプロキシサーバーを使用しない</b> <small>(Kaspersky Endpoint Security のインターフェイス内でのみ利用可能)</small>	<p>このチェックボックスをオンにすると、共有フォルダーからアップデートを行う際に、プロキシサーバーは使用されません。</p>

## 補足資料 2 : アプリケーション許可グループ

Kaspersky Endpoint Security は、コンピューターで起動したすべてのアプリケーションを許可グループに分類します。アプリケーションがオペレーティングシステムに及ぼす脅威レベルに応じて、アプリケーションはいずれかの許可グループに分類されます。

許可グループは次の通りです :

- **許可** : このグループには次の条件の1つ以上を満たすアプリケーションが含まれます :

- 信頼できる開発元によってデジタル署名されたアプリケーション。
- Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されたアプリケーション。
- ユーザーがアプリケーションを「許可」グループに配置した。

これらのアプリケーションでは、ブロックされる操作はありません。

- **弱い制限付き** : このグループには次の条件を満たすアプリケーションが含まれます :

- 信頼できる開発元によってデジタル署名されていないアプリケーション。
- Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
- ユーザーがアプリケーションを「弱い制限付き」グループに配置した。

これらのアプリケーションはオペレーティングシステムリソースへのアクセスに最小限の制限が付けられます。

- **強い制限付き** : このグループには次の条件を満たすアプリケーションが含まれます :

- 信頼できる開発元によってデジタル署名されていないアプリケーション。
- Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
- ユーザーがアプリケーションを「強い制限付き」グループに配置した。

これらのアプリケーションはオペレーティングシステムリソースへのアクセスに強い制限が付けられます。

- **ブロック** : このグループには次の条件を満たすアプリケーションが含まれます :

- 信頼できる開発元によってデジタル署名されていないアプリケーション。
- Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
- ユーザーがアプリケーションを「ブロック」グループに配置した。

これらのアプリケーションでは、すべての操作がブロックされます。

## 補足資料 3 : リムーバブルドライブの簡易スキャンのファイル拡張子

com – アプリケーションの実行ファイル (64 KB 以下)

exe – 実行ファイルまたは自己解凍型アーカイブ

sys – Microsoft Windows システムファイル

prg – dBase™、Clipper または Microsoft Visual FoxPro® のプログラムテキスト、または WAVmaker プログラム

bin – バイナリファイル

bat – バッチファイル

cmd – Microsoft Windows NT (DOS のバッチファイルに類似)、OS/2 のコマンドファイル

dpl – Borland Delphi の圧縮ライブラリ

dll – ダイナミックリンクライブラリ

scr – Microsoft Windows スプラッシュスクリーン

cpl – Microsoft Windows コントロールパネルモジュール

ocx – Microsoft OLE (オブジェクトのリンクと埋め込み) オブジェクト

tsp – スプリットタイムモードで実行されているプログラム

drv – デバイスドライバー

vxd – Microsoft Windows 仮想デバイスドライバー

pif – プログラム情報ファイル

lnk – Microsoft Windows リンクファイル

reg – Microsoft Windows システムレジストリキーファイル

ini – Microsoft Windows、Windows NT、および一部のアプリケーションの構成データを含む設定ファイル

cla – Java クラス

vbs – Visual Basic® スクリプト

vbe – BIOS Video Extension

js、jse – JavaScript ソーステキスト

htm – ハイパーテキストドキュメント

htt – Microsoft Windows ハイパーテキストヘッダー

hta – Microsoft Internet Explorer® のハイパーテキストプログラム

asp – Active Server Pages スクリプト

chm – コンパイル済み HTML ファイル

pht – 統合 PHP スクリプトを含む HTML ファイル

php – HTML ファイルに組み込まれたスクリプト

wsh – Microsoft Windows スクリプトホストファイル

wsf – Microsoft Windows スクリプト

the – Microsoft Windows 95 デスクトップ壁紙ファイル

hlp – Windows ヘルプファイル

eml – Microsoft Outlook Express メール

nws – Microsoft Outlook Express の新規メール

msg – Microsoft Mail メール

plg – メール

mbx – 保存されている Microsoft Office Outlook メールメッセージ

doc\* – Microsoft Office Word ドキュメント (doc – Microsoft Office Word ドキュメント、docx – XML のサポートを含む Microsoft Office Word 2007 ドキュメント、docm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメント)

dot\* – Microsoft Office Word ドキュメントテンプレート (dot – Microsoft Office Word ドキュメントテンプレート、dotx – Microsoft Office Word 2007 ドキュメントテンプレート、dotm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメントテンプレート)

fpm – データベースプログラム、Microsoft Visual FoxPro 開始ファイル

rtf – リッチテキストフォーマットドキュメント

shs – Shell Scrap Object Handler フラグメント

dwg – AutoCAD® 図面データベース

msi – Microsoft Windows インストールパッケージ

otm – Microsoft Office Outlook 用 VBA プロジェクト

pdf – Adobe Acrobat ドキュメント

swf – Shockwave® Flash パッケージオブジェクト



jpg、jpeg – 圧縮イメージグラフィック形式

emf – Enhanced Metafile 形式のファイル

ico – オブジェクトアイコンファイル

ov? – Microsoft Office Word 実行ファイル

xl\* – Microsoft Office Excel ドキュメントおよびファイル（xla – Microsoft Office Excel の拡張子、xlc – ダイアグラム、xlt – ドキュメントテンプレート、xlsx – Microsoft Office Excel 2007 ブック、xltm – マクロのサポートを含む Microsoft Office Excel 2007 ブック、xlsb – バイナリ（非 XML）形式の Microsoft Office Excel 2007 ブック、xltx – Microsoft Office Excel 2007 テンプレート、xlsm – マクロのサポートを含む Microsoft Office Excel 2007 テンプレート、xlam – マクロのサポートを含む Microsoft Office Excel 2007 プラグイン）

pp\* – Microsoft Office PowerPoint® ドキュメントおよびファイル（pps – Microsoft Office PowerPoint スライド、ppt – プレゼンテーション、pptx – Microsoft Office PowerPoint 2007 プレゼンテーション、pptm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーション、potx – Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、potm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、ppsx – Microsoft Office PowerPoint 2007 スライドショー、ppsm – マクロのサポートを含む Microsoft Office PowerPoint 2007 スライドショー、ppam – マクロのサポートを含む Microsoft Office PowerPoint 2007 プラグイン）

md\* – Microsoft Office Access® ドキュメントおよびファイル（mda – Microsoft Office Access ワークグループ、mdb – データベース）

sldx – Microsoft PowerPoint 2007 スライド

sldm – マクロのサポートを含む Microsoft PowerPoint 2007 スライド

thmx – Microsoft Office 2007 テーマ

## 補足資料 4：メール脅威対策用の添付ファイルフィルターのファイル種別

注意：実際のファイル形式は、そのファイル名の拡張子と一致しないことがあります。

添付ファイルのフィルタリングを有効にした場合、メール脅威対策によって、次の拡張子をもつファイルの名前が変更されたり、ファイルが削除されることがあります：

com – アプリケーションの実行ファイル（64 KB 以下）

exe – 実行ファイルまたは自己解凍型アーカイブ

sys – Microsoft Windows システムファイル

prg – dBase™、Clipper または Microsoft Visual FoxPro® のプログラムテキスト、または WAVmaker プログラム

bin – バイナリファイル

bat – バッチファイル

cmd – Microsoft Windows NT（DOS のバッチファイルに類似）、OS/2 のコマンドファイル

dpl – Borland Delphi の圧縮ライブラリ

dll – ダイナミックリンクライブラリ

scr – Microsoft Windows スプラッシュスクリーン

cpl – Microsoft Windows コントロールパネルモジュール

ocx – Microsoft OLE（オブジェクトのリンクと埋め込み）オブジェクト

tsp – スプリットタイムモードで実行されているプログラム

drv – デバイスドライバー

vxd – Microsoft Windows 仮想デバイスドライバー

pif – プログラム情報ファイル

lnk – Microsoft Windows リンクファイル

reg – Microsoft Windows システムレジストリキーファイル

ini – Microsoft Windows、Windows NT、および一部のアプリケーションの構成データを含む設定ファイル

cla – Java クラス

vbs – Visual Basic® スクリプト

vbe – BIOS Video Extension

js、jse – JavaScript ソーステキスト

htm – ハイパーテキストドキュメント

htt – Microsoft Windows ハイパーテキストヘッダー

hta – Microsoft Internet Explorer® のハイパーテキストプログラム

asp – Active Server Pages スクリプト

chm – コンパイル済み HTML ファイル

pht – 統合 PHP スクリプトを含む HTML ファイル

php – HTML ファイルに組み込まれたスクリプト

wsh – Microsoft Windows スクリプトホストファイル

wsf – Microsoft Windows スクリプト

the – Microsoft Windows 95 デスクトップ壁紙ファイル

hlp – Windows ヘルプファイル

eml – Microsoft Outlook Express メール

nws – Microsoft Outlook Express の新規メール

msg – Microsoft Mail メール

plg – メール

mbx – 保存されている Microsoft Office Outlook メールメッセージ

doc\* – Microsoft Office Word ドキュメント (doc – Microsoft Office Word ドキュメント、docx – XML のサポートを含む Microsoft Office Word 2007 ドキュメント、docm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメント)

dot\* – Microsoft Office Word ドキュメントテンプレート (dot – Microsoft Office Word ドキュメントテンプレート、dotx – Microsoft Office Word 2007 ドキュメントテンプレート、dotm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメントテンプレート)

fpm – データベースプログラム、Microsoft Visual FoxPro 開始ファイル

rtf – リッチテキストフォーマットドキュメント

shs – Shell Scrap Object Handler フラグメント

dwg – AutoCAD® 図面データベース

msi – Microsoft Windows インストールパッケージ

otm – Microsoft Office Outlook 用 VBA プロジェクト

pdf – Adobe Acrobat ドキュメント

swf – Shockwave® Flash パッケージオブジェクト

jpg、jpeg – 圧縮イメージグラフィック形式

emf – Enhanced Metafile 形式のファイル

ico – オブジェクトアイコンファイル

ov? – Microsoft Office Word 実行ファイル

xl\* – Microsoft Office Excel ドキュメントおよびファイル (xla – Microsoft Office Excel の拡張子、xlc – ダイアグラム、xlt – ドキュメントテンプレート、xlsx – Microsoft Office Excel 2007 ブック、xltm – マクロのサポートを含む Microsoft Office Excel 2007 ブック、xlsb – バイナリ (非 XML) 形式の Microsoft Office Excel 2007 ブック、xltx – Microsoft Office Excel 2007 テンプレート、xlsm – マクロのサポートを含む Microsoft Office Excel 2007 テンプレート、xlam – マクロのサポートを含む Microsoft Office Excel 2007 プラグイン)

pp\* – Microsoft Office PowerPoint® ドキュメントおよびファイル (pps – Microsoft Office PowerPoint スライド、ppt – プレゼンテーション、pptx – Microsoft Office PowerPoint 2007 プレゼンテーション、pptm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーション、potx – Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、potm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、ppsx – Microsoft Office PowerPoint 2007 スライドショー、ppsm – マクロのサポートを含む Microsoft Office PowerPoint 2007 スライドショー、ppam – マクロのサポートを含む Microsoft Office PowerPoint 2007 プラグイン)

md\* – Microsoft Office Access® ドキュメントおよびファイル（mda – Microsoft Office Access ワークグループ、mdb – データベース）

sldx – Microsoft PowerPoint 2007 スライド

sldm – マクロのサポートを含む Microsoft PowerPoint 2007 スライド

thmx – Microsoft Office 2007 テーマ

## 補足資料 5：外部サービスとの相互作用のためのネットワーク設定

Kaspersky Endpoint Security は以下のネットワーク設定を使用して外部サービスと相互に作用します。

ネットワークの設定

アドレス	説明
activation- v2.kaspersky.com/activation-service/activation-service.svc プロトコル：HTTPS ポート：443	製品のアクティベーション
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com cm.k.kaspersky-labs.com プロトコル：HTTPS ポート：443	定義データベースと機能のアップデート中

downloads.upd.kaspersky.com

プロトコル：HTTPS

ポート：443

- 定義データベースと機能のアップデート中

- カスペルスキーのサーバーにアクセスできるかどうかの確認。システム DNS を使用してサーバーにアクセスできない場合は、パブリック DNS を使用します。これは、確実に定義データベースをアップデートし、コンピューターのセキュリティレベルを維持するために必要です。

Kaspersky Endpoint Security は一連のパブリック DNS サーバーを次の順番で使用します。

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

本製品は DNS サーバーを使用して TCP/UDP 接続を確立するため、本製品の要求にはドメインのアドレスと予備ユーザーのパブリック IP アドレスが含まれることがあります。この情報は、HTTPS を使用している場合に Web リソースの証明書を検証するためなどに必要になります。Kaspersky Endpoint Security がパブリック DNS サーバーを使用している場合、データは対応するサービスのプライバシーポリシーに従って処理されます。Kaspersky Endpoint Security がパブリック DNS サーバーを使用しないようにする場合は、テクニカルサポートに連絡してプライベートパッチを依頼してください。

<p>touch.kaspersky.com          プロトコル : HTTP</p>	<ul style="list-style-type: none"> <li>• 証明書の有効期間確認の信頼できる時刻の受信 (TLS 接続)</li> <li>• ブラウザーでの Web リソースへのアクセス拒否に関する警告 (ウェブ脅威対策およびウェブコントロール)</li> </ul>
<p>p00.upd.kaspersky.com          p01.upd.kaspersky.com          p02.upd.kaspersky.com          p03.upd.kaspersky.com          p04.upd.kaspersky.com          p05.upd.kaspersky.com          p06.upd.kaspersky.com          p07.upd.kaspersky.com          p08.upd.kaspersky.com          p09.upd.kaspersky.com          p10.upd.kaspersky.com          p11.upd.kaspersky.com          p12.upd.kaspersky.com          p13.upd.kaspersky.com          p14.upd.kaspersky.com          p15.upd.kaspersky.com          p16.upd.kaspersky.com          p17.upd.kaspersky.com          p18.upd.kaspersky.com          p19.upd.kaspersky.com          downloads.kaspersky-labs.com          cm.k.kaspersky-labs.com          プロトコル : HTTP          ポート : 80</p>	<p>定義データベースと機能のアップデート中</p>
<p>ds.kaspersky.com          プロトコル : HTTPS          ポート : 443</p>	<p>Kaspersky Security Network の使用。</p>
<p>ksn-a-stat-geo.kaspersky-labs.com          ksn-file-geo.kaspersky-labs.com          ksn-verdict-geo.kaspersky-labs.com          ksn-url-geo.kaspersky-labs.com          ksn-a-p2p-geo.kaspersky-labs.com          ksn-info-geo.kaspersky-labs.com          ksn-cinfo-geo.kaspersky-labs.com</p>	<p>Kaspersky Security Network を使用する</p>



プロトコル : Any ポート : 443、1443	
click.kaspersky.com redirect.kaspersky.com プロトコル : HTTPS	インターフェイスからのリンク を使用
cr1.kaspersky.com ocsp.kaspersky.com プロトコル : HTTP ポート : 80	公開鍵基盤 (PKI)

## 補足資料 6 : Windows イベントログのアプリケーションイベントログ

Windows イベントログには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

### [システム監査](#)

イベントのコード

イベント ID		説明	既定で有効
201	❗	使用許諾契約書違反。	✓
203	❗	ライセンスの有効期間が終了する。	-
206	❗	定義データベースが存在しないか、破損している。	-
207	❗	定義データベースが長期間アップデートされていない。	-
209	❗	コンピューター起動時の自動起動が無効になっている。	-
229	❗	アクティベーションエラー。	✓
231	❗	アクティブな脅威が検知された。特別な駆除を開始する必要があります。	-
2023	❗	KSN サーバーが使用できない。	-
237	⚠	前回のセッション中にアプリケーションがクラッシュした。	✓
204	⚠	ライセンスの有効期間がまもなく終了する。	-
208	⚠	定義データベースがアップデートされていない。	-
210	⚠	アップデートの自動開始が無効になっている。	-
211	⚠	セルフディフェンスが無効になっている。	-
214	⚠	保護機能が無効になっている。	-
215	⚠	コンピューターがセーフモードで動作している。	-
216	⚠	未処理のファイルがある。	-
219	⚠	グループポリシーが適用された。	✓
224	⚠	アップデートを完了するため、再起動する必要がある。	-
225	⚠	コンピューターの再起動が要求された。	✓
226	⚠	ライセンスがインストールされていないコンポーネントの使用を許可している。	-
232	⚠	特別な駆除が開始された。	-
233	⚠	特別な駆除が完了した。	-
230	⚠	予備のアクティベーションコードが正しくない。	-
336	⚠	バックアップからオブジェクトが復元できない。	✓
2001	⚠	疑わしいネットワークの動作を検知した。	-
250	⚠	暗号化された接続が切断された。	✓
2021	⚠	KSN への参加が無効になった。	-
245	⚠	OS の機能の一部の処理が無効になった。	✓
235	🕒	アプリケーションが開始された。	✓
236	🕒	アプリケーションが停止された。	✓
213	🕒	製品リソースの操作がセルフディフェンスによってブロックされている。	-
217	🕒	レポートが消去された。	✓

220	①	グループポリシーが無効化された。	-
218	①	製品設定が変更された。	✓
227	①	ライセンスによって定義されているすべてのコンポーネントがインストールされ、通常モードで動作している。	-
238	①	定額制サービスの設定が変更された。	✓
239	①	定額制サービスが更新された。	✓
335	①	バックアップからオブジェクトが復元された。	✓
2000	①	ユーザー名とパスワードを入力してください。	-
2020	①	KSN への参加が有効になった。	-
2022	①	KSN サーバーが使用可能。	-
2024	①	本製品が動作し、適用法のもとデータを処理し、適切な環境で使用する。	✓
212	①	タスクが実行できない。	-
221	①	タスクが開始された。	-
222	①	タスクが停止された。	-
223	①	タスクが完了した。	-
227	①	インストールされた機能がライセンスと一致している。	-
240	①	ライセンスの有効期間がまもなく終了する。	✓
708	①	タスク設定が正常に適用された。	-

## ふるまい検知

イベントのコード

イベント ID		説明	既定で有効
302		悪意のあるオブジェクトが検知された。	-
313		削除できない。	-
452		プロセスが終了した。	-
453		プロセスを終了できない。	-
455		ロールバックが完了した。	-
331		ブロックされた。	-
307		オブジェクトが削除された。	-
323		オブジェクトは再起動時に削除される。	-
311		バックアップコピーを作成できない。	-
303		ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
457		ファイルが復元された。	-
308		オブジェクトのバックアップコピーが作成された。	-
458		レジストリ値が復元された。	-
459		レジストリ値が削除された。	-
329		オブジェクトの名前が変更された。	-

**脆弱性攻撃ブロック**

イベントのコード

イベント ID		説明	既定で有効
302		悪意のあるオブジェクトが検知された。	-
331		ブロックされた。	-
455		ロールバックが完了した。	-
307		オブジェクトが削除された。	-
323		オブジェクトは再起動時に削除される。	-
457		ファイルが復元された。	-
458		レジストリ値が復元された。	-
459		レジストリ値が削除された。	-
329		オブジェクトの名前が変更された。	-

**ホスト侵入防止**

イベントのコード

イベントID		説明	既定で有効
302	❌	悪意のあるオブジェクトが検知された。	-
312	❌	駆除できない。	-
313	❌	削除できない。	-
317	❌	処理エラー。	✓
452	❌	プロセスが終了した。	-
453	❌	プロセスを終了できない。	-
310	⚠️	バックアップコピーを作成できない。	-
314	⚠️	オブジェクトが処理されなかった。	-
320	⚠️	オブジェクトが暗号化された。	-
321	⚠️	オブジェクトが破損している。	-
323	⚠️	オブジェクトは再起動時に削除される。	-
324	⚠️	オブジェクトが再起動時に駆除される。	-
303	⚠️	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
336	⚠️	バックアップからオブジェクトが復元できない。	✓
307	⚠️	オブジェクトが削除された。	-
306	⚠️	オブジェクトが駆除された。	-
301	🕒	オブジェクトが処理された。	-
308	🕒	オブジェクトのバックアップコピーが作成された。	-
315	🕒	オブジェクトがスキップされた。	-
318	🕒	アーカイブが検知された。	-
319	🕒	圧縮されたオブジェクトが検知された。	-
327	🕒	以前駆除したファイルのコピーで上書きした。	-
332	🕒	検知したオブジェクトに関する情報。	-
322	🕒	パスワードで保護されている圧縮ファイルが検知された。	-
335	🕒	バックアップからオブジェクトが復元された。	-
401	🕒	アプリケーションが「許可」グループに割り当てられた。	-
402	🕒	アプリケーションが「制限付き」グループに割り当てられた。	-
403	🕒	ホスト侵入防止がトリガーされた。	-
340	🕒	オブジェクトはプライベート KSN の許可リストに記載されている。	✓

**ファイル脅威対策**

イベントのコード

イベントID		説明	既定で有効
302	❌	悪意のあるオブジェクトが検知された。	✓
312	❌	駆除できない。	-
313	❌	削除できない。	-
317	❌	処理エラー。	✓
452	❌	プロセスが終了した。	-
453	❌	プロセスを終了できない。	-
310	⚠️	バックアップコピーを作成できない。	-
314	⚠️	オブジェクトが処理されなかった。	-
320	⚠️	オブジェクトが暗号化された。	-
321	⚠️	オブジェクトが破損している。	-
323	⚠️	オブジェクトは再起動時に削除される。	-
324	⚠️	オブジェクトが再起動時に駆除される。	-
303	⚠️	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
336	⚠️	バックアップからオブジェクトが復元できない。	✓
307	⚠️	オブジェクトが削除された。	-
306	⚠️	オブジェクトが駆除された。	-
455	⚠️	ロールバックが完了した。	-
301	🕒	オブジェクトが処理された。	-
308	🕒	オブジェクトのバックアップコピーが作成された。	-
315	🕒	オブジェクトがスキップされた。	-
318	🕒	アーカイブが検知された。	-
319	🕒	圧縮されたオブジェクトが検知された。	-
325	🕒	以前駆除したファイルのコピーで上書きした。	-
322	🕒	パスワードで保護されている圧縮ファイルが検知された。	-
332	🕒	検知したオブジェクトに関する情報。	-
335	🕒	バックアップからオブジェクトが復元された。	-
329	🕒	オブジェクトの名前が変更された。	-
340	🕒	オブジェクトはプライベート KSN の許可リストに記載されている。	✓



イベントのコード

イベントID		説明	既定で有効
302	🚫	悪意のあるオブジェクトが検知された。	✓
362	🚫	危険なリンクがブロックされた。	✓
363	🚫	危険なリンクが開かれた。	✓
1201	🚫	以前開かれた危険なリンクが検知された。	✓
317	🚫	処理エラー。	✓
303	⚠️	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
331	⚠️	ブロック	-
341	⚠️	オブジェクトのダウンロードがブロックされた。	-
321	⚠️	オブジェクトが破損している。	-
301	🕒	オブジェクトが処理された。	-
301	🕒	リンクが処理された	-
332	🕒	検知したオブジェクトに関する情報。	-
319	🕒	圧縮されたオブジェクトが検知された。	-
318	🕒	アーカイブが検知された。	-
322	🕒	パスワードで保護されている圧縮ファイルが検知された。	-
329	🕒	オブジェクトの名前が変更された。	-
1211	🕒	以前開かれた悪意のあるリンクが検知された。	✓
370	🕒	リンクはプライベート KSN の許可リストに記載されている。	✓
370	🕒	オブジェクトはプライベート KSN の許可リストに記載されている。	✓

メール脅威対策 

イベントのコード

イベント ID		説明	既定で有効
302	❗	悪意のあるオブジェクトが検知された。	✓
312	❗	駆除できない。	-
317	❗	処理エラー。	✓
314	⚠	オブジェクトが処理されなかった。	-
303	⚠	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
321	⚠	オブジェクトが破損している。	-
336	⚠	バックアップからオブジェクトが復元できない。	-
307	⚠	オブジェクトが削除された。	-
306	⚠	オブジェクトが駆除された。	-
301	ℹ	オブジェクトが処理された。	-
308	ℹ	オブジェクトのバックアップコピーが作成された。	-
318	ℹ	アーカイブが検知された。	-
319	ℹ	圧縮されたオブジェクトが検知された。	-
329	ℹ	オブジェクトの名前が変更された。	-
332	ℹ	検知したオブジェクトに関する情報。	-
322	ℹ	パスワードで保護されている圧縮ファイルが検知された。	-
335	ℹ	バックアップからオブジェクトが復元された。	-
340	ℹ	オブジェクトはプライベート KSN の許可リストに記載されている。	✓

## ファイアウォール

イベントのコード

イベント ID		説明	既定で有効
602	❗	ネットワーク動作がブロックされた。	-
601	ℹ	ネットワーク動作が許可された。	-

## ネットワーク脅威対策

イベントのコード

イベント ID		説明	既定で有効
651	❗	ネットワーク攻撃が検知された。	-

## 有害 USB 攻撃ブロック

イベントのコード

イベント ID		説明	既定で有効
2051	❌	キーボードは認証されていない。	✓
2052	⚠	キーボード認証エラー。	✓
2050	🕒	キーボードが認証された。	-

**AMSI 保護**

イベントのコード

イベント ID		説明	既定で有効
302	❌	悪意のあるオブジェクトが検知された。	✓
2200	❌	AMSI リクエストがブロックされた。	✓
317	❌	処理エラー。	✓
314	⚠	オブジェクトが処理されなかった。	-
320	⚠	オブジェクトが暗号化された。	-
321	⚠	オブジェクトが破損している。	-
303	⚠	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
1512	⚠	オブジェクトのスキャン結果がサードパーティ製品に送信された。	-
301	🕒	オブジェクトが処理された。	-
315	🕒	オブジェクトがスキップされた。	-
318	🕒	アーカイブが検知された。	-
319	🕒	圧縮されたオブジェクトが検知された。	-
322	🕒	パスワードで保護されている圧縮ファイルが検知された。	-
332	🕒	検知したオブジェクトに関する情報。	-
340	🕒	オブジェクトはプライベート KSN の許可リストに記載されている。	✓
329	🕒	オブジェクトの名前が変更された。	-

**アプリケーションコントロール**

イベントのコード

イベント ID		説明	既定で有効
702		アプリケーションの起動が禁止された。	-
710		Kaspersky Endpoint Security for Windows の開始前に禁止対象のプロセスが開始された。	-
707		タスク設定のエラー。タスク設定は適用されません。	-
708		タスク設定が正常に適用された。	-
701		アプリケーションの起動が許可された。	-
703		アプリケーションの起動がテストモードでブロックされた。	-
704		アプリケーションの起動がテストモードで許可された。	-

## デバイスコントロール

イベントのコード

イベント ID		説明	既定で有効
802		端末の操作が禁止された。	-
809		ネットワーク接続がブロックされた。	-
803		端末への一時アクセスがアクティベートされた。	✓
801		端末の操作が許可された。	-
808		ファイルの操作が実行された。	-

## ウェブコントロール

イベントのコード

イベント ID		説明	既定で有効
752		アクセスが拒否された。	-
753		望ましくないコンテンツに関する警告。	-
754		望ましくないコンテンツの警告後にアクセスが試行された。	-
751		アクセスが許可された。	-
751		許可されたページを開いた。	-

## アダプティブアノマリーコントロール

イベントのコード

イベント ID		説明	既定で有効
2200	❌	プロセスの処理がブロックされた。	✓
2201	ⓘ	プロセスの処理がスキップされた。	-

## データ暗号化 [?](#)

イベントのコード

イベントID		説明	既定で有効
904	❗	暗号化または復号化ルールの適用にエラーが発生した。	✓
912	❗	ファイルの暗号化または復号化エラー。	✓
940	❗	ファイルのアクセスがブロックされた。	✓
951	❗	ポータブルモードの有効化エラー。	✓
953	❗	ポータブルモードの無効化エラー。	✓
931	❗	暗号化されたパッケージの作成エラー。	✓
1305	❗	端末の暗号化または復号化エラー。	✓
1311	❗	暗号化モジュールの読み込みに失敗した。	✓
1340	❗	認証エージェントアカウントの管理タスクがエラーで終了した。	✓
1312	❗	ポリシーが適用できない。	✓
1342	❗	FDE アップグレードに失敗した。	✓
1344	❗	ディスク全体の暗号化のアップグレードのロールバックがエラーで終了した。	✓
903	⚠	暗号化または復号化ルールの適用が中断された。	-
914	⚠	ファイルの暗号化 / 復号化が中断された。	-
1303	⚠	デバイスの暗号化 / 復号化が中断された。	-
1306	⚠	ユーザーが暗号化ポリシーを拒否した。	-
1345	⚠	WinRE イメージ内で Kaspersky Disk Encryption ドライバーのインストールまたはアップグレードに失敗した。	✓
901	🕒	暗号化または復号化ルールの適用を開始した。	-
902	🕒	暗号化または復号化ルールの適用を完了した。	-
905	🕒	暗号化または復号化ルールの適用を再開した。	-
910	🕒	ファイルの暗号化 / 復号化を開始した。	-
911	🕒	ファイルの暗号化 / 復号化を完了した。	-
913	🕒	ファイルは除外対象であるため暗号化されなかった。	-
950	🕒	ポータブルモードが有効になった。	-
952	🕒	ポータブルモードが無効になった。	-
1301	🕒	デバイスの暗号化 / 復号化が開始された。	-
1302	🕒	デバイスの暗号化 / 復号化が完了した。	-
1304	🕒	デバイスの暗号化 / 復号化が再開された。	-
1310	🕒	暗号化モジュールが読み込まれた。	-
1307	🕒	デバイスが暗号化されていない。	-
1308	🕒	ドライブの暗号化 / 復号化がアクティブモードに切り替わった。	-



1309	①	ドライブの暗号化 / 復号化がパッシブモードに切り替わった。	-
1330	①	新しい認証エージェントアカウントが作成された。	-
1331	①	認証エージェントアカウントが削除された。	-
1332	①	認証エージェントアカウントのパスワードが変更された。	-
1333	①	認証エージェントに正常にログインした。	-
1334	①	認証エージェントへのログインに失敗した。	-
1335	①	暗号化済みデバイスへのアクセスを要求する手順によってハードディスクにアクセスした。	-
1336	①	暗号化済みデバイスへのアクセスを要求する手順によるハードディスクへのアクセスに失敗した。	-
1337	①	アカウントが追加されなかった。このアカウントは既に存在しています。	-
1338	①	アカウントが編集できなかった。このアカウントは存在しません。	-
1339	①	アカウントは削除されなかった。このアカウントは存在しません。	-
1341	①	FDE アップグレードが成功した。	✓
1343	①	FDE アップグレードのロールバックが成功した。	✓
1346	①	WinRE イメージ内で Kaspersky Disk Encryption ドライバーのアンインストールに失敗した。	✓
1370	①	BitLocker 回復キーが変更された。	✓

## Endpoint Sensor

イベントのコード

イベントID		説明	既定で有効
2100	❌	Kaspersky Anti Targeted Attack Platform サーバーが使用できない。	-
2105	⚠️	アプリケーションの起動がブロックされた。	✓
2106	⚠️	ドキュメントを開く動作がブロックされた。	✓
2112	⚠️	ファイルイメージまたはストリームから開始されたすべてのプロセスが中断された。	✓
2113	⚠️	アプリケーションが開始された。	✓
2111	⚠️	Kaspersky Anti Targeted Attack Platform サーバー管理者によりファイルまたはストリームが削除された。	✓
2110	⚠️	管理者により Kaspersky Anti Targeted Attack Platform サーバーの隔離からファイルが復元された。	✓
2109	⚠️	管理者によりファイルが Kaspersky Anti Targeted Attack Platform サーバーに隔離された。	✓
2107	⚠️	すべてのサードパーティ製アプリケーションのネットワーク操作がブロックされた。	✓
2108	⚠️	すべてのサードパーティ製アプリケーションのネットワーク操作がブロック解除された。	✓
2104	🕒	Kaspersky Anti Targeted Attack Platform サーバーからのタスクが処理中。	-
2103	🕒	Kaspersky Anti Targeted Attack Platform サーバーからのタスクの処理が無効。	-
2101	🕒	Endpoint Sensor がサーバーに接続した。	-
2102	🕒	Kaspersky Anti Targeted Attack Platform サーバーへの接続が復元された。	-

コンピューターのスキャン 

イベントのコード

イベントID		説明	既定で有効
302	❌	悪意のあるオブジェクトが検知された。	✓
312	❌	駆除できない。	-
313	❌	削除できない。	-
317	❌	処理エラー。	-
452	❌	プロセスが終了した。	-
453	❌	プロセスを終了できない。	-
310	⚠️	バックアップコピーを作成できない。	-
314	⚠️	オブジェクトが処理されなかった。	-
320	⚠️	オブジェクトが暗号化された。	-
321	⚠️	オブジェクトが破損している。	-
323	⚠️	オブジェクトは再起動時に削除される。	-
324	⚠️	オブジェクトが再起動時に駆除される。	-
303	⚠️	ユーザーに損害を与える目的で悪用される可能性のある正規のソフトウェアを検知した。	-
336	⚠️	バックアップからオブジェクトが復元できない。	✓
307	⚠️	オブジェクトが削除された。	-
306	⚠️	オブジェクトが駆除された。	-
455	⚠️	ロールバックが完了した。	-
301	🕒	オブジェクトが処理された。	-
308	🕒	オブジェクトのバックアップコピーが作成された。	-
315	🕒	オブジェクトがスキップされた。	-
318	🕒	アーカイブが検知された。	-
319	🕒	圧縮されたオブジェクトが検知された。	-
327	🕒	以前駆除したファイルのコピーで上書きした。	-
332	🕒	検知したオブジェクトに関する情報。	-
322	🕒	パスワードで保護されている圧縮ファイルが検知された。	-
335	🕒	バックアップからオブジェクトが復元された。	✓
329	🕒	オブジェクトの名前が変更された。	-
340	🕒	オブジェクトはプライベート KSN の許可リストに記載されている。	✓

整合性チェック 

イベントのコード

イベント ID		説明	既定で有効
2002	⚠	システムモジュールの署名のチェックが失敗した	-




## データベースのアップデート

イベントのコード

イベントID		説明	既定で有効
1011	❗	コンポーネントのアップデートエラー。	-
1012	❗	コンポーネントのアップデートの配信エラー。	-
1014	❗	ローカルのアップデートエラー。	-
1015	❗	ネットワークのアップデートエラー。	-
1017	❗	同時に2つのタスクを開始できない。	-
1018	❗	アプリケーションの定義データベースおよびモジュールの検証中にエラーが発生した。	-
1019	❗	Kaspersky Security Center との対話中にエラーが発生した。	-
1021	❗	アップデートされていないコンポーネントがある。	-
1023	❗	アップデートが完了したが、アップデートの配信に失敗した。	-
101	❗	内部エラーが発生した。	✓
2153	❗	パッチのインストールが失敗した。	-
2156	❗	パッチのロールバックが失敗した。	-
1016	⚠	ユーザーによるキャンセル。	-
1001	🕒	アップデート元が選択された。	-
1002	🕒	プロキシサーバーが選択された。	-
1003	🕒	ファイルのダウンロード。	-
1004	🕒	ファイルがダウンロードされた。	-
1005	🕒	ファイルがインストールされた。	-
1006	🕒	ファイルがアップデートされた。	-
1007	🕒	アップデートエラーのためファイルがロールバックされた。	-
1008	🕒	ファイルをアップデート中。	-
1009	🕒	アップデートを配信中。	-
1010	🕒	ファイルをロールバック中。	-
1013	🕒	ダウンロードするファイルのリストを作成中。	-
1020	🕒	適用可能なアップデートがない。	-
1022	🕒	アップデートの配信が正常に完了した。	-
2150	🕒	パッチのダウンロード中。	-
2151	🕒	パッチのインストール中。	-
2152	🕒	パッチがインストールされた。	-
2154	🕒	パッチのロールバック中。	-
2155	🕒	パッチがロールバックされた。	-

## データの消去





イベントのコード

イベント ID		説明	既定で有効
2252		削除できない。	-
2253		データ消去タスクの統計。	-
2251		オブジェクトが削除された。	-

## 補足資料 7 : Kaspersky Security Center イベントログ内の製品イベント

Kaspersky Security Center イベントログには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの完了状況、ならびに製品全体の操作に関する情報が記録されます。

Kaspersky Endpoint Security for Windows のイベント

イベント ID		説明	設定
GNRL_EV_VIRUS_FOUND		悪意のあるオブジェクトが検知された。	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_8 は Trojware などの脅威の別です。</li> <li>GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント (<a href="#">エンジン </a>)。 脅威検知技術 (<a href="#">方法 </a>)。 プライベート KSN により検知された脅威 (拒リスト) : true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。</li> </ul>
GNRL_EV_SUSPICIOUS_OBJECT_FOUND		ユーザーに損害を与える目的で	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> </ul>




		悪用される可能性のある正規のソフトウェアを検知した	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_5 は EICAR-Test-File など脅威の種別です。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_8 は Trojware などの脅威の種別です。</li> </ul>
GNRL_EV_OBJECT_CURED	⚠	オブジェクトが駆除された。	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_3 はオブジェクトの作成日 (省略可能)。</li> <li>GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_8 は Trojware などの脅威の種別です。</li> <li>GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント (<a href="#">エンジン</a>)。 脅威検知技術 (<a href="#">方法</a>)。 プライベート KSN により検知された脅威 (拒リスト) : true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。</li> </ul>
GNRL_EV_OBJECT_DELETED	⚠	オブジェクトが削除された。	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_3 はオブジェクトの作成日 (省略可能)。</li> <li>GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> </ul>






			<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_8 は Trojware などの脅威の別です。</li> <li>GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント (<a href="#">エンジン⑩</a>)。 脅威検知技術 (<a href="#">方法⑩</a>)。 プライベート KSN により検知された脅威 (拒リスト) : true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。</li> </ul>
GNRL_EV_OBJECT_NOTCURED	❗	駆除できない。	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_3 はオブジェクトの作成日 (省略可能)。</li> <li>GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント (<a href="#">エンジン⑩</a>)。 脅威検知技術 (<a href="#">方法⑩</a>)。 プライベート KSN により検知された脅威 (拒リスト) : true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。</li> </ul>
GNRL_EV_PASSWD_ARCHIVE_FOUND	①	パスワードで保護されている圧縮ファイルが検知された。	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_2 はオブジェクトの名前です。</li> <li>GNRL_EA_PARAM_3 はオブジェクトの作成日 (省略可能)。</li> <li>GNRL_EA_PARAM_7 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント (<a href="#">エンジン⑩</a>)。 脅威検知技術 (<a href="#">方法⑩</a>)。 プライベート KSN により検知された脅威 (拒リスト) : true または false。</li> </ul>
GNRL_EV_ATTACK_DETECTED	❗	ネットワ	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 は攻撃の名前です。</li> </ul>

		<p>ーク攻撃が検知された（ネットワーク脅威対策）</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 はプロトコルです。</li> <li>• GNRL_EA_PARAM_3 はネットワーク攻撃の攻撃として動作しているコンピューターの IP アドレスです。IP アドレスはホストのバイト順で示されます。たとえば、172.16.0.201 は 2886729929 となります。</li> <li>• GNRL_EA_PARAM_4 はポート番号です。</li> <li>• GNRL_EA_PARAM_5 は IPv6 アドレス（例：12B012B012B012B012B012B012B012B012B012B012B0）です。</li> <li>• GNRL_EA_PARAM_6 はネットワーク攻撃の対象になったコンピューターの IP アドレスです。IP アドレスはホストのバイト順で示されます。たとえば、172.16.0.201 は 2886729929 となります。</li> </ul>
GNRL_EV_APPLICATION_LAUNCHED	①	<p>アプリケーションの起動が許可された（アプリケーションコントロール）</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 は Kaspersky Security Cent の特殊な形式の、アプリケーションが最後に開始された時刻です。</li> <li>• GNRL_EA_PARAM_3 はアプリケーションが開始された回数の合計です。</li> <li>• GNRL_EA_PARAM_4 はアカウントセキュリティ別子（SID）です。</li> <li>• GNRL_EA_PARAM_5 アプリケーションのカテゴリ ID です（省略可能）。</li> <li>• GNRL_EA_PARAM_6 はセッションのユーザーの前です。</li> </ul>
GNRL_EV_APPLICATION_LAUNCH_DENIED	❗	<p>アプリケーションの起動が禁止された（アプリケーションコントロール）</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>• GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。</li> <li>• GNRL_EA_PARAM_4 アプリケーションのカテゴリ ID です（省略可能）。</li> <li>• GNRL_EA_PARAM_5 はアプリケーションのデジタル署名に関する情報です。</li> <li>• GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。</li> <li>• GNRL_EA_PARAM_7 は実行ファイルのパスです。</li> <li>• GNRL_EA_PARAM_8 はオブジェクトのハッシュ（SHA256）です。</li> </ul>

			<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。</li> </ul>
GNRL_EV_APP_LAUNCH_TESTED_DENIED	①	アプリケーションの起動がテストモードでブロックされた (アプリケーションコントロール)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。</li> <li>GNRL_EA_PARAM_4 はアカウントセキュリティ別子 (SID) です。</li> <li>GNRL_EA_PARAM_5 はアプリケーションのデジタル署名に関する情報です。</li> <li>GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。</li> <li>GNRL_EA_PARAM_7 は実行ファイルのパスです</li> <li>GNRL_EA_PARAM_8 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。</li> </ul>
GNRL_EV_APP_LAUNCH_TESTED_ALLOW	①	アプリケーションの起動がテストモードで許可された (アプリケーションコントロール)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。</li> <li>GNRL_EA_PARAM_4 はアカウントセキュリティ別子 (SID) です。</li> <li>GNRL_EA_PARAM_5 アプリケーションのカテゴリ ID です (省略可能)。</li> </ul>
GNRL_EV_AC_USER_REQUEST	⚠	アプリケーションの開始のブロックに関して	<ul style="list-style-type: none"> <li>c_er_descr はユーザーへのメッセージです。</li> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。</li> <li>GNRL_EA_PARAM_7 は実行ファイルのパスです</li> </ul>

		管理者に送信するメッセージ (アプリケーションコントロール)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_8 はオブジェクトのハッシュ (SHA256) です。</li> <li>GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。</li> </ul>
GNRL_EV_WEB_URL_BLOCKED		アクセスが拒否された (ウェブコントロール)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 は URL です。</li> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_3 ウェブコントロールルール名前です。</li> </ul>
GNRL_EV_WEB_URL_WARNING		望ましくないコンテンツに関する警告 (ウェブコントロール)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 は URL です。</li> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> <li>GNRL_EA_PARAM_3 ウェブコントロールルール名前です。</li> </ul>
GNRL_EV_WC_USER_REQUEST		Web ページへのアクセスのブロックに関して管理者に送信するメッセージ	<ul style="list-style-type: none"> <li>c_er_descr はユーザーへのメッセージです。</li> <li>GNRL_EA_PARAM_1 は URL です。</li> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> </ul>

		(ウェブコントロール)	
GNRL_EV_DC_USER_REQUEST		デバイスへのアクセスのブロックに関して管理者に送信するメッセージ (デバイスコントロール)	<ul style="list-style-type: none"> <li>• c_er_descr はユーザーへのメッセージです。</li> <li>• GNRL_EA_PARAM_1 はハードウェアのIDです (HWID)。</li> <li>• GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> </ul>
GNRL_EV_DEVCTRL_DEV_PLUGGED		端末が電源に接続された (デバイスコントロール)	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 はハードウェアのIDです (HWID)。</li> <li>• GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> </ul>
GNRL_EV_DEVCTRL_DEV_UNPLUGGED		端末が電源から接続解除された (デバイスコントロール)	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 はハードウェアのIDです (HWID)。</li> <li>• GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> </ul>
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		電源に接続された	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 はハードウェアのIDです (HWID)。</li> </ul>

	端末がブ ロックさ れた (デ バイ スコ ント ロー ル)	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_2 はセッションのユーザーの前です。</li> </ul>
--	--	--

## 補足資料 8 : 実行防止でサポートされるファイルの拡張子

Kaspersky Endpoint Security は特定のアプリケーションで開かれる Office 形式のファイルを開く動作を防止します。サポートされるファイルの拡張子に関する情報は次の表を参照してください。

実行防止でサポートされるファイルの拡張子

アプリケーション名	実行ファイル	ファイルの拡張子
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
ワードパッド	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltn xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx

		pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

## 補足資料 9 : サポートされるスクリプトインタープリター

実行防止は次のスクリプトインタープリターをサポートしています :

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe



- msbuild.exe
- mshta.exe
- msixexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacyelevated.exe
- wscript.exe
- wwaahost.exe

実行防止は Java Runtime Environment (java.exe および javaw.exe のプロセス) で動作する Java アプリケーションの動作をサポートします。

## 補足資料 10 : レジストリ内の IOC スキャン範囲 (RegistryItem)

IOC スキャン範囲にデータ種別 RegistryItem を追加すると、Kaspersky Endpoint Security は次のレジストリキーをスキャンします :

HKEY\_CLASSES\_ROOT\htafile

HKEY\_CLASSES\_ROOT\batfile

HKEY\_CLASSES\_ROOT\exefile

HKEY\_CLASSES\_ROOT\comfile

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Class

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

HKEY\_LOCAL\_MACHINE\Software\Classes\piffile

HKEY\_LOCAL\_MACHINE\Software\Classes\htafile

HKEY\_LOCAL\_MACHINE\Software\Classes\exefile

HKEY\_LOCAL\_MACHINE\Software\Classes\comfile

HKEY\_LOCAL\_MACHINE\Software\Classes\CLSID

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Active Setup\Installed Components

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebg

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

## 補足資料 11 : IOC ファイルの要件

IOC スキャンタスクを作成する際は、次の [IOC ファイル](#) の要件および制限を考慮してください：

- Kaspersky Endpoint Detection and Response Optimum は侵害インジケータの記述に OpenIOC のバージョン 1.0 および 1.1 の IOC および XML が含まれる IOC ファイルをサポートしています。
- IOC スキャンタスクの作成中にサポートされない IOC ファイルをアップロードした場合、本製品はタスクが実行されたときにサポートされる IOC ファイルのみを使用します。
- IOC スキャンタスクの作成中にサポートされない IOC ファイルのみをアップロードした場合、タスクは実行されますが侵害インジケータは検出されません。

- IOC ファイルの構文エラーおよびサポートされないIOC タームおよびタグがあってもタスクの実行は失敗しません。IOC ファイルのこのようなセクションでは、本製品は一致なしとして判断します。
- 単一のIOC スキャンタスクで使用されるすべてのIOC ファイルの識別子は一意である必要があります。同じ識別子を持つIOC ファイルが存在した場合、タスクの実行結果に影響を与えることがあります。
- 単一のIOC ファイルのサイズは3MB を超えることはできません。サイズの大きいファイルを使用するとIOC スキャンタスクはエラーで終了します。IOC コレクションに追加されるすべてのファイルの合計サイズが3MB を超えても問題ありません。
- 脅威ごとに1つのIOC ファイルを作成することを推奨します。IOC スキャンタスクの結果の解析がしやすくなるためです。

以下のリンクをクリックすることでダウンロードできるファイルには、Kaspersky Endpoint Detection and Response がサポートするすべてのOpenIOC 標準のIOC タームの一覧が含まれています。

 [こちらのリンクから IOC TERMS.XLSX ファイルをダウンロードできます](#)

本製品の OpenIOC 標準をサポートする機能および制限を次の表に示します。

OpenIOC バージョン 1.0 および 1.1 をサポートする機能および制限

サポートされる条件	OpenIOC 1.0 :  is isnot (セットからの例外として) contains containsnot (セットからの例外として) OpenIOC 1.1 :  is contains starts-with ends-with matches greater-than less-than
サポートされる条件の属性値	OpenIOC 1.1 :  preserve-case negate
サポートされる演算子	AND OR
サポートされるデータ種別	"date" : 日付 (適用可能な条件 : is、greater-than、less-than)  "int" : 整数 (適用可能な条件 : is、greater-than、less-than) "int" : 整数 (適用可能な条件 : is、greater-than、less-than)  "string" : 文字列 (適用可能な条件 : is、contains、matches、starts-with、ends-with)  "duration" : 期間 (秒) (適用可能な条件 : is、greater-than、less-than)
データ種別の解釈機能	"boolean string"、"restricted string"、"md5"、"IP"、"sha256" および "base64Binary" データ種別は文字列として解釈されます。

本製品はインターバルのフォームに設定されている場合はint および date データ種別の Content 設定の解釈をサポートします：

OpenIOC 1.0 :

Content フィールドの TO 演算子の使用：

<Content type="int">49600 TO 50700</Content>

<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>

<Content type="int">[154192 TO 154192]</Content>

OpenIOC 1.1 :

条件 greater-than および less-than の使用

Content フィールドでの演算子 TO の使用

ISO 8601、ズールー時間、UTC 形式でインジケータが設定されている場合、本製品はデータ種別 date および duration の解釈をサポートします。

## サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、ファイルlegal\_notices.txtに記載され、カスペルスキー製品のインストールフォルダーに保存されています。

## 商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、Reader、Shockwave は Adobe Systems Incorporated のアメリカ合衆国およびその他の国における商標または登録商標です。

Apple、FireWire、iTunes および Safari は Apple のアメリカ合衆国およびその他の国における登録商標です。

AutoCAD は、アメリカ合衆国およびその他の国における Autodesk, Inc. およびその子会社の商標または登録商標です。

文字商標 Bluetooth およびそのロゴは Bluetooth SIG, Inc. の所有財産です。

Borland は、Borland Software Corporation の商標または登録商標です。

Android および Google Chrome は、Google, Inc. の商標です。

Citrix および Citrix Provisioning Services および XenDesktop はアメリカ合衆国の特許庁およびその他の国で認定されている Citrix Systems, Inc. およびその子会社の登録商標です。

Dell は Dell, Inc. およびその子会社の商標です。

dBase は dataBased Intelligence, Inc. の商標です。

EMC は EMC Corporation のアメリカ合衆国およびほかの国における登録総評または商標です。

Radmin は Famatech の登録商標です。

IBM は、International Business Machines Corporation の世界各国における登録商標です。

ICQ は ICQ LLC の商標および登録商標です。

Intel は Intel Corporation のアメリカ合衆国およびその他の国における登録商標です。

IOS はアメリカ合衆国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Lenovo および ThinkPad are はアメリカ合衆国における Lenovo の商用です。

Linux はアメリカ合衆国およびその他の国における Linus Torvalds の登録商標です。

Logitech は Logitech のアメリカ合衆国および他の国における登録商標または商標です。

LogMeln Pro および Remotely Anywhere は LogMeln, Inc. の商標です。

Mail.ru は Mail.Ru, LLC の登録商標です。

McAfee は McAfee, のアメリカ合衆国およびほかの国における登録総評または商標です。

Microsoft、Access、Active Directory、ActiveSync、BitLocker、Excel、Internet Explorer、LifeCam Cinema、MSDN、MultiPoint、Outlook、PowerPoint、PowerShell、Visual Basic、Visual FoxPro、Windows、Windows PowerShell、Windows Server、Windows Store、MS-DOS、Surface および Hiyper-V は、アメリカ合衆国およびその他の国における Microsoft Corporation の登録商標です。

Mozilla、Firefox および Thunderbird は Mozilla Foundation の商標です。

Java および JavaScript は Oracle およびその子会社の登録商標です。

VERISIGN はアメリカ合衆国およびその他の国における VeriSign, Inc. およびその子会社の登録商標または未登録商標です。

VMware および VMware ESXi はアメリカ合衆国および世界各国における VMware, Inc. およびその子会社の商標または登録商標です。

Thawte は Symantec Corporation のアメリカ合衆国およびその他の国における子会社の商標または登録商標です。

SAMSUNG は SAMSUNG のアメリカ合衆国およびその他の国における商標です。