kaspersky

# Kaspersky Endpoint Security 10 Service Pack 2 for Windows

# 目次

# Kaspersky Endpoint Security 10 Service Pack 2 for Windows の概要

このセクションでは、Kaspersky Endpoint Security の機能、コンポーネントおよび配信キットについて説明すると共に、Kaspersky Endpoint Security におけるシステム要件の一覧を記載しています。

## 新機能

Kaspersky Endpoint Security 10 Service Pack 2 for Windows は、以下の機能と改良点を提供します：

1. アプリケーション起動コントロール：
   - サーバーオペレーティングシステムのサポート
   - DLL モジュールとドライバーのダウンロードの管理
   - インベントリタスク内のオブジェクト（DLL モジュールとスクリプトファイル）のリストの管理
   - 新しい条件（デジタル署名証明書の属性）に基づくオブジェクトの管理
   - ブロックされたアプリケーションのテスト起動に関するレポートの生成
   - アプリケーション起動コントロールでの 2 つの動作モード（ブラックリストとホワイトリスト）のサポート
   - SHA256 ハッシュによるオブジェクトの管理およびインベントリ
   - PowerShell インタープリターからのスクリプトの実行コントロール
   - 信頼するシステム証明書ストアの使用
2. Microsoft BitLocker 管理では、Microsoft の BitLocker 技術によるハードディスクの暗号化を有効にします：
   - 暗号化のリモート管理
   - 暗号化されたデバイスの監視
   - デバイス暗号化レポートの作成
   - 暗号化されたデバイスへのアクセスの復元
3. Kaspersky Disk Encryption：
   - 認証エージェントの起動前環境での仮想キーボードを使用した認証情報入力のサポート
   - デバイスの使用済み領域のみを暗号化する暗号化モード
   - タブレット（MS Surface バージョン 3、4）での暗号化のサポート
4. アプリケーション権限コントロール：
   - 音声および映像記録デバイスへのアプリケーションのアクセス管理

5. ウェブコントロール：

   - 追加の Web リソースのカテゴリに対する Web リソースへのアクセスルールの設定

6. デバイスコントロールを改善しました：

   - USB デバイスでのファイルの削除や保存に関するイベントを記録
   - ネットワーク名、暗号化種別、認証種別に基づき、信頼できる Wi-Fi ネットワークのリストを生成
   - CD/DVD 上のファイルの読み書きに対するユーザーアクセス権の管理

7. メールアンチウイルス：

   - メールアンチウイルスのスキャンで、アーカイブ内の特定の種別のファイルを削除または名前変更

8. Kaspersky Security Network：

   - Kaspersky Endpoint Security のレポートおよび Kaspersky Security Center のレポートで、オブジェクトの処理方法に関する決定の理由として KSN を表示
   - 選択したファイルの評価に関する KSN への問い合わせの送信
   - Kaspersky Endpoint Security がインストールされているクライアントコンピューターで KSN サーバーが使用できるかどうかのステータスを表示

## 製品の購入

Kaspersky Endpoint Security の配信キットには次のファイルが含まれます：

- 使用可能な方法のいずれかによって製品をインストールするのに必要な各ファイル。
- 製品のインストール時に使用されるアップデートパッケージファイル。
- Kaspersky Security Center 経由で Kaspersky Endpoint Security 管理プラグインをインストールするための klcfginst.msi ファイル。
- Kaspersky Security Network への参加条件を確認するための ksn_<言語 ID>.txt ファイル。
- 使用許諾契約書を確認するための license.txt ファイル。
- 共存できないソフトウェアのリストが含まれる incompatible.txt ファイル。
- 配信キットの内部設定を含む installer.ini ファイル。

  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。

ファイルにアクセスするには、配信キットを解凍する必要があります。

# コンピューター保護の編成

Kaspersky Endpoint Security 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。

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。

コンポーネントが提供するリアルタイム保護に加えて、コンピューターのウイルスや他の脅威を定期的にスキャンしてください。こうすることで、セキュリティレベルの設定が低いなどの理由により、保護コンポーネントで検知されないマルウェアが拡散する可能性を排除できます。

Kaspersky Endpoint Security 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。

管理コンポーネントとは、次にあげるコンポーネントを指します：

- **アプリケーション起動コントロール**：このコンポーネントは、ユーザーによるアプリケーションの起動の試みを追跡し、アプリケーションの起動を調節します。
- **アプリケーション権限コントロール**：オペレーティングシステムでのアプリケーションの処理を登録し、特定のアプリケーションの許可グループに応じてアプリケーション動作を調節します。アプリケーションのグループごとにルールのセットが指定されます。これらのルールによって、アプリケーションによるユーザーデータおよびオペレーティングシステムのリソースへのアクセスが規制されます。このようなデータには、ユーザーファイル（マイ ドキュメントフォルダー、クッキー、ユーザーアクティビティ情報）、ファイル、フォルダー、最もよく使用されるアプリケーションの設定や重要情報を含むレジストリキーがあります。
- **脆弱性モニター**：脆弱性モニターは、ユーザーのコンピューター上で起動された、あるいは実行されているアプリケーションのリアルタイム脆弱性スキャンを実行します。
- **デバイスコントロール**：このコンポーネントにより、データ保管領域（ハードディスク、リムーバブルドライブ、テープドライブ、CD/DVD など）、データ伝送装置（モデムなど）、情報をハードコピーに変換する装置（プリンターなど）、あるいはコンピューターに装置を接続するためのインターフェイス（USB、Bluetooth、赤外線など）へのアクセスに柔軟な制限を設定できます。
- **ウェブコントロール**：このコンポーネントでは、さまざまなユーザーグループの Web リソースへのアクセスに柔軟な制限を設定できます。

管理コンポーネントの動作は、次のルールに基づきます：

- アプリケーション起動コントロールはアプリケーション起動コントロールルールを使用します。
- アプリケーション権限コントロールはアプリケーション権限コントロールルールを使用します。
- デバイスコントロールはデバイスアクセスルールと接続バスアクセスルールを使用します。
- ウェブコントロールはWeb リソースアクセスルールを使用します。

次のコンポーネントが保護コンポーネントです：

- **ファイルアンチウイルス**：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。ファイルアンチウイルスは Kaspersky Endpoint Security の起動時に起動し、コンピューターのメモリ内で常時動作していま

す。また、コンピューター上および接続ドライブ上で開かれた、保存された、または起動されたすべてのファイルをスキャンします。ファイルアンチウイルスは、ファイルにアクセスしようとするすべての試みをインターセプトして、ファイルにウイルスや他の脅威がないかスキャンします。

- **システムウォッチャー**：このコンポーネントは、コンピューター上のアプリケーション動作を記録し、コンピューターの保護の効果を高めるためにこの情報を他のコンポーネントに提供します。
- **メールアンチウイルス**：受信 / 送信メールにウイルスや脅威などがないかスキャンします。
- **ウェブアンチウイルス**：HTTP および FTP プロトコルを介してコンピューターで受信されたトラフィックをスキャンし、URL を悪意のある Web サイトおよびフィッシングサイトの URL のデータベースと照合してチェックします。
- **メッセンジャーアンチウイルス**：このコンポーネントは、IM クライアントプロトコル経由でコンピューターが受信するトラフィックをスキャンします。このコンポーネントにより、多くの IM クライアントを安全に使用できます。
- **ファイアウォール**：コンピューターがインターネットまたはローカルエリアネットワークに接続されているときに、オペレーティングシステムに対する脅威を最大限にブロックして、コンピューターに保管されているデータを保護します。アプリケーションのネットワークルールとネットワークパケットルールの 2 種のルールに従って、すべてのネットワークの動作をフィルタリングします。
- **ネットワークモニター**：このコンポーネントを使用すると、コンピューターのネットワークアクティビティをリアルタイムで表示できます。
- **ネットワーク攻撃防御**：受信ネットワークトラフィックにおいて、典型的なネットワーク攻撃の活動があるかどうかをスキャンします。使用中のコンピューターを標的としてネットワーク攻撃が試行されたことが検知された場合、Kaspersky Endpoint Security は攻撃側コンピューターからのネットワークアクティビティをブロックします。

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

- **完全スキャン**：Kaspersky Endpoint Security は、RAM、起動時に読み込まれるオブジェクト、オペレーティングシステムのバックアップ記憶領域、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、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、RAM、およびルートキットの攻撃対象となるオブジェクトをスキャンします。
- **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。
- **脆弱性スキャン**：Kaspersky Endpoint Security は、オペレーティングシステムとインストールされたソフトウェアの脆弱性をスキャンします。このスキャンにより、侵入者が悪用する可能性のある潜在的な問題をタイムリーに検知して除去します。

ファイル暗号化機能により、ローカルコンピュータードライブ上に保存されているファイルやフォルダーを暗号化できます。ドライブの暗号化機能により、ハードディスクとリムーバブルドライブを暗号化できます。

## Kaspersky Security Center からのリモート管理

Kaspersky Security Center を使用すると、クライアントコンピューター上の Kaspersky Endpoint Security をリモートで起動、停止したり、製品設定をリモートで管理、構成したりできます。

## 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。サービス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およびタスクに関するレポートを保持します。このレポートには、Kaspersky Endpoint Security イベントと製品で実行されたすべての操作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。

- **データ保管領域**：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、感染したファイルや疑わしい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。感染の可能性があるファイルは、「隔離」と呼ばれる特別な保管領域に移動されます。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、「未処理ファイルのリスト」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。

- **通知サービス**：通知サービスにより、コンピューターの現在の保護ステータスおよび Kaspersky Endpoint Security の動作に関する情報がユーザーに常に通知されます。通知は画面に表示したり、メールで送信したりできます。

- **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レピュテーションに関する情報を全世界のユーザーからリアルタイムで収集できるため、コンピューター保護の効果が向上します。

- **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。ご購入元の販売代理店にお問い合わせください。

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）。

2. 機能が無効になったことをユーザーに通知します。

3. 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。

製品は、カスペルスキーで定義された専用のアルゴリズムを使用して、発生回数が多いエラーやハングアップに関する情報を受け取ります。

# 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：

- ハードディスク上の 2 GB 以上の空きディスクスペース

- クロック周波数 1 GHz のプロセッサ（SSE2 命令セット対応）
- RAM:
  - 1 GB（32 ビットオペレーティングシステム）
  - 2 GB（64 ビットオペレーティングシステム）

クライアントコンピューター用オペレーティングシステムのサポート：

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

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。

サーバー用オペレーティングシステムのサポート：

- Windows Small Business Server 2008 Standard / Premium（64 ビット）
- Windows Small Business Server 2011 Essentials / Standard（64 ビット）
- Windows MultiPoint Server 2011（64 ビット）
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 以降
- 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

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。

# 本製品のインストールと削除

このセクションでは、Kaspersky Endpoint Security のインストール、初期設定の完了、製品の旧バージョンからのアップグレード、製品の削除の各方法について説明します。

# 製品のインストール

このセクションでは、Kaspersky Endpoint Security をコンピューターにインストールして、製品の初期設定を完了する方法について説明します。

## 製品のインストール方法の概要

Kaspersky Endpoint Security 10 for Windows のインストールは、ローカルで（ユーザーのコンピューター上で直接）、または管理者のワークステーションからリモートで実行できます。

Kaspersky Endpoint Security 10 for Windows のローカルインストールは、次のいずれかのモードで実行できます：

- 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
  インタラクティブモードでは、セットアッププロセスでユーザーが入力を行う必要があります。
- コマンドラインを使用したサイレントモード
  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。

ネットワークコンピューター上にリモートで製品をインストールするには、以下を使用します：

- Kaspersky Security Center（『*Kaspersky Security Center 導入ガイド*』を参照）
- Microsoft Windows のグループポリシーエディター（オペレーティングシステムのヘルプファイルを参照）
- System Center Configuration Manager

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。

## セットアップウィザードを使用した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のページ間を移動するには、［**戻る**］と［**次へ**］を使用します。タスク完了後にセットアップウィザードを閉じるには、［**終了**］をクリックします。セットアップウィザードを任意の段階で停止するには、［**キャンセル**］をクリックします。

*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. 配信キットに入っているファイル setup.exe を実行します。
   セットアップウィザードが起動します。

2. セットアップウィザードの指示に従います。

ファイル setup.exe が起動すると、Kaspersky Endpoint Security は、共存できないソフトウェアがないかコンピューターをチェックします。既定では、共存できないソフトウェアを検出すると、インストールプロセスが中断され、Kaspersky Endpoint Security と共存できないアプリケーションのリストが表示されます。インストールを続行するには、これらのアプリケーションをコンピューターから削除してください。

## ステップ1：コンピューターがインストール要件を満たしていることの確認

Kaspersky Endpoint Security 10 for Windows 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デートしたりする前に、次の条件が満たされていることを確認してください：

- オペレーティングシステムおよびサービスパックが製品をインストールするためのソフトウェア要件を満たしているかどうか
- 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求められます。

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 10 Service Pack 2 for Windows のインストール時に使用されます。該当する製品バージョンは次のとおりです：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

## ステップ2：インストール手順の開始ページ

製品をインストールするためのすべての要件が満たされている場合、インストールパッケージを起動すると開始ページが表示されます。開始ページにより、コンピューターへの Kaspersky Endpoint Security のインストールが開始されたことが告げられます。

セットアップウィザードを続行するには、［**次へ**］をクリックします。

## ステップ 3：使用許諾契約書の表示

この手順では、お客様とカスペルスキーの間で締結される使用許諾契約を表示するよう求められます。

本契約を慎重に検討し、その条件のすべてに同意する場合は、［**使用許諾契約書の条件に同意する**］をオンにしてください。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 4：インストール種別の選択

この手順では、Kaspersky Endpoint Security の最適なインストール種別を選択できます：

- **基本インストール**：このインストール種別を選択すると、保護コンポーネント、アプリケーション権限コントロール、脆弱性モニターがカスペルスキーの推奨設定でコンピューターにインストールされます。
- **標準インストール**：このインストール種別を選択すると、保護および管理コンポーネントがカスペルスキーの推奨設定でコンピューターにインストールされます。
- **カスタムインストール**：このインストール種別を選択すると、インストールするコンポーネントの選択および、製品のインストール先フォルダーを指定することができます。

  この種別のインストールでは、基本インストールまたは標準インストールに含まれないコンポーネントをインストールできます。

既定では標準インストールが選択されます。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 5：インストールするコンポーネントの選択

この手順は、製品のカスタムインストールを選択した場合に実行します。

この手順では、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。ファイルアンチウイルスは必須のコンポーネントです。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
- ドライブの暗号化
- ファイルの暗号化
- Microsoft BitLocker の管理

- KATA Endpoint Sensor

*Microsoft BitLocker の管理*は、次の機能を実行します：

- Windows オペレーティングシステムに組み込まれている BitLocker 暗号化の管理
- 暗号化ポリシーの設定と管理対象コンピューターに対する適用の可否のチェック
- 暗号化および復号化処理の開始
- 管理対象コンピューターの暗号化ステータスの監視
- Kaspersky Security Center 管理コンソールでの回復キーの一元保管

*KATA Endpoint Sensor* は、Kaspersky Anti Targeted Attack Platform のコンポーネントです。このコンポーネントの目的は、標的型攻撃などの脅威を速やかに検知することです。このコンポーネントは、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 Kaspersky Anti Targeted Attack Platform に渡します。

インストールするコンポーネントを選択するには、コンポーネント名の横のアイコンをクリックし、コンテキストメニューから［**ローカルハードディスクにインストール**］を選択します。選択したコンポーネントで実行するタスク、およびコンポーネントのインストールに必要なディスクの空き容量に関する詳細については、現在のセットアップウィザードページの下部を参照してください。

ローカルハードディスクの空き容量の詳細情報を表示するには、［**ボリューム**］をクリックします。［**必要な容量**］ウィンドウが開き、情報が表示されます。

コンポーネントのインストールをキャンセルするには、コンテキストメニューから［**インストールしない**］を選択します。

既定でインストールされるコンポーネントリストに戻すには、［**リセット**］をクリックします。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 6：インストール先フォルダーの選択

この手順は、製品のカスタムインストールを選択した場合に利用できます。

この手順では、製品のインストール先フォルダーのパスを指定できます。製品のインストール先フォルダーを選択するには、［**参照**］をクリックします。

ローカルハードディスクの空き容量の情報を表示するには、［**ボリューム**］をクリックします。［**必要な容量**］ウィンドウが開き、情報が表示されます。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 7：スキャン対象から除外する範囲の追加

この手順は、製品のカスタムインストールを選択した場合に利用できます。

この手順では、製品設定に追加する除外設定を指定できます。

［**Microsoft が推奨する領域をスキャン範囲から除外する**］、［**Kaspersky Lab が推奨する領域をスキャン範囲から除外する**］では、それぞれ Microsoft またはカスペルスキーの推奨領域を信頼ゾーンに含めるかどうかを選択できます。

これらのチェックボックスのいずれかをオンにすると、それぞれに関して Microsoft またはカスペルスキーの推奨する領域が信頼ゾーンに含まれます。このような領域では、ウイルスなどの脅威がスキャンされません。

［**Microsoft が推奨する領域をスキャン範囲から除外する**］は、Kaspersky Endpoint Security がサーバー用の Microsoft Windows を実行するコンピューター上にインストールされている場合に使用できます。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 8：製品のインストールの準備

コンピューターが、Kaspersky Endpoint Security 10 for Windows のインストールを妨害する可能性がある悪意のあるプログラムに感染している場合があるため、インストールプロセスを保護してください。

既定では、インストールプロセスの保護が有効になっています。

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）。その場合、インストールを中断して、アプリケーションセットアップウィザードをもう一度実行してください。手順「製品のインストール準備」で、［**インストールのプロセスを保護する**］をオフにします。

［**Citrix Provisioning Services との互換性を確保する**］で、Citrix PVS 互換モードでドライバーをインストールする機能を有効または無効にします。

Citrix Provisioning Services を使用している場合のみ、このチェックボックスをオンにしてください。

［**avp.com ファイルのパスをシステム変数 %PATH% に追加する**］では、ファイル avp.com のパスを %PATH% システム変数に追加するオプションを有効 / 無効にします。

このチェックボックスをオンにすると、コマンドラインから Kaspersky Endpoint Security またはそのタスクを開始するのに、実行ファイルのパスを入力する必要はありません。実行ファイルの名前と特定のタスクを開始するコマンドを入力すれば十分です。

セットアップウィザードの直前の手順に戻るには、［**戻る**］をクリックします。プログラムをインストールするには、［**インストール**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

製品のインストール中に、現在のネットワーク接続が終了することがあります。終了したネットワーク接続は、ほとんどの場合、製品のインストールが完了すると回復します。

## ステップ 9：製品のインストール

製品のインストールには、時間がかかる場合があります。完了するまでお待ちください。

以前のバージョンからアップデートする場合、以前のバージョンの設定移行および削除もこの手順に含まれます。

Kaspersky Endpoint Security のインストールが完了すると、初期設定ウィザードが起動します。

## コマンドラインからの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。

*本製品をインストールまたは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ー（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|0] [/pADDLOCAL=<コンポーネント>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<user name> /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 <配布キット名> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<コンポーネント>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [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` | 使用許諾契約書の条項に対する同意するかどうか。次の値を設定できます：<br>• `1`：使用許諾契約書の条項に同意する<br>• `0`：使用許諾契約書の条項に同意しない<br>使用許諾契約書のテキストは、Kaspersky Endpoint Security の配布キットに含まれています。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。 |
| `PRIVACYPOLICY` | プライバシーポリシーに同意するかどうか。次の値を設定できます：<br>• `1`：プライバシーポリシーに同意する<br>• `0`：プライバシーポリシーに同意しない |

| | |
|---|---|
| | プライバシーポリシーのテキストは、Kaspersky Endpoint Security の配布キットに含まれています。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。 |
| KSN | 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：<br>• 1：KSN への参加に同意する<br>• 0：KSN への参加に同意しない（既定値）<br>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。 |
| ALLOWREBOOT=1 | 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。<br>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。 |
| ADDLOCAL | インストールする追加のコンポーネントの選択。既定では、次のコンポーネント以外のすべての製品コンポーネントがインストールされます：有害 USB 攻撃ブロック、ファイルレベルの暗号化、ディスク全体の暗号化、BitLocker の管理、KATA Endpoint Sensor。次の値を設定できます：<br>• MSBitLockerFeature：BitLocker の管理をインストールします。<br>• AntiAPTFeature：KATA Endpoint Sensor をインストールします。 |
| SKIPPRODUCTCHECK=1 | 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、配布キットに含まれている 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。 |
| SKIPPRODUCTUNINSTALL=1 | 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。 |
| KLLOGIN | 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（パスワードによる保護コンポーネント）。ユーザー名は、「KLPASSWD」および「KLPASSWDAREA」の設定と合わせて指定します。既定のユーザー名は KLAdmin です。 |
| KLPASSWD | 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「KLLOGIN」および「KLPASSWDAREA」パラメータと合わせて指定します）。<br>「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、KLAdmin が既定のユーザー名として使用されます。 |
| KLPASSWDAREA | 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：<br>• SET：製品設定の変更<br>• EXIT：製品の終了<br>• DISPROTECT：保護コンポーネントの停止とスキャンタスクの停止<br>• DISPOLICY：Kaspersky Security Center ポリシーの無効化<br>• UNINST：コンピューターからの製品の削除<br>• DISCTRL：管理コンポーネントの停止<br>• REMOVELIC：ライセンスの削除<br>• REPORTS：レポートの表示 |
| ENABLETRACES | 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」フォルダーに保存します。次の値を設定できます：<br>• 1：トレース記録をオンにする<br>• 0：トレース記録をオフにする（既定値） |
| TRACESLEVEL | トレース記録の詳細度。次の値を設定できます：<br>• 100（緊急）：重大なエラーメッセージのみ。<br>• 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。<br>• 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。<br>• 400（重要）：通常のエラーと重大なエラーに関するメッセージとすべての警告、および一部の詳細情報を含むメッセージ。<br>• 500（通常）：通常のエラーと重大なエラーに関するメッセージとすべての警告、および製品の正常な動作に関する詳細情報を含むメッセージ（既定値）。<br>• 600（低）：すべてのメッセージ。 |

例：

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

本製品のインストール後、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 は試用版ライセンスでアクティベーションを行います。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、製品版ライセンスでアクティベーションを行ってください。

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：一般的なアプリケーションセットアップ設定
- install.cfg：Kaspersky Endpoint Security のローカル設定
- 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。

## System Center Configuration Manager を使用した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 の配信キットを含むフォルダーのパスを指定します。
   b. ［**プログラムの種類**］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の名前（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。

この手順は任意です。

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、配信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。

setup.ini ファイルには次のセクションが含まれています：

- `[Setup]`：一般的な製品インストール設定
- `[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。ファイルアンチウイルス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。
- `[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` | 使用許諾契約書の条項に対する同意するかどうか。次の値を設定できます：<br>• `1`：使用許諾契約書の条項に同意する<br>• `0`：使用許諾契約書の条項に同意しない<br>使用許諾契約書のテキストは、Kaspersky Endpoint Security の配布キットに含まれています。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。 |
| | `PrivacyPolicy` | プライバシーポリシーに同意するかどうか。次の値を設定できます：<br>• `1`：プライバシーポリシーに同意する<br>• `0`：プライバシーポリシーに同意しない |

| | | |
|---|---|---|
| | | プライバシーポリシーのテキストは、Kaspersky Endpoint Security の配布キットに含まれています。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。 |
| | KSN | 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：<br>• 1：KSN への参加に同意する<br>• 0：KSN への参加に同意しない（既定値）<br>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。 |
| | Login | 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（パスワードによる保護コンポーネント）。ユーザー名は、「Password」および「PasswordArea」の設定と合わせて指定します。既定のユーザー名は KLAdmin です。 |
| | Password | 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」パラメータと共に指定します）。<br>パスワードを指定しても Login パラメータでユーザー名を指定しなかった場合、KLAdmin が既定のユーザー名として使用されます。 |
| | PasswordArea | 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（「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。次の値を設定できます：<br>• SET：製品設定の変更<br>• EXIT：製品の終了<br>• DISPROTECT：保護コンポーネントの停止とスキャンタスクの停止<br>• DISPOLICY：Kaspersky Security Center ポリシーの無効化<br>• UNINST：コンピューターからの製品の削除 |

| | | |
|---|---|---|
| | | • DISCTRL：管理コンポーネントの停止<br>• REMOVELIC：ライセンスの削除<br>• REPORTS：レポートの表示 |
| | SelfProtection | 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：<br>• 1：製品のインストール保護メカニズムを有効にする<br>• 0：製品のインストール保護メカニズムを無効にする<br>インストールの保護をオフにすることができます。インストールの保護機能には、マルウェアによる配布パッケージのスプーフィングの防止、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ハイブ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）。 |
| | Reboot=1 | 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。<br>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。 |
| | AddEnvironment | %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かどうか。次の値を設定できます：<br>• 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<br>• 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 |
| | AMPPL | AM-PPL（Antimalware Protected Process Light）技術を使用した Kaspersky Endpoint Security サービスの保護を有効にするかどうか。次の値を設定できます： |

| | | |
|---|---|---|
| | | • 1：AM-PPL 技術を使用した Kaspersky Endpoint Security サービスの保護を有効にする<br>• 0：AM-PPL 技術を使用した Kaspersky Endpoint Security サービスの保護を無効にする |
| | SetupReg | 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。 |
| | EnableTraces | 本製品のインストールのトレース記録を有効にするかどうか。Kaspersky Endpoint Security は、トレースファイルを「%ProgramData%/Kaspersky Lab」フォルダーに保存します。次の値を設定できます：<br>• 1：本製品のインストールのトレース記録をオンにする<br>• 0：本製品のインストールのトレース記録をオフにする（既定値） |
| | TracesLevel | トレース記録の詳細度。次の値を設定できます：<br>• 100（緊急）：重大なエラーメッセージのみ。<br>• 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。<br>• 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。<br>• 400（重要）：通常のエラーと重大なエラーに関するメッセージとすべての警告、および一部の詳細情報を含むメッセージ。<br>• 500（通常）：通常のエラーと重大なエラーに関するメッセージとすべての警告、および製品の正常な動作に関する詳細情報を含むメッセージ（既定値）。<br>• 600（低）：すべてのメッセージ。 |
| [Components] | ALL | すべてのコンポーネントをインストールする。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。 |
| | MailAntiVirus | メールアンチウイルス |
| | IMAntiVirus | メッセンジャーアンチウイルス |
| | WebAntiVirus | ウェブアンチウイルス |
| | ApplicationPrivilegeControl | アプリケーション権限コントロール |
| | SystemWatcher | システムウォッチャー |
| | Firewall | ファイアウォール |

| | | |
|---|---|---|
| | NetworkAttackBlocker | ネットワーク攻撃防御 |
| | WebControl | ウェブコントロール |
| | DeviceControl | デバイスコントロール |
| | ApplicationStartupControl | アプリケーション起動コントロール |
| | 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 |
| | VulnerabilityAssessment | 脆弱性モニター |
| | KeyboardAuthorization | 有害 USB 攻撃ブロック |
| | AntiAPT | KATA Endpoint Sensor |
| | MSBitLocker | Microsoft BitLocker の管理 |
| | AdminKitConnector | Kaspersky Security Center から製品をリモート管理するためのネットワークエージェントコネクター。次の値を設定できます：<br>• 1：ネットワークエージェントコネクターをインストールする<br>• 0：ネットワークエージェントコネクターをインストールしない |
| [Tasks] | ScanMyComputer | 完全スキャンタスク。次の値を設定できます：<br>• 1：タスクを Kaspersky Endpoint Security のタスクリストに含める<br>• 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない |
| | ScanCritical | 簡易スキャンタスク。次の値を設定できます：<br>• 1：タスクを Kaspersky Endpoint Security のタスクリストに含める<br>• 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない |
| | Updater | アップデートタスク。次の値を設定できます：<br>• 1：タスクを Kaspersky Endpoint Security のタスクリストに含める<br>• 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない |

## 初期設定ウィザード

Kaspersky Endpoint Security の初期設定ウィザードは、アプリケーションセットアップ手順が終了したときに開始されます。この初期設定ウィザードでは、製品をアクティベートしたり、オペレーティングシステムに含まれるアプリケーションに関する情報を収集したりできます。このようなアプリケーションは、オペレーティングシステム内の処理であれば何の制約も受けない、信頼するアプリケーションのリストに追加されます。

初期設定ウィザードのインターフェイスは、一連のページ（手順）で構成されています。初期設定ウィザードのページ間を移動するには、［**戻る**］と［**次へ**］を使用します。初期設定ウィザードを完了するには、［**終了**］をクリックします。初期設定ウィザードの手順を任意の段階で停止するには、［**キャンセル**］をクリックします。

初期設定ウィザードが何らかの理由で中断された場合は、すでに指定されている設定は保存されません。次回この製品を使用するときに、初期設定ウィザードが再び起動し、設定を最初からやり直す必要があります。

## 製品のアクティベーション

本製品は、現在のシステム日時でアクティベートする必要があります。アクティベーション後にシステム日時を変更すると、ライセンスは機能しなくなります。アップデートのない動作モードに切り替わり、Kaspersky Security Network は使用できなくなります。ライセンスの機能を取り戻すには、オペレーティングシステムを再インストールするしか方法はなくなります。

この手順では、次の Kaspersky Endpoint Security アクティベーションオプションのいずれかを選択します：

- **アクティベーションコードによるアクティベーション**：アクティベーションコードによるアクティベーションを実行するには、このオプションを選択してアクティベーションコードを入力します。
- **ライセンス情報ファイルによるアクティベーション**：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、このオプションを選択します。
- **試用版のアクティベーション**：製品の試用版をアクティベートするには、このオプションを選択します。アプリケーションの試用版のライセンスによって規定される期間限定でアプリケーションの完全機能版を使用できます。ライセンスの有効期間が終了すると、製品の機能は使用できなくなります。試用版のアクティベーションを再度実行することはできません。
- **後でアクティベーション**：Kaspersky Endpoint Security のアクティベーションをスキップしたい場合は、このオプションを選択します。ファイルアンチウイルスとファイアウォールのみ使用ができます。インストール後、Kaspersky Endpoint Security の定義データベースとモジュールを一度だけアップデートできます。［**後でアクティベーション**］は、製品をインストールした直後に、初期設定ウィザードを初めて起動したときにのみ利用できます。

製品の試用版をアクティベートしたり、アクティベーションコードを使用して製品をアクティベートしたりするには、インターネット接続が必要です。

初期設定ウィザードを進めるには、アクティベーションオプションを選択して、［**次へ**］をクリックします。初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## アクティベーションコードによるアクティベーション

この手順は、アクティベーションコードを使用して、製品をアクティベートする場合にのみ利用できます。この手順は、試用版をアクティベートする場合またはライセンス情報ファイルを使用して製品をアクティベートする場合にはスキップされます。

この手順では、Kaspersky Endpoint Security は、入力されたアクティベーションコードをアクティベーションサーバーに次のように送信して検証します：

- アクティベーションコードの検証に成功すると、初期設定ウィザードで自動的に次のウィンドウが開きます。
- アクティベーションコードの検証が失敗した場合は、対応するメッセージが表示されます。このような場合は、Kaspersky Endpoint Security ライセンスを購入したソフトウェア販売業者に問い合わせてください。
- アクティベーションコードによるアクティベーションの回数が超過した場合は、対応する通知が表示されます。初期設定ウィザードが中断した場合、テクニカルサポートに問い合わせてください。

初期設定ウィザードの直前の手順に戻るには、［**戻る**］をクリックします。初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## ライセンス情報ファイルを使用したアクティベーション

この手順は、ライセンス情報ファイルを使用して、製品をアクティベートする場合にのみ利用できます。

この手順では、ライセンス情報ファイルのパスを指定します。ライセンス情報ファイルを指定するには、［**参照**］をクリックして、<ファイル ID>.key 形式のライセンス情報ファイルを選択します。

ライセンス情報ファイルを選択すると、ウィンドウ下部に次の情報が表示されます：

- ライセンス
- ライセンスの種類（製品版か試用版か）とこのライセンスを使用できるコンピューターの台数
- コンピューター上での製品のアクティベーションの実行日付
- ライセンスの有効期限
- ライセンスで許可される製品機能
- ライセンスに関する問題の通知（ある場合）。たとえば、「*ライセンスのブラックリストが破損しています*」。

初期設定ウィザードの直前の手順に戻るには、［**戻る**］をクリックします。初期設定ウィザードを続行するには、［**次へ**］をクリックします。初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## アクティベートする機能の選択

この手順は、試用版をアクティベートする場合にのみ利用できます。

この手順では、製品をアクティベートしたあとで使用可能になる機能を選択できます：

- **基本インストール**：このオプションを選択する場合、製品のアクティベーション後利用できるのは、保護コンポーネント、アプリケーション権限コントロール、脆弱性モニターだけです。
- **標準インストール**：このオプションを選択する場合、本製品のアクティベーション後に使用できるのは、製品の保護コンポーネントおよび管理コンポーネントのみです。
- **完全インストール**：このオプションを選択する場合、本製品のアクティベーション後に使用できるのは、データ暗号化機能を含むすべてのインストールされたコンポーネントです。

インストール時に、入手したライセンスで許可されているより多くのコンポーネントを選択した場合、アプリケーションのアクティベーション後、ライセンスで使用できないコンポーネントはインストールされますが動作しません。購入したライセンスで現在インストールされているコンポーネントより多くのコンポーネントを使用できる場合は、本製品のアクティベート後に、インストールされていないコンポーネントが［**ライセンス**］セクションにリストされます。

既定では標準インストールが選択されます。

初期設定ウィザードの直前の手順に戻るには、［**戻る**］をクリックします。初期設定ウィザードを続行するには、［**次へ**］をクリックします。初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## アクティベーションの完了

この手順では、Kaspersky Endpoint Security のアクティベーションが正常に完了したことが通知されます。次のライセンス情報も表示されます：

- ライセンスの種類（製品版か試用版か）とこのライセンスを使用できるコンピューターの台数
- ライセンスの有効期限
- ライセンスで許可される製品機能

初期設定ウィザードを続行するには、［**次へ**］をクリックします。初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## オペレーティングシステムの分析

この手順では、オペレーティングシステムに組み込まれるアプリケーションに関する情報が収集されます。このようなアプリケーションは、オペレーティングシステム内の処理であれば何の制約も受けない、信頼するアプリケーションのリストに追加されます。

これ以外のアプリケーションは、Kaspersky Endpoint Security インストール後に初めて起動されたときに分析されます。

初期設定ウィザードを停止するには、［**キャンセル**］をクリックします。

## 本製品の初期設定の終了

［初期設定ウィザード］ウィンドウに、Kaspersky Endpoint Security インストールプロセスの完了に関する情報が表示されます。

Kaspersky Endpoint Security を起動する場合は、［**終了**］をクリックします。

Kaspersky Endpoint Security を起動せずに初期設定ウィザードを終了する場合は、［**Kaspersky Endpoint Security 10 for Windows の起動**］をオフにして、［**終了**］をクリックします。

## Kaspersky Security Network に関する声明

この手順では、Kaspersky Security Network に参加するよう求められます。

Kaspersky Security Network に関する声明を確認します。

- すべての条項に同意する場合は、初期設定ウィザードのウィンドウで［**Kaspersky Security Network への参加条件に同意する**］をオンにします。
- Kaspersky Security Network の参加条件に同意しない場合は、初期設定ウィザードのウィンドウで［**Kaspersky Security Network への参加条件に同意しない**］をオンにします。

初期設定ウィザードを続行するには、［**OK**］をクリックします。

## 旧バージョンの製品のアップグレード方法の概要

以前のバージョンの製品を Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードするには、暗号化されたハードディスクをすべて復号化します。

以下の製品は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードできます：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1（ビルド 6.0.4.1424） / MP4 CF2（ビルド 6.0.4.1611）
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4（ビルド 6.0.4.1424） / MP4 CF2（ビルド 6.0.4.1611）
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows（ビルド 10.2.2.10535）
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows（ビルド 10.2.2.10535（MR1））
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows（ビルド 10.2.4.674）
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows（ビルド 10.2.5.3201）

上記のいずれかの製品を Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードする場合、隔離とバックアップの内容は移行されません。

以前のバージョンの製品からは、次の方法でアップグレードできます：

- セットアップウィザードを使用したローカルのインタラクティブモード
- ローカルのサイレントモードで、コマンドラインを使用
- Kaspersky Security Center を使用してリモートで（『*Kaspersky Security Center 導入ガイド*』を参照）

- Microsoft Windows のグループポリシーエディターからリモートで（オペレーティングシステムのヘルプファイルを参照）

以前のバージョンから Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードする場合、以前のバージョンを削除する必要はありません。以前のバージョンからアップグレードする前に、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。

# 製品の削除

このセクションでは、コンピューターから Kaspersky Endpoint Security を削除する方法について説明します。

## 製品の削除方法の概要

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 は、いくつかの方法でコンピューターからアンインストールできます：

- ローカルのインタラクティブモードで、セットアップウィザードを使用
- ローカルのサイレントモードで、コマンドラインを使用
- Kaspersky Security Center を使用してリモートで（詳細は『*Kaspersky Security Center 導入ガイド*』を参照）
- Microsoft Windows のグループポリシーエディターからリモートで（オペレーティングシステムのヘルプファイルを参照）

## セットアップウィザードを使用したアプリケーションの削除

*セットアップウィザードを使用して Kaspersky Endpoint Security を削除するには：*

1. ［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Endpoint Security 10 for Windows**］ - ［**変更、修復、削除**］の順に選択します。
   セットアップウィザードが起動します。
2. セットアップウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウで、［**アンインストール**］をクリックします。
3. セットアップウィザードの指示に従います。

## ステップ 1：将来的に使用するための製品データの保存

この手順では、製品の次回インストール時（新しいバージョンのインストール時など）に使用するために保存しておく、製品で使用する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。

*将来使用する製品データを保存するには：*

保存するデータ種別の隣にあるチェックボックスをオンにします：

- **ライセンスを保存する**：将来インストールする製品のアクティベートを不要にするデータ。インストール時までにライセンスの有効期間が終了していない限り、現在のライセンスを使用して自動的にアクティベートされます。
- **バックアップファイルと隔離ファイルを保存する**：製品によってスキャンされ、バックアップまたは隔離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と隔離ファイルにアクセスするには、これらのファイルを保存するために使用したも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および隔離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保管領域から復元してください。ただし、バックアップと隔離にあるファイルはコンピューターに損害を与える可能性があるため、これらのファイルを復元することは推奨されません。

- **設定を保存する**：製品の設定時に選択される製品の設定値。
- **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デバイスへの直接アクセスを提供するデータ。暗号化されたファイルおよびドライブへは、製品を暗号化機能とともに再インストールした後で直接アクセスできます。

  既定では、このチェックボックスはオンです。

セットアップウィザードを続行するには、［**次へ**］をクリックします。セットアップウィザードを停止するには、［**キャンセル**］をクリックします。

## ステップ 2：製品の削除の確認

製品を削除すると、コンピューターのセキュリティが危険にさらされるため、製品を削除するかどうか確認するよう求められます。これを行うには、［**削除**］をクリックします。

製品の削除を停止する場合、［**キャンセル**］をクリックすると、この操作をいつでもキャンセルできます。

## ステップ 3：製品の削除：削除の完了

この手順では、コンピューターから製品を削除します。製品の削除が完了するまで待機してください。

製品を削除すると、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。今すぐ再起動しない場合、製品の削除手順は、オペレーティングシステムが再起動されるまで、あるいはコンピューターの電源がオフになって再度オンになるまで完了しません。

## コマンドラインからの製品の削除

製品のアンインストールプロセスをコマンドラインから開始できます。アンインストールは、インタラクティブモードまたはサイレントモードで（アプリケーションセットアップウィザードを起動せずに）実行します。

*インタラクティブモードで製品のアンインストールプロセスを開始するには：*

コマンドラインに、「`setup.exe /x`」または「`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`」と入力します。

セットアップウィザードが起動します。セットアップウィザードの指示に従います。

*サイレントモードで製品のアンインストールプロセスを開始するには：*

コマンドラインに、「`setup.exe /s /x`」または「`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`」と入力します。

製品のアンインストールプロセスがサイレントモードで（セットアップウィザードを起動せずに）開始されます。

製品のアンインストールの操作がパスワードで保護されている場合、ユーザー名およびパスワードをコマンドラインに入力する必要があります。

*Kaspersky Endpoint Security の削除、変更、修復の認証用のユーザー名とパスワードが設定されたとき、インタラクティブモードでコマンドラインから製品を削除するには：*

コマンドラインに、「`setup.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /x`」または

「`msiexec.exe KLLOGIN=<User name> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`」と入力します。

セットアップウィザードが起動します。セットアップウィザードの指示に従います。

*Kaspersky Endpoint Security の削除、変更、修復の認証用のユーザー名とパスワードが設定されたとき、サイレントモードでコマンドラインから製品を削除するには：*

コマンドラインに、「`setup.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /s /x`」または

「`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<User name> KLPASSWD=***** /qn`」と入力します。

## 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方法には次の 2 通りがあります：

- 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。

*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ているオブジェクトとデータを削除するには：*

1. 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残っているシステムハードディスクが接続されているコンピューターで、Kaspersky Endpoint Security によって作成される実行ファイル fdert.exe を実行し、復元ツールを起動します。
2. 復元ツールのウィンドウの［**デバイスの選択**］で、オブジェクトとデータを削除する対象のシステムのハードディスクを選択します。
3. ［**スキャン**］をクリックします。
4. ［**認証エージェントのオブジェクトとデータの削除**］をクリックします。

   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プロセスが開始します。

認証エージェントのテスト操作後に残っていたオブジェクトとデータを削除した後で、認証エージェントと互換性のないアプリケーションに関する情報の削除がさらに必要になることがあります。

*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。

`avp pbatestreset` コマンドを実行するには、暗号化コンポーネントをインストールする必要があります。

# 製品のインターフェイス

このセクションでは、製品インターフェイスの主な要素について説明します。

# 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

## 製品の動作の表示

製品アイコンには、製品の動作を表示するという役割があります。

- アイコンは、製品のすべての保護コンポーネントが有効であることを示しています。
- アイコンは、Kaspersky Endpoint Security の動作時に、注意が必要な重要イベントが発生したことを示しています。たとえば、ファイルアンチウイルスの無効化、定義データベースの有効期間終了などです。
- アイコンは、Kaspersky Endpoint Security の動作時に、クリティカルイベントが発生したことを示しています。たとえば、コンポーネントの機能障害、定義データベースの破損などです。

# 製品アイコンのコンテキストメニュー

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 10 for Windows**：メインウィンドウに［**プロテクションとコントロール**］タブが表示されます。［**プロテクションとコントロール**］タブでは、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。
- **設定**：メインウィンドウに［**設定**］タブが表示されます。［**設定**］タブでは、既定の製品設定を変更することができます。
- **プロテクションとコントロールの一時停止 / プロテクションとコントロールの再開**：保護および管理コンポーネントの動作を一時的に停止 / 再開します。このコンテキストメニュー項目は、Kaspersky Security Center のポリシーが無効のときにのみ使用することができ、アップデートタスクおよびスキャンタスクには影響しません。
- **ポリシーを無効にする / ポリシーを有効にする**：Kaspersky Security Center のポリシーを無効 / 有効にします。このコンテキストメニュー項目は、Kaspersky Endpoint Security がポリシーに従って動作しており、Kaspersky Security Center のポリシーを無効にするためのパスワードが設定されている場合に使用できます。
- **製品情報**：この項目を指定すると、製品の詳細が表示された情報ウィンドウが開きます。

- **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

製品アイコンのコンテキストメニューを開くには、Microsoft Windows のタスクバーの通知領域で製品アイコンにカーソルを合わせて右クリックします。

## メインウィンドウ

Kaspersky Endpoint Security のメインウィンドウのインターフェイス要素を使用して、製品のメイン機能を利用できます。

本製品のメインウィンドウは 4 つの部分に分かれています（下図を参照）。

- ウィンドウの上部のインターフェイス要素では、次の情報を表示できます：
  - 製品の詳細情報
  - Kaspersky Security Network の統計情報
  - 未処理ファイルのリスト
  - 検知された脆弱性のリスト
  - 隔離されたファイルのリスト
  - 製品が検知した感染したファイルのコピーが保存されている領域
  - 製品全体または個別のコンポーネントの動作中もしくはタスクの実行中に発生したイベントに関するレポート
- ［**プロテクションとコントロール**］タブでは、コンポーネントの動作とタスクの実行を調整できます。［**プロテクションとコントロール**］タブは、メインウィンドウを開くと表示されます。
- ［**設定**］タブでは、既定の製品設定を編集できます。
- このウィンドウの下部には、次の要素があります：
  - ：このボタンをクリックすると、Kaspersky Endpoint Security のヘルプに移動します。
  - ：このボタンをクリックすると、オペレーティングシステムに関する情報、Kaspersky Endpoint Security の現在のバージョン、およびカスペルスキー情報リソースへのリンクを含む［**サポート**］ウィンドウが開きます。
  - または ：このボタンをクリックすると、現在のライセンスに関する情報を表示する［**ライセンス**］ウィンドウが開きます。
  - / / ：このボタンをクリックすると［**イベント**］ウィンドウが開き、適用可能なアップデートの情報や、暗号化されたファイルおよびデバイスへのアクセス要求に関する情報が表示されます。

このボタンは、アクセス要求や未インストールのアップデートがある場合にのみ表示されます。


メインウィンドウ

*次のいずれかの方法で Kaspersky Endpoint Security のメインウィンドウを開くことができます：*

- Microsoft Windows taskbar タスクバーの通知領域にある製品アイコンをクリックする
- 製品アイコンのコンテキストメニューから、［**Kaspersky Endpoint Security 10 for Windows**］を選択する

## ［設定］タブ

Kaspersky Endpoint Security の設定タブでは、製品の全般設定、個別コンポーネント、レポートと保管領域、スキャンタスク、アップデートタスク、脆弱性スキャンタスク、および Kaspersky Security Network サーバーとの通信などを設定できます。

［設定］タブは 2 つの部分で構成されます（下図を参照）。

- 左の部分には、製品のコンポーネント、タスク、詳細設定の各セクションがあり、それぞれにサブセクションがあります。
- 右の部分には、ウィンドウの左で選択したコンポーネントまたはタスクと詳細設定を設定するためのコントロール要素があります。


［設定］タブ

*次のいずれかの方法で［設定］タブを開くことができます：*

- メインウィンドウで、［**設定**］タブを選択します。
- 製品アイコンのコンテキストメニューから［**設定**］を選択します。

# ［プロテクションとコントロール］タブ

Kaspersky Endpoint Security の［プロテクションとコントロール］タブは、すべてのタスクの実行とすべての製品コンポーネントの動作の全般的な情報の提供を目的としています。このタブでは、コンポーネントの動作やタスクの実行の管理もできます。

［プロテクションとコントロール］タブは 3 つの部分で構成されます（下図を参照）：

- ［**エンドポイントコントロール**］セクションには、管理コンポーネントのリストがあります。
- ［**プロテクション**］セクションには、保護コンポーネントのリストがあります。
- ［**タスク**］セクションには、コンピューターで実行されるローカルタスクのリストがあります。

それぞれのセクションに、コンポーネントの動作の有効化と無効化、選択したコンポーネントやタスクの設定への移動、選択したコンポーネントやタスクの動作状況の表示に使用できるコントロール要素があります。


［プロテクションとコントロール］タブ

*次のいずれかの方法で［プロテクションとコントロール］タブを開くことができます：*

- メインウィンドウで、［**プロテクションとコントロール**］タブを選択します。
- Microsoft Windows taskbar タスクバーの通知領域にある製品アイコンをクリックする
- 製品アイコンのコンテキストメニューから、［**Kaspersky Endpoint Security 10 for Windows**］を選択する

# 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係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をインタラクティブ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。

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。

現在のライセンスを取得すると、次の種類のサービスを利用できます：

- 使用許諾契約書の条件に従った製品の使用
- テクニカルサポート

サービスの範囲と製品の使用に関する条件は、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。

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：

- 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、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。期限付き月額制サービスの有効期間が終了した後も Kaspersky Endpoint Security の動作を維持するには、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では、有効期間終了後に更新のための猶予期間が与えられる場合があり、その間は製品の機能が維持されます。サービスプロバイダーは、猶予期間を提供するかどうかを決定し、提供する場合はその期間を決定します。

月額制サービスのもとで 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が適用されると、現在のライセンスがインストールされます。現在のライセンスは、月額制サービスのもとで本製品を使用するためのライセンスを定義します。予備のライセンスは、アクティベーションコードを使用してのみインストールでき、ライセンス情報ファイルまたは月額制サービスを使用してインストールすることはできません。

月額制サービスで使用できる本製品の機能は、次の種別の製品版の機能に対応します：Standard、Kaspersky Business Space Security、Kaspersky Enterprise Space Security。これらの種別のライセンスは、サーバー、ワークステーション、およびモバイルデバイスを保護する目的、さらにワークステーションとモバイルデバイスで管理コンポーネントをサポートする目的で設計されたものです。

月額制サービスの管理に使用できるオプションは、サービスプロバイダーごとに異なります。サービスプロバイダーによっては、月額制サービス更新のための猶予期間（本製品の機能を維持する期間）を提供していないことがあります。

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。

## アクティベーションコードの概要

*アクティベーションコード*とは、Kaspersky Endpoint Security の製品版ライセンスを購入する際に受け取るコードのことで、20 桁のアルファベットと数字からなる一意の英数字文字列です。

アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーへのインターネット接続が必要です。

本製品がアクティベーションコード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インストールされます。予備のライセンスは、アクティベーションコードを使用してのみインストールでき、ライセンス情報ファイルまたは月額制サービスを使用してインストールすることはできません。

製品のアクティベーション後にアクティベーションコードを紛失した場合、アクティベーションコードを復元できます。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、アクティベーションコードが必要となる場合があります。アクティベーションコードを復元するには、テクニカルサポートに連絡してください。

## ライセンスについて

*ライセンス*とは、一意の英数字文字列です。ライセンスは、ライセンス証明書で明示される条件（ライセンスの種別、ライセンスの有効期限、ライセンスの制限）に従い、製品の使用を可能にします。

ライセンス証明書は、月額制サービスのもとでインストールされたライセンスには提供されません。

ライセンスは、アクティベーションコードまたはライセンス情報ファイルを使用して本製品に追加できます。

ライセンスの追加、編集、削除が可能です。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。ライセンスがブラックリストに登録された場合、製品を使用し続けるには別のライセンスを追加する必要があります。

有効期間が終了したライセンスを削除すると、製品の機能は使用できなくなります。削除したライセンスを再度追加することはできません。

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。

ライセンスがブラックリストに登録されている場合、本製品がアクティベートされたライセンスによって定義される機能は、8 日間利用できます。Kaspersky Security Network と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は、制限なしで利用できます。ライセンスがブラックリストに登録されている場合は、ユーザーに通知されます。8 日経過すると、本製品の機能は、ライセンスの有効期間が終了してから利用できる機能レベルに制限されます。アップデートなしで動作し、Kaspersky Security Network が利用できなくなります。

## ライセンス情報ファイルについて

*ライセンス情報ファイル*は、Kaspersky Endpoint Security の購入後カスペルスキーから受け取る、拡張子 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で製品をアクティベートするために、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

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：

- ライセンスの提供元へ問い合わせる
- カスペルスキーの Web サイトで、使用可能なアクティベーションコードを使用してライセンス情報ファイルを取得する

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。

## データ提供について

使用許諾契約書に同意することで、お客様は、本製品の使用情報、インストールされている製品の種別、バージョン、使用言語、製品のインストーラーの一意の識別子、インストールの種別、現在のライセンスと予備のライセンスのデータ（ライセンスの種別、有効期間、製品のアクティベーションの日付とライセンスの有効期限の日付、ライセンスの数、ライセンスの現在の状態、アクティベーションサーバーとの通信用プロトコルのバージョンなど）の情報を自動で送信することに同意したことになります。

アクティベーションコードで製品をアクティベートした場合、ライセンス所有者の製品の配信および使用に関する統計情報を受け取るために、お客様は、現在使用している製品のバージョン（インストールされている製品のアップデート情報、製品のインストーラーの識別子、ライセンス情報など）、オペレーティングシステムのバージョンおよび、情報の提供時に有効になっている製品コンポーネントの識別子を自動で提供することに同意したことになります。

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。

カスペルスキーは、取得した情報を匿名として一般的な統計情報の形式でのみ使用します。一般的な統計情報は、最初に取得した情報をもとに自動生成されます。あらゆる個人情報や機密情報は含まれません。取得した情報は、蓄積されると破棄されます（1年に1回）。一般的な統計情報は無期限に保管されます。

使用許諾契約書および KSN に関する声明の同意後の製品使用状況に関する情報の収集、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 サイトを参照してください。使用許諾契約書と KSN に関する声明は、ファイル license.txt および ksn.txt で確認できます。これらのファイルは、配信パッケージに含まれます。

## ライセンス情報の表示

*ライセンス情報を表示するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある または をクリックします。

［**ライセンス**］ウィンドウが開きます。ライセンスに関する情報は、［**ライセンス**］ウィンドウの上部にあるセクションに表示されます。

## ライセンスの購入

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入手できます。

*ライセンスを購入するには、次の手順を実行します：*

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある または をクリックします。
［**ライセンス**］ウィンドウが開きます。
3. ［**ライセンス**］ウィンドウで、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 サイトが開きます。

## ライセンスの更新

ライセンスの有効期間が終了しそうな場合は、更新できます。有効期間が終了する前に更新しておけば、既存のライセンスの有効期間が終了しても、コンピューターの保護が途切れることはありません。また、更新したライセンスは、新しいライセンスで製品をアクティベートするまで有効です。

*ライセンスを更新するには、次の手順を実行します：*

1. 製品の新しい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入手します。

2. 入手したアクティベーションコードまたはライセンス情報ファイルを使用して予備のライセンスを追加します。

これにより、予備のライセンスが追加されます。このライセンスは、ライセンスの有効期間が終了した時点でアクティブになります。

カスペルスキーのアクティベーションサーバー間での負荷分散のため、ライセンスを「予備のライセンス」から「現在のライセンス」に更新するには多少時間がかかる可能性があります。

## 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に問い合わせます。

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有効期間が終了した後で月額制サービスの更新が可能な猶予期間）が終了する日に、Kaspersky Endpoint Security が該当する通知を表示して、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。

［**ライセンス**］ウィンドウで、月額制サービスの契約のステータスを手動で更新できます。これは、猶予期間が過ぎてから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。

## サービスプロバイダーの Web サイトへのアクセス

*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. メインウィンドウを開きます。
2. メインウィンドウの下部にある または をクリックします。
   ［**ライセンス**］ウィンドウが開きます。
3. ［**ライセンス**］ウィンドウで、［**月額制サービスの契約プロバイダーに問い合わせる**］をクリックします。

## 製品のアクティベーション方法の概要

*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。ライセンスの追加は、製品のアクティベーションプロセスの1つです。

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：

- アプリケーションのインストール時に、初期設定ウィザードを使用。この方法では現在のライセンスを追加できます。
- アプリケーションインターフェイスからローカルでアクティベーションウィザードを使用。この方法では現在のライセンスと予備のライセンスを追加できます。
- 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。この方法では現在のライセンスと予備のライセンスを追加できます。
- リモートで Kaspersky Security Center の管理サーバー上のライセンス保管領域に保存されているライセンスおよび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信（詳細は、『*Kaspersky Security Center 管理者用ガイド*』を参照）。この方法では現在のライセンスと予備のライセンスを追加できます。

  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の負荷分散のため、（リモートまたはサイレントモードでのインストールの場合）アクティベーションコードを使った製品のアクティベーションには多少時間がかかる可能性があります。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。

## 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. メインウィンドウの下部にある または をクリックします。
   ［**ライセンス**］ウィンドウが開きます。
2. ［**ライセンス**］ウィンドウで、［**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。
3. アクティベーションウィザードの指示に従います。

   製品のアクティベーションの詳しい手順については、初期設定ウィザードのセクションを参照してください。

## コマンドラインからの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 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> /password=<パスワード> と入力します。

# 製品の起動と終了

このセクションでは、アプリケーションの自動起動の設定、アプリケーションの手動による起動または終了、保護および管理コンポーネントの一時停止または再開の方法について説明します。

## 製品の自動起動の有効化と無効化

自動起動とは、オペレーティングシステムの起動直後に、ユーザーが介入しなくても Kaspersky Endpoint Security が起動することを意味します。この製品起動オプションは、既定で有効になっています。

インストール完了後、Kaspersky Endpoint Security は初回は自動的に起動します。以降、オペレーティングシステムを起動すると製品は自動的に起動します。

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。すでに読み込まれ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。

*製品の自動起動を有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. 次のいずれかの手順を実行します：
   - 製品の自動起動を有効にするには、［**コンピューターの起動時に自動的に起動する**］をオンにします。
   - 製品の自動起動を無効にするには、［**コンピューターの起動時に自動的に起動する**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## 製品の手動での起動と終了

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、手動で終了しないでください。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。

製品の自動起動を無効にしている場合は、Kaspersky Endpoint Security を手動で起動する必要があります。

*製品を手動で起動するには*

［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Endpoint Security 10 for Windows**］の順に選択します。

*製品を手動で終了するには：*

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［**終了**］を選択します。

## 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無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すで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［**プロテクションとコントロールの一時停止**］を選択します。
   ［**プロテクションの一時停止**］ウィンドウが開きます。
3. 次のいずれかのオプションを選択します：
   - **指定した時間だけ一時停止する** - 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。
   - **再起動まで一時停止する** - 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. 前の手順で［**指定した時間だけ一時停止する**］を選択した場合、ドロップダウンリストで時間を選択します。

*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［**プロテクションとコントロールの再開**］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。

# ファイルシステムの保護：ファイルアンチウイルス

このセクションでは、ファイルアンチウイルスに関する情報と、このコンポーネントの設定方法について説明します。

## ファイルアンチウイルスの概要

ファイルアンチウイルスは、コンピューターのファイルシステムの感染を防止します。既定では、ファイルアンチウイルスは Kaspersky Endpoint Security と同時に起動し、コンピューター内のメモリに常駐して、コンピューターとそれに接続されているすべてのドライブで開かれたファイル、保存されたファイル、実行されたファイルすべてにウイルスなどの脅威がないかスキャンします。

ファイルに脅威を検知すると、次の処理が実行されます：

1. ファイルで検知されたオブジェクトの種別が検知されます（*ウイルス*、*トロイの木馬*など）。
2. ファイルが感染しているかどうかスキャンによって判断できない場合は、そのファイルを「感染している可能性がある」としてラベル付けします。ファイルには、ウイルスなどのマルウェアの典型的なコード、または既知のウイルスを改変したコードが含まれている可能性があります。
3. ファイルで検知された悪意のあるオブジェクトに関する通知が表示され（通知が設定されている場合）、ファイルアンチウイルスの設定で指定した処理がファイルに対して実行されます。

## ファイルアンチウイルスの有効化と無効化

既定ではファイルアンチウイルスは有効になっており、カスペルスキーのエキスパートによって推奨されているモードで実行されています。必要に応じて、ファイルアンチウイルスを無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでファイルアンチウイルスを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. ファイルアンチウイルスに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：

- ファイルアンチウイルスを有効にするには、メニューの［**開始**］を選択します。

  ［**ファイルアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

- ファイルアンチウイルスを無効にするには、メニューの［**停止**］を選択します。

  ［**ファイルアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからファイルアンチウイルスを有効または無効にするには：*

1. ［アプリケーション設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
3. 次のいずれかの手順を実行します：

   - ファイルアンチウイルスを有効にするには、［**ファイルアンチウイルスを有効にする**］をオンにします。
   - ファイルアンチウイルスを無効にするには、［**ファイルアンチウイルスを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## ファイルアンチウイルスの自動一時停止

指定した時間に、または特定のプログラムの処理時にファイルアンチウイルスが自動的に一時停止するように設定できます。

一部のプログラムと競合した際のファイルアンチウイルスの自動一時停止は応急の措置です。コンポーネントの動作中に競合が発生した場合は、テクニカルサポート（https://companyaccount.kaspersky.com）にお問い合わせください。サポート担当者が、ファイルアンチウイルスをセットアップするお手伝いをします。

*ファイルアンチウイルスの自動一時停止を設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
3. ［**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。

   ［**ファイルアンチウイルス**］ウィンドウが開きます。
4. ［**ファイルアンチウイルス**］ウィンドウで、［**詳細**］タブを選択します。
5. ［**タスクの一時停止**］セクションで、次の手順を実行します：

- 特定の時間にファイルアンチウイルスが自動的に一時停止するように設定するには、［**特定の時間帯**］をオンにして、［**設定**］をクリックします。

  ［**タスクの一時停止**］ウィンドウが開きます。

- 特定のアプリケーションの起動時にファイルアンチウイルスが自動的に一時停止するように設定するには、［**特定のアプリケーションの起動時**］をオンにして、［**設定**］をクリックします。

  ［**アプリケーション**］ウィンドウが開きます。

6. 次のいずれかの手順を実行します：

   - 特定の時間にファイルアンチウイルスが自動的に一時停止するように設定する場合は、［**タスクの一時停止**］ウィンドウで、［**一時停止する時刻**］と［**再開する時刻**］を使用して、ファイルアンチウイルスを一時停止させる期間（HH:MM 形式）を指定します。［OK］をクリックします。

   - 特定のアプリケーションの起動時にファイルアンチウイルスが自動的に一時停止するように設定する場合は、［**アプリケーション**］ウィンドウで、［**追加**］、［**編集**］、および［**削除**］を使用して、動作時にファイルアンチウイルスを一時停止させるアプリケーションのリストを作成します。［OK］をクリックします。

7. ［**ファイルアンチウイルス**］ウィンドウで［OK］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## ファイルアンチウイルスの設定

ファイルアンチウイルスを設定するには、次の手順に従います：

- セキュリティレベルを変更します。

  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。

- 感染したファイルの検知時に、ファイルアンチウイルスによって実行される処理を変更します。

- ファイルアンチウイルスの保護範囲を編集します。

  保護範囲を拡張または制限するには、スキャンオブジェクトを追加または削除するか、スキャン対象のファイルの種類を変更します。

- ヒューリスティック分析を設定します。

  ファイルアンチウイルスは、「シグネチャ分析」と呼ばれる技術を使用します。ファイルアンチウイルス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従い、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。ファイルアンチウイルス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オブジェクトの動作が分析されます。ヒューリスティック分析を利用すると、現在定義データベース内にレコードが存在していない、新しい悪意のあるオブジェクトを検知できます。

- スキャンを最適化します。

  ファイルアンチウイルスによって実行される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後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。

- 複合ファイルのスキャンを設定します。
- ファイルスキャン方法を変更します。

## セキュリティレベルの変更

コンピューターのファイルシステムを保護するために、ファイルアンチウイルスは、各種の設定グループを適用します。これらの設定グループは、「セキュリティレベル」と呼ばれます。セキュリティレベルには［**高**］、［**推奨**］、［**低**］の 3 種類があらかじめ設定されています。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。

*セキュリティレベルを変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
3. ［**セキュリティレベル**］セクションで、次のいずれかを実行します：
   - 事前に設定されているセキュリティレベル（［**高**］、［**推奨**］、または［**低**］）のいずれかを設定する場合は、スライダーを使って選択します。
   - カスタムのセキュリティレベルを設定する場合は、［**設定**］をクリックして［**ファイルアンチウイルス**］ウィンドウを開き、カスタム設定を入力します。
     カスタムのセキュリティレベルを設定すると、［**セキュリティレベル**］セクションのセキュリティレベルの名前が［**カスタム**］に変更されます。
   - セキュリティレベルを［**推奨**］に変更する場合は、［**既定**］をクリックします。
4. 変更を保存するには［**保存**］をクリックします。

## 感染したファイルに対するファイルアンチウイルス処理の変更

*感染したファイルに対するファイルアンチウイルス処理を変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
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。
   - **自動処理**：

- **次の処理を常に実行：駆除する。駆除できない場合は削除する**
- **次の処理を常に実行：駆除する**

  このオプションが選択されている場合でも、Kaspersky Endpoint Security は［**削除する**］の処理を Windows ストアアプリの一部であるファイルに適用します。

- **次の処理を常に実行：削除する**
- **次の処理を常に実行：ブロックする**

4. 変更を保存するには［**保存**］をクリックします。

## ファイルアンチウイルスの保護範囲の編集

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。スキャンするファイルの場所と種類は、ファイルアンチウイルスの保護範囲のプロパティです。既定では、ファイルアンチウイルスは、すべてのハードディスク、ネットワークドライブ、またはリムーバブルドライブに保存されている感染可能なファイルのみをスキャンします。

*保護範囲を作成するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
3. ［**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。

   ［**ファイルアンチウイルス**］ウィンドウが開きます。
4. ［**ファイルアンチウイルス**］ウィンドウで、［**全般**］タブを選択します。
5. ［**ファイル種別**］セクションで、ファイルアンチウイルスがスキャンするファイルの種別を指定します。
   - すべてのファイルをスキャンする場合は、［**すべてのファイルをスキャン**］を選択します。
   - 感染に対して最も脆弱な形式のファイルをスキャンする場合は、［**ファイル形式でファイルをスキャン**］を選択します。
   - 感染に対して最も脆弱な拡張子のファイルをスキャンする場合は、［**拡張子でファイルをスキャン**］を選択します。

   スキャンするファイルの種類を選択するときには、次の点に留意してください：

   - 悪意のあるコードの侵入とその後の有効化の確率がきわめて低い形式のファイル（txt など）があります。一方で、実行コードを含んでいるか含んでいる可能性がある形式のファイル（exe、dll、doc など）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きわめて高くなります。

- 侵入者はウイルスやその他の悪意のあるプログラムの拡張子を 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。ファイル形式でのファイルのスキャンを選択すると、拡張子に関係なく、ファイルアンチウイルスによりファイルヘッダーが分析されます。この分析により、このようなファイルが exe 形式のファイルであることが判明する可能性があります。このようなファイルについては、徹底的にウイルスとその他のマルウェアのスキャンが実行されます。

6. ［**保護範囲**］リストで、次のいずれかを実行します：

   - スキャン範囲に新しいオブジェクトを追加するには、［**追加**］をクリックします。

   - オブジェクトの場所を変更する場合は、スキャン範囲からオブジェクトを選択し、［**編集**］をクリックします。

   ［**スキャン範囲を選択**］ウィンドウが開きます。

   - スキャンするオブジェクトのリストからオブジェクトを削除する場合は、リストでオブジェクトを選択し、［**削除**］をクリックします。

     削除を確認するウィンドウが開きます。

7. 次のいずれかの手順を実行します：

   - 新しいオブジェクトを追加するか、スキャンするオブジェクトのリストからオブジェクトの場所を変更する場合は、［**スキャン範囲を選択**］ウィンドウでオブジェクトを選択し、［**追加**］をクリックします。

     ［**スキャン範囲を選択**］ウィンドウで選択したすべてのオブジェクトは、［**ファイルアンチウイルス**］ウィンドウの［**保護範囲**］リストに表示されます。

     ［**OK**］をクリックします。

   - オブジェクトを削除する場合は、削除を確認するウィンドウで［**はい**］をクリックします。

8. 必要に応じて、ステップ 6 ～ 7 を繰り返してオブジェクトを追加、移動、あるいはスキャンするオブジェクトのリストからオブジェクトを削除します。

9. スキャンするオブジェクトのリストからオブジェクトを除外するには、［**保護範囲**］リストの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。ただし、オブジェクトはファイルアンチウイルスのスキャン対象からは除外されますが、スキャンするオブジェクトのリストには残ります。

10. ［**ファイルアンチウイルス**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

## ファイルアンチウイルスでのヒューリスティック分析の使用

*ファイルアンチウイルス処理でのヒューリスティック分析の使用方法を設定するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。

3. ［**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。
   ［**ファイルアンチウイルス**］ウィンドウが開きます。
4. ［**ファイルアンチウイルス**］ウィンドウで、［**パフォーマンス**］タブを選択します。
5. ［**スキャン方法**］セクションで、次の手順を実行します：
   - ファイルアンチウイルスでヒューリスティック分析を使用する場合は、［**ヒューリスティック分析**］をオンにして、スライダーでヒューリスティック分析のレベルを［**低**］、［**中**］、［**高**］のいずれかに設定します。
   - ファイルアンチウイルスでヒューリスティック分析を使用しない場合は、［**ヒューリスティック分析**］をオフにします。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## ファイルアンチウイルス処理でのスキャン技術の使用

*ファイルアンチウイルス処理でのスキャン技術の使用方法を設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。
3. ［**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。
   ［**ファイルアンチウイルス**］ウィンドウが開きます。
4. ［**ファイルアンチウイルス**］ウィンドウで、［**詳細**］タブを選択します。
5. ［**スキャン技術**］セクション：
   - 使用したい技術のチェックボックスをオンにします。
   - ファイルアンチウイルスの処理に使用したくないテクノロジーの名前のチェックボックスをオフにします。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## スキャンの最適化

*ファイルスキャンを最適化するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。

3. ［**設定**］をクリックします。

   ［**ファイルアンチウイルス**］ウィンドウが開きます。

4. ［**ファイルアンチウイルス**］ウィンドウで、［**パフォーマンス**］タブを選択します。

5. ［**スキャンの最適化**］セクションで、［**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。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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の種類を限定することで、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。

ファイルアンチウイルスでは、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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。

3. ［**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。

   ［**ファイルアンチウイルス**］ウィンドウが開きます。

4. ［**ファイルアンチウイルス**］ウィンドウで、［**パフォーマンス**］タブを選択します。

5. ［**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。

6. 作成または更新された複合ファイルのみをスキャンする場合は、［**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。

   あらゆる種別の作成または更新された複合ファイルのみがスキャンされます。

7. ［**詳細**］をクリックします。

［**複合ファイル**］ウィンドウが開きます。

8. ［**バックグラウンドスキャン**］セクションで、次のいずれかを実行します：

   - ファイルアンチウイルスによるバックグラウンドでの複合ファイルの解凍をブロックする場合は、［**複合ファイルをバックグラウンドで展開する**］をオフにします。

   - バックグラウンドでのスキャン時にファイルアンチウイルスによる複合ファイルの解凍を許可する場合は、［**複合ファイルをバックグラウンドで展開する**］をオンにし、［**最小サイズ**］に任意の値を入力します。

9. ［**サイズ制限**］セクションで、次のいずれかを実行します：

   - 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をスキャンしない**］をオンにし、［**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。

   - ファイルアンチウイルスでサイズの大きい複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

     ファイルのサイズが［**最大サイズ**］の値を超えている場合、そのファイルはサイズの大きいファイルに分類されます。

> ［**大きな複合ファイルをスキャンしない**］がオンになっているかどうかに関係なく、アーカイブから展開されるサイズの大きいファイルは、ファイルアンチウイルスによってスキャンされます。

10. ［**OK**］をクリックします。

11. ［**ファイルアンチウイルス**］ウィンドウで［**OK**］をクリックします。

12. 変更を保存するには［**保存**］をクリックします。

## スキャン方法の変更

「スキャン方法」とは、ファイルアンチウイルスがファイルのスキャンを開始する条件を意味します。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。このファイルスキャン方法の場合、ファイルアンチウイルスでは、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、ファイルをスキャンするかどうかが判断されます。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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイルアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ファイルアンチウイルスの設定が表示されます。

3. ［**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。

   ［**ファイルアンチウイルス**］ウィンドウが開きます。

4. ［**ファイルアンチウイルス**］ウィンドウで、［**詳細**］タブを選択します。

5. ［**スキャン方法**］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**
- **ファイルのアクセス時と更新時にスキャン**
- **ファイルのアクセス時にスキャン**
- **ファイルの実行時にスキャン**

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

# メールの保護：メールアンチウイルス

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、メールアンチウイルスに関する情報と、このコンポーネントの設定方法について説明します。

## メールアンチウイルスの概要

メールアンチウイルスは受信メールと送信メールにウイルスなどの脅威がないかスキャンします。また、メールアンチウイルスは Kaspersky Endpoint Security と同時に起動して、コンピューターのメモリに常駐し、POP3、SMTP、IMAP、MAPI、NNTP プロトコルで送受信されるメッセージをすべてスキャンします。メッセージに脅威が検知されなければ、メッセージを閲覧または処理できます。

メールに脅威を検知すると、次の処理が実行されます：

1. メールで検知されたオブジェクトの種別が特定されます（トロイの木馬など）。
2. メールに次のいずれかのステータスが割り当てられます：
   - *感染の可能性あり*：このステータスは、メールが確かに感染しているかどうか判断できない場合に割り当てられます。メールには、ウイルスなどのマルウェアに典型的なコード、または既知のウイルスを改変したコードが含まれている可能性があります。
   - *感染*：このステータスは、メールのスキャンによって、Kaspersky Endpoint Security の定義データベースに含まれている既知のウイルスのコードが見つかった場合に、オブジェクトに割り当てられます。
   - *見つかりません*：このステータスは、メールのスキャンによってウイルスなどの脅威が検出されなかった場合に、オブジェクトに割り当てられます。

メールがブロックされ、検知されたオブジェクトについての通知が表示されて（通知設定で指定されている場合）、メールアンチウイルスで設定された処理が実行されます。

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に組み込むことができる機能拡張を使用して、メールのスキャン設定を調整できます。メールアンチウイルス機能拡張は、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。

メールアンチウイルスの動作は、タスクバーの通知領域に表示される製品アイコンによって示されます。メールアンチウイルスがメールをスキャンしているときは、製品アイコンが に変わります。

## メールアンチウイルスの有効化と無効化

既定ではメールアンチウイルスは有効になっており、カスペルスキーのエキスパートによって推奨されているモードで実行されています。必要に応じて、メールアンチウイルスを無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでメールアンチウイルスを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. メールアンチウイルスに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - メールアンチウイルスを有効にするには、メニューの［**開始**］を選択します。
     ［**メールアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - メールアンチウイルスを無効にするには、メニューの［**停止**］を選択します。
     ［**メールアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからメールアンチウイルスを有効または無効にするには：*

1. ［アプリケーション設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、メールアンチウイルスの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - メールアンチウイルスを有効にするには、［**メールアンチウイルスを有効にする**］をオンにします。
   - メールアンチウイルスを無効にするには、［**メールアンチウイルスを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## メールアンチウイルスの設定

メールアンチウイルスを設定するには、次の手順に従います：

- メールセキュリティレベルを変更します。
  事前にインストールされたメールセキュリティレベルのいずれかを選択することも、カスタムのメールセキュリティレベルを設定することもできます。

メールセキュリティレベルの設定を変更した場合、いつでも推奨のメールセキュリティレベル設定に戻すことができます。

- 感染したメッセージに対して Kaspersky Endpoint Security が実行する処理を変更します。
- メールアンチウイルスの保護範囲を編集します。
- メールに添付されている複合ファイルのスキャンを設定します。

  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。
- メールの添付ファイルの種別によるフィルタリングを設定します。

  メッセージの添付ファイルの種別によるフィルタリングにより、特定の種別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。
- ヒューリスティック分析を設定します。

  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。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では、Kaspersky Endpoint Security の定義データベースに現在レコードが存在しない、メッセージに含まれる脅威を検知することができます。
- Microsoft Office Outlook におけるメールのスキャンを設定します。

  Microsoft Office Outlook メールクライアントに組み込むことができる機能拡張を使用して、メールのスキャン設定を簡単に調整できます。

  Microsoft Outlook Express®、Windows メール、Mozilla™ Thunderbird™ などの他のメールクライアントを使用している場合、メールアンチウイルスは、SMTP、POP3、IMAP、NNTP プロトコルのトラフィックをスキャンします。

  > 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、メールアンチウイルスは 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。

## メールセキュリティレベルの変更

メールアンチウイルスは、メールを保護するために各種の設定グループを適用します。これらの設定グループは、「メールセキュリティレベル」と呼ばれます。以下のメールセキュリティレベルがあります：［**高**］、［**推奨**］、［**低**］。［**推奨**］メールセキュリティレベルは、カスペルスキーが推奨する最適な設定です。

*メールセキュリティレベルを変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、メールアンチウイルスの設定が表示されます。
3. ［**セキュリティレベル**］セクションで、次のいずれかを実行します：
   - 事前にインストールされているメールセキュリティレベル（［**高**］、［**推奨**］、または［**低**］）のいずれかに変更する場合は、スライダーを使って1つ選択します。

- カスタムメールセキュリティレベルを設定する場合は、［**設定**］をクリックして［**メールアンチウイルス**］ウィンドウを開き、設定を入力します。

  カスタムメールセキュリティレベルを設定すると、［**セキュリティレベル**］セクションのセキュリティレベルの名前が［**カスタム**］に変更されます。

- メールセキュリティレベルを［**推奨**］に変更する場合は、［**既定**］をクリックします。

4. 変更を保存するには［**保存**］をクリックします。

## 感染したメールに対する処理の変更

*感染したメールに対する処理を変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、メールアンチウイルスの設定が表示されます。
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。

   - **自動処理**：
   - **次の処理を常に実行：駆除する。駆除できない場合は削除する**
   - **次の処理を常に実行：駆除する**
   - **次の処理を常に実行：削除する**
   - **次の処理を常に実行：ブロックする**
4. 変更を保存するには［**保存**］をクリックします。

## メールアンチウイルスの保護範囲の編集

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。メールアンチウイルスの保護範囲プロパティには、メールアンチウイルスをメールクライアントに統合するための設定と、メールアンチウイルスがトラフィックをスキャンするメールの種別および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。

*メールアンチウイルスの保護範囲の作成*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。

ウィンドウの右側に、メールアンチウイルスの設定が表示されます。

3. ［**設定**］をクリックします。
［**メールアンチウイルス**］ウィンドウが開きます。

4. ［**全般**］タブを選択します。

5. ［**保護範囲**］セクションで、次のいずれかを実行します：

- メールアンチウイルスでコンピューター上の着信と発信のすべてのメッセージをスキャンする場合は、［**送受信メッセージ**］を選択します。
- メールアンチウイルスでコンピューター上の着信メッセージのみをスキャンする場合は、［**受信メッセージ**］を選択します。

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。

6. ［**接続性とプラグイン**］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メールアンチウイルスでスキャンする場合は、［**POP3 / SMTP / NNTP / IMAP トラフィック**］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メールアンチウイルスでスキャンしない場合は、［**POP3 / SMTP / NNTP / IMAP トラフィック**］をオフにします。この場合、［**Microsoft Office Outlook アドイン**］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アンチウイルス機能拡張によってスキャンされます。

Microsoft Office Outlook 以外のメールクライアントを使用している場合は、［**POP3/SMTP/NNTP/IMAP トラフィック**］をオフにすると、メールアンチウイルスは POP3、SMTP、NNTP、IMAP プロトコル経由で送信される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できるようにするには、［**Microsoft Office Outlook アドイン**］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ようにするには、［**Microsoft Office Outlook アドイン**］をオフにします。

メールアンチウイルス機能拡張は、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。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、メールアンチウイルスの設定が表示されます。
3. ［**設定**］をクリックします。
   ［**メールアンチウイルス**］ウィンドウが開きます。
4. ［**全般**］タブを選択します。
5. ［**複合ファイルのスキャン**］セクションで、次の手順を実行します：
   - メールアンチウイルスで、メールに添付されたアーカイブをスキップする場合は、［**添付のアーカイブのスキャン**］をオフにします。
   - メールアンチウイルスで、指定したファイルサイズより大きなメール添付ファイルをスキップする場合は、［**次のサイズを超えるアーカイブをスキャンしない**］をオンにします。このチェックボックスをオンにする場合は、チェックボックス名のフィールドに最大アーカイブサイズを指定します。
   - メールアンチウイルスで、スキャンの実行時間が指定した時間以上に必要となるメール添付ファイルをスキップしない場合は、［**次の時間を超えてアーカイブをスキャンしない**］をオフにします。
6. ［OK］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## メールの添付ファイルのフィルター処理

悪意のあるプログラムは、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の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。特定の種別の添付ファイルの名前を変更することにより、悪意のあるプログラム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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、メールアンチウイルスの設定が表示されます。
3. ［**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。
   ［**メールアンチウイルス**］ウィンドウが開きます。

4. ［**メールアンチウイルス**］ウィンドウで、［**添付ファイル**］タブを選択します。

5. 次のいずれかの手順を実行します：

- メールアンチウイルスを使用してメールの添付ファイルをフィルター処理しない場合は、［**すべての添付ファイルを受信する**］をオンにします。

- メールアンチウイルスを使用してメールの特定の種別の添付ファイルの名前を変更するには、［**選択した添付ファイルの名前を変更して受信する**］をオンにします。

実際のファイル形式が、そのファイル名の拡張子と一致しないことがあることに注意してください。

メールに添付されているオブジェクトのフィルタリングを有効にした場合、メールアンチウイルスによって、次の拡張子の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 メールの拡張子

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。次世代の Microsoft Windows オペレーティングシステムメタファイル。16 ビット Microsoft Windows では、EMF ファイルはサポートされません。

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

- メールアンチウイルスを使用してメールの特定の種別の添付ファイルを削除するには、［**選択した添付ファイルを削除して受信する**］をオンにします。

6. 前の手順で［**選択した添付ファイルの名前を変更して受信する**］または［**選択した添付ファイルを削除して受信する**］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。

   ファイルの種別のリストを変更するには、［**追加**］、［**編集**］、および［**削除**］の各ボタンを使用します。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

# 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、メールアンチウイルス機能拡張が 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 内からメールアンチウイルス設定を開いたり、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。Outlook 用メールアンチウイルス機能拡張では、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 のインターフェイスで［**Microsoft Office Outlook アドイン**］がオンになっている場合、メールアンチウイルスの設定を Outlook で直接指定できます。

Outlook では、受信メッセージはまずメールアンチウイルスによって（Kaspersky Endpoint Security のインターフェイスで［**POP3 / SMTP / NNTP / IMAP トラフィック**］がオンになっている場合）スキャンされ、次に Outlook のメールアンチウイルス機能拡張によってスキャンされます。メールアンチウイルスがメッセージに悪意のあるオブジェクトを検出すると、そのイベントに関する通知が表示されます。

通知ウィンドウで選択した処理によって、メールアンチウイルスと Outlook 用メールアンチウイルス機能拡張のどちらがメッセージの脅威を取り除くかが決まります。

- 通知ウィンドウで［**駆除**］または［**削除**］を選択すると、脅威の除去はメールアンチウイルスによって実行されます。
- 通知ウィンドウで［**スキップ**］を選択すると、Outlook 用メールアンチウイルス機能拡張が脅威を除去します。

送信メッセージは、最初に Outlook 用メールアンチウイルス機能拡張によってスキャンされ、次にメールアンチウイルスによってスキャンされます。

# Outlook でのメールスキャンの設定

*Outlook 2007 でメールスキャンを設定するには：*

1. Outlook 2007 のメインウィンドウを開きます。
2. メニューバーで［**サービス**］ - ［**設定**］の順に選択します。
   ［**オプション**］ウィンドウが開きます。
3. ［**オプション**］ウィンドウで、［**メールアンチウイルス**］タブを選択します。

*Outlook 2010 または 2013 でメールスキャンを設定するには：*

1. Outlook のメインウィンドウを開きます。
   左上端にある［**ファイル**］タブを選択します。
2. ［**オプション**］をクリックします。
   ［**Outlook のオプション**］ウィンドウが開きます。
3. ［**アドイン**］セクションを選択します。
   ウィンドウの右側に、Outlook に組み込まれたプラグインの設定が表示されます。

4. ［**アドイン オプション**］をクリックします。

## Kaspersky Security Center を使用したメールスキャンの設定

メールのスキャンに Outlook 用メールアンチウイルス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（https://technet.microsoft.com/ja-jp/library/cc179175.aspx）を参照してください。

*Kaspersky Security Center を使用して、Outlook 用メールアンチウイルス機能拡張の動作方法を設定するには：*

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、メールスキャンを設定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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**プロテクション**］セクションで、［**メールアンチウイルス**］サブセクションを選択します。
7. ［**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。
   ［**メールアンチウイルス**］ウィンドウが開きます。
8. ［**接続性とプラグイン**］セクションの［**設定**］をクリックします。
   ［**メールアンチウイルス**］ウィンドウが開きます。
9. ［**メールアンチウイルス**］ウィンドウで、次の操作を実行します：
   - Outlook 用メールアンチウイルス機能拡張を使用して、受信トレイに届く受信メッセージをスキャンするには、［**メール受信時にスキャンする**］をオンにします。
   - Outlook 用メールアンチウイルス機能拡張を使用して、受信メッセージをユーザーが開いたときにスキャンするには、［**メール閲覧時にスキャンする**］をオンにします。
   - Outlook 用メールアンチウイルス機能拡張を使用して、送信メッセージを送信時にスキャンするには、［**メール送信時にスキャンする**］をオンにします。
10. ［**メールアンチウイルス**］ウィンドウで［OK］をクリックします。
11. ［**メールアンチウイルス**］ウィンドウで［OK］をクリックします。
12. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

# インターネット上のプロテクション：ウェブアンチウイルス

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、ウェブアンチウイルスに関する情報と、このコンポーネントの設定方法について説明します。

## ウェブアンチウイルスの概要

コンピューターがオンラインになるたびに、コンピューターに保管されている情報がウイルスやマルウェアなどにさらされます。ウイルスやマルウェアは、フリーソフトウェアをダウンロードしているとき、または犯罪者による攻撃を受けている Web サイトを閲覧しているときにコンピューターに侵入する可能性があります。Web サイトを開いたりファイルをダウンロードしたりする前であっても、インターネット接続を確立するとすぐにネットワークワームがコンピューターに侵入する可能性があります。

ウェブアンチウイルスは、HTTP および FTP プロトコルを介してコンピューターから受信したデータ、またはコンピューターに送信したデータを保護し、URL を悪意のある Web サイトおよびフィッシングサイトの URL のデータベースと照合してチェックします。

ウェブアンチウイルスは、ユーザーまたはアプリケーションが HTTP プロトコルや FTP プロトコル経由でアクセスしたすべての Web サイトやファイルをインターセプトし、ウイルスや他の脅威が含まれていないかどうかを分析します。この後は、次のようになります：

- ページまたはファイルに悪意のあるコードが含まれていないことが分かった場合、ユーザーはそのページやファイルにすぐにアクセスできます。
- ユーザーが悪意のあるコードを含む Web サイトやファイルにアクセスすると、ウェブアンチウイルスの設定で指定した処理が実行されます。

## ウェブアンチウイルスの有効化と無効化

既定ではウェブアンチウイルスは有効になっており、カスペルスキーのエキスパートによって推奨されているモードで実行されています。必要に応じて、ウェブアンチウイルスを無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブ
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでウェブアンチウイルスを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。

3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。

4. ウェブアンチウイルスに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。

5. 次のいずれかの手順を実行します：

   - ウェブアンチウイルスを有効にするには、メニューの［**開始**］を選択します。
     ［**ウェブアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

   - ウェブアンチウイルスを無効にするには、メニューの［**停止**］を選択します。
     ［**ウェブアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからウェブアンチウイルスを有効または無効にするには：*

1. ［アプリケーション設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。

3. 次のいずれかの手順を実行します：

   - ウェブアンチウイルスを有効にするには、［**ウェブアンチウイルスを有効にする**］をオンにします。

   - ウェブアンチウイルスを無効にするには、［**ウェブアンチウイルスを有効にする**］をオフにします。

4. 変更を保存するには［**保存**］をクリックします。

## ウェブアンチウイルスの設定

ウェブアンチウイルスを設定すると、次のことが可能になります：

- Web トラフィックセキュリティレベルを変更します。
  HTTP および FTP プロトコルで送受信される Web トラフィックについて、あらかじめインストールされたセキュリティレベルのいずれかを選択できます。あるいは、カスタム Web トラフィックセキュリティレベルを設定します。
  Web トラフィックセキュリティレベル設定を変更すると、いつでも推奨 Web トラフィックセキュリティレベル設定に戻せます。

- Kaspersky Endpoint Security が悪意のある Web トラフィックオブジェクトに対して実行する処理を変更します。
  HTTP オブジェクトの分析によって悪意のあるコードが含まれていることが示される場合、ウェブアンチウイルスの対応は、ユーザーが事前に指定した処理によって異なります。

- ウェブアンチウイルスの URL スキャンを設定します。このスキャンでは URL をフィッシングサイトおよび悪意のある URL のデータベースと照合します。

- Web トラフィックにウイルスや他の悪意のあるプログラムがないかスキャンする場合に、ヒューリスティック分析を使用するように設定します。

  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。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。

- Web サイトのフィッシングリンクをスキャンする場合に、ヒューリスティック分析を使用するように設定します。

- ウェブアンチウイルスによる、HTTP および FTP プロトコル経由で送受信される Web トラフィックのスキャンを最適化します。

- 信頼する Web サイトのリストを作成します。

  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。ウェブアンチウイルスでは、信頼する Web サイトからの情報にウイルスおよびその他の脅威が含まれるかどうかは分析されません。たとえば、ウェブアンチウイルスが既知の Web サイトからのファイルダウンロードをブロックしている場合などに、このオプションが有効なことがあります。

  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。

## Web トラフィックセキュリティレベルの変更

HTTP や FTP プロトコルで送受信されるデータを保護するために、ウェブアンチウイルスは各種の設定グループを適用します。このような設定グループは、「Web トラフィックセキュリティレベル」と呼ばれます。Web トラフィックセキュリティレベルには［**高**］、［**推奨**］、［**低**］の 3 種類があらかじめ設定されています。［**推奨**］ Web トラフィックセキュリティレベルは、カスペルスキーが推奨する最適な設定です。

*Web トラフィックセキュリティレベルを変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。
3. ［**セキュリティレベル**］セクションで、次のいずれかを実行します：

   - 事前にインストールされている Web トラフィックセキュリティレベル（［**高**］、［**推奨**］、または［**低**］）のいずれかに変更する場合は、スライダーを使って 1 つ選択します。
   - カスタム Web トラフィックセキュリティレベルを設定する場合は、［**設定**］をクリックして［**ウェブアンチウイルス**］ウィンドウを開き、設定を入力します。

     Web トラフィックセキュリティレベルをカスタマイズすると、［**セキュリティレベル**］セクションのセキュリティレベルの名前が［**カスタム**］に変更されます。
   - Web トラフィックセキュリティレベルを［**推奨**］に変更する場合は、［**既定**］をクリックします。
4. 変更を保存するには［**保存**］をクリックします。

## 悪意のある Web トラフィックオブジェクトに対する処理の変更

*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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。
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。
   - **自動処理**：
   - **ダウンロードのブロック**
   - **ダウンロードの許可**
4. 変更を保存するには［**保存**］をクリックします。

## 悪意のある Web サイトおよびフィッシングサイトの URL のデータベースとの照合によるウェブアンチウイルスのスキャン

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、銀行からのメールに、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な場合です。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、ブラウザー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えることがあります。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、ウェブアンチウイルスモニターは、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 の配布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 URL のデータベースと照合して URL を確認するようにウェブアンチウイルスを設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。
3. ［**設定**］をクリックします。

   ［**ウェブアンチウイルス**］ウィンドウが表示されます。
4. ［**ウェブアンチウイルス**］ウィンドウで、［**全般**］タブを選択します。

5. 次の手順に従います：

   - ウェブアンチウイルスで、悪意のある URL のデータベースと照合して URL を確認する場合は、［**スキャン方法**］セクションで［**悪意のあるリンクのデータベースに登録されているかチェックする**］をオンにします。
   - ウェブアンチウイルスで、フィッシングサイトの URL のデータベースと照合して URL を確認する場合は、［**アンチフィッシングの設定**］セクションで［**フィッシングリンクのデータベースに登録されているかチェックする**］をオンにします。

   また、リンクを Kaspersky Security Network のレピュテーションデータベースと照合して確認することもできます。

6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## ウェブアンチウイルスでのヒューリスティック分析の使用

*ヒューリスティック分析の使用を設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。
3. ［**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。
   ［**ウェブアンチウイルス**］ウィンドウが開きます。
4. ［**全般**］タブを選択します。
5. ウェブアンチウイルスでヒューリスティック分析を使用して Web トラフィックのウイルスなどのマルウェアをスキャンする場合は、［**スキャン方法**］セクションで［**ウイルス検知用のヒューリスティック分析**］をオンにして、スライダーでヒューリスティック分析のレベルを［**低**］、［**中**］、［**高**］のいずれかに設定します。
6. ウェブアンチウイルスでヒューリスティック分析を使用して Web サイトのフィッシングリンクをスキャンする場合は、［**アンチフィッシングの設定**］セクションで［**フィッシングリンク検知用のヒューリスティック分析**］をオンにします。
7. ［**OK**］をクリックします。
8. 変更を保存するには［**保存**］をクリックします。

## 信頼する Web サイトの編集

*信頼する Web サイトを作成するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ウェブアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、ウェブアンチウイルスの設定が表示されます。

3. ［**設定**］をクリックします。

   ［**ウェブアンチウイルス**］ウィンドウが表示されます。

4. ［**信頼する URL**］タブを選択します。

5. ［**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。

6. 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。リストを作成するには：

   a. ［**追加**］をクリックします。

      ［**URL または URL マスク**］ウィンドウが表示されます。

   b. Web サイト / Web ページのアドレス、または Web サイト / Web ページのアドレスマスクを入力します。

   c. ［**OK**］をクリックします。

      信頼する Web サイトのリストに新しいレコードが表示されます。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

# インスタントメッセージングクライアントトラフィックの保護：メッセンジャーアンチウイルス

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、メッセンジャーアンチウイルスに関する情報と、このコンポーネントの設定方法について説明します。

## メッセンジャーアンチウイルスの概要

メッセンジャーアンチウイルスは、インスタントメッセージクライアント（「*IM クライアント*」）のトラフィックをスキャンします。

メッセンジャーアンチウイルスは、暗号化された経路で送信されるメッセージをスキャンしません。

メッセンジャークライアント経由で送信されるメッセージには、次の種類のセキュリティ脅威が含まれていることがあります：

- コンピューターへの悪意のあるプログラムのダウンロードを試みる URL
- 侵入者がフィッシング攻撃に使用する悪意のあるプログラムや Web サイトへの URL

  フィッシング攻撃の目的は、銀行のカード番号、パスポート情報、銀行支払いシステムや他のオンラインサービス（ソーシャルネットワークサイトまたはメールアカウントなど）のパスワードなど、ユーザーの個人情報を盗むことです。

メッセンジャークライアント経由でファイルが転送されることがあります。これらのファイルを保存しようとすると、ファイルアンチウイルスによりファイルがスキャンされます。

メッセンジャーアンチウイルスは、ユーザーがメッセンジャークライアント経由で送受信したすべてのメッセージをインターセプトし、コンピューターのセキュリティを脅かすリンクが含まれていないかスキャンします。

- メッセージに危険な URL が検知されなければ、ユーザーはそのメールを閲覧できます。
- メッセージに危険なリンクが検知された場合、メッセンジャーアンチウイルスは、アクティブなインスタントメッセンジャーのメッセージウィンドウに、脅威に関する情報をメッセージの代わりに表示します。

## メッセンジャーアンチウイルスの有効化と無効化

既定ではメッセンジャーアンチウイルスは有効になっており、カスペルスキーのエキスパートによって推奨されているモードで実行されています。必要に応じて、メッセンジャーアンチウイルスを無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでメッセンジャーアンチウイルスを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. ［**メッセンジャーアンチウイルス**］行を右クリックして、コンポーネント処理のコンテキストメニューを表示します。
5. 次のいずれかの手順を実行します：
   - メッセンジャーアンチウイルスを有効にするには、コンテキストメニューの［**開始**］を選択します。
     ［**メッセンジャーアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - メッセンジャーアンチウイルスを無効にするには、コンテキストメニューの［**停止**］を選択します。
     ［**メッセンジャーアンチウイルス**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからメッセンジャーアンチウイルスを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メッセンジャーアンチウイルス**］サブセクションを選択します。
   ウィンドウの右側に、メッセンジャーアンチウイルスの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - メッセンジャーアンチウイルスを有効にするには、［**メッセンジャーアンチウイルスを有効にする**］をオンにします。
   - メッセンジャーアンチウイルスを無効にするには、［**メッセンジャーアンチウイルスを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## メッセンジャーアンチウイルスの設定

メッセンジャーアンチウイルスを設定するには、次の操作を実行します：

- 保護範囲を設定します。

スキャン対象のメッセージの種別を変更することで、保護範囲を広げたり狭めたりすることができます。

- メッセージ内のリンクを、悪意のある URL およびフィッシング URL のデータベースと照合してスキャンするかどうか設定します。

## メッセンジャーアンチウイルスの保護範囲の作成

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。メッセンジャーアンチウイルスの保護範囲の特性は、スキャン対象のメッセージの種類で、着信または発信です。既定では、メッセンジャーアンチウイルスは着信と発信の両方のメッセージをスキャンします。発信トラフィックのスキャンは無効にすることができます。

*保護範囲を作成するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メッセンジャーアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、メッセンジャーアンチウイルスの設定が表示されます。
3. ［**保護範囲**］セクションで、次のいずれかを実行します：
   - メッセンジャーアンチウイルスで IM クライアントの着信と発信のすべてのメッセージをスキャンする場合は、［**送受信メッセージ**］を選択します。
   - メッセージアンチウイルスで IM クライアントの着信メッセージのみをスキャンする場合は、［**受信メッセージ**］を選択します。
4. 変更を保存するには［**保存**］をクリックします。

## 悪意のある URL およびフィッシングサイトの URL のデータベースとの照合による、メッセンジャーアンチウイルスでの URL のスキャン

*メッセンジャーアンチウイルスで、悪意のある Web サイトおよびフィッシングサイトの URL のデータベースと照合して URL をチェックするように設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**メッセンジャーアンチウイルス**］サブセクションを選択します。

   ウィンドウの右側に、メッセンジャーアンチウイルスの設定が表示されます。
3. ［**スキャン方法**］セクションで、メッセンジャーアンチウイルスで使用したい方法を選択します。
   - メッセージ内のリンクを、悪意のある Web サイトの URL のデータベースと照合してチェックする場合は、［**悪意のあるリンクのデータベースに登録されているかチェックする**］をオンにします。
   - メッセージ内のリンクを、フィッシングサイトの URL のデータベースと照合してチェックする場合は、［**フィッシングリンクのデータベースに登録されているかチェックする**］をオンにします。

4. 変更を保存するには［**保存**］をクリックします。

# システムウォッチャー

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、システムウォッチャーに関する情報を記載し、このコンポーネントの設定方法について説明します。

## システムウォッチャーの概要

システムウォッチャーは、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収集し、この情報をより信頼性の高い保護を提供する別のコンポーネントに送信します。

### Behavior Stream Signatures

Behavior Stream Signatures（BSS）には、Kaspersky Endpoint Security によって「危険」に分類されたアプリケーションの一連の処理が格納されます。アプリケーションの動作が Behavior Stream Signatures と一致する場合、指定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。

既定では、アプリケーションの動作が Behavior Stream Signatures と一致すると、システムウォッチャーはそのアプリケーションの実行ファイルを隔離に移動します。

### マルウェアによって実行された処理のロールバック

Kaspersky Endpoint Security では、システムウォッチャーが収集した情報に基づいて、駆除の実行中に、**オペレーティングシステムでマルウェアによって実行された処理をロールバック**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、悪意のあるプログラムによって作成され、ネットワークメディア以外のすべての場所にある実行ファイルを削除します。

  悪意のあるプログラム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。

  変更された、または削除されたファイルは復元しません。

- レジストリの動作

  Kaspersky Endpoint Security はマルウェアによって作成されたパーティションとレジストリキーを削除します。

  Kaspersky Endpoint Security は修正または削除されたパーティションおよびレジストリキーを復元しません。

- システムの動作

  Kaspersky Endpoint Security は悪意のあるプログラムによって開始されたプロセスを終了します。

  悪意のあるプログラムが侵入したプロセスを終了します。

  悪意のあるプログラム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

  悪意のあるプログラムのネットワーク動作をブロックします。

  悪意のあるプログラムが侵入したプロセスの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、ファイルアンチウイルスで開始するか、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。

## システムウォッチャーの有効化と無効化

既定では、システムウォッチャーは有効になっており、カスペルスキーによって推奨されているモードで実行されています。必要に応じて、システムウォッチャーを無効にすることができます。

システムウォッチャーは、保護コンポーネントのパフォーマンスに影響を与えるため、絶対に必要な場合を除いて無効にしないでください。検知された脅威をより正確に特定するために、保護コンポーネントがシステムウォッチャーによって収集されたデータを要求する場合があります。

システムウォッチャーを有効または無効にするには、次の 2 つの方法があります：

- メインウィンドウの［**プロテクションとコントロール**］タブ
- 製品の設定ウィンドウから

*メインウィンドウの［**プロテクションとコントロール**］タブを使用して、システムウォッチャーを有効または無効にするには、次の操作を行います：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. 右クリックして、システムウォッチャーに関する情報が含まれる行のコンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - システムウォッチャーを有効にするには、［**開始**］を選択します。
     ［**システムウォッチャー**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - システムウォッチャーを無効にするには、［**停止**］を選択します。
     ［**システムウォッチャー**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウから、システムウォッチャーを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**システムウォッチャー**］サブセクションを選択します。
   ウィンドウの右側に、**システムウォッチャー**の設定が表示されます。
3. 次のいずれかの手順を実行します：
   - システムウォッチャーを有効にするには、［**システムウォッチャーを有効にする**］をオンにします。
   - システムウォッチャーを無効にするには、［**システムウォッチャーを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## システムウォッチャーの設定

システムウォッチャーの設定では、次の操作を実行できます：

- 脆弱性攻撃ブロックを有効または無効にする
- 悪意のある動作がプログラムで検知された際の処理を選択する
- 駆除中のマルウェアによる変更のロールバックを有効または無効にする

## 脆弱性攻撃ブロックを有効または無効にする

*脆弱性攻撃ブロックを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**システムウォッチャー**］サブセクションを選択します。
   ウィンドウの右側に、**システムウォッチャー**の設定が表示されます。
3. 次のいずれかの手順を実行します：
   - 脆弱性のあるプログラムによって使用されるファイルを起動したときに、これらのファイルを監視するには［**脆弱性攻撃ブロックを有効にする**］をオンにします。
     脆弱性のあるプログラムによって使用されているファイルがユーザー以外によって起動されたことを検知したら、［**脅威の検知時の処理**］で選択した内容に従って処理します。
   - 脆弱性のあるプログラムによって使用されるファイルを起動したときに、これらのファイルを監視するには［**脆弱性攻撃ブロックを有効にする**］をオンにします。
4. 変更を保存するには［**保存**］をクリックします。

## 悪意のある動作がプログラムで検知されたイベントでの処理の選択

*悪意のある動作を行うプログラム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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**システムウォッチャー**］サブセクションを選択します。
   ウィンドウの右側に、**システムウォッチャー**の設定が表示されます。
3. ［**脅威の検知時の処理**］セクションの［**危険な動作の検知時**］ポップアップリストで、次の処理を選択します：
   - **自動処理**：
   - **ファイルの隔離**
   - **悪意のあるプログラムの終了**
   - **スキップ**
4. 変更を保存するには［**保存**］をクリックします。

## 駆除中のマルウェアによる変更のロールバックの有効化と無効化

*駆除中のマルウェアによる変更のロールバックを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**システムウォッチャー**］サブセクションを選択します。

   ウィンドウの右側に、**システムウォッチャー**の設定が表示されます。
3. 次のいずれかの手順を実行します：

   - マルウェアによるオペレーティングシステム内の変更を駆除の際にロールバックする場合は、［**駆除中にマルウェアによる変更をロールバックする**］をオンにします。
   - マルウェアによるオペレーティングシステム内の変更を駆除の際にロールバックしない場合は、［**駆除中にマルウェアによる変更をロールバックする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

# Firewall

このセクションでは、ファイアウォールに関する情報と、このコンポーネントの設定方法について説明します。

## ファイアウォールの概要

LAN およびインターネットの使用中に、コンピューターは、ウイルス、その他のマルウェア、およびオペレーションシステムとソフトウェアの脆弱性を利用するさまざまな攻撃にさらされます。

コンピューターがインターネットや LAN に接続されているとき、ファイアウォールが、オペレーティングシステムに影響を与える可能性がある脅威のほとんどをブロックして、ユーザーのコンピューターに保管されている個人情報を保護します。またファイアウォールは、ユーザーのコンピューターのすべてのネットワーク接続を検知し、既定のネットワーク接続のステータスと共に、IP アドレスのリストを表示します。

ファイアウォールは、ネットワークルールに従ってすべてのネットワークアクティビティをフィルタリングします。ネットワークルールを設定すると、すべてのアプリケーションのインターネットアクセスをブロックすることから、アクセスを無制限に許可することまで、目的のコンピューター保護レベルを指定できます。

## 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。必要に応じて、ファイアウォールを無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブを使用して、ファイアウォ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. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. ［**ファイアウォール**］行を右クリックして、ファイアウォール処理のコンテキストメニューを開きます。
5. 次のいずれかの手順を実行します：
   - ファイアウォールを有効にするには、コンテキストメニューで［**開始**］を選択します。
     ［**ファイアウォール**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - ファイアウォールを無効にするには、コンテキストメニューの［**停止**］を選択します。
     ［**ファイアウォール**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウから、ファイアウォ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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］を選択します。
   ウィンドウの右側に、ファイアウォールの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - ファイアウォールを有効にするには、［**ファイアウォールを有効にする**］をオンにします。
   - ファイアウォールを無効にするには、［**ファイアウォールを無効にする**］をオンにします。
4. 変更を保存するには［**保存**］をクリックします。

## ネットワークルールの概要

ネットワークルールを使用すると、ネットワーク接続試行の検知時にファイアウォールによって実行される動作を許可またはブロックできます。

ファイアウォールは、ネットワークレベルとプログラムレベルの 2 つのレベルで、異なる種類のネットワーク攻撃からコンピューターを保護します。ネットワークレベルの保護を行うには、ネットワークパケットルールを適用します。プログラムレベルの保護を行うには、インストールされたアプリケーションがネットワークリソースにアクセスするためのルールを適用します。

ファイアウォールの 2 つのレベルの保護に基づいて、次のルールを作成できます：

- *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、プログラムに関係なく、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。既定では、ファイアウォールによって、特定のネットワークパケットルールが指定されます。
- 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。このルールを使用して、ネットワークの動作のフィルタリングを詳細に調整できます。たとえば、特定の種類のネットワーク接続を一部のアプリケーションではブロックし、他のアプリケーションでは許可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。

各ネットワークパケットルール、およびアプリケーションのネットワークルールには、実行優先順位を指定できます。

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、ブラウザー 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。その後ブラウザー X（親アプリケーション）からブラウザー Y（子プロセス）のインストールを開始した場合、ブラウザー 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、ブラウザー 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ー Y のネットワークアクティビティを禁止するには、ブラウザー 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。

## ネットワーク接続種別の概要

ファイアウォールはユーザーのコンピューターのネットワーク接続をすべてコントロールし、検知された各ネットワーク接続にステータスを自動的に割り当てます。

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**アンチウイルス製品、ファイアウォール、またはフィルターによって保護されないネットワークのステータス（インターネットカフェのネットワークなど）です。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。外部ユーザーも、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したり、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したりすることはできません。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**このステータスは、そのネットワークからユーザーがこのコンピューターのファイルやプリンターにアクセスすることを信頼するネットワーク（LAN またはホームネットワークなど）に割り当てられます。

- **許可するネットワーク**このステータスは、コンピューターが攻撃されない、または不正にアクセスされない安全なネットワークに割り当てられます。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。

## ネットワーク接続種別の変更

*ネットワーク接続種別を変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。

   ウィンドウの右側に、ファイアウォールの設定が表示されます。
3. ［**使用可能なネットワーク**］をクリックします。

［**ファイアウォール**］ウィンドウが表示されます。

4. スタータスを変更するネットワーク接続を選択します。
5. コンテキストメニューで、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**
   - **プライベートネットワーク**
   - **許可するネットワーク**
6. ［**ファイアウォール**］ウィンドウで［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## 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と編集

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ことに留意する必要があります。

*ネットワークパケットルールを作成または編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］を選択します。
3. ［**ネットワークパケットルール**］をクリックします。
4. ［**ファイアウォール**］ウィンドウの［**ネットワークパケットルール**］タブが開きます。
   このタブには、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。
5. 次のいずれかの手順を実行します：
   - 新しいネットワークパケットルールを作成するには、［**追加**］をクリックします。
   - ネットワークパケットルールを編集するには、ネットワークパケットルールのリストから選択し、［**編集**］をクリックします。

   ［**ネットワークルール**］ウィンドウが開きます。
6. ［**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**
7. ［**名前**］で、次のいずれかの方法でネットワークサービス名を指定します：
   - ［**名前**］の右側の アイコンをクリックし、ドロップダウンリストからネットワークサービス名を選択します。
     ドロップダウンリストには、使用する頻度が最も多いネットワーク接続を定義するネットワークサービスが含まれています。
   - ［**名前**］に、ネットワークサービスの名前を手動で入力します。
8. データ転送プロトコルを指定します。
   a. ［**プロトコル**］をオンにします。
   b. ドロップダウンリストで、ネットワークの動作が監視されるプロトコルの種類を選択します。

TCP、UDP、ICMP、ICMPv6、IGMP、GRE プロトコルを使用するネットワーク接続がファイアウォールによって監視されます。

［**名前**］からネットワークサービスを選択すると、［**プロトコル**］が自動的にオンになり、このチェックボックスの横にあるドロップダウンリストに、選択したネットワークサービスに対応するプロトコル種別が含まれます。既定では、［**プロトコル**］はオフです。

9. ［**通信方向**］では、監視されたネットワークの動作の方向を選択します。

   次の方向のネットワーク接続がファイアウォールによって監視されます：

   - **受信（パケット）**
   - **受信**
   - **受信 / 送信**
   - **送信（パケット）**
   - **送信**

10. 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指定できます。

    a. ［**ICMP 種別**］をオンにし、ドロップダウンリストで ICMP パケットの種類を選択します。

    b. ［**ICMP コード**］をオンにし、ドロップダウンリストで ICMP パケットコードを選択します。

11. 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。

    a. ［**リモートポート**］にはリモートコンピューターのポートを入力します。

    b. ［**ローカルポート**］にはローカルコンピューターのポートを入力します。

12. ［**ネットワークアダプター**］テーブルで、ネットワークパケットを送信または受信するネットワークアダプターの設定を指定します。これを行うには、［**追加**］、［**編集**］、［**削除**］を使用します。

13. ネットワークパケットの管理を生存時間（TTL）によって制限する場合、［**TTL**］をオンにし、その横のフィールドで、送受信ネットワークパケットの生存時間の範囲を指定します。

    生存時間が指定値を超えないネットワークパケットの送信がネットワークルールによって制御されます。

    そうしない場合、［**TTL**］をオフにします。

14. 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を指定します。そのためには、［**リモートアドレス**］で次のいずれかの値を選択します：

    - **すべてのネットワークアドレス**：ネットワークルールは、すべての IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。
    - **選択したネットワークアドレス**：ネットワークルールは、［**許可するネットワーク**］、［**プライベートネットワーク**］、［**パブリックネットワーク**］の中から選択されたネットワーク種別に関連付けられている IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。
    - **設定したネットワークアドレス**：ネットワークルールは、［**追加**］、［**編集**］、［**削除**］の各ボタンを使用して、下のリストで指定した IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。

15. Kaspersky Endpoint Security がインストールされていて、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を指定します。そのためには、［**ローカルアドレス**］で次のいずれかの値を選択します：

    - **すべてのネットワークアドレス**：ネットワークルールは、Kaspersky Endpoint Security がインストールされている、すべての IP アドレスのコンピューターで送信または受信されるネットワークパケットを管理します。

    - **設定したネットワークアドレス**：ネットワークルールは、Kaspersky Endpoint Security がインストールされているコンピューターのうち、［**追加**］、［**編集**］、［**削除**］の各ボタンを使用して、下のリストで指定した IP アドレスのコンピューターで送信または受信されるネットワークパケットを管理します。

    ネットワークパケットを処理する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。その場合、**ローカルアドレス**設定の値は無視されます。

16. 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、［**イベントの記録**］をオンにします。

17. ［**ネットワークルール**］ウィンドウで［OK］をクリックします。

    新しいネットワークルールを作成すると、［**ファイアウォール**］ウィンドウの［**ネットワークパケットルール**］タブに表示されます。既定では、新しいネットワークルールは、ネットワークパケットルールのリストの最後に追加されます。

18. ［**ファイアウォール**］ウィンドウで［OK］をクリックします。

19. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。

    ウィンドウの右側に、ファイアウォールの設定が表示されます。

3. ［**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**］ウィンドウの［**ネットワークパケットルール**］タブが開きます。

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. 次のいずれかの手順を実行します：

    - ルールを有効にするには、ネットワークパケットルール名の隣にあるチェックボックスをオンにします。

    - ルールを無効にするには、ネットワークパケットルール名の隣にあるチェックボックスをオフにします。

6. ［OK］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。

   ウィンドウの右側に、ファイアウォールの設定が表示されます。
3. ［**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**］ウィンドウの［**ネットワークパケットルール**］タブが開きます。
4. リストで、処理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. ［**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：

   - **許可**
   - **ブロック**
   - **アプリケーションルールに準拠**
   - **イベントの記録**
6. ［**ファイアウォール**］ウィンドウで［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。

   ウィンドウの右側に、ファイアウォールの設定が表示されます。

3. ［**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**］ウィンドウの［**ネットワークパケットルール**］タブが開きます。

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**］および［**下へ**］を使用して、ネットワークパケットルールをリストの適切な場所に移動します。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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。

アプリケーション権限コントロールと同様に、既定では、グループ内の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リングするときに、ファイアウォールがアプリケーショングループネットワークルールを適用します。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。

アプリケーションに対するネットワークルールの管理では、次の操作を実行できます：

- 新しいネットワークルールを作成する。

  新しいネットワークルールを作成できます。ファイアウォールは、アプリケーションまたは選択されたグループに属するアプリケーションのネットワークの動作を、このルールによって規制します。

- ネットワークルールを有効化または無効化する。

  すべてのネットワークルールは、「*有効*」ステータスでアプリケーションに対するネットワークルールのリストに追加されます。ネットワーク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。

  手動で作成したネットワークルールを無効にできます。ネットワーク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。

- ネットワークルールの設定を変更する。

新しいネットワークルールを作成した後は、必要に応じていつでも設定に戻って編集できます。

- ネットワークルールに対する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のリストでは、アプリケーションまたはアプリケーショングループでネットワークの動作が検出されたときに、ネットワークルールに従ってファイアウォールが適用する処理を変更できます。

- ネットワークルールの優先度を変更する。

  カスタマイズされたネットワークルールの優先度を変更することができます。

- ネットワークルールを削除する。

  カスタマイズされたネットワークルールを削除して、選択したアプリケーションまたはアプリケーショングループのネットワークの動作をファイアウォールが検出したときにネットワークルールを適用しないようにしたり、アプリケーションネットワークルールのリストにルールが表示されないようにしたりできます。

## アプリケーションネットワークルールの作成と編集

*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または編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。
3. ［**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。

   ［**ファイアウォール**］ウィンドウの［**アプリケーションコントロールルール**］タブが開きます。
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、必要に応じて［**アプリケーションルール**］または［**グループのルール**］を選択します。

   ［**アプリケーションコントロールルール**］ウィンドウまたは［**アプリケーショングループコントロールルール**］ウィンドウが開きます。
6. 開くウィンドウで、［**ネットワークルール**］タブを選択します。
7. 次のいずれかの手順を実行します：

   - 新しいネットワークルールを作成するには、［**追加**］をクリックします。
   - ネットワークルールを編集するには、ネットワークルールのリストから選択し、［**編集**］をクリックします。

   ［**ネットワークルール**］ウィンドウが開きます。
8. ［**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**

9. ［**名前**］で、次のいずれかの方法でネットワークサービス名を指定します：

   - ［**名前**］の右側の アイコンをクリックし、ドロップダウンリストからネットワークサービス名を選択します。

     ドロップダウンリストには、使用する頻度が最も多いネットワーク接続を定義するネットワークサービスが含まれています。

   - ［**名前**］に、ネットワークサービスの名前を手動で入力します。

10. データ転送プロトコルを指定します。

    a. ［**プロトコル**］をオンにします。

    b. ドロップダウンリストで、ネットワークの動作を監視するプロトコルの種類を選択します。

    TCP、UDP、ICMP、ICMPv6、IGMP、GRE プロトコルを使用するネットワーク接続がファイアウォールによって監視されます。

    ［**名前**］からネットワークサービスを選択すると、［**プロトコル**］が自動的にオンになり、このチェックボックスの横にあるドロップダウンリストに、選択したネットワークサービスに対応するプロトコル種別が含まれます。既定では、［**プロトコル**］はオフです。

11. ［**通信方向**］では、監視されたネットワークの動作の方向を選択します。

    次の方向のネットワーク接続がファイアウォールによって監視されます：

    - **受信**
    - **受信 / 送信**
    - **送信**

12. 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指定できます。

    a. ［**ICMP 種別**］をオンにし、ドロップダウンリストで ICMP パケットの種類を選択します。

    b. ［**ICMP コード**］をオンにし、ドロップダウンリストで ICMP パケットコードを選択します。

13. 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。

    a. ［**リモートポート**］にはリモートコンピューターのポートを入力します。

    b. ［**ローカルポート**］にはローカルコンピューターのポートを入力します。

14. 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を指定します。そのためには、［**リモートアドレス**］で次のいずれかの値を選択します：

    - **すべてのネットワークアドレス**：ネットワークルールは、すべての IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。
    - **選択したネットワークアドレス**：ネットワークルールは、［**許可するネットワーク**］、［**プライベートネットワーク**］、［**パブリックネットワーク**］の中から選択されたネットワーク種別に関連付けられている IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。

- **設定したネットワークアドレス**：ネットワークルールは、［**追加**］、［**編集**］、［**削除**］の各ボタンを使用して、下のリストで指定した IP アドレスのリモートコンピューターで送信または受信されるネットワークパケットを管理します。

15. Kaspersky Endpoint Security がインストールされていて、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を指定します。そのためには、［**ローカルアドレス**］で次のいずれかの値を選択します：

    - **すべてのネットワークアドレス**：ネットワークルールは、Kaspersky Endpoint Security がインストールされている、すべての IP アドレスのコンピューターで送信または受信されるネットワークパケットを管理します。

    - **設定したネットワークアドレス**：ネットワークルールは、Kaspersky Endpoint Security がインストールされているコンピューターのうち、［**追加**］、［**編集**］、［**削除**］の各ボタンを使用して、下のリストで指定した IP アドレスのコンピューターで送信または受信されるネットワークパケットを管理します。

    ネットワークパケットを処理する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。その場合、**ローカルアドレス**設定の値は無視されます。

16. 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、［**イベントの記録**］をオンにします。

17. ［**ネットワークルール**］ウィンドウで［OK］をクリックします。
    新しいネットワークルールを作成すると、そのルールが［**ネットワークルール**］タブに表示されます。

18. アプリケーションのグループ向けのルールの場合［**アプリケーショングループコントロールルール**］ウィンドウで、アプリケーション向けのルールの場合［**アプリケーションコントロールルール**］ウィンドウで、［OK］をクリックします。

19. ［**ファイアウォール**］ウィンドウで［OK］をクリックします。

20. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。
   ウィンドウの右側に、ファイアウォールの設定が表示されます。

3. ［**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。
   ［**ファイアウォール**］ウィンドウの［**アプリケーションコントロールルール**］タブが開きます。

4. リストで、ネットワークルールを有効または無効に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、必要に応じて［**アプリケーションルール**］または［**グループのルール**］を選択します。

［**アプリケーションコントロールルール**］ウィンドウまたは［**アプリケーショングループコントロールルール**］ウィンドウが開きます。

6. 開くウィンドウで、［**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。

8. 次のいずれかの手順を実行します：

   - ルールを有効にするには、ネットワークルール名の隣にあるチェックボックスをオンにします。
   - ルールを無効にするには、ネットワークルール名の隣にあるチェックボックスをオフにします。

   > 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. アプリケーションのグループ向けのルールの場合［**アプリケーショングループコントロールルール**］ウィンドウで、アプリケーション向けのルールの場合［**アプリケーションコントロールルール**］ウィンドウで、［**OK**］をクリックします。

10. ［**ファイアウォール**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。
   ウィンドウの右側に、ファイアウォールの設定が表示されます。

3. ［**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。
   ［**ファイアウォール**］ウィンドウの［**アプリケーションコントロールルール**］タブが開きます。

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. ［**ネットワーク接続**］列を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から選択します。

   - **継承**
   - **許可**

- **ブロック**

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

*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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］を選択します。
   ウィンドウの右側に、ファイアウォールの設定が表示されます。

3. ［**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。
   ［**ファイアウォール**］ウィンドウの［**アプリケーションコントロールルール**］タブが開きます。

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、必要に応じて［**アプリケーションルール**］または［**グループのルール**］を選択します。
   ［**アプリケーションコントロールルール**］ウィンドウまたは［**アプリケーショングループコントロールルール**］ウィンドウが開きます。

6. 開くウィンドウで、［**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：

   - **許可**
   - **ブロック**
   - **イベントの記録**

9. アプリケーションのグループ向けのルールの場合［**アプリケーショングループコントロールルール**］ウィンドウで、アプリケーション向けのルールの場合［**アプリケーションコントロールルール**］ウィンドウで、［**OK**］をクリックします。

10. ［**ファイアウォール**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ファイアウォール**］サブセクションを選択します。

   ウィンドウの右側に、ファイアウォールの設定が表示されます。
3. ［**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。

   ［**ファイアウォール**］ウィンドウの［**アプリケーションコントロールルール**］タブが開きます。
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、必要に応じて［**アプリケーションルール**］または［**グループのルール**］を選択します。

   ［**アプリケーションコントロールルール**］ウィンドウまたは［**アプリケーショングループコントロールルール**］ウィンドウが開きます。
6. 開くウィンドウで、［**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. アプリケーションのグループ向けのルールの場合［**アプリケーショングループコントロールルール**］ウィンドウで、アプリケーション向けのルールの場合［**アプリケーションコントロールルール**］ウィンドウで、［OK］をクリックします。
10. ［**ファイアウォール**］ウィンドウで［OK］をクリックします。
11. 変更を保存するには［**保存**］をクリックします。

# ネットワークモニター

このセクションでは、ネットワークモニターに関する情報と、ネットワークモニターの起動方法について説明します。

# ネットワークモニターの概要

*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の開始

*ネットワークモニターを開始するには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. ［**ファイアウォール**］行を右クリックして、ファイアウォール処理のコンテキストメニューを開きます。
5. コンテキストメニューから［**ネットワークモニター**］を選択します。
   ［**ネットワークモニター**］ウィンドウが開きます。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。
   - ［**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。
   - ［**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、ユーザーのコンピューターと他のコンピューターの間の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攻撃防御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。

# ネットワーク攻撃防御

このセクションでは、ネットワーク攻撃防御に関する情報と、このコンポーネントの設定方法について説明します。

## ネットワーク攻撃防御の概要

ネットワーク攻撃防御は、受信ネットワークトラフィックにおいて、典型的なネットワーク攻撃の活動があるかどうかをスキャンします。使用中のコンピューターを標的としてネットワーク攻撃が試行されたことが検知された場合、Kaspersky Endpoint Security は攻撃元コンピューターからのネットワーク動作をブロックします。ネットワーク攻撃が試行されたことを示す警告が表示され、攻撃元コンピューターに関する情報が示されます。

1時間にわたって、攻撃元コンピューターからのネットワークトラフィックがブロックされます。攻撃元コンピューターをブロックするための設定を編集できます。

既知の種類のネットワーク攻撃の説明およびその対処方法は、Kaspersky Endpoint Security の定義データベースで提供されています。ネットワーク攻撃防御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。

## ネットワーク攻撃防御の有効化と無効化

既定では、ネットワーク攻撃防御は有効で、最適モードで動作します。必要に応じて、ネットワーク攻撃防御を無効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*ネットワーク攻撃防御を有効または無効にするには、メインウィンドウの［プロテクションとコントロール］タブで、次の手順を実行します：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**プロテクション**］セクションをクリックします。
   ［**プロテクション**］セクションが開きます。
4. ［**ネットワーク攻撃防御**］行を右クリックして、ネットワーク攻撃防御のコンテキストメニューを表示します。
5. 次のいずれかの手順を実行します：
   - ネットワーク攻撃防御を有効にするには、コンテキストメニューの［**開始**］を選択します。
     ［**ネットワーク攻撃防御**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - ネットワーク攻撃防御を無効にするには、コンテキストメニューの［**停止**］を選択します。

［**ネットワーク攻撃防御**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからネットワーク攻撃防御を有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ネットワーク攻撃防御**］サブセクションを選択します。

   ネットワーク攻撃防御の設定がウィンドウの右側に表示されます。
3. 次の手順に従います：
   - ネットワーク攻撃防御を有効にするには、［**ネットワーク攻撃防御を有効にする**］をオンにします。
   - ネットワーク攻撃防御を無効にするには、［**ネットワーク攻撃防御を有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## ネットワーク攻撃防御の設定

ネットワーク攻撃防御の設定では、次の操作を実行できます：

- 攻撃元コンピューターのブロックに使用する設定の編集
- ブロックから除外するアドレスのリストの生成

## 攻撃元コンピューターのブロックに使用する設定の編集

*攻撃元コンピューターをブロックする設定を編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ネットワーク攻撃防御**］サブセクションを選択します。

   ネットワーク攻撃防御の設定がウィンドウの右側に表示されます。
3. ［**攻撃元コンピューターからの接続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、ネットワーク攻撃の試行が検知された場合、ネットワーク攻撃防御により、指定した期間、そのコンピューターからのネットワークトラフィックがブロックされます。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、コンピューターが自動的に保護されます。

   このチェックボックスをオフにすると、ネットワーク攻撃の試行が検知された場合、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するネットワーク攻撃防御による自動保護が有効になりません。
4. ［**攻撃元コンピューターからの接続をブロックする時間**］の横にあるフィールドで、攻撃元コンピューターをブロックする時間を設定します。
5. 変更を保存するには［**保存**］をクリックします。

# ブロックから除外するアドレスの設定

*ブロックから除外するアドレスを設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**ネットワーク攻撃防御**］サブセクションを選択します。

   ネットワーク攻撃防御の設定がウィンドウの右側に表示されます。
3. ［**除外リスト**］をクリックします。

   ［**除外リスト**］ウィンドウが開きます。
4. 次のいずれかの手順を実行します：

   - 新しい IP アドレスを追加するには、［**追加**］をクリックします。
   - すでに追加された IP アドレスを編集するには、アドレスをリストから選択し、［**編集**］をクリックします。

   ［**IP アドレスの編集**］ウィンドウが開きます。
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. ［**IP アドレスの編集**］ウィンドウで［**OK**］をクリックします。
7. ［**除外リスト**］ウィンドウで［**OK**］をクリックします。
8. 変更を保存するには［**保存**］をクリックします。

# 有害 USB 攻撃ブロック

このセクションでは、有害 USB 攻撃ブロックに関する情報を提供します。

## 有害 USB 攻撃ブロックについて

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。

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 デバイスを製品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セキュリティキーボード（使用可能である場合）から入力するようユーザーに要求します。この手順をキーボード承認と呼びます。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、コンポーネントのインストール後すぐに、バックグラウンドモードで実行されます。製品に Kaspersky Security Center ポリシーが適用されない場合、コンピューターのプロテクションとコントロールの一時停止と再開によって、有害 USB 攻撃ブロックの有効化と無効化を切り替えることができます。

## 有害 USB 攻撃ブロックのインストール

Kaspersky Endpoint Security のインストール時に基本インストールまたは標準インストールを選択した場合、有害 USB 攻撃ブロックは使用できません。インストールするには、製品コンポーネントの設定を変更する必要があります。

*有害 USB 攻撃ブロックをインストールするには：*

1. ［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Endpoint Security 10 for Windows**］ - ［**変更、修復、削除**］の順に選択します。

   セットアップウィザードが起動します。

2. セットアップウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウで、［**変更**］をクリックします。

   セットアップウィザードの［**カスタムインストール**］ウィンドウが開きます。

3. ［**有害 USB 攻撃ブロック**］の横にあるアイコンのコンテキストメニューから、［**ローカルハードディスクにインストール**］を選択します。

4. ［**次へ**］をクリックします。

5. セットアップウィザードの指示に従います。

## 有害 USB 攻撃ブロックの有効化と無効化

*有害 USB 攻撃ブロックを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**有害 USB 攻撃ブロック**］サブセクションを選択します。

   有害 USB 攻撃ブロックの設定がウィンドウの右側に表示されます。
3. 次のいずれかの手順を実行します：
   - 有害 USB 攻撃ブロックを有効にするには、［**有害 USB 攻撃ブロックを有効にする**］をオンにします。
   - 有害 USB 攻撃ブロックを無効にするには、［**有害 USB 攻撃ブロックを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## セキュリティキーボードを使用した承認の許可とブロック

セキュリティキーボードは、ランダムな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）の承認時にのみ使用してください。未知の USB デバイスの承認時に、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承認を許可またはブロックするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションで、［**有害 USB 攻撃ブロック**］サブセクションを選択します。

   コンポーネントの設定が、ウィンドウの右側に表示されます。
3. 次のいずれかの手順を実行します：
   - 承認時にセキュリティキーボードの使用をブロックする場合は、［**承認時にセキュリティキーボードの使用をブロックする**］をオンにします。
   - 承認時にセキュリティキーボードの使用を許可する場合は、［**承認時にセキュリティキーボードの使用をブロックする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## キーボード承認

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、承認済みとみなされます。

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 デバイスの承認が要求されるのは、USB キーボードの承認要求が有効なときだけです。承認されていないキーボードは、承認されるまでユーザーは使用できません。

USB キーボード承認要求を無効にすると、ユーザーはすべての接続されたキーボードを使用できます。USB キーボード承認要求を有効にするとすぐに、接続されていて承認されていない各キーボードに対して、承認が要求されます。

*キーボードを承認するには：*

1. USB キーボード承認を有効にして、キーボードを USB ポートに接続します。

   ［**キーボード承認 - <キーボード名>**］ウィンドウが開き、接続されたキーボードの詳細およびその承認用の数値コードが表示されます。

2. ランダムに生成された数値コードを、接続されたキーボードまたはセキュリティキーボード（使用可能な場合）から承認ウィンドウに入力します。

3. ［OK］をクリックします。

   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、承認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、承認が繰り返されることはありません。

   > 承認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、このキーボードの承認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。数値コードが入力できるのは、3 回までです。数値コードの入力が 3 回連続で失敗したとき、または［**キーボード承認 - <キーボード名>**］ウィンドウが閉じられると、このキーボードからの入力がブロックされます。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、キーボード承認を再度実行するようユーザーに要求します。

# アプリケーション起動コントロール

このセクションでは、アプリケーション起動コントロールに関する情報と、このコンポーネントの設定方法を記載しています。

## アプリケーション起動コントロールの概要

アプリケーション起動コントロールは、アプリケーションを起動しようとするユーザーの試みを監視し、*アプリケーション起動コントロールルール*を使用してアプリケーションの起動を調節します。

設定がアプリケーション起動コントロールルールと一致していないアプリケーションの起動は、このコンポーネントで選択されている動作モードによって制御されます。既定では、［*ブラックリスト*］モードが選択されています。このモードでは、すべてのユーザーがすべてのアプリケーションを起動できます。

アプリケーションを起動しようとするユーザーの試みは、レポートにすべて記録されます。

## アプリケーション起動コントロールの有効化と無効化

既定では、アプリケーション起動コントロールが無効になっていますが、必要に応じて、アプリケーション起動コントロールを有効にできます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブ
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでアプリケーション起動コントロールを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションをクリックします。
   ［**エンドポイントコントロール**］セクションが開きます。
4. アプリケーション起動コントロールに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - アプリケーション起動コントロールを有効にするには、メニューの［**開始**］を選択します。
     **アプリケーション起動コントロール**行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - アプリケーション起動コントロールを無効にするには、メニューの［**停止**］を選択します。
     **アプリケーション起動コントロール**行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからアプリケーション起動コントロールを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - アプリケーション起動コントロールを有効にするには、［**アプリケーション起動コントロールを有効にする**］をオンにします。
   - アプリケーション起動コントロールを無効にするには、［**アプリケーション起動コントロールを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## アプリケーション起動コントロール機能の制限

アプリケーション起動コントロールの動作は、以下の場合に制限されます：

- 本製品のバージョンをアップグレードするとき、アプリケーション起動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。

  アプリケーション起動コントロールの機能を復元するには、コンポーネントを再度設定する必要があります。

- 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。アプリケーションの情報がローカル定義データベースにない場合、アプリケーションは許可グループに配置されません。

  KSN サーバーと接続されているときのアプリケーションの分類は、KSN サーバーと接続されていないときの分類と異なる場合があります。

- 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起動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。

- 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：

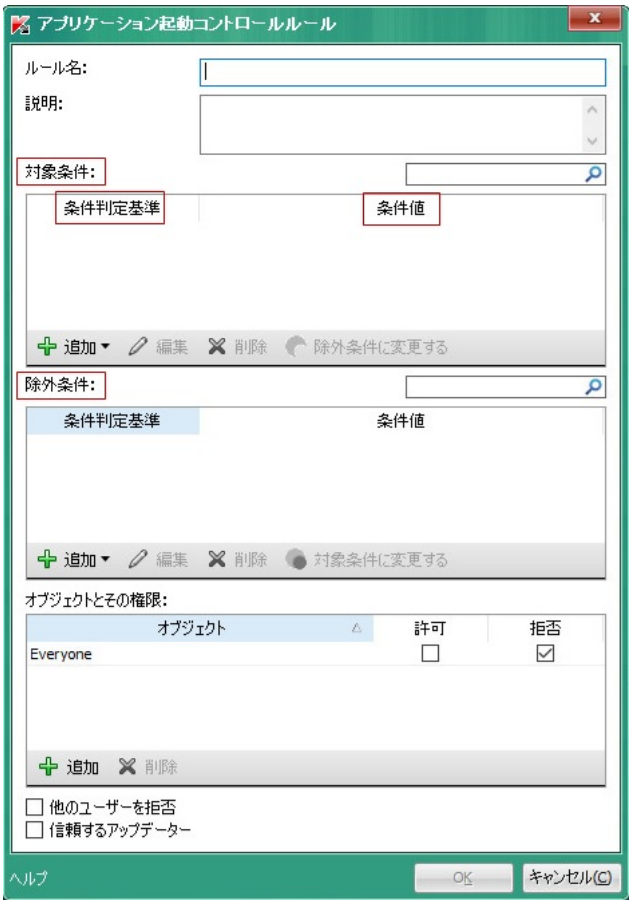
- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

## アプリケーション起動コントロールルールの概要

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。アプリケーション起動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起動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は、条件の種別、基準値、条件値の組み合わせです（下図を参照）。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）。




アプリケーション起動コントロールルール：ルールを適用する条件パラメータ

ルールは対象条件と除外条件を使用します：

- *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、オブジェクト、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、アプリケーション起動コントロールは、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、アプリケーション起動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。

### ルールが適用されたときのアプリケーション起動コントロールの処理

ルールが適用されると、アプリケーション起動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、アプリケーション起動コントロールの許可ルールがユーザーグループに設定されていて、アプリケーション起動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 人のユーザーに設定されている場合、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

アプリケーション起動コントロールルールの動作ステータスは、次の 2 つのいずれかです：

- **有効**
  このルール動作ステータスは、ルールが有効であることを示します。
- **無効**
  このルールステータスは、ルールが無効であることを示します。

### 既定のアプリケーション起動コントロールルール

既定では、アプリケーション起動コントロールはブラックリストモードで動作します。この場合、すべてのユーザーがすべてのアプリケーションを起動できます。アプリケーション起動コントロールルールでブロックされているアプリケーションをユーザーが起動しようとすると、Kaspersky Endpoint Security はそのアプリケーションの起動をブロックするか（［**ブロック**］処理が選択されている場合）、アプリケーションの起動に関する情報をレポートに保存します（［**通知**］処理が選択されている場合）。

## アプリケーション起動コントロールルールの管理

アプリケーション起動コントロールルールに対して、次の操作を実行できます：

- 新しいルールを追加する
- ルールを適用する条件を作成または変更する
- ルールステータスを編集する

  アプリケーション起動コントロールルールは、有効（ルールの横のチェックボックスがオン）または無効（ルールの横のチェックボックスがオフ）にできます。アプリケーション起動コントロールルールは、作成すると既定で有効になります。
- ルールを削除する

## アプリケーション起動コントロールルールの追加と編集

*アプリケーション起動コントロールルールを追加または編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。
3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。
4. 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。

   ［**アプリケーション起動コントロールルール**］ウィンドウが開きます。
5. ルールの設定を指定または編集します：
   a. ［**ルール名**］にルール名を入力するか編集します。

   b. ［**対象条件**］テーブルの［**追加**］、［**編集**］、［**削除**］、［**除外条件に変更する**］をクリックして、ルールを適用する対象条件のリストを作成または編集します。

   c. ［**除外条件**］テーブルの［**追加**］、［**編集**］、［**削除**］、［**対象条件に変更する**］をクリックして、ルールを適用する除外条件のリストを作成または編集します。

   d. 必要に応じて、ルールの適用条件の種類を変更します：
      - 条件の種類を対象条件から除外条件に変更するには、［**対象条件**］テーブルで条件を選択して［**除外条件に変更する**］をクリックします。
      - 条件の種類を除外条件から対象条件に変更するには、［**除外条件**］テーブルで条件を選択して［**対象条件に変更する**］をクリックします。

e. 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。

Microsoft Windows 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。このウィンドウで、ユーザーまたはユーザーグループを選択できます。

既定では、ユーザーのリストに「**Everyone**」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。

f. ［**オブジェクトとその権限**］テーブルで、ユーザーまたはユーザーグループの横にある［**許可**］または［**拒否**］をオンにして、アプリケーションを起動する権限を設定します。

既定でオンになっているチェックボックスは、アプリケーション起動コントロールの動作モードによって異なります。

g. ［**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。

h. 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、アプリケーション起動コントロールルールが定義されていない他のアプリケーションの起動を許可するには、［**信頼するアップデーター**］をオンにします。

6. ［OK］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## アプリケーション起動コントロールルールの適用条件の追加

*アプリケーション起動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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。

ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。

3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。

4. 次のいずれかの手順を実行します：

- ルールを新規作成して適用条件を追加するには、［**追加**］をクリックします。
- 既存のルールに適用条件を追加するには、ルールのリストからルールを選択して、［**編集**］をクリックします。

［**アプリケーション起動コントロールルール**］ウィンドウが表示されます。

5. ［**対象条件**］または［**除外条件**］で、［**追加**］をクリックします。

［**追加**］のドロップダウンリストを使用して、さまざまな適用条件をルールに追加できます（以下の手順を参照）。

*指定したフォルダー内のファイルのプロパティに基づくルールの適用条件を追加するには：*

1. ［**追加**］のドロップダウンリストで、［**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**］を選択します。

［**オブジェクトの選択**］ウィンドウが表示されます。

2. ［**オブジェクトの選択**］ウィンドウで、ルールを適用する1つ以上の条件の基準として使用するプロパティを持つアプリケーションの実行ファイルが格納されているフォルダーを選択します。

3. ［**OK**］をクリックします。

［**条件の追加**］ウィンドウが表示されます。

4. ［**条件を表示**］で、ルールを適用する条件を作成する基準を、［**ファイルのハッシュ値**］、［**証明書**］、［**KL カテゴリ**］、［**メタデータ**］、［**フォルダーパス**］から選択します。

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。

5. ［**ルールを表示**］で［**メタデータ**］を選択した場合は、ルールを適用する条件で使用する実行ファイルのプロパティを［**ファイル名**］、［**ファイルバージョン**］、［**アプリケーション名**］、［**バージョン**］、［**製造元**］のいずれかから選択し、その横のチェックボックスをオンにします。

どのプロパティも指定されていない場合、ルールは保存できません。

6. ［**ルールを表示**］で［**証明書**］を選択した場合は、ルールを適用する条件で使用する設定を［**発行元**］、［**オブジェクト**］、［**ハッシュ値**］のいずれかから選択し、その横のチェックボックスをオンにします。

どの設定も指定されていない場合、ルールは保存できません。

ルールを適用する条件として［**発行元**］と［**オブジェクト**］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。

7. ルールを適用する条件に含めるプロパティを持つアプリケーションの実行ファイル名の横にあるチェックボックスをオンにします。

8. ［**次へ**］をクリックします。

ルール適用条件が式の形式でリスト表示されます。

9. ルール適用条件式のリストで、アプリケーション起動コントロールルールに追加するルール適用条件の横にあるチェックボックスをオンにします。

10. ［**終了**］をクリックします。

*コンピューターで起動したことのあるアプリケーションのプロパティに基づくルールを適用する条件を追加するには：*

1. ［**追加**］のドロップダウンリストで、［**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**］を選択します。

2. ［**条件の追加**］ウィンドウの［**条件を表示**］で、ルールを適用する条件を作成する基準を、［**ファイルのハッシュ値**］、［**証明書**］、［**KL カテゴリ**］、［**メタデータ**］、［**フォルダーパス**］から選択します。

3. ［**ルールを表示**］で［**メタデータ**］を選択した場合は、ルールを適用する条件で使用する実行ファイルのプロパティを［**ファイル名**］、［**ファイルバージョン**］、［**アプリケーション名**］、［**バージョン**］、［**製造元**］のいずれかから選択し、その横のチェックボックスをオンにします。

   どのプロパティも指定されていない場合、ルールは保存できません。

4. ［**ルールを表示**］で［**証明書**］を選択した場合は、ルールを適用する条件で使用する設定を［**発行元**］、［**オブジェクト**］、［**ハッシュ値**］のいずれかから選択し、その横のチェックボックスをオンにします。

   どの設定も指定されていない場合、ルールは保存できません。

   > ルールを適用する条件として［**発行元**］と［**オブジェクト**］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。

5. ルールを適用する条件に含めるプロパティを持つアプリケーションの実行ファイル名の横にあるチェックボックスをオンにします。

6. ［**次へ**］をクリックします。

   ルール適用条件が式の形式でリスト表示されます。

7. ルール適用条件式のリストで、アプリケーション起動コントロールルールに追加するルール適用条件の横にあるチェックボックスをオンにします。

8. ［**終了**］をクリックします。

*KL カテゴリに基づいたルールを適用する条件を追加するには：*

1. ［**追加**］のドロップダウンリストで、［**「KL カテゴリ」による条件設定**］を選択します。

   *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、カスペルスキーによって管理されます。たとえば、「Office アプリケーション」の 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。

2. ［**「KL カテゴリ」による条件設定**］ウィンドウで、ルールを適用する条件を作成する際にベースとなる KL カテゴリの名前のチェックボックスをオンにします。

3. ［**OK**］をクリックします。

*ルールを適用するカスタム条件を追加するには：*

1. ［**追加**］のドロップダウンリストで、［**カスタム条件設定**］を選択します。

2. ［**カスタム条件設定**］ウィンドウで、［**選択**］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。

3. ルールを適用する条件を作成する基準を、［**ファイルのハッシュ値**］、［**証明書**］、［**メタデータ**］、［**ファイルまたはフォルダーのパス**］から選択します。

［**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、アプリケーション起動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。

4. 必要に応じて、選択した基準の設定を指定します。

5. ［**OK**］をクリックします。

*アプリケーションの実行ファイルが格納されているドライブに関する情報に基づいてルールを適用する条件を追加するには：*

1. ［**追加**］のドロップダウンリストで、［**ドライブによる条件設定**］を選択します。

2. ［**ドライブによる条件設定**］ウィンドウの［**ドライブ**］で、アプリケーションの起動がルールを適用する条件となるドライブの種別を選択します。

3. ［**OK**］をクリックします。

## アプリケーション起動コントロールルールのステータスの変更

*アプリケーション起動コントロールルールのステータスを変更するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。

3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。

4. ステータスを編集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、ルールの横にあるチェックボックスをオンにします。
   - ルールの使用を無効にする場合は、ルールの横にあるチェックボックスをオフにします。

6. 変更を保存するには［**保存**］をクリックします。

## アプリケーション起動コントロールルールのテスト

アプリケーション起動コントロールルールが業務で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、新しく作成したルールはテストモードにして動作を検証してください。

アプリケーション起動コントロールルールの動作をテストモードで検証するには、Kaspersky Security Center に報告されるアプリケーション起動コントロールイベントを確認します。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の起動が許可されれば、ルールは正しく作成されています。そうでなければ、作成したルールの設定を変更してください。

アプリケーション起動コントロールのテストモードは、既定では無効です。

*アプリケーション起動コントロールルールをテストするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。
3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。
4. ［**アプリケーション起動コントロールモード**］から、次のいずれかを選択します：
   - **ブラックリスト**：ブロックルールで指定した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。
   - **ホワイトリスト**：許可ルールで指定した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ブロックします。
5. ［**処理**］で［**通知**］を選択します。
6. 変更を保存するには［**保存**］をクリックします。

Kaspersky Endpoint Security は、アプリケーション起動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、その起動についての通知を管理サーバーに送信します。

## アプリケーション起動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起動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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。
3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。
4. ［**テンプレート**］をクリックします。
   ［**メッセージのテンプレート**］ウィンドウが開きます。
5. 次のいずれかの手順を実行します：
   - アプリケーションの起動がブロックされている場合に表示されるメッセージのテンプレートを変更するには、［**ブロック**］タブを選択します。

- LAN 管理者に送信されるメッセージのテンプレートを変更するには、［**管理者に送信するメッセージ**］タブを選択します。

6. アプリケーションの起動がブロックされている場合に表示されるメッセージまたは管理者に送信するメッセージのテンプレートを修正します。それには、［**既定**］および［**変数**］を使用します。

7. ［OK］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## アプリケーション起動コントロールの動作モードの概要

アプリケーション起動コントロールは 2 つのモードで機能します。

- **ブラックリスト**：このモードでは、アプリケーション起動コントロールのブロックルールで指定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が、すべてのユーザーに対して許可されます。

  既定では、このアプリケーション起動コントロールのモードが有効になっています。

- **ホワイトリスト**：このモードでは、アプリケーション起動コントロールの許可ルールで指定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が、すべてのユーザーに対してブロックされます。

  アプリケーション起動コントロールの許可ルールを完全に設定すると、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。

それぞれのモードについて、アプリケーションの起動時の処理が 2 つあります。アプリケーション起動コントロールルールに合致するアプリケーションに対して、アプリケーションの起動をブロックするか、アプリケーションの起動をユーザーに通知できます。

アプリケーション起動コントロールは、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。

しかし、Kaspersky Security Center は、Kaspersky Endpoint Security のローカルインターフェイスで使用できないツールを提供します。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起動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。

- LAN 上のコンピューターにインストールされたアプリケーションについての情報の収集

そのため、アプリケーション起動コントロールの動作設定には Kaspersky Security Center を使用してください。

## アプリケーション起動コントロールモードの選択

*アプリケーション起動コントロールモードを選択するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション起動コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。

3. ［**アプリケーション起動コントロール**］を選択すると、コンポーネントの設定が編集可能になります。

4. ［**アプリケーション起動コントロールモード**］から、次のいずれかを選択します：

   - **ブラックリスト**：ブロックルールで指定した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。
   - **ホワイトリスト**：許可ルールで指定した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ブロックします。

     このモードを選択すると、［**ゴールデンイメージ**］と［**信頼するアップデーター**］の 2 つのアプリケーション起動コントロールルールが既定で作成されます。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。これらのルールは、ルールの横にあるチェックボックスをオンまたはオフにすることで、有効または無効にできます。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。ルールの使用を再開するには、［**アプリケーション起動コントロールモード**］で必要なモードを選択します。

5. ［**処理**］で、アプリケーション起動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。

6. 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 とモジュールを管理**］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。

   このチェックボックスをオンにすると、Kaspersky Endpoint Security を起動する前に DLL モジュールとドライバを監視します。これ以降の、製品起動前のすべての DLL モジュールとドライバの監視を設定するには、［**DLL とモジュールを管理**］をオンにしてコンピューターを再起動します。コンピューターの再起動ができない場合、［**DLL とモジュールを管理**］をオンにすると Kaspersky Endpoint Security の実行中に DLL モジュールとドライバを読み込めます。この場合、監視対象となるのは、Kaspersky Endpoint Security の実行中に読み込まれた DLL モジュールとドライバのみです。

   DLL モジュールとドライバの監視を行う際、KL カテゴリをベースに作成したアプリケーション起動コントロールルールは使用しないでください。DLL モジュールとドライバに対する KL カテゴリの決定（「オペレーティングシステムとそのコンポーネント」ルール内を含む）が正常に機能しない場合があります。具体的には、「オペレーティングシステムとそのコンポーネント」ルールが既定で作成され、DLL モジュールとドライバの起動時に配信されない場合です。この機能を有効にする場合、DLL モジュールとドライバの許可ルールは別途作成するようにしてください。このような許可ルールがない状態で［**DLL とモジュールを管理**］を使用すると、システムが不安定になる可能性があります。

   プログラム設定の編集に対して、パスワードによる保護を有効にしてください。Kaspersky Security Center ポリシーの設定を変更しなくても、特に重要な DLL モジュールとドライバーの起動をブロックする許可ルールを無効にすることができます。

7. 変更を保存するには［**保存**］をクリックします。

# Kaspersky Security Center を使用したアプリケーション起動コントロールルールの管理

このセクションでは、Kaspersky Security Center を使用してアプリケーション起動コントロールルールを設定する方法と、アプリケーション起動コントロールの最適な使用についての推奨事項について説明します。

## ユーザー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収集

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、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信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**］フォルダーと［**実行ファイル**］フォルダーにあります。［**アプリケーションレジストリ**］フォルダーと［**実行ファイル**］フォルダーは、Kaspersky Security Center コンソールツリーの［**アプリケーションの管理**］フォルダーにあります。

フォルダー［**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**］フォルダーには、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**］フォルダーまたは［**実行ファイル**］フォルダー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。

## アプリケーションカテゴリの作成

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すると、アプリケーション起動コントロールルールの作成時に使用できます。

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**］フォルダーを選択します。

3. 作業領域で［**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開きます。

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。

## Kaspersky Security Center を使用したアプリケーション起動コントロールルールの作成

*Kaspersky Security Center を使用してアプリケーション起動コントロール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、該当するクライアントコンピューターを含む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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**エンドポイントコントロール**］セクションの［**アプリケーション起動コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。

7. ［**追加**］をクリックします。

   ［**アプリケーション起動コントロールルール**］ウィンドウが開きます。

8. ［**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。

9. 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。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。

   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。このウィンドウで、ユーザーまたはユーザーグループを選択できます。

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、ユーザーの横にある［**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、ユーザーの横にある［**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. ルールで指定されたカテゴリに属す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、アプリケーション起動コントロールルールが定義されていない他のアプリケーションを起動する権限を付与するには、［**信頼するアップデーター**］をオンにします。

13. ［**OK**］をクリックします。

14. ポリシープロパティウィンドウの［**アプリケーション起動コントロール**］セクションで、［**適用**］をクリックします。

## Kaspersky Security Center を使用したアプリケーション起動コントロールルールのステータスの変更

*アプリケーション起動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、該当するクライアントコンピューターを含む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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**エンドポイントコントロール**］セクションの［**アプリケーション起動コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション起動コントロールの設定が表示されます。

7. ステータスを変更するアプリケーション起動コントロールルールを選択します。

8. ［**ステータス**］列で、次のいずれかの手順を実行します：

   - ルールの使用を有効にする場合は、ルールの横にあるチェックボックスをオンにします。
   - ルールの使用を無効にする場合は、ルールの横にあるチェックボックスをオフにします。

9. ［**適用**］をクリックします。

# アプリケーション権限コントロール

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、アプリケーション権限コントロールに関する情報と、このコンポーネントの設定方法を記載しています。

## アプリケーション権限コントロールの概要

アプリケーション権限コントロールは、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 ID データへのアクセスを管理します。

このコンポーネントは、アプリケーションコントロールルールを使用して、保護対象のリソース（ファイルおよびフォルダー、レジストリキーなど）へのアクセスを含む、アプリケーションの処理を管理します。アプリケーションコントロールルールは、アプリケーションのオペレーティングシステムでのさまざまな処理、およびコンピューターリソースへのアクセス権限に適用される一連の制限です。

アプリケーションのネットワーク動作は、ファイアウォールによって監視されます。

アプリケーションが初めて起動すると、アプリケーション権限コントロールがアプリケーションをスキャンし、許可グループの 1 つに割り当てます。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アプリケーションコントロールルールを定義します。

アプリケーション権限コントロールの機能をより効果的にするには、Kaspersky Security Network に参加してください。Kaspersky Security Network から取得したデータを使用して、アプリケーションをより正確にグループに分類し、最適なアプリケーションコントロールルールを適用することができます。

次回アプリケーションが起動したときに、アプリケーション権限コントロールはアプリケーションの整合性を検証します。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コントロール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、アプリケーション権限コントロールは、最初に起動されたときと同様に、そのアプリケーションを再度スキャンします。

## 音声および映像デバイスコントロールの制限

### 音声ストリームの保護について

音声ストリームの保護には、次の考慮事項があります：

- この機能が動作するには、アプリケーション権限コントロールが有効になっている必要があります。
- アプリケーション権限コントロール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。

- アプリケーションの音声録音デバイスへのアクセス設定を変更したのち（たとえば、アプリケーションコントロール設定ウィンドウで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 のインストールおよびアップグレード時の音声および映像デバイスの保護に関する考慮事項

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。

## Web カメラへのアプリケーションのアクセスについて

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。

## サポートされる Web カメラ

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。

## アプリケーション権限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権限コントロール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ます。必要に応じて、アプリケーション権限コントロールを停止することができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブでアプリケーション権限コントロールを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションをクリックします。
   ［**エンドポイントコントロール**］セクションが開きます。
4. アプリケーション権限コントロールに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - アプリケーション権限コントロールを有効にするには、［**開始**］を選択します。
     ［アプリケーション権限コントロール］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - アプリケーション権限コントロールを無効にするには、［**停止**］を選択します。
     ［アプリケーション権限コントロール］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウからアプリケーション権限コントロールを有効または無効にするには：*

1. ［アプリケーション設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ウィンドウの右側で、次のいずれかの手順を実行します：

- アプリケーション権限コントロールを有効にするには、［**アプリケーション権限コントロールを有効にする**］をオンにします。
- アプリケーション権限コントロールを無効にするには、［**アプリケーション権限コントロールを有効にする**］をオフにします。

4. 変更を保存するには［**保存**］をクリックします。

## アプリケーション許可グループの管理

アプリケーションが初めて起動するたびに、アプリケーション権限コントロール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。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、［**許可グループの選択**］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。

このコンポーネントは、Kaspersky Endpoint Security より前に起動したアプリケーションのネットワーク動作のみを、ファイアウォール設定で設定されたネットワークルールに従って管理します。

## アプリケーションを許可グループに割り当てるための設定

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 からの返答に基づいて、アプリケーションがアプリケーション権限コントロールの設定で指定されているものとは別の許可グループに移動することがあります。

*アプリケーションを許可グループに割り当てるための設定を構成するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. 信頼済みの製造元によって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自動的に割り当てる場合は、［**デジタル署名があるアプリケーションを信頼する**］をオンにします。

   *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。
4. 不明なアプリケーションを許可グループに割り当てる方法を選択します。

- 不明なアプリケーションを許可グループに割り当てるためにヒューリスティック分析を使用する場合は、［**ヒューリスティック分析を使用して信頼度を決定する**］を選択し、起動したアプリケーションのスキャンに割り当てる時間を［**グループを決定するまでの最大時間**］で指定します。

- すべての不明なアプリケーションを指定した許可グループに割り当てる場合は、［**次のグループに自動的に移動する**］を選択して、ドロップダウンリストから該当する許可グループを選択します。

  セキュリティ上の理由で、［**次のグループに自動的に移動する**］の値には［**許可**］が含まれません。

5. 変更を保存するには［**保存**］をクリックします。

## 許可グループの変更

アプリケーションが初めて起動したときに、Kaspersky Endpoint Security は自動的にアプリケーションを1つの許可グループに含めます。必要に応じて、アプリケーションを手動で別の許可グループへ移動できます。

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、個別のアプリケーションのルールを編集することができます。

*アプリケーションが初めて起動したときに Kaspersky Endpoint Security によって自動的に割り当てられた許可グループを変更するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。

3. ［**アプリケーション**］をクリックします。

   ［**アプリケーション**］ウィンドウに［**アプリケーションコントロールルール**］タブが表示されます。

4. ［**アプリケーションコントロールルール**］タブで、目的のアプリケーションを選択します。

5. 次のいずれかの手順を実行します：

   - 右クリックして、アプリケーションのコンテキストメニューを表示します。アプリケーションのコンテキストメニューから、［**グループへ移動**］ - ［**<グループ名>**］の順に選択します。

   - ［**許可**］/［**弱い制限付き**］/［**強い制限付き**］/［**ブロック**］をクリックしてコンテキストメニューを開きます。コンソールツリーで、目的の許可グループを選択します。

6. ［OK］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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

このコンポーネントは、Kaspersky Endpoint Security より前に起動したアプリケーションのネットワーク動作のみを管理します。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したがって実行されます。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。

*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には：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**編集**］をクリックします。
   ［**許可グループの選択**］ウィンドウが開きます。
4. 必要な許可グループを選択します。
5. ［**OK**］をクリックします。
6. 変更を保存するには［**保存**］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、アプリケーションコントロール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アプリケーションコントロールルールを編集できます。

許可グループ内の個々の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定義されるアプリケーションコントロールルールは、許可グループに対して定義されるアプリケーションコントロールルールよりも優先されます。つまり、信頼グループ内の個別のアプリケーションまたはアプリケーションのグループのアプリケーションコントロールルールの設定が、信頼グループのアプリケーションコントロールルールの設定と異なる場合、アプリケーション権限コントロールは、信頼グループ内のアプリケーションまたはアプリケーショングループのアプリケーションコントロールルールに従って、アプリケーションあるいはアプリケーショングループの動作をコントロールします。

## 許可グループおよびアプリケーショングループに対するアプリケーションコントロールルールの変更

既定では、信頼するグループごとに最適なアプリケーションコントロールルールが作成されます。アプリケーショングループコントロールルール設定の値は、信頼するグループコントロールルールの設定値から継承されます。事前設定されている信頼するグループのコントロールルール、およびアプリケーショングループコントロールルールを編集できます。

*信頼するグループのコントロールルール、またはアプリケーショングループコントロールルールを編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**アプリケーション**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**アプリケーションコントロールルール**］タブが表示されます。
4. 必要な許可グループまたはアプリケーショングループを選択します。
5. 許可グループまたはアプリケーショングループのコンテキストメニューから、［**グループのルール**］を選択します。
   ［**アプリケーショングループコントロールルール**］ウィンドウが開きます。
6. ［**アプリケーショングループコントロールルール**］ウィンドウで、次のいずれかの手順を実行します：
   - 許可グループやアプリケーショングループにおけるオペレーティングシステムのレジストリ、ユーザーファイル、および製品設定へのアクセス権限を管理する、許可グループコントロールルールおよびアプリケーショングループコントロールルールを編集するには、［**個人情報とオペレーティングシステム**］タブを選択します。
   - 許可グループやアプリケーショングループにおけるオペレーティングシステムのプロセスとオブジェクトへのアクセス権限を管理する、許可グループコントロールルールおよびアプリケーショングループコントロールルールを編集するには、［**権限**］タブを選択します。
7. 必要なリソースについて、対応する処理の列を右クリックして、コンテキストメニューを開きます。
8. このコンテキストメニューから必要な項目を選択します。
   - **継承**
   - **許可**
   - **ブロック**
   - **イベントの記録**

   信頼するグループのコントロールルールを編集している場合、［**継承**］項目は使用できません。
9. ［**OK**］をクリックします。
10. ［**アプリケーション**］ウィンドウで［**OK**］をクリックします。
11. 変更を保存するには［**保存**］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編集

既定では、アプリケーショングループまたは信頼するグループに属するアプリケーションのアプリケーションコントロールルールの設定値は、信頼するグループのコントロールルールの設定値を継承します。アプリケーションコントロールルールの設定を編集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変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**アプリケーション**］をクリックします。

   ［**アプリケーション権限コントロール**］ウィンドウで［**アプリケーションコントロールルール**］タブが表示されます。
4. 必要なアプリケーションを選択します。
5. 次のいずれかの手順を実行します：

   - 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**］タブの右下隅にある［**詳細**］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。
6. ［**アプリケーションコントロールルール**］ウィンドウで、次のいずれかの手順を実行します：

   - アプリケーションにおけるオペレーティングシステムのレジストリ、ユーザーファイル、および製品設定へのアクセス権限を管理するアプリケーションコントロールルールを編集するには、［**個人情報とオペレーティングシステム**］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とオブジェクトへのアプリケーションのアクセス権限を管理するアプリケーションコントロールルールを編集するには、［**権限**］タブを選択します。
7. 必要なリソースについて、対応する処理の列を右クリックして、コンテキストメニューを開きます。
8. このコンテキストメニューから必要な項目を選択します。

   - **継承**
   - **許可**
   - **ブロック**
   - **イベントの記録**
9. ［**OK**］をクリックします。
10. ［**アプリケーション**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

## Kaspersky Security Network データベースからのアプリケーションコントロールルールのダウンロードとアップデートの無効化

既定では、アプリケーションの新しい情報が Kaspersky Security Network データベースに見つかると、Kaspersky Endpoint Security は KSN データベースからダウンロードしたコントロールルールをアプリケーションに適用します。アプリケーションのコントロールルールは手動で編集できます。

始めて起動したときにアプリケーションが Kaspersky Security Network データベースになく、その情報がデータベースに後で追加される場合は、既定では Kaspersky Endpoint Security はアプリケーションのコントロールルールを自動でアップデートします。

Kaspersky Security Network データベースからのアプリケーションコントロールルールのダウンロード、および以前未知であったアプリケーションのコントロールルールの自動アップデートを無効にすることができます。

*Kaspersky Security Network データベースからのアプリケーションコントロールルールのダウンロードおよびアップデートを無効にするには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。

   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**未知のアプリケーションのコントロールルールを KSN データベースからアップデートする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## 親プロセスからの制限の継承の無効化

アプリケーションは、ユーザーまたは実行中の他のアプリケーションによって開始されます。アプリケーションが他のアプリケーションによって開始される場合、親プロセスと子プロセスからなる起動シーケンスが作成されます。

アプリケーションが保護対象のリソースにアクセスしようとすると、アプリケーション権限コントロールによって、このアプリケーションの親プロセスがすべて分析され、保護対象のリソースにアクセスできる権限があるか決定されます。最も低い優先度ルールが順守されます。つまり、アプリケーションのアクセス権限と親プロセスのアクセス権限が照合される際に、優先度が最も低いアクセス権限がそのアプリケーションのアクティビティに適用されます。

アクセス権限の優先度は次のとおりです：

1. **許可**：このアクセス権限には最も高い優先度が設定されています。
2. **ブロック**：このアクセス権限には最も低い優先度が設定されています。

この機構によって、信頼されないアプリケーションや権限が制限されているアプリケーションが、信頼するアプリケーションを使用して、特定の権限が必要な処理を実行することを回避することができます。

親プロセスに付与されている権限が足りないことが原因で、アプリケーションのアクティビティがブロックされる場合は、これらの権限を編集するか親プロセスからの制限の継承を無効にします。

*親プロセスからの制限の継承を無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**アプリケーション**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**アプリケーションコントロールルール**］タブが表示されます。
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［**アプリケーションルール**］を選択します。
   ［**アプリケーションコントロールルール**］ウィンドウが開きます。
6. ［**アプリケーションコントロールルール**］ウィンドウで［**除外リスト**］タブを選択します。
7. ［**親プロセス（親アプリケーション）の制限を継承しない**］をオンにします。
8. ［**OK**］をクリックします。
9. ［**アプリケーション**］ウィンドウで［**OK**］をクリックします。
10. 変更を保存するには［**保存**］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からの特定のアプリケーション処理の除外

*アプリケーションコントロールルールから特定のアプリケーションの処理を除外するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**アプリケーション**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**アプリケーションコントロールルール**］タブが表示されます。
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［**アプリケーションルール**］を選択します。
   ［**アプリケーションコントロールルール**］ウィンドウが開きます。

6. ［**除外リスト**］タブを選択します。
7. 監視する必要がないアプリケーションの処理の隣にあるチェックボックスをオンにします。
8. ［**OK**］をクリックします。
9. ［**アプリケーション**］ウィンドウで［**OK**］をクリックします。
10. 変更を保存するには［**保存**］をクリックします。

## 古くなったアプリケーションコントロールルールの削除

既定では、60 日間起動されなかったアプリケーションのコントロールルールは自動的に削除されます。未使用アプリケーションのコントロールルールの保管期間を変更するか、ルールの自動削除を無効にすることができます。

*古くなったアプリケーションコントロールルールを削除するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - Kaspersky Endpoint Security で未使用アプリケーションのコントロールルールを削除する場合は、［**次の期間以上使用されていないアプリケーションのルールを削除する**］をオンにして、目的の日数を指定します。
   - 未使用アプリケーションのコントロールルールの自動削除を無効にするには、［**次の期間以上使用されていないアプリケーションのルールを削除する**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## オペレーティングシステムのリソースと ID データの保護

アプリケーション権限コントロールでは、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 ID データを処理するアプリケーション権限を管理します。

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。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。

次の操作を実行できます：

- 保護対象のリソースのカテゴリを追加する
- 保護対象のリソースを追加する

- リソースのプロテクションを無効にする

## 保護対象のリソースのカテゴリの追加

*保護対象のリソースのカテゴリを追加するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**リソース**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**保護対象のリソース**］タブが表示されます。
4. ［**保護対象のリソース**］タブの左側で、新しい保護対象のリソースの追加先となる保護対象のリソースのセクションまたはカテゴリを選択します。
5. ［**追加**］をクリックし、ドロップダウンリストから［**カテゴリ**］を選択します。
   ［**保護対象のリソースのカテゴリ**］ウィンドウが開きます。
6. ［**保護対象のリソースのカテゴリ**］ウィンドウが開き、そのウィンドウで、保護対象のリソースの新しいカテゴリ名を入力します。
7. ［**OK**］をクリックします。
   保護対象のリソースのカテゴリのリストに新しい項目が表示されます。
8. ［**アプリケーション権限コントロール**］ウィンドウで［**OK**］をクリックします。
9. 変更を保存するには［**保存**］をクリックします。

保護対象のリソースのカテゴリを追加したら、［**保護対象のリソース**］タブの左上にある［**編集**］または［**削除**］をクリックして、そのカテゴリを編集または削除することができます。

## 保護対象のリソースの追加

*保護対象のリソースを追加するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。
3. ［**リソース**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**保護対象のリソース**］タブが表示されます。

4. ［**保護対象のリソース**］タブの左側で、新しい保護対象のリソースの追加先となる保護対象のリソースのカテゴリを選択します。

5. ［**追加**］をクリックし、ドロップダウンリストから追加する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**
   - **レジストリキー**

   ［**保護対象のリソース**］ウィンドウが開きます。

6. ［**保護対象のリソース**］ウィンドウの［**名前**］に、保護対象のリソースの名前を入力します。

7. ［**参照**］をクリックします。

8. 開いたウィンドウで、追加する保護対象のリソースの種別に応じて、必要な設定を指定します。［**OK**］をクリックします。

9. ［**保護対象のリソース**］ウィンドウで［**OK**］をクリックします。
   ［**保護対象のリソース**］タブで選択したカテゴリの保護対象のリソースのリストに、新しい項目が表示されます。

10. ［**アプリケーション権限コントロール**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

保護対象のリソースを追加したら、［**保護対象のリソース**］タブの左上にある［**編集**］または［**削除**］をクリックして、そのリソースを編集または削除することができます。

## リソースプロテクションの無効化

*リソースプロテクションを無効にするには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**アプリケーション権限コントロール**］サブセクションを選択します。
   ウィンドウの右側に、アプリケーション権限コントロールの設定が表示されます。

3. ウィンドウの右側で、［**リソース**］をクリックします。
   ［**アプリケーション権限コントロール**］ウィンドウで［**保護対象のリソース**］タブが表示されます。

4. 次のいずれかの手順を実行します：

   - タブの左側にある保護対象のリソースのリストで、プロテクションを無効にするリソースを選択し、その名前の横のチェックボックスをオフにします。
   - ［**除外リスト**］をクリックして、次の手順に従います：

     a. ［**除外リスト**］ウィンドウで、［**追加**］をクリックします。ドロップダウンリストで、アプリケーション権限コントロールのプロテクションから除外するリソースのリストに追加するリソースの種別を

［**ファイルまたはフォルダー**］または［**レジストリキー**］から選択します。

［**保護対象のリソース**］ウィンドウが開きます。

b. ［**保護対象のリソース**］ウィンドウの［**名前**］に、保護対象のリソースの名前を入力します。

c. ［**参照**］をクリックします。

d. 開いたウィンドウで、アプリケーション権限コントロールのプロテクションから除外するリソースのリストに追加する保護対象のリソースの種別に応じて、必要な設定を指定します。

e. ［**OK**］をクリックします。

f. ［**保護対象のリソース**］ウィンドウで［**OK**］をクリックします。

アプリケーション権限コントロールのプロテクションから除外するリソースのリストに、新しい要素が表示されます。

> アプリケーション権限コントロールのプロテクションから除外するリソースのリストにリソースを追加したら、［**除外リスト**］ウィンドウの上部にある［**編集**］または［**削除**］をクリックして、そのリソースを編集または削除することができます。

g. ［**除外リスト**］ウィンドウで［**OK**］をクリックします。

5. ［**アプリケーション権限コントロール**］ウィンドウで［**OK**］をクリックします。

6. 変更を保存するには［**保存**］をクリックします。

# 脆弱性モニター

このコンポーネントは、ワークステーション用の Microsoft 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 Microsoft 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。

このセクションでは、脆弱性モニターに関する情報と、脆弱性モニターを有効または無効にする方法について説明します。

## 脆弱性モニターの概要

脆弱性モニターは、ユーザーのコンピューター上で実行されているアプリケーションおよびユーザーが起動したアプリケーションの脆弱性スキャンをリアルタイムで実行します。脆弱性モニターが有効のときは、脆弱性スキャンタスクを開始する必要はありません。このスキャンは、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に対して脆弱性スキャンタスクがまったく実行されていない場合や、長期間実行されていない場合に有用です。

## 脆弱性モニターの有効化と無効化

脆弱性モニターは、既定では無効になっていますが、必要に応じて、有効にすることができます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［プロテクションとコントロール］タブを使用して、脆弱性モニターを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションをクリックします。
   ［**エンドポイントコントロール**］セクションが開きます。
4. 右クリックして、脆弱性モニターについての情報が含まれる行のコンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - 脆弱性モニターを有効にするには、［**開始**］を選択します。
     ［**脆弱性モニター**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。
   - 脆弱性モニターを無効にするには、［**停止**］を選択します。

［**脆弱性モニター**］行の左側に表示されているコンポーネントステータスアイコン が に変わります。

*［設定］ウィンドウから、脆弱性モニターを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**脆弱性モニター**］を選択します。
   ウィンドウの右側に、脆弱性モニターの設定が表示されます。
3. ウィンドウの右側で、次のいずれかの手順を実行します：
   - ユーザーのコンピューター上で実行されるアプリケーションまたはユーザーが起動するアプリケーションの脆弱性スキャンを Kaspersky Endpoint Security に開始させる場合は、［**脆弱性モニターを有効にする**］をオンにします。
   - ユーザーのコンピューター上で実行されるアプリケーションまたはユーザーが起動するアプリケーションの脆弱性スキャンを Kaspersky Endpoint Security に開始させたくない場合は、［**脆弱性モニターを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

# 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 Microsoft 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 Microsoft 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。

このセクションでは、デバイスコントロールに関する情報と、このコンポーネントの設定方法について説明します。

## デバイスコントロールの概要

デバイスコントロールは、コンピューターに内蔵または接続される次のデバイスへのユーザーアクセスを制限して個人情報のセキュリティを確保します：

- ストレージ機器（ハードディスク、リムーバブルドライブ、テープドライブ、CD/DVD ドライブ）
- データ転送デバイス（モデム、外部ネットワークカード）
- データをハードコピーに変換するために設計されたデバイス（プリンター）
- 接続バス（「バス」とも呼ばれる）。デバイスをコンピューターに接続するためのインターフェイス（USB、FireWire、赤外線など）を指します。

デバイスコントロールは、デバイスアクセスルール（「アクセスルール」とも呼ばれます）と*接続バスアクセスルール*（「バスアクセスルール」とも呼ばれます）を適用することにより、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は、必要に応じて停止できます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［**プロテクションとコントロール**］タブでデバイスコントロールを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションをクリックします。
   ［**エンドポイントコントロール**］セクションが開きます。

4. デバイスコントロールに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。

   コンポーネントの処理を選択するメニューが表示されます。

5. 次のいずれかの手順を実行します：

   - デバイスコントロールを有効にするには、メニューの［**開始**］を選択します。
   - デバイスコントロールを無効にするには、メニューの［**停止**］を選択します。

*［設定］ウィンドウからデバイスコントロールを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。

3. 次のいずれかの手順を実行します：

   - デバイスコントロールを有効にするには、［**デバイスコントロールを有効にする**］をオンにします。
   - デバイスコントロールを無効にするには、［**デバイスコントロールを有効にする**］をオフにします。

4. 変更を保存するには［**保存**］をクリックします。

## デバイスと接続バスのアクセスルールの概要

デバイスアクセスルールとは、デバイスコントロールの次の機能を定義するパラメータの組み合わせです：

- 選択したユーザーまたはユーザーグループが特定の時間に特定の種別のデバイスにアクセスすることを許可します。

  ユーザーまたはユーザーグループを選択して、デバイスへのアクセスのスケジュールを作成することができます。

- 記憶装置のコンテンツを読み取る権限を設定します。
- 記憶装置のコンテンツを編集する権限を設定します。

既定では、アクセスルールは、デバイスコントロールの分類によってすべての種別のデバイスに対して作成されます。このようなルールにより、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が常に付与されるようになります。

接続バスアクセスルールにより、接続バスへのアクセスが許可またはブロックされます。

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または接続バスアクセスルールを作成したり削除したりすることはできません。これらのルールは編集のみできます。

# 信頼するデバイスの概要

「*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は、次の処理を行うことができます：

- 信頼するデバイスのリストにデバイスを追加する。
- 信頼するデバイスにアクセスできるユーザーまたはユーザーグループを変更する。
- 信頼するデバイスのリストからデバイスを削除する。

信頼するデバイスのリストにデバイスを追加し、この種別のデバイスのアクセスルールを作成してアクセスをブロックまたは制限すると、Kaspersky Endpoint Security はそのデバイスが信頼するデバイスのリストに登録されているかどうかに基づいて、デバイスにアクセス権を付与するかどうかを決定します。信頼するデバイスのリストに登録されているデバイスは、アクセスルールより優先度が高くなります。

# デバイスへのアクセスに関する標準の決定

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。

デバイスへのアクセスに関する標準の決定

| No. | 初期条件 | デバイスへのアクセスに関する決定が実行されるまでの一時的なステップ | | | デバイスへのアクセスの決定 |
|---|---|---|---|---|---|
| | | 接続されているデバイスが信頼するデバイスのリストにあるかどうかの確認 | アクセスルールに基づいたデバイスへのアクセスのテスト | バスアクセスルールに基づいたバスへのアクセスのテスト | |
| 1 | デバイスがデバイスコントロールのデバイス種別にない | 信頼するデバイスのリストにない | アクセスルールがない | スキャンは実行されない | アクセスが許可される |
| 2 | デバイスが信頼できる | 信頼するデバイスのリストにある | スキャンは実行されない | スキャンは実行されない | アクセスが許可される |
| 3 | デバイスへのアクセスが許可される | 信頼するデバイスのリストにない | アクセスが許可される | スキャンは実行されない | アクセスが許 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 可される |
| 4 | デバイスへのアクセスはバスに依存する | 信頼するデバイスのリストにない | アクセスはバスに依存する | アクセスが許可される | アクセスが許可される |
| 5 | デバイスへのアクセスはバスに依存する | 信頼するデバイスのリストにない | アクセスはバスに依存する | アクセスがブロックされる | アクセスがブロックされる |
| 6 | デバイスへのアクセスが許可されるバスアクセスルールが見つからない | 信頼するデバイスのリストにない | アクセスが許可される | バスアクセスルールがない | アクセスが許可される |
| 7 | デバイスへのアクセスがブロックされる | 信頼するデバイスのリストにない | アクセスがブロックされる | スキャンは実行されない | アクセスがブロックされる |
| 8 | デバイスアクセスルールまたはバスアクセスルールがない | 信頼するデバイスのリストにない | アクセスルールがない | バスアクセスルールがない | アクセスが許可される |
| 9 | デバイスアクセスルールがない | 信頼するデバイスのリストにない | アクセスルールがない | アクセスが許可される | アクセスが許可される |
| 10 | デバイスアクセスルールがない | 信頼するデバイスのリストにない | アクセスルールがない | アクセスがブロックされる | アクセスがブロックされる |

デバイスにアクセスした後でデバイスアクセスルールを編集できます。接続されたデバイスへのアクセスがアクセスルールによって許可され、後からアクセスルールを編集してアクセスをブロックした場合、Kaspersky Endpoint Security は次回のデバイスからのファイル操作要求（フォルダーツリーの表示、読み取り、書き込み）があったときに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。

## デバイスアクセスルールの編集

デバイスの種別ごとに、デバイスにアクセスできるユーザーのリストやアクセスできる時間帯、アクセスの許可または拒否など、さまざまなアクセス設定が可能です。

*デバイスアクセスルールを編集するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。
3. ウィンドウの右側で、［**デバイス種別**］タブを選択します。

   ［**デバイス種別**］タブには、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. 編集するアクセスルールを選択します。
5. ［**編集**］をクリックします。このボタンは、ファイルシステムを持つ種類のデバイスでのみ利用できます。

   ［**デバイスアクセスルールの設定**］ウィンドウが開きます。

   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。このアクセスルールは、［**ユーザーまたはユーザーのグループ**］リストに［Everyone］グループを含みます。このアクセスルールは、［**選択されたユーザーグループのアクセススケジュールごとの権限**］テーブルに、デバイスのあらゆる動作の権限を付与する［**既定のスケジュール**］を含みます。
6. デバイスアクセスルールの設定を編集するには：

   a. ［**ユーザーまたはユーザーのグループ**］リストからユーザーまたはユーザーグループを選択します。

      ［**ユーザーまたはユーザーのグループ**］リストを編集するには、［**追加**］、［**編集**］、［**削除**］を使用します。

   b. ［**選択されたユーザーグループのアクセススケジュールごとの権限**］テーブルで、選択したユーザーまたはユーザーグループのデバイスへのアクセスのスケジュールを設定します。これを行うには、編集するデバイスアクセスルールで使用するデバイスのアクセススケジュール名の横にあるチェックボックスをオンにします。

      デバイスへのアクセスのスケジュールリストを編集するには、［**選択されたユーザーグループのアクセススケジュールごとの権限**］テーブルの［**新規作成**］、［**編集**］、［**コピー**］、［**削除**］を使用します。

   c. 編集するルールで使用するデバイスへのアクセスのスケジュールごとに、デバイス操作時に許可する処理を指定します。そのためには、［**選択されたユーザーグループのアクセススケジュールごとの権限**］テーブルで、目的の操作名の列にあるチェックボックスをオンにします。

d. ［**OK**］をクリックします。

デバイスアクセスルールの既定の設定を編集すると、［**デバイス種別**］タブの［**アクセス**］列で、デバイス種別のアクセス設定の値が［*ルールによって制限する*］に変わります。

7. 変更を保存するには［**保存**］をクリックします。

## イベントログでのレコードの追加と除外

イベントは、リムーバブルドライブ上のファイルに対する操作でのみ記録できます。

*イベントの記録を有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。
   ウィンドウの右側には、デバイスコントロールの設定が表示されます。
3. ウィンドウの右側で、［**デバイス種別**］タブを選択します。
   ［**デバイス種別**］タブには、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. デバイスのテーブルで［**リムーバブルドライブ**］を選択します。
   テーブルの上部にある［**ログ**］が使用可能になります。
5. ［**ログ**］をクリックします。
   ［**ログの設定**］ウィンドウが開きます。
6. 次のいずれかの手順を実行します：
   - リムーバブルドライブでのファイルの削除および書き込み操作を記録するには、［**ログを有効にする**］をオンにします。
     ユーザーがリムーバブルドライブ上のファイルに対して削除または書き込み処理を実行すると、イベントがログファイルに保存され、メッセージが Kaspersky Security Center の管理サーバーに送信されます。
   - そうしない場合、［**ログを有効にする**］をオフにします。
7. 記録する操作を指定します。そのためには、次のいずれかの操作を行います：
   - すべてのイベントを記録するには、［**すべてのファイルの情報を保存する**］をオンにします。
   - 特定の形式のファイルに関する情報のみを記録するには、［**ファイル形式でフィルタリング**］セクションで、目的のファイル形式の横にあるチェックボックスをオンにします。
8. 操作を記録するユーザーを指定します。次の手順に従います：
   a. ［**ユーザー**］セクションで、［**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。

b. ユーザーまたはユーザーグループのリストを指定または編集します。

［**ユーザー**］セクションで指定したユーザーが、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 の管理サーバーにメッセージが送信されます。

9. ［**ログの設定**］ウィンドウで［**OK**］をクリックします。

10. 変更を保存するには［**保存**］をクリックします。

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。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。

3. ウィンドウの右側で、［**デバイス種別**］タブを選択します。

   ［**デバイス種別**］タブには、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**］デバイスに対する［**アクセス**］列で、右クリックしてコンテキストメニューを開きます。

5. ［**例外を除きブロック**］を選択します。

6. デバイスリストで［**Wi-Fi**］を選択し、［**編集**］をクリックします。

   ［**信頼する Wi-Fi ネットワーク**］ウィンドウが開きます。

7. ［**追加**］をクリックします。

   ［**信頼する Wi-Fi ネットワーク**］ウィンドウが開きます。

8. ［**信頼する Wi-Fi ネットワーク**］で、次の操作を実行します：

   - ［**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。
   - ［**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。
   - ［**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。
   - ［**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。

9. ［**信頼する Wi-Fi ネットワーク**］で［OK］をクリックします。
10. ［**信頼する Wi-Fi ネットワーク**］で［OK］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。
   ウィンドウの右側には、デバイスコントロールの設定が表示されます。
3. ［**接続バス**］タブを選択します。
   ［**接続バス**］タブには、デバイスコントロールで分類されたすべての接続バスのアクセスルールが表示されます。
4. 編集するバス接続のルールを選択します。
5. アクセスパラメータの値を変更するには、次の手順を実行します：
   - 接続バスへのアクセスを許可するには、［**アクセス**］列をクリックしてコンテキストメニューを開き、［**許可**］を選択します。
   - 接続バスへのアクセスをブロックするには、［**アクセス**］列をクリックしてコンテキストメニューを開き、［**ブロック**］を選択します。
6. 変更を保存するには［**保存**］をクリックします。

# 信頼するデバイスを使用した処理

このセクションでは、信頼するデバイスでの処理について説明します。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。

3. 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。

4. ［**選択**］をクリックします。

   ［**信頼するデバイスの選択**］ウィンドウが開きます。

5. 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。

   ［**デバイス**］列内のリストは、［**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。

6. ［**選択**］をクリックします。

   Microsoft Windows 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。

7. Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで、ユーザーおよびユーザーのグループ、またはそのいずれかを選択します。このユーザーとユーザーのグループについて、選択したデバイスが信頼できることが認識されます。

   Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで指定したユーザーまたはユーザーグループの名前が、［**許可するユーザーまたはユーザーグループ**］に表示されます。

8. ［**信頼するデバイスの選択**］ウィンドウで［OK］をクリックします。

   ［**デバイスコントロール**］ウィンドウの［**信頼するデバイス**］タブの表に、追加された信頼するデバイスのパラメータを示す行が表示されます。

9. 特定のユーザーまたはユーザーグループの信頼するデバイスのリストに追加するデバイスごとに手順 4 ～ 7 を繰り返します。

10. 変更を保存するには［**保存**］をクリックします。

## デバイスモデルまたは ID に基づく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。

*デバイスモデルまたは ID に基づいて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. 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、信頼するデバイスのリストを作成する管理グループ名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. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**エンドポイントコントロール**］セクションの［**デバイスコントロール**］サブセクションを選択します。

7. 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。

8. ［**追加**］をクリックします。
   コンテキストメニューが開きます。

9. ［**追加**］のコンテキストメニューで、次のいずれかの操作を行います：

   - 既知の一意の ID を持つデバイスを選択して、信頼するデバイスのリストに追加する場合は、［**ID によるデバイス**］を選択します。

   - ［**モデルによるデバイス**］を選択して、VID（製造元 ID）および PID（製品 ID）が既知の信頼するデバイスをリストに追加します。

10. 開いたウィンドウの［**デバイス種別**］で、以下の表に示すデバイスの種別を選択します。

11. ［**更新**］をクリックします。
    デバイス ID またはデバイスモデルが既知であり、［**デバイス種別**］で選択される種別に属するデバイスのリストが表に示されます。

12. 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。

13. ［**選択**］をクリックします。
    Microsoft Windows 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。

14. Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで、ユーザーおよびユーザーのグループ、またはそのいずれかを選択します。このユーザーとユーザーのグループについて、選択したデバイスが信頼できることが認識されます。
    Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで指定したユーザーまたはユーザーグループの名前が、［**許可するユーザーまたはユーザーグループ**］に表示されます。

15. ［**OK**］をクリックします。
    追加された信頼するデバイスのパラメータの行が、［**信頼するデバイス**］タブのテーブルに表示されます。

16. ［**OK**］または［**適用**］をクリックして、変更内容を保存します。

## デバイス ID のマスクに基づく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。

デバイスを ID のマスクに基づいて信頼リストに追加するのは、Kaspersky Security Center の管理コンソールでのみ行えます。

*ID のマスクに基づいて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. 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、信頼するデバイスのリストを作成する管理グループ名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. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**エンドポイントコントロール**］セクションの［**デバイスコントロール**］サブセクションを選択します。

7. 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。

8. ［**追加**］をクリックします。
   コンテキストメニューが開きます。

9. ［**追加**］のコンテキストメニューで、［**ID マスクによるデバイス**］を選択します。
   ［**信頼済みデバイスを ID マスクで追加する**］ウィンドウが開きます。

10. ［**信頼済みデバイスを ID マスクで追加する**］ウィンドウの［**マスク**］に、デバイス ID のマスクを入力します。

11. ［**選択**］をクリックします。
    Microsoft Windows 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。

12. Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで、ユーザーまたはユーザーグループを選択します。このユーザーまたはユーザーグループに対して、モデルまたは ID が指定されたマスクと一致した場合に、デバイスが信頼できると認識されます。
    Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで指定したユーザーまたはユーザーグループの名前が、［**許可するユーザーまたはユーザーグループ**］に表示されます。

13. ［**OK**］をクリックします。
    ［**デバイスコントロール**］ウィンドウの［**信頼するデバイス**］タブの表に、デバイス ID のマスクで信頼するデバイスのリストにデバイスを追加するためのルールの設定の行が表示されます。

14. 変更を保存するには［**保存**］をクリックします。

## 信頼するデバイスへのユーザーアクセスの設定

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。信頼するデバイスへのユーザー（またはユーザーグループ）のアクセスを設定できます。

*信頼するデバイスへのユーザーアクセスを設定するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。

3. 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。

4. 信頼するデバイスのリストで、アクセスルールを編集するデバイスを選択します。

5. ［**編集**］をクリックします。

   ［**信頼済みデバイスのアクセスルールの設定**］ウィンドウが開きます。

6. ［**選択**］をクリックします。

   Microsoft Windows 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。

7. Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで、ユーザーおよびユーザーのグループ、またはそのいずれかを選択します。このユーザーとユーザーのグループについて、選択したデバイスが信頼できることが認識されます。

8. ［**OK**］をクリックします。

   Microsoft Windows の［**ユーザーまたはグループの選択**］ウィンドウで指定したユーザーまたはユーザーグループの名前が、［**信頼済みデバイスのアクセスルールの設定**］ウィンドウの［**許可するユーザーまたはユーザーグループ**］に表示されます。

9. ［**OK**］をクリックします。

10. 変更を保存するには［**保存**］をクリックします。

## 信頼するデバイスのリストからのデバイスの削除

*信頼するデバイスのリストからデバイスを削除するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。

3. 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。

4. 信頼するデバイスのリストから削除するデバイスを選択します。

5. [**削除**］をクリックします。

6. 変更を保存するには［**保存**］をクリックします。

信頼するデバイスのリストから削除したデバイスへのアクセスについての判断は、Kaspersky Endpoint Security が、デバイスアクセスルールと接続バスアクセスルールに基づいて行います。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**デバイスコントロール**］サブセクションを選択します。

   ウィンドウの右側には、デバイスコントロールの設定が表示されます。
3. ウィンドウの右側で、［**テンプレート**］をクリックします。

   ［**メッセージのテンプレート**］ウィンドウが開きます。
4. 次のいずれかの手順を実行します：

   - 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または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のテンプレートを変更するには、［**ブロック**］タブを選択します。
   - LAN 管理者に送信されるメッセージのテンプレートを変更するには、［**管理者に送信するメッセージ**］タブを選択します。
5. メッセージテンプレートを編集します。［**変数**］、［**既定**］、［**リンク**］（［**ブロック**］タブでのみ使用できます）を使用することもできます。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## ブロックされたデバイスへのアクセスの取得

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

> デバイスへの一時アクセス権を付与する Kaspersky Endpoint Security の機能は、Kaspersky Endpoint Security が Kaspersky Security Center のポリシーに従って動作している場合にのみ利用できます（『*Kaspersky Security Center 管理者用ガイド*』参照）。

*［デバイスコントロール］ウィンドウからブロックされたデバイスへのアクセスを要求するには：*

1. メインウィンドウで、［**プロテクションとコントロール**］タブを選択します。
2. ［**エンドポイントコントロール**］セクションをクリックします。

   ［**エンドポイントコントロール**］セクションが開きます。

3. デバイスコントロールに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。

   コンポーネントの処理を選択するメニューが表示されます。

4. ［**デバイスへのアクセス**］をクリックします。

   ［**デバイスへのアクセス要求**］ウィンドウが開きます。

5. 接続されているデバイスのリストから、アクセスするデバイスを選択します。

6. ［**アクセス要求ファイルを生成**］をクリックします。

   ［**アクセス要求ファイルの作成**］ウィンドウが開きます。

7. ［**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。

8. ［**保存**］をクリックします。

   Microsoft Windows 標準の［**アクセス要求ファイルを保存**］ウィンドウが開きます。

9. Microsoft Windows の［**アクセス要求ファイルを保存**］ウィンドウで、デバイスのアクセス要求ファイルを保存するフォルダーを選択し、［**保存**］をクリックします。

10. デバイスのアクセス要求ファイルを LAN 管理者に送信します。

11. デバイスのアクセスキーファイルを LAN 管理者から受け取ります。

12. ［**デバイスへのアクセス要求**］ウィンドウで、［**アクセスキーの有効化**］をクリックします。

    Microsoft Windows 標準の［**アクセスキーを開く**］ウィンドウが開きます。

13. Microsoft Windows の［**アクセスキーを開く**］ウィンドウで、LAN 管理者から受け取ったアクセスキーファイルを選択し、［**開く**］をクリックします。

    ［**デバイスのアクセスキーを有効化**］ウィンドウが開き、付与されたアクセスに関する情報が表示されます。

14. ［**デバイスのアクセスキーを有効化**］ウィンドウで、［**OK**］をクリックします。

*デバイスがブロックされていることを通知するメッセージのリンクをクリックしてブロックされたデバイスへのアクセスを要求するには：*

1. デバイスまたは接続バスがブロックされていることを通知するメッセージが表示されているウィンドウで、［**アクセスを要求する**］をクリックします。

   ［**アクセス要求ファイルの作成**］ウィンドウが開きます。

2. ［**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。

3. ［**保存**］をクリックします。

   Microsoft Windows 標準の［**アクセス要求ファイルを保存**］ウィンドウが開きます。

4. Microsoft Windows の［**アクセス要求ファイルを保存**］ウィンドウで、デバイスのアクセス要求ファイルを保存するフォルダーを選択し、［**保存**］をクリックします。

5. デバイスのアクセス要求ファイルを LAN 管理者に送信します。

6. デバイスのアクセスキーファイルを LAN 管理者から受け取ります。

7. ［**デバイスへのアクセス要求**］ウィンドウで、［**アクセスキーの有効化**］をクリックします。

Microsoft Windows 標準の［**アクセスキーを開く**］ウィンドウが開きます。

8. Microsoft Windows の［**アクセスキーを開く**］ウィンドウで、LAN 管理者から受け取ったアクセスキーファイルを選択し、［**開く**］をクリックします。

   ［**デバイスのアクセスキーを有効化**］ウィンドウが開き、付与されたアクセスに関する情報が表示されます。

9. ［**デバイスのアクセスキーを有効化**］ウィンドウで、［**OK**］をクリックします。

デバイスへのアクセスが許可される時間は、要求した時間によって異なることがあります。デバイスへのアクセスは、LAN 管理者がデバイスアクセスキーを生成したときに指定した時間だけ許可されます。

## Kaspersky Security Center を使用した、ブロックされたデバイスのアクセスキーの作成

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場合、アクセスキーが必要です。Kaspersky Security Center を使用してアクセスキーを作成できます。

*ブロックされたデバイスのアクセスキーを作成するには：*

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、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デバイスおよびデータへのアクセスを許可する**］を選択します。

   ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウが開きます。

6. ［**デバイスコントロール**］タブを選択します。

7. ［**デバイスコントロール**］タブで［**参照**］をクリックします。

   Microsoft Windows 標準の［**アクセス要求ファイルを選択**］ウィンドウが開きます。

8. ［**アクセス要求ファイルの選択**］ウィンドウで、ユーザーから受け取ったアクセス要求ファイルを選択し、［**開く**］をクリックします。

   ［**デバイスコントロール**］には、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詳細が表示されます。

9. ［**アクセス期間**］設定の値を指定します。

   この設定では、ユーザーがブロックされたデバイスへのアクセスを許可される時間の長さを定義します。既定値は、アクセス要求ファイルの作成時にユーザーが指定した値です。

10. ［**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アクティベートできる期間を定義します。

11. ［**保存**］をクリックします。

    Microsoft Windows 標準の［**アクセスキーファイルの保存**］ウィンドウが開きます。

12. ブロックされたデバイスのアクセスキーが入ったファイルを保存するフォルダーを選択します。

13. ［**保存**］をクリックします。

# 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 Microsoft 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 Microsoft 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。

このセクションでは、ウェブコントロールに関する情報と、このコンポーネントの設定方法について説明します。

## ウェブコントロールの概要

ウェブコントロールは、Web リソースへのアクセスを制限またはブロックすることによって、LAN 内でのユーザー処理をコントロールします。

Web リソースとは、個別の Web サイトまた複数の Web サイト、あるいは 1 つの Web サイトまたは共通点のある複数の Web サイトのことです。

ウェブコントロールには、次のオプションがあります：

- トラフィックの抑制

  トラフィックは、マルチメディアファイルのダウンロードを制限またはブロックするか、ユーザーの業務に無関係な Web リソースへのアクセスを制限またはブロックすることによってコントロールされます。

- Web リソースのコンテンツカテゴリによるアクセスの制限

  トラフィックを抑制するとともに、勤務時間の浪費による潜在的な損失を削減するために、特定のカテゴリの Web リソースへのアクセスを制限またはブロックすることができます（たとえば、「インターネットコミュニケーション」カテゴリに属する Web リソースへのアクセスをブロックできます）。

- Web リソースへのアクセスの一元化

  Kaspersky Security Center を使用する場合、Web リソースへのアクセスの個人設定およびグループ設定を使用できます。

Web リソースへのアクセスに適用されているすべての制限およびブロックは、Web リソースアクセスルールとして実行されます。

## 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。必要に応じて、ウェブコントロールを無効にできます。

次の 2 つの場所から、コンポーネントを有効または無効にすることができます：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

*メインウィンドウの［**プロテクションとコントロール**］タブでウェブコントロールを有効または無効にするには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションをクリックします。
   ［**エンドポイントコントロール**］セクションが開きます。
4. ウェブコントロールに関する情報が含まれる行を右クリックして、コンテキストメニューを表示します。
   コンポーネントの処理を選択するメニューが表示されます。
5. 次のいずれかの手順を実行します：
   - ウェブコントロールを有効にするには、メニューの［**開始**］を選択します。
   - ウェブコントロールを無効にするには、メニューの［**停止**］を選択します。

*［設定］ウィンドウからウェブコントロールを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。
   ウィンドウの右側に、ウェブコントロールの設定が表示されます。
3. 次のいずれかの手順を実行します：
   - ウェブコントロールを有効にするには、［**ウェブコントロールを有効にする**］をオンにします。
   - ウェブコントロールを無効にするには、［**ウェブコントロールを有効にする**］をオフにします。

   ウェブコントロールを無効にした場合、Kaspersky Endpoint Security は Web リソースへのアクセスを管理しません。
4. 変更を保存するには［**保存**］をクリックします。

# Web リソースのコンテンツカテゴリ

以下のリストに示す Web リソースのコンテンツカテゴリ（以降、「カテゴリ」）は、Web リソースによってホストされるデータのブロックを十分説明するために、機能や主題を考慮に入れて選択されています。このリストに示すカテゴリの順序は、インターネットのカテゴリの相対的な重要性や普及率を反映したものではありません。カテゴリ名は暫定的なもので、カスペルスキー製品や Web サイトでのみ使用されます。これらの名前は、法律で示す意味を必ずしも反映しているわけではありません。1つの Web リソースが、同時に複数のカテゴリに属す可能性があります。

## アダルト

このカテゴリには、次の種別の Web リソースが含まれます：

- 人間や人間型の生物の生殖器、性行為、または自慰行為を描写する写真やビデオの題材が含まれる Web リソース。
- 人間や人間型の生物の生殖器、性行為、または自慰行為を描写する、文学的または芸術的な題材などのテキスト題材が含まれる Web リソース。
- 人間関係の性的な側面を重点的に議論する Web リソース。

> 「インターネットコミュニケーション」カテゴリと重複します。

- 性的な資料、人間の性行為を現実的に描写する作品、または性的興奮を刺激することを目的とした芸術作品を含む Web リソース。
- 人間関係の性的な側面を重点的に取り上げる特別なセクションや各記事を含む、対象読者が確立された公式的なメディアの店舗やオンラインコミュニティの Web リソース。
- 性的倒錯を重点的に取り上げる Web リソース。
- 性行為で使用して性的興奮を刺激するアイテム、性的なビデオチャットや「テレフォンセックス」「セクスティング」（「仮想セックス」）など、オンラインで提供するサービスを含む性的サービスや親密なデートを広告して販売する Web リソース。
- 以下の内容を含む Web コンテンツ：
  - 性教育に関連する記事およびブログのエントリ（内容が科学的か一般的かは問わない）。
  - 生殖行為に関するセクションを含む医学百科事典。
  - 臨床資料において、生殖器を扱う症例に関する情報。

## ソフトウェア、音楽、映像

このカテゴリには以下のサブカテゴリがあり、個別に選択できます：

- **音声と映像**

  このサブカテゴリには、映画、スポーツ中継、コンサート中継、曲、動画、映像、そして音楽や映像を録画するためのチュートリアルなど、音楽や映像の題材を配信するリソースが含まれます。

- **Torrent**

  このサブカテゴリには、無制限のサイズのファイルを共有するための Torrent トラッカーの Web サイトが含まれます。

- **ファイル共有**

  このサブカテゴリには、配信するファイルの物理的な場所を問わないファイル共有 Web サイトが含まれます。

## アルコール、タバコ、麻薬

このカテゴリには、アルコールまたはアルコールを含む製品、タバコ製品、さらには麻薬や向精神薬、酩酊状態を引き起こす物質と直接的または間接的に関連するコンテンツを持つ Web リソースが含まれます。

- そのような物質とそれを摂取するための用具を広告して販売する Web リソース。

「電子商取引」カテゴリと重複します。

- 麻薬や向精神薬、または酩酊状態を引き起こす物質の摂取と作成の方法を説明する Web リソース。

このカテゴリには、科学的、医学的なトピックを取り上げる Web リソースが含まれます。

## 暴力

このカテゴリには、人間に対する物理的または精神的な暴力行為や、動物への残虐行為を説明する画像、動画、テキストの題材を持つ Web リソースが含まれます。

- 処刑、拷問、虐待の情景描写や、そのような行為で使用するためのツールの説明を含む Web リソース。

「武器、爆発物、花火」カテゴリと重複します。

- 殺人、格闘、殴打、レイプなど、人間、動物、または想像上の生物を虐待したり辱めたりするシーンの描写や記述のある Web リソース。
- 自傷行為や自殺など、生命や健康を脅かす行為を扇動する情報を持つ Web リソース。
- 暴力行為や残虐行為の許容を実証化または正当化する情報や、人間や動物に対する暴力行為を扇動する情報を持つ Web リソース。
- 戦争、武力紛争、軍事衝突、事故、惨事、自然災害、産業的または社会的な大変動、人間の苦悩の様子など、犠牲者や残酷さの詳しい描写や記述のある Web リソース。
- 「シューティング」「格闘」「スラッシャー」などと呼ばれる、暴力や残虐行為のシーンがあるブラウザーのコンピューターゲーム。

「コンピューターゲーム」カテゴリと重複します。

## 武器、爆発物、花火

このカテゴリには、武器、爆発物、花火製品に関する情報の Web リソースが含まれます：

- 武器、爆発物、花火製品の製造元と販売店の Web サイト。

「電子商取引」カテゴリと重複します。

- 武器、爆発物、花火製品の製造または使用を重点的に取り上げる Web リソース。
- 武器、爆発物、花火製品の分析、歴史、製造、および百科事典的な題材を重点的に取り上げる Web リソース。

「武器」という用語は、人間および動物の生命や健康を脅かし、設備や建築物を破損することを目的とした器具、商品、手段を指します。

## 過激な表現

このカテゴリには、過激な言葉が検知された Web リソースが含まれます。

「アダルト」カテゴリと重複します。

このカテゴリには、研究の主題として過激な表現を含む言語学的または文献学的な題材を持つ Web リソースも含まれます。

## ギャンブル、宝くじ、懸賞

このカテゴリには、Web サイトへのアクセスで金銭的な参加が必須条件でなくても、金銭を賭けたギャンブルの参加をユーザーに提供する Web リソースが含まれます。このカテゴリには、以下を提供する Web リソースが含まれます：

- 参加者が金銭的な寄与を求められるギャンブル。

  「コンピューターゲーム」カテゴリと重複します。

- 金銭の賭けを含む懸賞。
- 宝くじの券や番号の購入を含む宝くじ。
- ギャンブル、懸賞、宝くじに参加したい欲望を引き起こす可能性がある情報。

「電子商取引」カテゴリと重複します。

このカテゴリには、無料で参加できるモードを別に提供するゲームと、このカテゴリに当てはまる Web リソースをユーザーに向けて積極的に広告する Web リソースが含まれます。

## インターネットコミュニケーション

このカテゴリには、ユーザー（登録の必要性は問わない）が関連のある Web リソースやその他のオンラインサービスの他のユーザーにパーソナルメッセージを送信したり、関連がある Web リソースに特定の用語に関するコンテンツを追加（一般公開されているか制限があるかは問わない）できる Web リソースが含まれます。次のサブカテゴリを個別に選択できます：

- **チャットと掲示板**

このサブカテゴリには、専用の Web アプリケーションを使用してさまざまな話題について公開で議論するための Web リソースや、リアルタイムでコミュニケーションできるインスタントメッセージングアプリケーションを配信またはサポートすることを目的とした Web リソースが含まれます。

- **ブログ**

  このサブカテゴリには、ブログの作成や管理を有料または無料で提供する Web サイトであるブログプラットフォームが含まれます。

- **ソーシャルネットワーク**

  このサブカテゴリには、個人、組織、政府間での連絡先の作成、表示、管理を目的とし、参加条件としてユーザーアカウントの登録が必要な Web サイトが含まれます。

- **出会い系サイト**

  このサブカテゴリには、有料または無料のサービスを提供するソーシャルネットワークの変種として機能する Web リソースが含まれます。

  「アダルト」および「電子商取引」カテゴリと重複します。

- **Web メール**

  このサブカテゴリには、メールおよび関連するデータ（個人の連絡先など）を含むメールサービスとメールボックスのページに排他的にログインするページが含まれます。このカテゴリには、メールサービスも提供するインターネットサービスプロバイダーの他の Web ページは含まれません。

## オンラインストア、銀行、支払いシステム

このカテゴリには、専用の Web アプリケーションを使用して、現金以外の手段でオンライン取引を行うために設計された Web リソースが含まれます。次のサブカテゴリを個別に選択できます：

- **ショッピングとオークション**

  このサブカテゴリには、さまざまな商品、労働やサービスを個人や法人に販売するオンラインショップやオンラインオークションが含まれます。オンラインでのみ販売を行う店の Web サイトやオンライン決済が可能な実店舗の Web サイトを含みます。

- **銀行**

  このサブカテゴリには、オンラインバンキング機能（銀行口座間の電信送金、預金、両替、サードパーティのサービスへの支払いなどを含む）を持つ銀行の専用の Web サイトが含まれます。

- **支払いシステム**

  このサブカテゴリには、ユーザーの個人アカウントにアクセスできる電子マネーシステムの Web サイトが含まれます。

技術用語で、決済は、あらゆる種別のカード（実在のカードまたは仮想のカード、デビットカードまたはクレジットカード、国内専用または海外使用可能）と電子マネーの両方を使用して行うことができます。SSL プロトコルや 3D Secure 認証などを使用したデータ送信など、技術的な側面があるかどうかにかかわらず、Web リソースがこのカテゴリに該当する場合があります。

## 求人情報

このカテゴリには、雇用者と求職者を結びつけるための Web リソースが含まれます：

- 人材紹介エージェントの Web サイト（求人やスカウトのエージェント）。
- 雇用者が募集中の職種とメリットを説明している Web サイト。
- 雇用者や人材紹介エージェントの募集をあっせんする独立系ポータル。
- 就職先を積極的に探していない専門職の人材に関する情報を公開または検索できる、その他すべての専門職向けの SNS。

> 「インターネットコミュニケーション」カテゴリと重複します。

## 匿名化

このカテゴリには、専用の Web アプリケーションを使用して、以下の目的を持つ他の Web リソースのコンテンツをダウンロードするための仲介者として機能する Web リソースが含まれます：

- Web アドレスや IP アドレスへのアクセスにおいて LAN の管理者が課す制限を迂回する。
- 特定の IP アドレスまたはそのグループ（発生した国でまとめられた IP アドレスなど）からの HTTP 要求を限定的に拒否する Web リソースが含まれ、匿名で Web リソースにアクセスする。

> このカテゴリには、上述の目的（匿名化）のために排他的に設計された Web リソースと、技術的に類似する機能を持つ Web リソースが含まれます。

## コンピューターゲーム

このカテゴリには、さまざまなジャンルのコンピューターゲーム専用の Web リソースが含まれます：

- コンピューターゲームの開発者の Web サイト。
- コンピューターゲームを重点的に議論する Web リソース。

> 「インターネットコミュニケーション」カテゴリと重複します。

- オンラインでゲームに参加できる技術的な性能を提供する Web リソース。他の参加者と一緒にプレーする場合と個人でプレーする場合があり、アプリケーションをローカルにインストールするものとインストールのいらないもの（「ブラウザーゲーム」）があります。
- ゲームソフトの宣伝、配信、サポートのための Web リソース。

> 「電子商取引」カテゴリと重複します。

## 宗教

このカテゴリには、宗教的なイデオロギー、またはカルト的な兆候を持つ住民運動、団体、組織に関する題材を持つ Web リソースが含まれます。

- 国際的な宗教組織から地域の宗教団体まで、さまざまなレベルの公的な宗教組織の Web サイト。
- 歴史的には優勢な宗教団体や共同体から分裂して登場した、登録されていない宗教団体の Web サイト。
- 特定の創設者の主導により、伝統的な宗教運動とは無関係に出現した宗教団体や共同体の Web サイト。
- さまざまな伝統的宗教の代表によって異なる宗教間の連帯を目的とした組織の Web サイト。
- 宗教を主題とする学術的、歴史的、百科事典的な題材の Web リソース。
- 神や、超自然的な力を持つと信じられている生物、物体の崇拝などの儀式を含む、カルト宗教による崇拝の詳しい描写や記述のある Web リソース。

### ニュース

このカテゴリには、マスメディアによって作成されて公開されたニュースコンテンツや、ユーザーがニュースレポートを追加できるオンライン出版の Web リソースが含まれます：

- 公的なメディアの Web サイト。
- 公的な情報源が帰属する情報サービスを提供する Web サイト。
- さまざまな公式および非公式な情報源からニュースの情報を収集する、集約サービスの Web サイト。
- ニュースコンテンツをユーザー自身が作成する Web サイト（「ソーシャルニュースサイト」）。

> 「インターネットコミュニケーション」カテゴリと重複します。

### バナー

このカテゴリには、バナーを伴う Web リソースが含まれます：バナーの広告は作業中の集中力を阻害する一方、バナーのダウンロードによってトラフィック量が増大します。

## Web リソースアクセスルールの概要

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 リソースのプール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。特定のカテゴリのコンテンツとデータの種類を含む 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を指定した場合で、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、選択したコンテンツカテゴリやデータ種別カテゴリにある Web リソースへのアクセスは管理されません。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へのアクセスだけが制限されます。

- **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」ルール - 任意の 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。

## Web リソースアクセスルールを使用した処理

Web リソースアクセスルールに対して、次の処理を実行することができます：

- 新しいルールを追加する

- ルールを編集する

- ルールに優先度を割り当てる

  ルールの優先度は、ウェブコントロールの設定ウィンドウのアクセスルールテーブルで、ルールの簡単な説明を含む行の位置によって決まります。つまり、アクセスルールテーブル内で上にあるルールの優先度は、その下にあるルールより高くなります。

  ユーザーがアクセスしようと試みる Web リソースがいくつかのルールのパラメータと一致すると、Kaspersky Endpoint Security は最高優先度のルールに従って処理を実行します。

- ルールをテストする

  ルールの一貫性をチェックするには、ルール診断機能を使用します。

- ルールを有効 / 無効にする

  Web リソースアクセスルールを、有効化（動作ステータス［*有効*］）または無効化（動作ステータス［*無効*］）できます。既定では、ルールを作成すると、そのルールが有効（動作ステータス［*有効*］）になります。ルールは無効にすることもできます。

- ルールを削除する

## Web リソースへのアクセスルールの追加と編集

*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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。

   ウィンドウの右側に、ウェブコントロールの設定が表示されます。
3. 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。
   - ルールを編集するには、ルールを選択して［**編集**］をクリックします。

   ［**Web リソースへのアクセスルール**］ウィンドウが開きます。
4. ルールの設定を指定または編集します。次の手順に従います：

   a. ［**名前**］にルール名を入力するか編集します。

   b. ［**コンテンツのフィルタリング**］の次のオプションから、該当するオプションを選択します：

      - **すべてのコンテンツ**
      - **コンテンツカテゴリ**
      - **データ種別**
      - **コンテンツカテゴリとデータ種別**

   c. ［**すべてのコンテンツ**］以外のオプションを選択すると、コンテンツカテゴリまたはデータ種別を選択するセクションが開きます。目的のコンテンツカテゴリまたはデータ種別の名前の横の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の名前の横の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。

   d. ［**適用するアドレス**］の次のオプションから、任意のオプションを選択します：

      - **すべてのアドレス**
      - **個別のアドレス**

   e. ［**個別のアドレス**］を選択すると、Web リソースのリストを作成するセクションが開きます。［**追加**］、［**編集**］、［**削除**］を使用して、Web リソースのアドレスを追加および編集できます。

   f. ［**ユーザーまたはグループの選択**］をオンにします。

   g. ［**選択**］をクリックします。

      Microsoft Windows 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。

   h. ルールによって規定される Web リソースへのアクセスを許可またはブロックするユーザーまたはユーザーグループのリストを指定または編集します。

   i. ［**処理**］の次のオプションから、任意の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。

j. ［**ルールスケジュール**］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：

1. ［**ルールスケジュール**］の横にある［**設定**］をクリックします。
   ［**ルールスケジュール**］ウィンドウが開きます。
2. ルールが適用されない時間帯をルールスケジュールに追加するには、ルールスケジュールが表示されているテーブルで、選択する時刻と曜日に対応するテーブルのセルをクリックします。
   セルの色が灰色に変わります。
3. ルールが適用される時間帯をルールが適用されない時間帯に置き換えるには、選択する時刻と曜日に対応するテーブルの灰色のセルをクリックします。
   セルの色が緑に変わります。
4. ［**名前を付けて保存**］をクリックします。
   ［**ルールスケジュール名**］ウィンドウが開きます。
5. ルールスケジュール名を入力するか、既定の名前を変更せずに使用します。
6. ［**OK**］をクリックします。

5. ［**Web リソースへのアクセスルール**］ウィンドウで［**OK**］をクリックします。
6. 変更を保存するには［**保存**］をクリックします。

## Web リソースアクセスルールの優先度の割り当て

ルールを特定の順序で配列することにより、ルールリストから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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。
   ウィンドウの右側に、ウェブコントロールの設定が表示されます。
3. ウィンドウの右側で、優先度を変更したいルールを選択します。
4. ［**上へ**］と［**下へ**］を使用して、ルールをルールリストの所定のランクに移動します。

5. 優先度を変更したい各ルールについて、手順 3〜4 を繰り返します。

6. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。

   ウィンドウの右側に、ウェブコントロールの設定が表示されます。

3. ウィンドウの右側で、［**診断**］をクリックします。

   ［**ルールの診断**］ウィンドウが開きます。

4. ［**条件**］セクションのフィールドに、次のように入力します：

   a. 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。

   b. 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。

   c. 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。

   d. 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。

5. ［**テスト**］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、［**テスト**］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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。

ウィンドウの右側に、ウェブコントロールの設定が表示されます。

3. ウィンドウの右側で、有効または無効にするルールを選択します。

4. ［**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。

5. 変更を保存するには［**保存**］をクリックします。

## 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

本製品の Service Pack 1 Maintenance Release 1 以前のバージョンを Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードすると、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が、次のように移行されます：

- 「フォーラムとチャット」「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、支払いシステム」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。

## 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エクスポートするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。

   ウィンドウの右側に、ウェブコントロールの設定が表示されます。

3. ファイルにエクスポートする 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。

4. ［**編集**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが開きます。

5. Web リソースアドレスのリスト全体ではなく、一部のみをエクスポートする場合は、任意の Web リソースアドレスを選択します。

6. Web リソースアドレスのリストが表示されるフィールドの右側にある ボタンをクリックします。
   処理の確認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：

   - Web リソースアドレスリストのうち、選択した項目のみをエクスポートする場合は、処理の確認ウィンドウで［**はい**］をクリックします。

   - Web リソースアドレスリストのすべての項目をエクスポートする場合は、処理の確認ウィンドウで［**いいえ**］をクリックします。
     Microsoft Office の標準の［**名前を付けて保存**］ウィンドウが開きます。

8. Microsoft Windows の［**名前を付けて保存**］ウィンドウで、Web リソースアドレスのリストをエクスポートするファイルを選択します。［**保存**］をクリックします。

*Web リソースアドレスのリストをファイルからルールにインポートするには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。
   ウィンドウの右側に、ウェブコントロールの設定が表示されます。

3. 次のいずれかの手順を実行します：

   - 新しい Web リソースアクセスルールを作成するには、［**追加**］をクリックします。

   - 編集する Web リソースアクセスルールを選択します。次に、［**編集**］をクリックします。

   ［**Web リソースへのアクセスルール**］ウィンドウが開きます。

4. 次のいずれかの手順を実行します：

   - 新しい Web リソースアクセスルールを作成している場合は、［**適用するアドレス**］から［**個別のアドレス**］を選択します。

   - Web リソースアクセスルールを編集している場合は、この手順のステップ 5 に進みます。

5. Web リソースアドレスのリストが表示されるフィールドの右側にある ボタンをクリックします。
   新しいルールを作成している場合は、Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが開きます。
   ルールを編集している場合は、確認を求めるウィンドウが開きます。

6. 次のいずれかの手順を実行します：

   - 新しい Web リソースアクセスルールを編集している場合は、この手順のステップ 7 に進みます。

- Web リソースアクセスルールを編集している場合は、処理の確認ウィンドウで次の処理のいずれかを実行します：

  - インポートした Web リソースアドレスの項目を既存の項目に追加する場合は、［**はい**］をクリックします。

  - Web リソースアドレスリストの既存の項目を削除し、インポートした項目を追加する場合は、［**いいえ**］をクリックします。

Microsoft Windows の［**ファイルを開く**］ウィンドウが開きます。

7. Microsoft Windows の［**ファイルを開く**］ウィンドウで、インポートする Web リソースアドレスのリストが記述されたファイルを選択します。

8. ［**開く**］をクリックします。

9. ［**Web リソースへのアクセスルール**］ウィンドウで［OK］をクリックします。

## 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

   * 文字をアドレスマスクに含める場合は、* 文字を二回入力します。

2. 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 として扱われます。

3. 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。

4. アドレスマスクの先頭にある `*.` 文字のシーケンスは、`*.` または空文字列として解釈されます。

   例：アドレスマスク http://www.*.example.com には http://www2.example.com も含まれます。

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（abc 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 のアドレスには http://example.com および https://example.com が含まれます。

- 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。

アドレスマスク作成ルールの使用例

| No. | 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 1 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、2 を参照 |
| 7 | www.example.com | https://www.example.com | 含まれる | ルール 1、2 を参照 |
| 8 | http://www.*.example.com | http://123.example.com | 含まれる | ルール 1、2、4 を参照。 |
| 9 | www.example.com | http://www.example.com/abc | 含まれる | ルール 1、2、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、<br>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。 |

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**エンドポイントコントロール**］セクションで、［**ウェブコントロール**］サブセクションを選択します。

   ウィンドウの右側に、ウェブコントロールの設定が表示されます。
3. ウィンドウの右側で、［**テンプレート**］をクリックします。

   ［**メッセージのテンプレート**］ウィンドウが開きます。
4. 次のいずれかの手順を実行します：

   - Web リソースへのアクセスに対して警告するメッセージのテンプレートを修正する場合は、［**警告**］タブを選択します。
   - Web リソースへのアクセスがブロックされていることをユーザーに通知するメッセージのテンプレートを修正する場合は、［**ブロック**］タブを選択します。

- 管理者に送信されるメッセージのテンプレートを修正するには、［**管理者に送信するメッセージ**］タブを選択します。

5. メッセージテンプレートを編集します。［**変数**］、［**既定**］、［**リンク**］（［**管理者に送信するメッセージ**］タブでは使用できません）を使用することもできます。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

# KATA Endpoint Sensor

KATA Endpoint Sensor は、Kaspersky Security Center の管理コンソールでのみ設定できます。このコンポーネントを使用するには、管理プラグインをインストールする必要があります。

このセクションでは、KATA Endpoint Sensor に関する情報と、KATA Endpoint Sensor を有効または無効にする方法について説明します。

## KATA Endpoint Sensor について

*KATA Endpoint Sensor* は、Kaspersky Anti Targeted Attack Platform のコンポーネントです。このコンポーネントの目的は、標的型攻撃などの脅威を速やかに検知することです。

このコンポーネントは、クライアントコンピューターにインストールされます。コンピューター上で、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 Kaspersky Anti Targeted Attack Platform に渡します。

このコンポーネントの機能が使用可能なオペレーティングシステムは次のとおりです：

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1、Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8.1 Enterprise x86 Edition、Microsoft Windows 8.1 Enterprise x64 Edition
- Microsoft Windows 10 Pro / Enterprise x86 Edition、Microsoft Windows 10 Pro / Enterprise x64 Edition
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition、Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition
- Microsoft Windows Server 2016

本文書に掲載されていない　Kaspersky Anti Targeted Attack Platformに関するより詳しい情報は、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

KATA Endpoint Sensor がインストールされたコンピューターへの接続は、Kaspersky Anti Targeted Attack Platform サーバーからのプロキシサーバーを介さない直接接続のみが許可されます。

## KATA Endpoint Sensor の有効化と無効化

*KATA Endpoint Sensor 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、ポリシー設定の編集対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**詳細設定**］セクションで［**KATA Endpoint Sensor**］サブセクションを選択します。

7. 次のいずれかの手順を実行します：

   - KATA Endpoint Sensor を有効にするには、［**KATA Endpoint Sensor**］をオンにします。
   - KATA Endpoint Sensor を無効にするには、［**KATA Endpoint Sensor**］をオフにします。

8. 前の手順で［**KATA Endpoint Sensor**］をオンにした場合、［**サーバーのアドレス**］で、Kaspersky Anti Targeted Attack Platform サーバーのアドレスを指定します。これは次の部分からなります：

   a. プロトコル名

   b. サーバーの IP アドレスまたは完全修飾ドメイン名（FDQN）

   c. サーバー上の Windows Event Collector のパス

9. ［**OK**］をクリックします。

10. ポリシーを適用します。

    Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

# データ暗号化

Microsoft Windows for Workstations 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、データの暗号化機能はすべて使用できます。Microsoft Windows for File Servers 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ハードディスクの暗号化のみ使用できます。

このセクションでは、ハードディスク、リムーバブルドライブ、およびローカルコンピューターのドライブ上のファイルおよびフォルダーの暗号化と復号化について説明します。また、Kaspersky Endpoint Security と Kaspersky Endpoint Security 管理プラグインを使用してデータ暗号化および復号化を設定および実行する方法についても説明します。

暗号化されたデータにアクセスする手段がない場合は、暗号化されたデータの特殊な使用方法についての説明を参照してください（ファイルの暗号化機能が制限されたイベントでの暗号化ファイルの使用、暗号化されたデバイスにアクセスできない場合での暗号化デバイスの使用）。

## Kaspersky Security Center ポリシーでの暗号化設定の表示の有効化

*Kaspersky Security Center ポリシーで暗号化設定の表示を有効にするには：*

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［**管理サーバー – <コンピューター名>**］のコンテキストメニューで、［**表示**］ - ［**インターフェイスの設定**］の順に選択します。
   ［**インターフェイスの設定**］ウィンドウが開きます。
3. ［**インターフェイスの設定**］ウィンドウで、［**データ暗号化と保護機能の表示**］をオンにします。
4. ［**OK**］をクリックします。

## データ暗号化の概要

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、ポータブルコンピューター、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れのリスクを最小限に抑えることができます。

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、編集中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とき、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のファイルの暗号化**：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。Kaspersky Security Center の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

  Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

- **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。

  製品は、Kaspersky Security Center ポリシーが適用されると、暗号化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。

- **暗号化されたアーカイブの作成**：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。

- **ドライブの暗号化**：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。

  既定のハードディスク暗号化ルールを指定して、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、ハードディスク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。Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

  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。認証エージェントアカウントを管理してシングルサインオン（SSO）技術を使用することもできます。この技術により、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でオペレーティングシステムに自動でログインできます。

  > 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 管理者用ガイド*』を参照してください。

  > 本製品のバージョンを Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードする場合、認証エージェントアカウントのリストは保存されません。

  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、ハードディスク暗号化機能を含む 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。そのため、［**使用されているディスク領域のみを暗号化**］機能が有効になっているコンピューターで通常の暗号化を開始した際に新しいファイルが新しいデバイスに書き込まれても、一定の時間が経過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。暗号化されたファイルを持つコンピューターが、何らかの理由で、別の管理サーバーのコントロール下にあることが判明した場合、この暗号化ファイルがまだ一度もアクセスされていなければ、次のいずれかの方法で、このファイルにアクセスすることができます。

- LAN 管理者から、暗号化されたオブジェクトへのアクセスを要求する。
- 暗号化されたデバイスのデータの復元ツールによる復元
- 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 2 ～ 3% 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 Endpoint Security と Kaspersky Anti-Virus for UEFI の暗号化機能の互換性はサポートされていません。Kaspersky Anti-Virus for UEFI がインストールされているコンピューター上のハードディスクを暗号化すると、Kaspersky Anti-Virus for UEFI が動作できなくなります。

## 暗号化機能の制限

暗号化されたハードディスクに新しいパーティションを作成したり、暗号化されたハードディスク内の既存のパーティションをフォーマットしたりすると、ハードディスク内のデータが消失する可能性があります。

Kaspersky Disk Encryption 技術を使用したハードディスクの暗号化は、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 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。
- Intel® Rapid Start Technology と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）。
- 5 つ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 2% 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。

## 暗号化アルゴリズムの変更

データの暗号化のために Kaspersky Endpoint Security が使用する暗号化アルゴリズムは、配信キットに含まれる暗号化ライブラリによって異なります。

*暗号化アルゴリズムを変更するには：*

1. 暗号化アルゴリズムを変更する前に Kaspersky Endpoint Security によって暗号化されているオブジェクトを復号化します。

   暗号化アルゴリズムを変更すると、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. ビット数が異なる暗号化ライブラリを含む配信キットからKaspersky Endpoint Security をインストールします。

## 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。

*シングルサインオン（SSO）技術を有効にするには：*

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、シングルサインオン（SSO）技術の有効化の対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**暗号化の共通設定**］サブセクションを選択します。
7. ［**暗号化の共通設定**］サブセクションで、［**パスワードの設定**］セクションにある［**設定**］をクリックします。
   これにより、［**暗号化パスワードの設定**］ウィンドウの［**認証エージェント**］タブが開きます。

8. ［**シングルサインオン（SSO）技術を使用する**］をオンにします。

9. ［**OK**］をクリックします。

10. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

11. ポリシーを適用します。

    Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

## ファイル暗号化の考慮事項

ファイル暗号化機能を使用する際は、次の点にご注意ください：

- リムーバブルドライブの暗号化に関する事前設定は Kaspersky Security Center 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に対するファイル暗号化ポリシーや復号化ポリシー適用の結果は、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、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。

- 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。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の定義済みフォルダー、およびリダイレクトされたフォルダーについては、ファイルの暗号化や復号化は行いません。カスペルスキーが暗号化を推奨する標準フォルダーのリストには、次のフォルダーが含まれます：

  - マイドキュメント
  - お気に入り
  - Cookie
  - デスクトップ
  - Internet Explorer の一時ファイル
  - 一時ファイル
  - Outlook ファイル

- 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、ファイルやフォルダーを暗号化しません。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%、%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。暗号化しないファイルまたはフォルダーのリストに含まれるファイルやフォルダーは暗号化リストに追加できますが、ファイルやフォルダーの暗号化タスクで暗号化されることはありません。

- 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

# ローカルコンピュータードライブのファイルの暗号化

ローカルコンピュータードライブのファイルの暗号化は、ワークステーション用の Microsoft 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使用できます。ローカルコンピュータードライブのファイルの暗号化は、サーバー用の Microsoft 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使用できません。

このセクションは、ローカルコンピュータードライブでのファイルの暗号化を対象にしており、Kaspersky Endpoint Security と Kaspersky Endpoint Security 管理プラグインを使用したローカルコンピュータードライブでのファイルの暗号化の設定と実行の方法について説明します。

# ローカルコンピュータードライブのファイルの暗号化

*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、ローカルドライブ上でのファイルの暗号化設定の対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ファイルとフォルダーの暗号化**］サブセクションを選択します。
7. ウィンドウの右側で、［**暗号化**］タブを選択します。
8. ［**暗号化モード**］で、［**ルールに従う**］を選択します。
9. ［**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。

［**定義済みフォルダーの選択**］ウィンドウが開きます。

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。

［**カスタムフォルダーの追加**］ウィンドウが開きます。

c. ファイルの拡張子を暗号化ルールに追加するには、［**ファイルの拡張子による指定**］を選択します。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。

［**ファイル拡張子のリストの追加 / 編集**］ウィンドウが開きます。

d. ファイルの拡張子のグループを暗号化ルールに追加するには、［**ファイルの拡張子のグループによる指定**］を選択します。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。

［**ファイル拡張子のグループの選択**］ウィンドウが開きます。

10. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

11. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

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。

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。

暗号化されていないファイルのプロパティ（ファイルパス、ファイル名、ファイル拡張子）が変更され、その結果が暗号化ルールに一致する場合、そのファイルは暗号化されます。

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。

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。

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。

## 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、アプリケーションの暗号化ファイルアクセスルールの設定対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**ファイルとフォルダーの暗号化**］サブセクションを選択します。

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。

   ［**Kaspersky Security Center のリストからのアプリケーションの追加**］ウィンドウが開きます。

   次の手順に従います：

   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、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。

   d. ［**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。

   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。

   f. ［**OK**］をクリックします。

   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。

    ［**アプリケーションの実行ファイル名の追加 / 編集**］ウィンドウが開きます。

    次の手順に従います：

    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。

d. ［**OK**］をクリックします。

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. ［**OK**］をクリックして、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、特定のアプリケーションによって作成されたファイルの暗号化を設定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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ファイルとフォルダーの暗号化**］サブセクションを選択します。
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。

   ［**Kaspersky Security Center のリストからのアプリケーションの追加**］ウィンドウが開きます。

   次の手順に従います：

   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オンにします。

   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。

   f. ［**OK**］をクリックします。

   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。

    ［**アプリケーションの実行ファイル名の追加 / 編集**］ウィンドウが開きます。

    次の手順に従います：

    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。

    d. ［**OK**］をクリックします。

    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. ［**OK**］をクリックして、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、復号化するファイルのリスト作成の対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**ファイルとフォルダーの暗号化**］サブセクションを選択します。

7. ウィンドウの右側で、［**復号化**］タブを選択します。

8. ［**暗号化モード**］で、［**ルールに従う**］を選択します。

9. ［**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。

   ［**定義済みフォルダーの選択**］ウィンドウが開きます。

   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。

   ［**カスタムフォルダーの追加**］ウィンドウが開きます。

   c. ファイルの拡張子を復号化ルールに追加するには、［**ファイルの拡張子による指定**］を選択します。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。

   ［**ファイル拡張子のリストの追加 / 編集**］ウィンドウが開きます。

   d. ファイルの拡張子のグループを復号化ルールに追加するには、［**ファイルの拡張子のグループによる指定**］を選択します。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。

   ［**ファイル拡張子のグループの選択**］ウィンドウが開きます。

10. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

11. ポリシーを適用します。

    Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

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、ローカルドライブ上でのファイルの復号化設定の対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ファイルとフォルダーの暗号化**］サブセクションを選択します。
7. ウィンドウの右側で、［**暗号化**］タブを選択します。
8. 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複合化**］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。
9. ファイル復号化リストを作成します。
10. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。
11. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

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

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。

*暗号化されたパッケージを作成するには：*

1. 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コンピューターで、任意のファイルマネージャーを使用して暗号化されたパッケージに追加するファイルや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、［**暗号化されたパッケージへの追加**］を選択します。

   Microsoft Windows 標準のダイアログボックス［**暗号化されたパッケージの保存先のパスを選択**］が開きます。

3. Microsoft Windows 標準のダイアログボックス［**暗号化されたパッケージの保存先のパスを選択**］で、リムーバブルドライブ上の暗号化されたパッケージの保存先を選択します。［**保存**］をクリックします。

   ［**暗号化されたパッケージへの追加**］ウィンドウが開きます。

4. ［**暗号化されたパッケージへの追加**］ウィンドウで、パスワードを入力して確認します。

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。プロセスが終了すると、パスワードで保護された自己解凍式の暗号化されたパッケージが、リムーバブルドライブ上の選択した保存先フォルダーに作成されます。

ユーザーが暗号化されたパッケージの作成を取り消すと、Kaspersky Endpoint Security は次の操作を行います：

1. ファイルのパッケージへのコピープロセスを中断し、進行中のパッケージ暗号化操作があればすべて終了します。

2. パッケージの作成と暗号化プロセスで作成されたすべての一時ファイルと暗号化されたパッケージ自体のファイルを削除します。

3. 暗号化されたパッケージの作成プロセスが強制的に中止されたことをユーザーに通知します。

## 暗号化されたパッケージの解凍

*暗号化されたパッケージを解凍するには：*

1. 任意のファイルマネージャーで、暗号化されたパッケージを選択します。クリックして、解凍ウィザードを開始します。

   ［**パスワードの入力**］ウィンドウが開きます。

2. 暗号化されたパッケージを保護するパスワードを入力します。

3. ［**パスワードの入力**］ウィンドウで［**OK**］をクリックします。

   パスワードの入力に成功すると、Microsoft Windows 標準のダイアログ［**フォルダーの参照**］が開きます。

4. Microsoft Windows 標準のダイアログボックス［**フォルダーの参照**］で、暗号化されたパッケージの解凍先フォルダーを選択して、［**OK**］をクリックします。

   暗号化されたパッケージの解凍先フォルダーへの解凍プロセスが開始されます。

指定している解凍先フォルダーに暗号化パッケージが以前に解凍されている場合、フォルダー内の既存のファイルは暗号化パッケージから抽出されたファイルで上書きされます。

ユーザーが暗号化されたパッケージの解凍を取り消すと、Kaspersky Endpoint Security は次の操作を行います：

1. パッケージの復号化プロセスを停止し、暗号化パッケージからのファイルコピー操作が進行中の場合はすべて終了します。

2. 暗号化パッケージの復号化と解凍のプロセスで作成された一時ファイルをすべて削除します。同時に、暗号化パッケージから解凍先フォルダーにコピーされているファイルもすべて削除します。

3. 暗号化されたパッケージの解凍プロセスが強制的に中止されたことをユーザーに通知します。

# 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は、ワークステーション用の Microsoft 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。リムーバブルドライブの暗号化は、サーバー用の Microsoft 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。

このセクションでは、リムーバブルドライブの暗号化についての情報を提供し、Kaspersky Endpoint Security と Kaspersky Endpoint Security 管理プラグインを使用してリムーバブルドライブの暗号化を設定および実行する手順について説明します。

## 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、リムーバブルドライブの暗号化設定の対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**リムーバブルドライブの暗号化**］サブセクションを選択します。

7. ［**暗号化モード**］で、選択された管理グループのコンピューターに接続されているすべてのリムーバブルドライブに対して Kaspersky Endpoint Security が行う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**：この項目をオンにすると、Kaspersky Endpoint Security は、リムーバブルドライブに対して指定した暗号化設定で Kaspersky Security Center ポリシーを適用するときにリムーバブルドライブの内容をセクター単位で暗号化します。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、リムーバブルドライブのファイルシステムも暗号化されます。Kaspersky Endpoint Security は、すでに暗号化されているリムーバブルドライブの再暗号化は行いません。

この暗号化方式は、Kaspersky Endpoint Security のハードディスク暗号化機能により有効になります。

- **すべてのファイルの暗号化**：この項目を選択した場合、リムーバブルドライブに対して指定した暗号化設定で Kaspersky Security Center 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。Kaspersky Endpoint Security は、暗号化が済んでいるファイルの再暗号化は行いません。また、暗号化されたファイルの名前やフォルダー構造を含む、リムーバブルドライブのファイルシステムの暗号化も行われません。

- **新しいファイルのみ暗号化**：この項目をオンにすると、Kaspersky Endpoint Security は、リムーバブルドライブに対して指定した暗号化設定で Kaspersky Security Center ポリシーを適用するときに、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、ポリシーの前回の適用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回の適用後に変更されたファイルだけを暗号化します。

- **リムーバブルドライブ全体の復号化**：この項目をオンにすると、Kaspersky Endpoint Security は、リムーバブルドライブに対して指定した暗号化設定で Kaspersky Security Center ポリシーを適用するときに、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ファイルとリムーバブルドライブのファイルシステムを、以前に暗号化されていれば復号化します。

この暗号化方式は、Kaspersky Endpoint Security のファイル暗号化機能とハードディスク暗号化機能によって可能になります。

- **変更しない**：この項目をオンにすると、Kaspersky Endpoint Security は、リムーバブルドライブに対して指定した暗号化設定で Kaspersky Security Center ポリシーを適用するときに、リムーバブルドライブ上のファイルの暗号化も復号化も行いません。

8. 内容を暗号化するリムーバブルドライブ上のファイルの暗号化ルールを作成します。

9. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

リムーバブルドライブがすでに接続されている場合、Kaspersky Endpoint Security はポリシーの適用後すぐにユーザーに通知を行い、リムーバブルドライブが暗号化ルールの適用を受けるためリムーバブルドライブに保存されているデータが暗号化されることを知らせます。この通知は、ポリシーの適用時にリムーバブルドライブが接続されていない場合は、ユーザーがドライブを接続した時点で行われます。

リムーバブルドライブ上のデータの暗号化について「*変更しない*」ルールが指定されている場合は、ユーザーへの通知が表示されることはありません。

暗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。

また、暗号化操作の確認を指示するメッセージが表示され、次の処理が行われます：

- ユーザーが暗号化に同意する場合は、ポリシー設定に基づいてデータが暗号化されます。

- ユーザーが暗号化を拒否する場合は、データの暗号化は行われず、リムーバブルドライブのファイルへのアクセスが読み取りのみに制限されます。

- ユーザーが暗号化確認のメッセージを無視する場合は、データの暗号化は行われず、リムーバブルドライブのファイルへのアクセスが読み取りのみに制限されます。また、次回に Kaspersky Security Center ポリ

シーが適用されるときまたはリムーバブルドライブが接続されるときに暗号化確認のメッセージが再度表示されます。

リムーバブルドライブ上のデータの暗号化について事前設定を含む Kaspersky Security Center 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策定されます。このため、リムーバブルドライブに対するデータ暗号化の結果は、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。

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外そうとすると、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。

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、リムーバブルドライブの暗号化ルールを追加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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**リムーバブルドライブの暗号化**］サブセクションを選択します。
7. ［**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。

     ［**信頼するデバイスのリストからのデバイスの追加**］ウィンドウが表示されます。
   - 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。

     ［**Kaspersky Security Center リストからのデバイスの追加**］ウィンドウが開きます。
8. 前の手順で［**Kaspersky Security Center のデバイスリストから指定する**］を選択した場合、テーブルに表示するデバイスのフィルタリング設定を指定します。次の手順に従います：
   a. ［**次の属性が定義されているデバイスをリストに表示します**］、［**デバイス種別**］、［**デバイス名**］、［**コンピューター名**］、［**Kaspersky Disk Encryption**］の各パラメータの値を指定します。

b. ［**更新**］をクリックします。

9. ［**デバイス種別**］列で、暗号化ルールの作成対象にするリムーバブルドライブの名前のチェックボックスをオンにします。

10. ［**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。

11. 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。

12. 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。

    すで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。

13. ［**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。

14. ［**OK**］をクリックします。

    作成された暗号化ルールのパラメータを含む行が、［**カスタムルール**］テーブルに表示されます。

15. ［**OK**］をクリックして、変更内容を保存します。

追加されたリムーバブルドライブの暗号化ルールは、変更後の Kaspersky Security Center ポリシーによって管理されているすべて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編集

*リムーバブルドライブの暗号化ルールを編集するには：*

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、リムーバブルドライブの暗号化ルールを編集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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**リムーバブルドライブの暗号化**］サブセクションを選択します。

7. 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。

8. ［**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。
   ［**ルールの設定**］のコンテキストメニューが表示されます。

9. ［**ルールの設定**］のコンテキストメニューで、選択したリムーバブルドライブ上のファイルに対して Kaspersky Endpoint Security が行う処理を選択します。

10. ［**OK**］をクリックして、変更内容を保存します。

変更されたリムーバブルドライブの暗号化ルールが、変更後の Kaspersky Security Center ポリシーによりコントロールされているすべて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の有効化

*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にポータブルモードを有効にするには：*

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、リムーバブルドライブ上の暗号化されたファイルにアクセスするためにポータブルモードを有効に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**リムーバブルドライブの暗号化**］サブセクションを選択します。

7. ［**ポータブルモード**］をオンにします。

   ポータブルモードは、すべてのファイルの暗号化または新しいファイルのみの暗号化で使用できます。

8. ［**OK**］をクリックします。

9. ポリシーを適用します。

   Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

10. Kaspersky Security Center ポリシーが適用されたデバイスにリムーバブルドライブを接続します。

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. ［**OK**］をクリックします。

    Kaspersky Security Center ポリシーで定義されている暗号化ルールに従って、リムーバブルドライブ上のファイルが暗号化されます。暗号化されたファイルへのアクセスに使用す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書き込まれます。

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。

## リムーバブルドライブの復号化

*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、リムーバブルドライブの復号化設定の対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**リムーバブルドライブの暗号化**］サブセクションを選択します。

7. 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。

8. 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。

      ［**ルールの設定**］のコンテキストメニューが表示されます。

c. ［**ルールの設定**］のコンテキストメニューで、［**すべてのファイルの復号化**］項目を選択します。

9. ［OK］をクリックして、変更内容を保存します。

10. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

リムーバブルドライブがすでに接続されている場合、Kaspersky Endpoint Security はポリシーの適用後ユーザーに通知を行い、リムーバブルドライブが暗号化ルールの適用を受けるため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とリムーバブルドライブのファイルシステム（暗号化されている場合）が復号化されることを知らせます。この通知は、ポリシーの適用時にリムーバブルドライブが接続されていない場合は、ユーザーがドライブを接続した時点で行われます。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。

リムーバブルドライブ上のデータの暗号化について事前設定を含む Kaspersky Security Center 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策定されます。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。

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。

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。

# ドライブの暗号化

ワークステーション用の 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と Kaspersky Disk Encryption 技術を使用して暗号化を行えます。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しか使用できません。

このセクションでは、ハードディスクの暗号化についての情報を提供し、Kaspersky Endpoint Security と Kaspersky Endpoint Security コンソールプラグイン使用してハードディスクの暗号化を設定および実行する手順について説明します。

# ドライブの暗号化について

ハードディスク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が判断されます。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および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製品が開始されます。その後、ハードディスク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分かった場合は、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、ハードディスク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、ハードディスク暗号化の前に、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。

ハードディスクの暗号化の開始後、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。

ハードディスクの復号化の進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、次回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、ハードディスクの暗号化を再開します。

ハードディスク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の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、ハードディスクの暗号化を再開します。

ハードディスク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ハードディスク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。

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 のログオ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。

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）（USB）
- SafeNet eToken PRO 72K Java（USB）
- SafeNet eToken PRO 72K Java（スマートカード）
- SafeNet eToken 4100 72K Java（スマートカード）
- SafeNet eToken 5100（USB）
- SafeNet eToken 5105（USB）
- SafeNet eToken 7300（USB）
- EMC RSA SecurID 800 (USB)
- Rutoken EDS（USB）
- Rutoken EDS（Flash）
- Aladdin-RD JaCarta PKI（USB）
- Aladdin-RD JaCarta PKI （スマートカード）
- Athena IDProtect Laser（USB）

- Gemalto IDBridge CT40（リーダー）
- Gemalto IDPrime .NET 511

## Kaspersky Disk Encryption 技術を使用したハードディスクの暗号化

コンピューターのハードディスクを暗号化する前に、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のハードディスクを暗号化すると、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 技術を使用してハードディスクを暗号化するには：*

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、ハードディスクの暗号化の設定対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ドライブの暗号化**］サブセクションを選択します。
7. ［**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。

8. ［**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。

   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。

9. 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。

     すで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。

  この機能は、暗号化されていないデバイスにのみ適用されます。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、［**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. ［**OK**］をクリックして、変更内容を保存します。

11. ポリシーを適用します。

    Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

## BitLocker ドライブ暗号化技術を使用したハードディスクの暗号化

コンピューターのハードディスクを暗号化する前に、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のハードディスクを暗号化すると、ハードディスクが動作しなくなる可能性があります。

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 ドライブ暗号化技術を使用するには、ロールとコンポーネントを追加するウィザードから［**BitLocker ドライブ暗号化**］をインストールする必要がある場合があります。

*BitLocker ドライブ暗号化技術を使用してハードディスクを暗号化するには：*

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、ハードディスクの暗号化の設定対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**ドライブの暗号化**］サブセクションを選択します。

7. ［**暗号化技術**］で、［**BitLocker ドライブ暗号化**］を選択します。

8. ［**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。

9. 起動前環境でタッチスクリーンのキーボードを使用して情報を入力する場合、［**タブレットで起動前のキーボード入力が必要な認証の使用を許可**］をオンにします。

起動前環境で USB キーボードなど別のデータ入力ツールを使用できるデバイスでのみ、この設定をオンにしてください。

10. 次のいずれかの暗号化種別を選択します：

- ハードウェア暗号化を使用するには、［**ハードウェア暗号化を使用**］をオンにします。
- ソフトウェア暗号化を使用するには、［**ハードウェア暗号化を使用**］をオフにします。

11. 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。
- 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。

この機能は、暗号化されていないデバイスにのみ適用されます。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、［**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。

12. BitLocker で暗号化されたハードディスクにアクセスする方法を選択します。

- Trusted Platform Module（TPM）を使用して暗号鍵を保存する場合、［**Trusted Platform Module（TPM）を使用**］をオンにします。
- ハードディスクの暗号化に Trusted Platform Module（TPM）を使用しない場合、［**パスワードを使用**］オプションを選択し、パスワードの最小文字数を［**パスワードの最小文字数**］で指定します。

Windows 7、Windows 2008 R2 および以前のバージョンオペレーティングシステムでは、Trusted Platform Module（TPM）が使用可能であることが必須になっています。

13. 前の手順で［**Trusted Platform Module（TPM）を使用**］を選択した場合、次の手順を実行します：

- ユーザーが暗号鍵にアクセスしようとしたときに暗証番号を要求するよう設定するには、［**暗証番号を使用**］をオンにし、［**暗証番号の最小桁数**］で暗証番号の最小桁数を指定します。
- Trusted Platform Module が搭載されていないコンピューターでパスワードを使用して暗号化ハードディスクにアクセスする場合は、［**Trusted Platform Module（TPM）が使用できない場合、パスワードを使用**］をオンにし、［**パスワードの最小文字数**］でパスワードの最小文字数を指定します。

  この場合、暗号鍵には、［**パスワードを使用**］をオンにしたときと同様にパスワードを使用してアクセスできるようになります。

［**Trusted Platform Module (TPM)が使用できない場合、パスワードを使用**］をオンにせず、Trusted Platform Module も使用できない場合、ハードディスクの暗号化は行われません。

14. ［**OK**］をクリックして、変更内容を保存します。

15. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

Kaspersky Endpoint Security がインストールされているクライアントコンピューターにポリシーを適用すると、次の問い合わせが行われます。

- 暗号化ポリシーがシステムのハードディスクに適用された場合、Trusted Platform Module が使用中であれば暗証番号のウィンドウが表示されます。それ以外は、パスワードを要求するウィンドウが表示され、認証を事前に読み込みます。
- 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基準の互換モードが有効になっている場合、Windows 8 以降のオペレーティングシステムでは USB デバイスの接続を求めるウィンドウが表示され、回復キーのファイルを保存できます。

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 USB 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）。

## 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、暗号化から除外するハードディスクのリストの作成対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ドライブの暗号化**］サブセクションを選択します。
7. ［**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。
8. 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。
      ［**Kaspersky Security Center リストからのデバイスの追加**］ウィンドウが開きます。
   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 Encription**］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。

9. 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。

10. ［**OK**］をクリックして、変更内容を保存します。

## 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、ハードディスクの復号化設定の対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**ドライブの暗号化**］サブセクションを選択します。
7. ［**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。
8. 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**］テーブルに追加します。

このオプションは、Kaspersky Disk Encryption 技術でのみ使用できます。

9. ［OK］をクリックして、変更内容を保存します。

10. ポリシーを適用します。

Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

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、次回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。

## 認証エージェントの管理

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。

場合によっては、ユーザーが認証を受けられないことがあります。たとえば、ユーザーが認証エージェントアカウントの認証情報を忘れた場合や、トークンまたはスマートカードのパスワードを忘れた場合、あるいはトークンまたはスマートカードを紛失した場合は、認証を受けられません。

ユーザーが認証エージェントアカウントの認証情報や、トークンまたはスマートカードのパスワードを忘れてしまった場合は、企業 LAN の管理者に連絡して認証情報を復元してもらうことができます。

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。

## 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。そのためには、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作成コマンド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。

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。

  トークンまたはスマートカードの電子証明書がこの要件を満たしていない場合、管理プラグインは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組み込まず、エラーメッセージを表示します。

- 証明書の目的を定義する `KeyUsage` パラメータの値が、`keyEncipherment` または `dataEncipherment` である。

  トークンまたはスマートカードの電子証明書がこの要件を満たしていない場合、管理プラグインは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組み込み、警告メッセージを表示します。

- 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の要件を満たしていない場合、管理プラグインは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組み込まず、エラーメッセージを表示します。

## 認証エージェントのヘルプメッセージの編集

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。

*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、認証エージェントのヘルプメッセージを編集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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**データ暗号化**］セクションで［**暗号化の共通設定**］サブセクションを選択します。
7. ［**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**］ウィンドウが開きます。
8. 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。

9. 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。
10. ［**OK**］をクリックします。
11. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

## 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）
- ギリシア文字及びコプト文字（0370 ～ 03FF）
- キリール文字（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ファイルは、暗号化されたハードディスク上のデータを復元する必要がある場合に役立ちます。

*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（既定）**：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 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ことがあります。

   - **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ことがあります。

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、またはハードディスクが暗号化中の場合は、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、システム管理者は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。

# 認証エージェントアカウントの管理

認証エージェントアカウントの管理には、次の Kaspersky Security Center ツールを使用できます：

- 認証エージェントアカウントを管理するためのグループタスク。このタスクを使用すると、クライアントコンピューターのグループを対象に、認証エージェントアカウントを管理できます。
- 暗号化（アカウント管理）ローカルタスク。このタスクを使用すると、個々のクライアントコンピューターを対象に、認証エージェントアカウントを管理できます。

*認証エージェントアカウント管理タスクを設定するには：*

1. 認証エージェントアカウントの管理を作成します（ローカルタスクの作成、グループタスクの作成）。
2. ［**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ウィンドウで［**プロパティ**］セクションを開きます。
3. 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を追加します。
4. 認証エージェントアカウントを編集するためのコマンドを追加します。
5. 認証エージェントのユーザーアカウントを削除するためのコマンドを追加します。
6. 必要に応じて、認証エージェントアカウント管理のために追加したコマンドを編集します。そのためには、［**認証エージェントアカウントを管理するためのコマンド**］テーブルでコマンドを選択して［**編集**］をクリックします。
7. 必要に応じて、認証エージェントアカウント管理のために追加したコマンドを削除します。そのためには、［**認証エージェントアカウントを管理するためのコマンド**］テーブルでコマンドを選択して［**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。

8. 変更を保存するには、タスクのプロパティウィンドウで［**OK**］をクリックします。
9. タスクを実行します。

タスクに追加された認証エージェントアカウント管理コマンドが実行されます。

# 認証エージェントアカウント作成のためのコマンドの追加

*認証エージェントアカウント作成のためのコマンドを追加するには：*

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ウィンドウで［**プロパティ**］セクションを開きます。
2. ［**追加**］をクリックし、ドロップダウンリストから［**アカウント追加コマンド**］を選択します。
   ［**ユーザーアカウントの追加**］ウィンドウが表示されます。

3. ［**ユーザーアカウントの追加**］ウィンドウの［**Windows アカウント**］で、認証エージェントアカウント作成のベースにする Microsoft Windows アカウント名を指定します。

   この指定を行うには、アカウント名を手動で入力するか、または［**選択**］をクリックします。

4. Microsoft Windows アカウントの名前を手動で入力した場合は、［**解決**］をクリックして、アカウントのセキュリティ識別子（SID）を特定します。

   ［**解決**］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。

   > 認証エージェントアカウントの作成コマンドを追加するときに Microsoft Windows アカウントの SID を特定するのは、手動で入力した Microsoft Windows アカウントが正しいことを確認するのに便利な方法です。入力した Microsoft Windows のユーザーアカウントが存在しない場合や、信頼できないドメインに属している場合、または暗号化（アカウント管理）タスクの変更対象になっているコンピューター上に存在しない場合は、認証エージェントアカウント管理タスクはエラーで終了します。

5. この認証エージェントを対象に以前に作成され同じ名前が付いたアカウントを、作成されるアカウントと入れ替えるには、［**現在のユーザーアカウントを変更**］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のため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、暗号化（アカウント管理）ローカル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は使用できません。

6. ［**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。

7. 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。

8. 前の手順で［**パスワードベースの認証を有効にする**］をオンにした場合、次の手順を実行します：

   a. ［**パスワード**］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パスワードを入力します。

   b. ［**パスワードの確認**］で、前のステップで入力した認証エージェントアカウントのパスワードを確認します。

   c. 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でユーザーが最初に認証を受ける際に、パスワード変更要求を表示させる場合は、［**初回認証時にパスワードを変更する**］を選択します。
   - そうしない場合、［**パスワードの変更を求めない**］をオンにします。

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。

10. 前の手順で［**証明書ベースの認証を有効にする**］をオンにした場合、［**参照**］をクリックして、［**証明書ファイルを選択**］ウィンドウで、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選択します。

11. 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。

12. 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。

13. ［**ユーザーアカウントの追加**］ウィンドウで［OK］をクリックします。

## 認証エージェントアカウント編集のためのコマンドの追加

*認証エージェントアカウント編集のためのコマンドを追加するには：*

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ウィンドウの［**設定**］セクションで、［**追加**］のコンテキストメニューを開き、［**アカウント編集コマンド**］を選択します。

   ［**ユーザーアカウントの編集**］ウィンドウが開きます。

2. ［**ユーザーアカウントの編集**］ウィンドウの［**Windows アカウント**］で、編集する認証エージェントアカウントを作成した際にベースにした Microsoft Windows アカウントの名前を指定します。この指定を行うには、アカウント名を手動で入力するか、または［**選択**］をクリックします。

3. Microsoft Windows アカウントの名前を手動で入力した場合は、［**解決**］をクリックして、アカウントのセキュリティ識別子（SID）を特定します。

   ［**解決**］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。

   > 認証エージェントアカウントの編集コマンドを追加するときに Microsoft Windows アカウントの SID を特定するのは、手動で入力した Microsoft Windows アカウントが正しいことを確認するのに便利な方法です。入力した Microsoft Windows ユーザーアカウントが存在しない場合や、信頼できないドメインに属している場合、認証エージェントアカウント管理のためのグループタスクはエラーで終了します。

4. ［**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。

5. 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。

6. 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。

7. 前の手順で［**パスワードベースの認証を有効にする**］をオンにした場合、次の手順を実行します：

   a. ［**パスワード**］に、認証エージェントアカウントの新しいパスワードを入力します。

   b. ［**パスワードの確認**］で、前のステップで入力したパスワードを再度入力します。

8. ［**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に関するルールの編集**］をオンにします。

9. 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。

10. 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。

11. 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。

12. 前の手順で［**証明書ベースの認証を有効にする**］をオンにした場合、［**参照**］ボタンをクリックして、［**証明書ファイルを選択**］ウィンドウで、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へのアクセスに関するルールの編集**］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. ［**ユーザーアカウントの編集**］ウィンドウで、［**OK**］をクリックします。

## 認証エージェントアカウント削除のためのコマンドの追加

*認証エージェントアカウント削除のためのコマンドを追加するには：*

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ウィンドウの［**プロパティ**］セクションで、［**追加**］のコンテキストメニューを開き、［**アカウント削除コマンド**］を選択します。

   ［**ユーザーアカウントの削除**］ウィンドウが開きます。

2. ［**ユーザーアカウントの削除**］ウィンドウの［**Windows アカウント**］で、削除する認証エージェントアカウントを作成した際にベースにした Microsoft Windows アカウントの名前を指定します。この指定を行うには、アカウント名を手動で入力するか、または［**選択**］をクリックします。

3. Microsoft Windows アカウントの名前を手動で入力した場合は、［**解決**］をクリックして、アカウントのセキュリティ識別子（SID）を特定します。

   ［**解決**］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。

   > 認証エージェントアカウントの削除コマンドを追加するときに Microsoft Windows アカウントの SID を特定するのは、手動で入力した Microsoft Windows アカウントが正しいことを確認するのに便利な方法です。入力した Microsoft Windows ユーザーアカウントが存在しない場合や、信頼できないドメインに属している場合、認証エージェントアカウント管理のためのグループタスクはエラーで終了します。

4. ［**ユーザーアカウントの削除**］ウィンドウで、［**OK**］をクリックします。

# 認証エージェントのアカウント情報の復元

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*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復元するには：*

1. 暗号化されたハードディスクを備えるコンピューターでは、オペレーティングシステムの読み込み前に認証エージェントが読み込まれます。認証エージェントのインターフェイスで、［**Forgot your Password?**］をクリックして、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プロセスを開始します。

2. 認証エージェントの指示に従い、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復元するための要求を作成します。

3. 要求の内容を、コンピューター名とともに LAN 管理者に伝えます。

4. LAN 管理者が作成してユーザーに提供した応答の各セクションを、認証エージェントアカウントのユーザー名およびパスワード復元要求に入力します。

5. 認証エージェントアカウントの新しいパスワードを入力して確認します。

   認証エージェントアカウントのユーザー名は、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要求に対する応答を使用して定義されます。

認証エージェントアカウントの新しいパスワードを入力して確認すると、そのパスワードが保存され、暗号化されたハードディスクへのアクセス権が付与されます。

# 認証エージェントアカウント情報の復元要求への応答

*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要求に対する応答のユーザーセクションを作成して送信するには：*

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、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要求しているユーザーの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、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要求した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開きます。

5. コンテキストメニューで、［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］を選択します。

   ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウが開きます。

6. ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウで［**認証エージェント**］タブを選択します。

7. ［**使用中の暗号化アルゴリズム**］セクションで、暗号化アルゴリズムの種別を選択します。

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。

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。

    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についてのユーザー要求に対する応答の各セクションの内容が［**アクセスキー**］に表示されます。

11. 応答ブロックの内容をユーザーに提示します。

# データ暗号化の詳細の表示

このセクションでは、データ暗号化の詳細を表示する方法を説明します。

# 暗号化ステータスとは

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：

- *ポリシーが定義されていません*：このコンピューターでは Kaspersky Security Center ポリシーが定義されていません。
- *暗号化 / 復号化*：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または復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。
- *サポートされていません*：このコンピューターでは、データ暗号化機能を使用できません。

# 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、目的の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。

   ［**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す。

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。

   ［**暗号化ステータス**］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、コンピューターのハードディスクの暗号化、およびこのコンピューターに接続されたリムーバブルドライブの暗号化に関する情報をもとに作成されます。

## Kaspersky Security Center の情報ペインでの暗号化統計情報の表示

*Kaspersky Security Center の情報ペインで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開きます。

   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開きます。

   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. ［**情報ペイン**］セクションで、［**追加**］をクリックします。

      ［**新規情報ペイン**］ウィンドウが開きます。

   e. ［**新規情報ペイン**］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。

      暗号化管理のプロパティウィンドウが開きます。

   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。［**新規情報ペイン**］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［**情報ペイン**］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. 次のいずれかの手順を実行します：
   - コンピューターのコンテキストメニューから［**プロテクション**］を選択します。
   - 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の作成**］をクリックします。

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**

- **保存されているデバイスデータの暗号化レポート**
- **ファイルおよびフォルダーの暗号化エラーのレポート**
- **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。

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。

## 制限されたファイル暗号化機能による暗号化ファイルの管理

Kaspersky Security Center ポリシーの適用後、ファイルが暗号化されると、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が Kaspersky Endpoint Security に送信されます。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が削除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。

## Kaspersky Security Center に接続されていない場合の暗号化ファイルへのアクセス

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*Kaspersky Security Center に接続していない場合に暗号化ファイルにアクセスするには：*

1. 必要な暗号化ファイルへのアクセスを試みます。

   ユーザーが Kaspersky Security Center に接続されていない状態でコンピューターのローカルドライブに保存されているファイルへのアクセスを試みると、Kaspersky Endpoint Security はローカルコンピュータードライブに保存されているすべての暗号化ファイルへのアクセス要求を含むファイルを生成します。一方、ユーザーがリムーバブルドライブに保存されているファイルへのアクセスを試みると、Kaspersky Endpoint Security はその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ファイルへのアクセスを要求するファイルを生成します。［**ファイルへのアクセスがブロックされました**］ウィンドウが開きます。

2. 暗号化ファイルへのアクセス要求を含むファイルを、ローカルエリアネットワークの管理者に送信します。そのためには、次のいずれかの操作を行います：

   - 暗号化ファイルへのアクセスを要求するファイルをメールでローカルエリアネットワークの管理者に送信するには、［**メールで送信**］をクリックします。
   - 暗号化ファイルへのアクセスを要求するファイルを保存して、別の方法で LAN 管理者に送信するには、［**保存**］をクリックします。

3. ローカルエリアネットワークの管理者が作成してユーザーに提供しているライセンス情報ファイルを入手します。このファイルで暗号化されたファイルにアクセスできます。

4. 次のいずれかの方法で、暗号化されたファイルのアクセスキーを有効化します：

   - 任意のファイルマネージャーで、暗号化ファイルへのアクセスのためのキーファイルを選択します。このファイルをダブルクリックして開きます。
   - 次の手順に従います：

     a. Kaspersky Endpoint Security のメインウィンドウを開きます。

     b. をクリックします。
     ［**イベント**］ウィンドウが開きます。

     c. ［**ファイルとデバイスへのアクセスステータス**］タブを選択します。
     このタブには、すべての暗号化ファイルアクセス要求のリストが表示されます。

     d. 暗号化ファイルにアクセスするキーファイルの受け取りに使った要求を選択します。

     e. 暗号化ファイルにアクセスするために提供されたキーファイルを読み込むには、［**参照**］をクリックします。
     Microsoft Windows の標準ダイアログ［**アクセスキーファイルの選択**］が開きます。

     f. Microsoft Windows の標準ダイアログ［**アクセスキーファイルの選択**］で、管理者が提供したファイルを選択します。このファイルの拡張子は kesdr であり、ファイル名はアクセス要求ファイルのファイル名と一致します。

     g. ［**開く**］をクリックします。

     h. ［**イベント**］ウィンドウで［OK］をクリックします。

コンピューターのローカルドライブに保存されているファイルへのアクセスを試みているときに暗号化ファイルアクセス要求を含むファイルが生成されると、Kaspersky Endpoint Security はローカルコンピューターのドライブに保存されているすべての暗号化ファイルへのアクセス権を付与します。リムーバブルドライブに保存されているファイルへのアクセスを試みているときに暗号化ファイルのアクセス要求ファイルが生成されると、Kaspersky Endpoint Security はその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ファイルへのアクセス権を付与します。他の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、リムーバブル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。

## Kaspersky Security Center に接続していないユーザーに暗号化ファイルへのアクセスを許可する

*Kaspersky Security Center に接続していないユーザーに暗号化ファイルへのアクセスを許可するには：*

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、暗号化ファイル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が属してい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、暗号化ファイル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デバイスおよびデータへのアクセスを許可する**］を選択します。

   ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウが開きます。
6. ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウで［**暗号化**］タブを選択します。
7. ［**暗号化**］タブで［**参照**］をクリックします。

   Microsoft Windows の標準ダイアログ［**アクセス要求ファイルを選択**］が開きます。
8. ［**アクセス要求ファイルを選択**］ウィンドウで、ユーザーから受け取った要求ファイルのパスを指定して［**開く**］をクリックします。

   Kaspersky Security Center が暗号化ファイルアクセスキーファイルを生成します。ユーザーリクエストの詳細は、［**暗号化**］タブに表示されます。
9. 次のいずれかの手順を実行します：

   - 生成されたアクセスキーファイルをメールでユーザーに送る場合は、［**メールで送信**］をクリックします。
   - 暗号化ファイルのアクセスキーファイルを保存して、別の方法でユーザーに配信するには、［**保存**］をクリックします。

## 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、暗号化ファイルアクセス要求メッセージのテンプレート編集の対象に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、［**ポリシー**］タブを選択します。

4. 必要なポリシーを選択します。

5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

6. ［**データ暗号化**］セクションで［**暗号化の共通設定**］サブセクションを選択します。

7. ［**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**］ウィンドウが開きます。

8. 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**］ウィンドウが開きます。［**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を許可する**］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。

9. 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。

10. ［**OK**］をクリックします。

11. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

# 暗号化されたデバイスにアクセスできない場合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 暗号化ポリシーをキャンセルしてください。これにより、ドライブの再暗号化を防ぐことができます。

## 製品のインターフェイスから暗号化デバイスにアクセスする

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*製品のインターフェイスから暗号化デバイスにアクセスするには：*

1. 目的の暗号化デバイスへのアクセスを試みます。
   ［**ファイル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。

2. 暗号化されたデバイスに対する拡張子が kesdc のアクセス要求ファイルを、企業 LAN の管理者に送信します。そのためには、次のいずれかの操作を行います：

   - 暗号化されたデバイスに対して生成したアクセス要求ファイルを企業 LAN の管理者にメールで送信するには、［**メールで送信**］をクリックします。
   - 暗号化されたデバイスへのアクセス要求ファイルを保存して別の方法で企業 LAN の管理者に送信するには、［**保存**］をクリックします。

   アクセス要求ファイルの保存や、アクセス要求ファイルを企業 LAN の管理者に送信せずに［**ファイルへのアクセスがブロックされました**］ウィンドウを閉じた場合、これらの操作は［**イベント**］ウィンドウの［**ファイルとデバイスへのアクセスステータス**］タブでいつでも実行できます。このウィンドウは、メインウィンドウで をクリックすると開きます。

3. 暗号化されたデバイスのアクセスキーファイルを取得し保存します。このファイルは、企業 LAN の管理者によって作成され送信されます。

4. 次のいずれかの方法でアクセスキーを適用して、暗号化されたデバイスにアクセスします：

   - 任意のファイルマネージャーで暗号化されたデバイスのアクセスキーファイルを探し、ダブルクリックで開きます。
   - 次の手順に従います：

     a. Kaspersky Endpoint Security のメインウィンドウを開きます。

     b. をクリックすると、［**イベント**］ウィンドウが開きます。

     c. ［**ファイルとデバイスへのアクセスステータス**］タブを選択します。
     このタブには、暗号化されたファイルおよびデバイスに対するすべてのアクセス要求のリストが表示されます。

     d. 暗号化されたデバイスへのアクセスキーファイルを受信した要求を選択します。

     e. 受信したアクセスキーファイルを読み込むには、［**参照**］をクリックします。
     Microsoft Windows の標準ダイアログ［**アクセスキーファイルの選択**］が開きます。

     f. Microsoft Windows の標準ダイアログ［**アクセスキーファイルの選択**］で、管理者から提供されたファイルを選択します。このファイルの拡張子は kesdr で、ファイル名は暗号化されたデバイスのアクセス要求ファイルのファイル名と一致します。

     g. ［**開く**］をクリックします。

     h. ［**ファイルとデバイスへのアクセスステータス**］ウィンドウで、［OK］をクリックします。

Kaspersky Endpoint Security によって、暗号化された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へのアクセス権の付与

*暗号化されたデバイスへのアクセス権を付与するには：*

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、暗号化されたデバイス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が属してい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、暗号化デバイス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デバイスおよびデータへのアクセスを許可する**］を選択します。

   ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウが開きます。
6. ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウで［**暗号化**］タブを選択します。
7. ［**暗号化**］タブで［**参照**］をクリックします。

   Microsoft Windows の標準ダイアログ［**アクセス要求ファイルを選択**］が開きます。
8. ［**アクセス要求ファイルを選択**］ウィンドウで、ユーザーから送信された拡張子が kesdc の要求ファイルのパスを指定します。
9. ［**開く**］をクリックします。

   暗号化されたデバイスのアクセスキーファイルが生成されます。このファイルの拡張子は kesdr です。ユーザーリクエストの詳細は、［**暗号化**］タブに表示されます。
10. 次のいずれかの手順を実行します：

    - 生成されたアクセスキーファイルをメールでユーザーに送る場合は、［**メールで送信**］をクリックします。
    - 暗号化されたドライブのアクセスキーファイルを保存して、別の方法でユーザーに配信するには、［**保存**］をクリックします。

## BitLocker で暗号化されたハードディスクの回復キーをユーザーに提供

*BitLocker を使用して暗号化されたシステムハードディスクの回復キーをユーザーに送信するには：*

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、暗号化されたドライブ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が属してい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、暗号化されたドライブ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ます。

5. 右クリックしてコンテキストメニューを開き、［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］を選択します。

   ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］ウィンドウが開きます。

6. ［**オフラインモードでのデバイスおよびデータへのアクセスを許可する**］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 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。

8. ［**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。

*BitLocker を使用して暗号化されたシステムハードディスク以外のハードディスクの回復キーをユーザーに送信するには：*

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**］ - ［**データ暗号化と保護機能**］ - ［**暗号化されたデバイス**］フォルダーを選択します。

   作業領域に、暗号化されたデバイスのリストが表示されます。

3. 作業領域で、アクセスを復元する必要がある暗号化されたデバイスを選択します。

4. 右クリックしてコンテキストメニューを表示し、［**指定の暗号化されたデバイスのアクセスキーを取得**］を選択します。

   ［**BitLocker で暗号化されたディスクへのアクセスを復元**］ウィンドウが開きます。

5. BitLocker パスワード入力ウィンドウに示されている回復キー 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。

6. ［**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。

## 復元ツールの実行可能ファイルの作成

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*復元ツールの実行ファイルを作成するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの左下にある をクリックし、［**サポート**］ウィンドウを開きます。
3. ［**サポート**］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。
4. 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。
   ［**スタンドアロン復元ツールの作成**］ウィンドウが表示されます。
5. ［**保存先**］に、復元ツールの実行ファイルの保存先となるフォルダーのパスを入力するか、［**参照**］をクリックします。
6. ［**スタンドアロン復元ツールの作成**］ウィンドウの［**OK**］をクリックします。
   選択したフォルダーに、復元ツールの実行ファイル（fdert.exe）が保存されます。

## 暗号化されたデバイスのデータの復元ツールによる復元

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*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. 次のいずれかの方法で復元ツールを実行します：
   - Kaspersky Endpoint Security のメインウィンドウで をクリックして［**サポート**］ウィンドウを開き、［**暗号化されたデバイスの復元**］をクリックします。
   - 復元ツールの実行ファイル fdert.exe が起動します。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の［**デバイスの選択**］で、アクセス権を復元する対象の暗号化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求められます。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求められます。
4. 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収集速度が速くなります。
5. 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。
   ［**デバイスのロック解除設定**］または［**デバイスの復号化設定**］ウィンドウが表示されます。
6. 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：

a. ［**認証エージェントアカウント設定の使用**］を選択します。

b. ［**ユーザー名**］および［**パスワード**］で、認証エージェントアカウントの認証情報を指定します。

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。

7. アクセスキーを使用してデータを復元する場合：

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**］をクリックします。

c. ［**デバイスアクセスキーの取得**］ウィンドウが表示されます。

d. ［**保存**］をクリックして、拡張子が fdertc のアクセス要求ファイルを保存するフォルダーを選択します。

e. 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。

f. 企業 LAN の管理者によって作成および提供されたアクセスキーファイルを取得し保存します。

g. ［**読み込み**］をクリックして、表示されるウィンドウで拡張子が fdertr のアクセスキーファイルを選択します。

8. デバイスを復号化する場合は、［**デバイスの復号化設定**］ウィンドウで他の復号化設定も指定する必要があります。次の手順に従います：

- 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、［**開始**］と［**終了**］に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、［**復号化後にデータをファイルに保存**］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、［**復号化後にデータをファイルに保存**］をオンにし、データの保存先のパスを［**参照**］から指定します。

9. ［**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。

## 暗号化されたデバイスのデータの復元を求めるユーザーからの要求に対する対応

*暗号化されたデバイスにアクセスするためのキーファイルを作成してユーザーに提供するには：*

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**］ - ［**データ暗号化と保護機能**］ - ［**暗号化されたデバイス**］フォルダーを選択します。
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［**指定の暗号化されたデバイスのアクセスキーを取得**］を選択します。

   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**］ - ［**暗号化とデータの保護**］を選択し、作業領域で［**デバイスの暗号鍵を取得**］をクリックしてください。

   ［**デバイスへのアクセスを許可**］ウィンドウが表示されます。
4. 使用されている暗号化アルゴリズムを選択します。次の中からいずれかを選択します：
   - **AES256**：デバイスの暗号化が行われたコンピューターのフォルダー aes256 にある配布パッケージから Kaspersky Endpoint Security がインストールされた場合。
   - **AES56**：デバイスの暗号化が行われたコンピューターのフォルダー aes56 にある配布パッケージから Kaspersky Endpoint Security がインストールされた場合。
5. ［**参照**］をクリックします。

   Microsoft Windows の標準ダイアログ［**アクセス要求ファイルを選択**］が開きます。
6. ［**アクセス要求ファイルを選択**］ウィンドウで、ユーザーから受け取った要求ファイル（拡張子 fdertc）のパスを指定します。
7. ［**開く**］をクリックします。

   暗号化されたデバイスへのアクセスに使用するアクセスキーファイル（拡張子 fdertr）が生成されます。
8. 次のいずれかの手順を実行します：
   - 生成されたアクセスキーファイルをメールでユーザーに送る場合は、［**メールで送信**］をクリックします。
   - 暗号化されたドライブのアクセスキーファイルを保存して、別の方法でユーザーに配信するには、［**保存**］をクリックします。

# 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。

## 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。

# ネットワークプロテクション

このセクションでは、ネットワークトラフィックの監視方法および監視対象のネットワークポートの設定方法について説明します。

## ネットワークプロテクションについて

Kaspersky Endpoint Security の動作中に、メールアンチウイルス、ウェブアンチウイルス、メッセンジャーアンチウイルスなどのコンポーネントは、特定のプロトコルで送信され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、メールアンチウイルスは SMTP を使用して送信されるデータをスキャンしますが、ウェブアンチウイルスは HTTP または FTP を使用して送信されるデータをスキャンします。

Kaspersky Endpoint Security では、危険にさらされる可能性に応じて、オペレーティングシステムの TCP ポートと UDP ポートをいくつかのグループに分類しています。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。これらのポートは攻撃される可能性が大きいため、徹底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、メールアンチウイルス、ウェブアンチウイルス、およびメッセンジャーアンチウイルスの各コンポーネント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われます。

## ネットワークトラフィックの監視の設定

次の操作を実行して、ネットワークトラフィックの監視についての設定を行うことができます：

- 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

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**ネットワークポート**］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. 変更を保存するには［**保存**］をクリックします。

# 監視対象ネットワークポートのリストの作成

*監視されているネットワークポートのリストを作成するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**ネットワークポート**］セクションで、［**設定したネットワークポートのみを監視する**］を選択します。
4. ［**設定**］をクリックします。
   ［**監視するネットワークポート**］ウィンドウが開きます。［**監視する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。
5. ネットワークポートのリストで、次の手順を実行します：
   - 監視されているネットワークポートのリストに含めるネットワークポートのチェックボックスをオンにします。
     既定では、［**監視するネットワークポート**］ウィンドウにリスト表示されているネットワークポートのチェックボックスがすべてオンになっています。
   - 監視されているネットワークポートのリストから除外するネットワークポートのチェックボックスをオフにします。
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. ネットワークポートのリストで、［**追加**］をクリックして、［**ネットワークポートの編集**］ウィンドウを開きます。
   b. ［**ポート**］に、ネットワークポート番号を入力します。
   c. ［**説明**］に、ネットワークポートの名前を入力します。
   d. ［**OK**］をクリックします。
      ［**ネットワークポートの編集**］ウィンドウが閉じます。新しく追加されたネットワークポートがネットワークポートリストの一番下に表示されます。
7. ［**監視するネットワークポート**］ウィンドウで［**OK**］をクリックします。
8. 変更を保存するには［**保存**］をクリックします。

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。そのような接続を保護するには、［**ネットワークポート**］セクションの［**すべてのネットワークポートを監視する**］をオンにするか、FTP 接続を確立するアプリケーションのすべてのポートに対する監視を設定します。

# 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**ネットワークポート**］セクションで、［**設定したネットワークポートのみを監視する**］を選択します。
4. ［**設定**］をクリックします。
   ［**監視するネットワークポート**］ウィンドウが開きます。
5. ［**選択したアプリケーションのすべてのネットワークポートを監視する**］をオンにします。
6. ［**選択したアプリケーションのすべてのネットワークポートを監視する**］の下にあるアプリケーションのリストで、次の手順を実行します：
   - 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名前横にあるチェックボックスをオンにします。
     既定では、［**監視するネットワークポート**］ウィンドウにリスト表示されているすべてのアプリケーション横にあるチェックボックスがオンにされています。
   - すべてのネットワークポートを監視しないアプリケーションの名前横にあるチェックボックスをオフにします。
7. 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. アプリケーションのリストの下にある［**追加**］をクリックし、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、アプリケーションをリストに追加する方法を選択します。
      - 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リストからアプリケーションを選択するには、［**アプリケーション**］を選択します。［**アプリケーションの選択**］ウィンドウが開きます。このウィンドウで、アプリケーションの名前を指定します。
      - アプリケーションの実行ファイルの場所を指定するには、［**参照**］を選択します。Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが開きます。このウィンドウで、アプリケーションの実行ファイルの名前を指定します。

      アプリケーションを選択すると、［**アプリケーション**］ウィンドウが開きます。
   c. ［**名前**］に、選択したアプリケーションの名前を入力します。

d. ［**OK**］をクリックします。

［**アプリケーション**］ウィンドウが閉じます。追加したアプリケーションがアプリケーションのリストの一番下に表示されます。

8. ［**監視するネットワークポート**］ウィンドウで［**OK**］をクリックします。

9. 変更を保存するには［**保存**］をクリックします。

# 定義データベースとソフトウェアモジュールのアップデート

このセクションでは、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に関する情報と、アップデートの設定方法について説明します。

## 定義データベースとソフトウェアモジュールのアップデートの概要

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、接続設定を調整する必要があります。

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。保護コンポーネントは、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 定義データベースの現在のステータスに関する情報は、メインウィンドウの［**プロテクションとコントロール**］タブの［**タスク**］セクションにある［**アップデート**］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。

## アップデート元の概要

「*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。

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。

## アップデートの設定

アップデートの設定を行うには、次の操作を実行します：

- 新しいアップデート元を追加する。

  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。

  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次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。

  > LAN の外部にあるリソースをアップデート元として選択した場合、アップデートの実行時にインターネットに接続する必要があります。

- カスペルスキーのアップデートサーバーの地域を選択する。

  カスペルスキーのアップデートサーバーをアップデート元として使用する場合、アップデートパッケージのダウンロードに使用するカスペルスキーのアップデートサーバーの場所を選択できます。カスペルスキーのアップデートサーバーはいくつかの国に設置されています。最も近いカスペルスキーのアップデートサーバーを使用することにより、アップデートパッケージの取得に必要な時間を短縮することができます。

  既定では、オペレーティングシステムのレジストリにある現在の地域に関する情報が使用されます。

- 共有フォルダーから Kaspersky Endpoint Security のアップデートするための設定を行う。

  インターネットトラフィックの増加を抑えるために、LAN 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 Kaspersky Endpoint Security アップデートを設定できます。これを行うには、LAN 上のいずれかのコンピューターで Kaspersky Security Center 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最新のアップデートパッケージを受け取り、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。

- アップデートタスクの実行方法を選択する。

  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［**カスタム**］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。

- 別のユーザーアカウントの権利でアップデートタスクが実行されるように設定する。

## アップデート元の追加

*アップデート元を追加するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。
3. ［**実行方法とアップデート元**］セクションで、［**アップデート元**］をクリックします。
   ［**アップデート**］ウィンドウに［**ソース**］タブが表示されます。
4. ［**ソース**］タブで［**追加**］をクリックします。
   ［**アップデート元の選択**］ウィンドウが開きます。
5. ［**アップデート元の選択**］ウィンドウで、アップデートパッケージのあるフォルダーを選択するか、［**パス**］にフォルダーの完全パス名を入力します。
6. ［**OK**］をクリックします。
7. ［**アップデート**］ウィンドウで、［**OK**］をクリックします。
8. 変更を保存するには［**保存**］をクリックします。

## アップデートサーバーの地域の選択

*アップデートサーバーの地域を選択するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。
3. ［**実行方法とアップデート元**］セクションで、［**アップデート元**］をクリックします。
   ［**アップデート**］ウィンドウに［**ソース**］タブが表示されます。
4. ［**ソース**］タブの［**地域の設定**］セクションで、［**リストから選択**］を選択します。
5. ドロップダウンリストから、現在地に最も近い国を選択します。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

# 共有フォルダーからのアップデートの設定

共有フォルダーから Kaspersky Endpoint Security をアップデートするための設定を行うには、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. 特定の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 Kaspersky Endpoint Security をアップデート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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。
3. ［**詳細**］セクションで、［**アップデートをフォルダーにコピー**］をオンにします。
4. アップデートパッケージを保存する共有フォルダーのパスを指定します。それには、次のいずれかの方法があります：
   - ［**アップデートをフォルダーにコピー**］の下のフィールドに、アップデートフォルダーのパスを入力します。
   - ［**参照**］をクリックします。［**フォルダーの選択**］ウィンドウが開いたら、必要なフォルダーを選択して、［OK］をクリックします。
5. 変更を保存するには［**保存**］をクリックします。

*共有フォルダーから Kaspersky Endpoint Security をアップデートするための設定を行うには*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。
3. ［**実行方法とアップデート元**］セクションで、［**アップデート元**］をクリックします。
   ［**アップデート**］ウィンドウに［**ソース**］タブが表示されます。
4. ［**ソース**］タブで［**追加**］をクリックします。
   ［**アップデート元の選択**］ウィンドウが開きます。
5. ［**アップデート元の選択**］ウィンドウで、アップデートパッケージが保存されている共有フォルダーを選択するか、［**パス**］に共有フォルダーへの完全パスを入力します。
6. ［OK］をクリックします。
7. ［**ソース**］タブで、共有フォルダーとして指定していないアップデート元の名前の横にあるチェックボックスをオフにします。

8. ［**OK**］をクリックします。

9. 変更を保存するには［**保存**］をクリックします。

## アップデートタスクの実行方法の選択

*アップデートタスクの実行方法を選択するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。

3. ［**実行方法**］をクリックします。
   ［**アップデート**］ウィンドウに［**実行方法**］タブが表示されます。

4. ［**実行方法**］セクションで、アップデートタスクを開始するための次のオプションのいずれかを選択します：

   - 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開始スケジュールを設定するには、［**カスタム**］を選択します。

5. 次のいずれかの手順を実行します：

   - ［**自動開始**］または［**手動開始**］を選択した場合は、手順 6 に進みます。

   - ［**カスタム**］を選択した場合は、アップデートタスクの実行スケジュールの設定を指定します。次の手順に従います：

     a. ［**頻度**］ドロップダウンリストで、アップデートタスクの開始スケジュールを指定します。次のいずれかのオプションを選択します：［**分ごと**］、［**時間ごと**］、［**日ごと**］、［**毎週**］、［**1回のみ**］、［**毎月**］、［**本製品の起動後**］

     b. ［**頻度**］ドロップダウンリストで選択した項目に応じて、アップデートタスクの開始時間を定義する設定値を指定します。

     c. ［**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。

     ［**頻度**］ドロップダウンリストで［**本製品の起動後**］を選択した場合、［**本製品の起動からタスク開始までの時間**］は無効になります。

     d. Kaspersky Endpoint Security で、スキップされたアップデートタスクをすぐに実行するには、［**スキップしたスケジュールタスクを後で実行する**］をオンにします。

［**頻度**］ドロップダウンリストで［**時間ごと**］、［**分ごと**］、または［**本製品の起動後**］を選択した場合、［**スキップしたスケジュールタスクを後で実行する**］は無効になります。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 別のユーザーアカウントの権利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（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）、または認証プロキシサーバーユーザーの権利がないことが原因でアクセスできないアップデート元からアップデートすることができます。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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。

3. ［**実行方法とアップデート元**］セクションで、［**実行方法**］をクリックします。
   ［**アップデート**］ウィンドウに［**実行方法**］タブが表示されます。

4. ［**実行方法**］タブの［**ユーザー**］セクションで、［**他のユーザーでタスクを実行する**］をオンにします。

5. ［**ユーザー名**］に、アップデート元にアクセスするのに使用する権限のあるユーザーアカウントの名前を入力します。

6. ［**パスワード**］に、アップデート元にアクセスするのに使用する権限のあるユーザーのパスワードを入力します。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## ソフトウェアモジュールのアップデートの設定

*ソフトウェアモジュールのアップデートを設定するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。

3. ［**詳細**］セクションで、次のいずれかの操作を行います：

   - 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を含める場合は、［**ソフトウェアモジュールのアップデートをダウンロード**］をオンにします。

   - そうしない場合、［**ソフトウェアモジュールのアップデートをダウンロード**］をオフにします。

4. 前のステップで［**ソフトウェアモジュールのアップデートをダウンロード**］がオンにした場合は、ソフトウェアモジュールのアップデートをインストールする条件を指定します。

   - 本製品の重要なアップデートモジュールを自動的にインストールし、その他のアップデートは、インストールの承認を本製品のインターフェイスからローカルで行うか Kaspersky Security Center を使用して行った後でインストールするには、［**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**］を選択します。

   - インストールの承認を本製品のインターフェイスからローカルで行うか Kaspersky Security Center を使用して行った後でソフトウェアモジュールのアップデートをインストールするには、［**承認済みのアップデートのみをインストール**］を選択します。

5. 変更を保存するには［**保存**］をクリックします。

## 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。

カスペルスキーのサーバーからアップデートパッケージをダウンロードするには、インターネット接続が必要です。

*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. メインウィンドウを開きます。

2. ［**プロテクションとコントロール**］タブを選択します。

3. ［**タスク**］セクションをクリックします。
   ［**タスク**］セクションが開きます。

4. 右クリックして、アップデートタスク名が含まれる行のコンテキストメニューを表示します。
   この行をクリックすると、アップデートタスクで実行可能な処理のメニューが開きます。

5. 次のいずれかの手順を実行します：

   - アップデートタスクを開始する場合は、メニューから［**アップデートの実行**］を選択します。
     ［**アップデート**］の右側に表示されているアップデートタスクの進捗ステータスが［*実行中*］に変わります。

   - アップデートタスクを停止する場合は、メニューから［**アップデートの停止**］を選択します。
     ［**アップデート**］の右側に表示されているアップデートタスクの進捗ステータスが［*停止*］に変わります。

# 前回のアップデートへのロールバック

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（戻す）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. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**タスク**］セクションをクリックします。
   ［**タスク**］セクションが開きます。
4. ［**アップデート**］タスクを右クリックして、コンテキストメニューを表示します。
5. ［**アップデートのロールバック**］を選択します。

# プロキシサーバーの設定

*プロキシサーバーを設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**アップデート**］を選択します。
   ウィンドウの右側に、製品のアップデート設定が表示されます。
3. ［**プロキシサーバー**］セクションで、［**設定**］をクリックします。
   ［**プロキシサーバー設定**］ウィンドウが開きます。
4. ［**プロキシサーバー設定**］ウィンドウで、［**プロキシサーバーを使用する**］をオンにします。
5. プロキシサーバーの設定を指定します。
6. ［OK］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

プロキシサーバーは、メインウィンドウの［**設定**］タブの［**詳細設定**］セクションで設定することもできます。

# 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実行することで、セキュリティレベルの設定が低いなどの理由により、保護コンポーネント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。

このセクションでは、スキャンタスクの詳細と設定、セキュリティレベル、スキャン方式、テクノロジーについて説明します。また、Kaspersky Endpoint Security がスキャン中に処理しなかったファイルの処理方法についても説明します。

## スキャンタスクの概要

ウイルスやその他のマルウェアを検知して、ソフトウェアモジュールの統合性をチェックするために、Kaspersky Endpoint Security では次のタスクを実行します：

- **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 は、次のオブジェクトを既定でスキャンします：
  - カーネルメモリー
  - 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
- **簡易スキャン**：既定では、カーネルメモリー、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。
- **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：
  - カーネルメモリー
  - 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
  - メール
  - すべてのハードディスクドライブ、リムーバブルディスク、ネットワークドライブ
  - 選択した任意のファイル
- **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。

完全スキャンタスクと簡易スキャンタスクは、他のスキャンタスクとやや異なります。この 2 つのスキャンタスクでは、スキャン範囲を編集することは推奨されません。

スキャンタスクを開始すると、進捗状況が、実行中のスキャンタスク名の隣にあるフィールドに表示されます。このフィールドは Kaspersky Endpoint Security メインウィンドウの［**プロテクションとコントロール**］タブの［**タスク**］セクション内にあります。

スキャンタスクの実行中に発生したスキャン結果およびイベントに関する情報は、Kaspersky Endpoint Security レポートに記録されます。

## スキャンタスクの開始または停止

スキャンタスクは、選択したスキャンタスク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。

*スキャン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. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**タスク**］セクションをクリックします。
   ［**タスク**］セクションが開きます。
4. 右クリックして、スキャンタスク名が含まれる行のコンテキストメニューを表示します。
   スキャンタスク処理のメニューが開きます。
5. 次のいずれかの手順を実行します：

   - スキャンタスクを開始する場合は、メニューから［**スキャンの開始**］を選択します。
     このスキャンタスクの名前を持つボタンの右側に表示されるタスク進捗ステータスが［*実行中*］に変わります。
   - スキャンタスクを停止する場合は、メニューから［**スキャンの停止**］を選択します。
     このスキャンタスクの名前を持つボタンの右側に表示されるタスク進捗ステータスが［*停止*］に変わります。

## スキャンタスクの設定

スキャンタスクの設定を行うには、次の手順に従います：

- セキュリティレベルを変更します。
  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。
- Kaspersky Endpoint Security が感染したファイルを検知した場合に実行する処理を変更します。
- スキャン範囲を編集します。
  スキャン範囲を拡張または制限するには、スキャンオブジェクトを追加または削除するか、スキャン対象のファイルの種類を変更します。
- スキャンを最適化します。

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後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、単一のファイルを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）。

また、iChecker テクノロジーと 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。

- 複合ファイルのスキャンを設定します。
- スキャン方法を使用するかどうかを設定します。

  有効になっている場合、Kaspersky Endpoint Security は、シグネチャ分析を使用します。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従い、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。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オブジェクト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レコードが存在しない悪意のあるオブジェクトを検知できます。

- スキャンタスクの実行方法を選択します。

  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。

  アップデートタスクの実行方法に［**カスタム**］を選択した場合、および Kaspersky Endpoint Security の開始時間とスキャンタスクの実行スケジュールが一致する場合は、製品が開始されるまでスキャンタスクの開始を延期することができます。スキャンタスクは、Kaspersky Endpoint Security が起動して、指定の時間が経過した後にのみ実行できます。

- 別のユーザーアカウントでスキャンタスクが実行されるように設定します。
- リムーバブルドライブの接続時に、そのドライブがスキャンされるように設定します。

## セキュリティレベルの変更

Kaspersky Endpoint Security では、スキャンタスクを実行するためにさまざまな設定の組み合わせを使用します。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は、「*セキュリティレベル*」と呼ばれます。セキュリティレベルには［**高**］、［**推奨**］、［**低**］の 3 種類があらかじめ設定されています。［**推奨**］セキュリティレベルが最適な設定です。これはカスペルスキーによって推奨されています。

*セキュリティレベルを変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。
3. ［**セキュリティレベル**］セクションで、次のいずれかを実行します：

   - 事前に設定されているセキュリティレベル（［**高**］、［**推奨**］、または［**低**］）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。

- カスタムセキュリティレベルを設定する場合は、［**設定**］をクリックして、表示されるウィンドウで目的のスキャンタスク名の設定を指定します。

  カスタムのセキュリティレベルを設定すると、［**セキュリティレベル**］セクションのセキュリティレベルの名前が［**カスタム**］に変更されます。

- セキュリティレベルを［**推奨**］に変更する場合は、［**既定**］をクリックします。

4. 変更を保存するには［**保存**］をクリックします。

## 感染したファイルに対する処理の変更

*感染したファイルに対する処理を変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。
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。
   - **自動処理**：
   - **次の処理を常に実行**
4. 前の手順で［**次の処理を常に実行**］を選択した場合、以下のチェックボックスを設定します：
   - 脅威が検知されたオブジェクトを駆除する場合、［**駆除する**］をオンにします。

     > このオプションが選択されている場合でも、Kaspersky Endpoint Security は［**削除する**］の処理を Windows ストアアプリの一部であるファイルに適用します。

   - 脅威が検知されたオブジェクトを削除する場合、［**削除する**］をオンにします。
   - 脅威が検知されたオブジェクトの駆除を試み、駆除できないオブジェクトを削除する場合、［**駆除する**］と［**駆除できない場合は削除する**］の両方をオンにします。
   - 脅威が検知されたオブジェクトを処理せず、単にオブジェクトのスキャン結果を通知する場合、［**駆除する**］と［**削除する**］の両方をオフにします。
5. 変更を保存するには［**保存**］をクリックします。

## スキャンするオブジェクトのリストの生成

スキャンするオブジェクトのリストを生成するには、次の 2 つの方法があります：

- メインウィンドウの［**プロテクションとコントロール**］タブから

- 製品の設定ウィンドウから

この方法は、［**完全スキャン**］および［**簡易スキャン**］タスクでのみ使用できます。［**オブジェクトスキャン**］タスクのスキャン対象オブジェクトのリストは、［**プロテクションとコントロール**］タブでのみ作成できます。

*メインウィンドウの［プロテクションとコントロール］タブで、スキャンするオブジェクトのリストを作成するには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**タスク**］セクションをクリックします。
   ［**タスク**］セクションが開きます。
4. タスク名の行を右クリックしてコンテキストメニューを開き、［**スキャン範囲**］を選択します。
   ［**スキャン範囲**］ウィンドウが開きます。
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。
      ［**スキャン範囲を選択**］ウィンドウが開きます。
   b. オブジェクトを選択して［**追加**］をクリックします。
      ［**スキャン範囲を選択**］ウィンドウで選択したすべてのオブジェクトが、［**スキャン範囲**］リストに表示されます。
   c. ［**OK**］をクリックします。
6. スキャン範囲にあるオブジェクトのパスを変更するには：
   a. スキャン範囲にあるオブジェクトを選択します。
   b. ［**編集**］をクリックします。
      ［**スキャン範囲を選択**］ウィンドウが開きます。
   c. スキャン範囲にあるオブジェクトの新しいパスを入力します。
   d. ［**OK**］をクリックします。
7. スキャン範囲からオブジェクトを削除するには：
   a. スキャン範囲から削除するオブジェクトを選択します。
      複数のオブジェクトを選択するには、**CTRL** キーを押しながら選択します。
   b. [**削除**］をクリックします。
      削除を確認するウィンドウが開きます。
   c. 削除を確認するウィンドウで［**はい**］をクリックします。

既定でスキャン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。

8. スキャン範囲からオブジェクトを除外するには、［**スキャン範囲**］ウィンドウで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。

   オブジェクトはスキャン範囲のオブジェクトリストに残りますが、スキャンタスクが実行されてもスキャンされません。

9. ［**OK**］をクリックします。

10. 変更を保存するには［**保存**］をクリックします。

*製品の設定ウィンドウからスキャンするオブジェクトのリストを作成するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前を持つサブセクション（［**完全スキャン**］、［**簡易スキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**スキャン範囲**］をクリックします。

   ［**スキャン範囲**］ウィンドウが開きます。

4. 上記手順 5 ～ 10 の設定に従ってスキャンするオブジェクトのリストを作成します。

## スキャンするファイルの種別の選択

スキャンするファイルの種別を選択するには、次の 2 つの方法があります：

- メインウィンドウの［**プロテクションとコントロール**］タブから
- 製品の設定ウィンドウから

この方法は、［**完全スキャン**］および［**簡易スキャン**］タスクでのみ使用できます。［**オブジェクトスキャン**］タスクでスキャンするファイルの種別は、［**プロテクションとコントロール**］タブでのみ選択できます。

*メインウィンドウの［プロテクションとコントロール］タブで、スキャンするファイルの種別を作成するには：*

1. メインウィンドウを開きます。

2. ［**プロテクションとコントロール**］タブを選択します。

3. ［**タスク**］セクションをクリックします。

   ［**タスク**］セクションが開きます。

4. タスク名の行を右クリックしてコンテキストメニューを開き、［**設定**］を選択します。

   選択したスキャンタスク名のウィンドウが開きます。

5. 選択したスキャンタスク名のウィンドウで、［**全般**］タブを選択します。

6. ［**ファイル種別**］セクションで、選択したスキャンタスクの実行時にスキャンするファイルの種別を指定します。

   - すべてのファイルをスキャンする場合は、［**すべてのファイルをスキャン**］を選択します。
   - 感染に対して最も脆弱な形式のファイルをスキャンする場合は、［**ファイル形式でファイルをスキャン**］を選択します。
   - 感染に対して最も脆弱なことの多い拡張子のファイルをスキャンする場合は、［**拡張子でファイルをスキャン**］を選択します。

   スキャンするファイルの種類を選択するときには、次の点に留意してください：

   - 悪意のあるコードの侵入とその後の有効化の確率が低い形式のファイル（TXT など）があります。一方で、実行コードを含んでいるか含んでいる可能性がある形式のファイル（exe、dll、doc など）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。
   - 侵入者はウイルスやその他の悪意のあるプログラムの拡張子を 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を選択すると、拡張子に関係なくファイルのヘッダーを分析します。この分析の結果、形式が EXE であることが判明したファイルは、製品によってスキャンされます。

7. スキャンタスクの名前のウィンドウで［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

*製品の設定ウィンドウからスキャンするファイルの種別を作成するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前を持つサブセクション（［**完全スキャン**］、［**簡易スキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**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。

   選択したスキャンタスク名のウィンドウが開きます。

4. 選択したスキャンタスク名のウィンドウで、［**全般**］タブを選択します。

5. 上記手順の 5 ～ 7 を実施します。

## スキャンの最適化

*ファイルスキャンを最適化するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**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。
   選択したスキャンタスク名のウィンドウが開きます。

4. 表示されたウィンドウで、［**全般**］タブを選択します。

5. ［**スキャンの最適化**］セクションで、次の手順を実行します：

   - ［**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。
   - ［**スキャン時間が次を超えたファイルをスキップ**］をオンにして、単一ファイルのスキャン時間を指定します（秒単位）。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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の種別を限定することで、スキャンを高速化できます。

*複合ファイルのスキャンを設定するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。
   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**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。
   選択したスキャンタスク名のウィンドウが開きます。

4. 表示されたウィンドウで、［**全般**］タブを選択します。

5. ［**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をアーカイブファイル、インストールパッケージ、Office 形式のファイル、メール形式のファイル、パスワードで保護されたアーカイブファイルの中から選択します。

6. ［**スキャンの最適化**］セクションの［**作成または更新されたファイルのみスキャン**］をオフにすると、複合ファイルの名前の横にある［**すべての**］ / ［**作成または更新された**］をクリックして、その種別の複合ファイルをすべてスキャンするのか、新しいファイルのみをスキャンするのかを指定できます。
   このリンクをクリックすると、リンクのラベル値が変更されます。
   ［**作成または更新されたファイルのみスキャン**］をオンにすると、新しいファイルのみがスキャンされます。

7. ［**詳細**］をクリックします。

［**複合ファイル**］ウィンドウが開きます。

8. ［**サイズ制限**］セクションで、次のいずれかを実行します：

   - 大きな複合ファイルをスキャンしない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、［**最大サイズ**］に任意の値を入力します。
   - サイズの大きさにかかわらずすべての複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］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。

9. ［**OK**］をクリックします。
10. スキャンタスクの名前のウィンドウで［**OK**］をクリックします。
11. 変更を保存するには［**保存**］をクリックします。

## スキャン方法の使用

*スキャン方法を使用するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。
3. ［**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。

   選択したスキャンタスク名のウィンドウが開きます。
4. 開くウィンドウで、［**詳細**］タブを選択します。
5. スキャンタスクを実行するときに製品で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**］セクションの［**ヒューリスティック分析**］をオンにします。そして、スライダーを使用して、ヒューリスティック分析のレベルを［**低**］、［**中**］、［**高**］のいずれかに設定します。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## スキャン技術の使用

*スキャン技術を使用するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なスキャンタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**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。

   選択したスキャンタスク名のウィンドウが開きます。

4. 開くウィンドウで、［**詳細**］タブを選択します。

5. ［**スキャン技術**］セクションで、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。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## スキャンタスクの実行方法の選択

*スキャンタスクの実行方法を選択するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**実行方法**］をクリックします。

   選択したタスクのプロパティウィンドウが開き、［**実行方法**］タブが表示されます。

4. ［**実行方法**］セクションで、タスクの実行方法を［**手動開始**］または［**カスタム**］から選択します。

5. ［**カスタム**］を選択した場合は、スケジュール設定を指定します。次の手順に従います：

   a. ［**頻度**］ドロップダウンリストで、タスクの実行頻度を選択します（［**分ごと**］、［**時間ごと**］、［**日ごと**］、［**毎週**］、［**1回のみ**］、［**毎月**］、［**本製品の起動後**］、［**アップデート後**］）。

   b. 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。

   c. スキップされたスキャンタスクをできるだけ早く開始するには、［**スキップしたスケジュールタスクを後で実行する**］をオンにします。

   ［**頻度**］ドロップダウンリストで、［**分ごと**］、［**時間ごと**］、［**本製品の起動後**］または［**アップデート後**］を選択した場合、［**スキップしたスケジュールタスクを後で実行する**］は無効になります。

   a. コンピューターのリソースが制限されている場合にタスクを一時停止するには、［**コンピューターを使用していないときのみ実行**］をオンにします。

   このスケジュールオプションは、コンピューターの資源の節約に役立ちます。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 別のユーザーアカウントでのスキャンタスクの起動

既定では、スキャンタスクは、ユーザーがオペレーティングシステムにログインしたアカウントのアクセス権で実行されます。ただし、別のユーザーアカウントでスキャンタスクを実行することが必要になる場合があります。スキャンタスク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。

*別のユーザーアカウントでスキャンタスクを開始するように設定するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、必要なタスクの名前のサブセクション（［**完全スキャン**］、［**簡易スキャン**］、または［**オブジェクトスキャン**］）を選択します。

   ウィンドウの右側に、選択したスキャンタスクの設定が表示されます。

3. ［**実行方法**］をクリックします。

   選択したタスクのプロパティウィンドウが開き、［**実行方法**］タブが表示されます。

4. ［**実行方法**］タブの［**ユーザー**］セクションで、［**他のユーザーでタスクを実行する**］をオンにします。

5. ［**ユーザー名**］に、スキャンタスクを開始するのに使用する権限のあるユーザーアカウントの名前を入力します。

6. ［**パスワード**］に、スキャンタスクを開始するのに使用する権限のあるユーザーのパスワードを入力します。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## コンピューターに接続されたリムーバブルドライブのスキャン

悪意のあるプログラムの中には、オペレーティングシステムの脆弱性を利用して、ローカルネットワークやリムーバブルドライブを介して自己複製するものがあります。Kaspersky Endpoint Security を使用すると、コンピューターに接続されたリムーバブルドライブにウイルスやその他のマルウェアがないかスキャンできます。

*リムーバブルドライブが接続されたときにリムーバブルドライブをスキャンするように設定するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側で、［**スケジュールされているタスク**］セクションを選択します。

   コンポーネントの設定が、ウィンドウの右側に表示されます。

3. ［**リムーバブルドライブの検出時**］セクションで、［**リムーバブルドライブ接続時の処理**］ドロップダウンリストから必要な処理を選択します：

- **スキャンしない**
- **詳細スキャン**

  このモードでは、リムーバブルドライブにあるすべてのファイル（複合オブジェクト内のファイルを含む）をスキャンします。
- **簡易スキャン**

  このモードでは、感染の可能性があるファイルのみをスキャンします。複合オブジェクトは解凍しません。

4. 指定したサイズを越えないリムーバブルドライブのみをスキャンする場合、［**スキャンするドライブの最大サイズ**］をオンにして、横のフィールドに値をメガバイト単位で指定します。
5. 変更を保存するには［**保存**］をクリックします。

# 未処理ファイルの処理

このセクションでは、ウイルスや脅威のスキャン中に、Kaspersky Endpoint Security が処理しなかった感染したファイルおよび感染の可能性があるファイルの処理方法について説明します。

# 未処理ファイルの情報

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、未処理ファイルのリストにイベントの形式で記録されます。

ウイルスなどの脅威の検知のためのコンピュータースキャンの際に、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タースキャンの際に、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、このファイルは「未処理」とみなされます。

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。

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後、未処理ファイルのリスト内のファイルにおいてオブジェクトスキャンタスクを手動で開始できます。スキャンの後、ファイルのステータスが変わることがあります。ファイルのステータスに応じて、必要な処理を実行できます。

たとえば、次の処理を実行できます：

- ステータスが「*感染*」になっているファイルの削除
- 重要情報を含む感染したファイルの復元および「*駆除済み*」または「*感染していません*」とマークされたファイルの復元
- ステータスが「*感染の可能性あり*」になっているファイルの隔離

## 未処理ファイルのリストの管理

未処理ファイルのリストはテーブルの形式で表示されます。

未処理ファイルでは次の操作を実行できます：

- 未処理ファイルのリストを表示する。
- 現在のバージョンの Kaspersky Endpoint Security の定義データベースとモジュールを使用して、未処理ファイルをスキャンする
- 未処理ファイルのリストにあるファイルを元のフォルダーまたは選択した別のフォルダー（元のフォルダーに書き込めない場合）に復元する。
- 未処理ファイルのリストからファイルを削除する。
- 未処理ファイルが保存されていた元のフォルダーを開く。

テーブルのデータを管理しながら、次の処理も実行できます：

- 未処理ファイルイベントを列の値または絞り込み条件でフィルタリングする。
- 未処理ファイルイベントの検索機能を使用する。
- 未処理ファイルのイベントを並べ替える。
- 未処理ファイルのリストに表示される列とその順番を変更する。
- 未処理ファイルのイベントをグループ化する。

必要に応じて、選択した未処理ファイルイベントをクリップボードにコピーできます。

## 未処理ファイルに対するオブジェクトスキャンタスクの開始

未処理ファイルに対し、手動でオブジェクトスキャンタスクを開始できます。たとえば、前回のスキャンが何らかの理由で中断された場合や、Kaspersky Endpoint Security 定義データベースやソフトウェアモジュールの最新のアップデート後に未処理ファイルを再スキャンしたい場合などに、このスキャンを開始できます。

*未処理ファイルのオブジェクトスキャンを開始するには：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**未処理ファイル**］タブを選択します。
4. ［**未処理ファイル**］タブのテーブルで、スキャンするファイルに関するイベントを1つ以上選択します。
   複数のイベントを選択するには、**CTRL** キーを押しながらイベントを選択します。
5. 次のいずれかの方法で、オブジェクトスキャンタスクを開始します：
   - ［**再スキャン**］をクリックします。
   - 右クリックしてコンテキストメニューを表示し、［**再スキャン**］を選択します。

## 未処理ファイルのリストからのファイルの削除

*未処理ファイルのリストからファイルを削除するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**未処理ファイル**］タブを選択します。
4. ［**未処理ファイル**］タブのテーブルで、削除するファイルに関するイベントを1つ以上選択します。
   複数のイベントを選択するには、**CTRL** キーを押しながらイベントを選択します。
5. 次のいずれかの方法で、ファイルを削除します：
   - [**削除**］をクリックします。
   - 右クリックしてコンテキストメニューを表示し、［**削除**］を選択します。

# 脆弱性スキャン

このセクションでは、脆弱性スキャンタスクの詳細と設定、および脆弱性スキャンタスクの実行中に Kaspersky Endpoint Security によって検知される脆弱性のリストの管理方法について説明します。

# 実行アプリケーションの脆弱性に関する情報の表示

実行アプリケーションの脆弱性に関する情報は、ワークステーション用の Microsoft 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。この情報は、サーバー用の Microsoft 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。

*実行アプリケーションの脆弱性に関する情報を表示するには、次の手順を実行します：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**エンドポイントコントロール**］セクションが開きます。
4. ［**アプリケーション動作モニター**］をクリックします。

［**アプリケーション権限コントロール**］ウィンドウが開き、［**アプリケーション動作モニター**］タブが表示されます。［**アプリケーション動作モニター**］の表には、オペレーティングシステムで実行中のアプリケーションの動作の概要が表示されます。脆弱性モニターが判定した、実行アプリケーションの脆弱性の重要度が、［**脆弱性の重要度**］列に表示されます。

# 脆弱性スキャンタスクの概要

オペレーティングシステムの脆弱性は、プログラミングまたは設計上のエラー、強度が低いパスワード、マルウェアの動作などに起因する場合があります。製品は脆弱性のスキャンを実行するときに、オペレーティングシステムを分析し、Microsoft およびその他の開発元のアプリケーションに異常や破損した設定がないか検索します。

脆弱性スキャンはオペレーティングシステムのセキュリティ診断を実行します。また、侵入者が悪意のあるオブジェクトを拡散して個人情報にアクセスするために使用している可能性があるソフトウェアの特徴を検知します。

脆弱性スキャンタスクを開始すると、進捗状況が、Kaspersky Endpoint Security メインウィンドウにある［**プロテクションとコントロール**］タブの、［**タスク**］セクションの［**脆弱性スキャン**］タスク名の横のフィールドに表示されます。

脆弱性スキャンタスクの結果はレポートに記録されます。

# 脆弱性スキャンタスクの開始と終了

脆弱性スキャンタスクは、選択した実行方法に関係なく、いつでも開始または終了することができます。

*脆弱性スキャンタスクを開始または停止するには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**タスク**］セクションをクリックします。
   ［**タスク**］セクションが開きます。
4. 右クリックして、脆弱性スキャンタスク名が含まれる行のコンテキストメニューを表示します。
   脆弱性スキャンタスク操作のメニューが開きます。
5. 次のいずれかの手順を実行します：

   - 脆弱性スキャンタスクを開始するには、メニューで［**スキャンの開始**］を選択します。
     脆弱性スキャンタスクの名前を含むボタンの右側に表示されるタスクの進捗ステータスが、「*実行中*」に変わります。
   - 脆弱性スキャンタスクを停止するには、メニューで［**スキャンの停止**］を選択します。
     脆弱性スキャンタスクの名前を含むボタンの右側に表示されるタスクの進捗ステータスが、「*停止*」に変わります。

## 脆弱性スキャンの設定

脆弱性スキャンの設定では、次の処理を実行できます：

- 脆弱性スキャン範囲を作成する。
  脆弱性をスキャンするアプリケーションを追加または削除することで、スキャン範囲を拡大または縮小できます。
- 脆弱性スキャンタスクの実行方法を選択する。
  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。
- 別のユーザーアカウントの権利でタスクが実行されるように設定する。
  既定では、スキャンタスクは、ユーザーがオペレーティングシステムにログインしたアカウントのアクセス権で実行されます。ただし、別のユーザーアカウントでスキャンタスクを実行することが必要になる場合があります。タスク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タスクを実行できます。

## 脆弱性スキャン範囲の作成

脆弱性スキャン範囲は、ソフトウェア開発元のフォルダー、またはソフトウェアがインストールされているフォルダーのパスです（たとえば、フォルダー Program Files にインストールされているすべての Microsoft アプリケーション）。

*脆弱性スキャン範囲を作成するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**脆弱性スキャン**］を選択します。

   ウィンドウの右側に、脆弱性スキャンタスク設定が表示されます。

3. ［**スキャン範囲**］セクションで、次の手順を実行します：

   a. Kaspersky Endpoint Security を使用して、コンピューターにインストールされている Microsoft アプリケーションの脆弱性を探すには、［**Microsoft**］をオンにします。

   b. コンピューターにインストールされている Microsoft アプリケーション以外のすべてのアプリケーションで脆弱性を、Kaspersky Endpoint Security を使用して検知するには、［**その他の製造元**］をオンにします。

   c. ［**追加の脆弱性スキャン領域**］ウィンドウで、［**設定**］をクリックします。

   ［**脆弱性のスキャン範囲**］ウィンドウが開きます。

   d. ［**追加**］と［**削除**］を使用して脆弱性スキャン範囲を作成します。

   e. ［**脆弱性のスキャン範囲**］ウィンドウで、［**OK**］をクリックします。

4. 変更を保存するには［**保存**］をクリックします。

## 脆弱性スキャンタスクの実行方法の選択

*脆弱性スキャンタスクの実行方法を選択するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**脆弱性スキャン**］を選択します。

   ウィンドウの右側に、脆弱性スキャンタスク設定が表示されます。

3. ［**実行方法**］をクリックします。

   ［**脆弱性スキャン**］ウィンドウの［**実行方法**］タブが表示されます。

4. ［**実行方法**］セクションで、脆弱性スキャンタスクを開始する次の実行方法オプションのいずれかを選択します：

   - 脆弱性スキャンタスクを手動で開始するには、［**手動開始**］を選択します。
   - 脆弱性スキャンタスクの開始スケジュールを設定するには、［**カスタム**］を選択します。

5. 次のいずれかの手順を実行します：

   - ［**手動開始**］を選択した場合は、手順 6 に進んでください。
   - ［**カスタム**］を選択している場合は、脆弱性スキャンタスクの開始設定を指定します。次の手順に従います：

     a. ［**頻度**］ドロップダウンリストで、脆弱性スキャンタスクの開始スケジュールを指定します。次のいずれかのオプションを選択します：［**日ごと**］、［**毎週**］、［**1 回のみ**］、［**毎月**］、［**本製品の起動後**］、［**アップデート後**］。

b. ［**頻度**］ドロップダウンリストで選択した項目に応じて、脆弱性スキャンタスクの開始時間を定義する設定値を指定します。

c. Kaspersky Endpoint Security で、スキップされた脆弱性スキャンタスクをすぐに開始するには、［**スキップしたスケジュールタスクを後で実行する**］をオンにします。

［**頻度**］ドロップダウンリストで［**本製品の起動後**］または［**アップデート後**］を選択した場合、［**スキップしたスケジュールタスクを後で実行する**］はオフになります。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 別のユーザーアカウントの権利での脆弱性スキャンタスクの開始

既定では、脆弱性スキャンタスクは、ユーザーがオペレーティングシステムにログインしたアカウントで開始されます。ただし、別のユーザーアカウントで脆弱性スキャンタスクを開始することが必要になる場合があります。脆弱性スキャンタスクの設定で必要な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脆弱性スキャンタスクを開始できます。

*異なるユーザーアカウントによる脆弱性スキャンタスクの起動を設定するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**脆弱性スキャン**］を選択します。
   ウィンドウの右側に、脆弱性スキャンタスク設定が表示されます。

3. ［**実行方法**］をクリックします。
   ［**脆弱性スキャン**］ウィンドウの［**実行方法**］タブが表示されます。

4. ［**実行方法**］タブの［**ユーザー**］セクションで、［**他のユーザーでタスクを実行する**］をオンにします。

5. ［**ユーザー名**］に、脆弱性スキャンタスクの開始に使用できる権限のあるユーザーのアカウント名を入力します。

6. ［**パスワード**］に、脆弱性スキャンタスクの開始に使用できる権限のあるユーザーのパスワードを入力します。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## 脆弱性のリストの管理

脆弱性のリストを管理する場合、次の処理を実行できます：

- 脆弱性のリストを表示する。

- 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た後で、脆弱性スキャンタスクを再開する。
- セクションごとに、脆弱性の詳細情報とその修正に関する推奨策を表示する。
- 脆弱性のリストでエントリを非表示にする。
- 重要度レベルによる脆弱性のリストをフィルタリングする
- 「解決済み」と「非表示」のステータス値によって脆弱性のリストをフィルタリングする。

テーブルのデータを管理しながら、次の処理も実行できます：

- 列の値またはカスタムフィルター条件によって脆弱性のリストをフィルタリングする。
- 脆弱性の検索機能を使用する。
- 脆弱性のリスト内でエントリを並べ替える
- 脆弱性のリストに表示される列の順番と配置を変更する。
- 脆弱性のリスト内のエントリをグループ化する。

## 脆弱性のリストについて

Kaspersky Endpoint Security は、［脆弱性スキャン］タスクの結果を脆弱性のリストに記録します。

特定の脆弱性を確認して修正のために推奨される処理を実行すると、脆弱性のステータスは「*解決済み*」に変更されます。

特定の脆弱性についてのエントリを脆弱性リストに表示しない場合、それらを非表示にすることができます。このような脆弱性の「非表示」ステータスは、Kaspersky Endpoint Security が割り当てます。

脆弱性のリストはテーブルの形式で表示されます。各テーブル列には次の情報が含まれています：

- 脆弱性の重要度レベルを示すアイコン。脆弱性の重要度には以下のものがあります：
  - アイコン：**緊急**：この重要度レベルは、すぐに修正が必要な、非常に危険性の高い脆弱性に適用されます。侵入者はこのレベルの脆弱性を積極的に利用し、コンピューターのオペレーティングシステムをウイルスに感染させたり、ユーザーの個人情報にアクセスしたりします。すぐに、重要度レベルが「緊急」の脆弱性の修正に必要な手順をすべて実行してください。
  - アイコン：**注意**：この重要度レベルは、すぐに修正が必要な、重要な脆弱性に適用されます。侵入者はこのレベルの脆弱性を積極的に利用できます。現在、侵入者は重要度レベルが「重要」の脆弱性を積極的には利用していません。すぐに、重要度レベルが「重要」の脆弱性の修正に必要な手順をすべて実行してください。
  - アイコン：**警告**：この重要度レベルは、すぐに解決しなくても差し支えがない脆弱性に適用されます。しかし、今後このような脆弱性がコンピューターのセキュリティを脅かすおそれがあります。
- 脆弱性 ID
- 脆弱性が検知されたアプリケーションの名前

- 脆弱性の簡単な説明
- デジタル署名に示されているソフトウェアの発行元に関する情報
- 脆弱性を修正する処理の結果

## 脆弱性スキャンタスクの再開

以前に検知した脆弱性に関する情報を更新するには、再度脆弱性スキャンタスクを開始できます。たとえば、何らかの理由で脆弱性スキャンが中断した場合や、最新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後にコンピューターの脆弱性をスキャンするような場合に、スキャンの再開が必要となる場合があります。

*脆弱性スキャンタスクを再開するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**脆弱性**］タブを選択します。
   ［**脆弱性**］タブには、脆弱性スキャンタスク中に Kaspersky Endpoint Security が検知した脆弱性のリストが表示されます。
4. ［**保管領域**］ウィンドウの右下で、［**再スキャン**］をクリックします。

Kaspersky Endpoint Security は、脆弱性のリストにある脆弱性に関する詳細情報を更新します。

提案されたパッチのインストールによって修正された脆弱性のステータスは、新たに脆弱性スキャンを実行しても変わりません。

## 脆弱性の解決

脆弱性を修正するには、オペレーティングシステムのアップデートプログラムのインストール、アプリケーションの設定変更、あるいはアプリケーションパッチのインストールのいずれかを実行します。

検知された脆弱性がインストールされているアプリケーションではなく、そのアプリケーションのコピーに適用されることがあります。パッチによって脆弱性を修正できるのは、アプリケーションがインストールされている場合に限られます。

*脆弱性を修正するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**脆弱性**］タブを選択します。

［**脆弱性**］タブには、脆弱性スキャンタスク中に Kaspersky Endpoint Security が検知した脆弱性のリストが表示されます。

4. 脆弱性のリストで、目的の脆弱性に対応するエントリを選択します。

   この脆弱性に関する情報および推奨される修正方法が、脆弱性のリストの下のセクションに表示されます。

   選択した脆弱性ごとに次の情報が表示されます：

   - 脆弱性が検知されたアプリケーションの名前
   - 脆弱性が検知されたアプリケーションのバージョン
   - 脆弱性の重要度
   - 脆弱性 ID
   - 脆弱性が前回検知された日時
   - 脆弱性の修正に関する推薦事項（たとえば、オペレーティングシステムのアップデートプログラムまたはアプリケーションのパッチを配信する Web サイトへのリンク）
   - 脆弱性の説明が記載されている Web サイトへのリンク

5. 脆弱性の詳細説明を表示するには、［**補足情報**］をクリックして、選択されている脆弱性に関連する脅威の説明を含む Web サイトを開きます。この Web サイト（threats.kaspersky.com）では、現在のバージョンのアプリケーションの必要なアップデートパッケージをダウンロードしてインストールできます。

6. 脆弱性を修正するには、次のいずれかの方法を選択します：

   - アプリケーションで1つ以上のパッチが使用可能な場合は、パッチ名の隣に表示される指示に従って、必要なパッチをインストールします。
   - オペレーティングシステムのアップデートプログラムが使用可能な場合は、アップデートプログラム名の隣に表示される指示に従って必要なアップデートプログラムをインストールします。

   パッチまたはアップデートプログラムをインストールすると、脆弱性が修正されます。Kaspersky Endpoint Security はこの脆弱性に、脆弱性が修正済みであることを示すステータスを割り当てます。修正された脆弱性に関するエントリは、脆弱性リストでは灰色表示されます。

7. 画面下部に脆弱性の修正方法に関する情報が表示されていない場合、Kaspersky Endpoint Security の定義データベースとモジュールをアップデートしてから、脆弱性スキャンタスクを再び開始することができます。Kaspersky Endpoint Security は脆弱性のデータベースと照合してシステムに脆弱性がないかスキャンするので、アプリケーションのアップデート後に、修正済みの脆弱性に関する項目が表示されることがあります。

## 脆弱性のリストでのエントリの非表示

選択した脆弱性のエントリを非表示にできます。脆弱性のリストで選択されたエントリには「非表示」というステータスが割り当てられ、非表示として示されます。脆弱性のリストを*「非表示」のステータス値でフィルタリング*できます。

*脆弱性のリストでエントリを非表示にするには：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。

3. ［**保管領域**］ウィンドウで、［**脆弱性**］タブを選択します。

   ［**脆弱性**］タブには、脆弱性スキャンタスク中に Kaspersky Endpoint Security が検知した脆弱性のリストが表示されます。

4. 脆弱性のリストで、非表示にする脆弱性についてのエントリを選択します。

   この脆弱性に関する情報および推奨される修正方法が、脆弱性のリストの下のセクションに表示されます。

5. ［**非表示**］をクリックします。

   Kaspersky Endpoint Security は、選択されている脆弱性に「非表示」ステータスを割り当てます。［*非表示*］ステータスの脆弱性についてのエントリが、脆弱性のリストの最後に移され、灰色表示されます。

6. 脆弱性のリストで脆弱性についてのエントリを非表示にするには、リストの上にある［**非表示**］をオンにします。

## 重要度レベルによる脆弱性のリストのフィルタリング

*脆弱性のリストを重要度レベルでフィルタリングするには、次の手順を実行します：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。

3. ［**保管領域**］ウィンドウで、［**脆弱性**］タブを選択します。

   ［**脆弱性**］タブには、脆弱性スキャンタスク中に Kaspersky Endpoint Security が検知した脆弱性のリストが表示されます。脆弱性のリストの上部にある［**重要度**］列に、脆弱性の重要度レベルにおける 3 つのアイコン（警告、重要、緊急）が表示されます。これらのアイコンをクリックすると、脆弱性のリストを重要度レベルでフィルタリングできます。

4. 脆弱性の重要度レベルのアイコンを、1つ以上クリックします。選択された重要度レベルと一致する脆弱性がリストに表示されます。特定の重要度レベルと一致する脆弱性の表示を止めるには、該当する重要度レベルのアイコンを再度クリックします。重要度レベルが1つも選択されなかった場合、脆弱性のリストは空白です。

   ［**保管領域**］ウィンドウを閉じると、指定した脆弱性項目のフィルタリング条件が保存されます。

## 解決済みと非表示のステータス値による脆弱性のリストのフィルタリング

*脆弱性のリストを解決済みと非表示のステータス値でフィルタリングするには：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。

3. ［**保管領域**］ウィンドウで、［**脆弱性**］タブを選択します。

   ［**脆弱性**］タブには、脆弱性スキャンタスク中に Kaspersky Endpoint Security が検知した脆弱性のリストが表示されます。

4. 脆弱性のステータスを示すチェックボックスが［**表示する脆弱性**］設定の横に表示されます。脆弱性のリストを「解決済み」のステータスでフィルタリングするには、次のいずれかの手順を実行します：

   - 脆弱性のリストで解決された脆弱性についてのエントリを表示するには、［**修正済み**］をオンにします。脆弱性リストでは、修正済みの脆弱性に関するエントリは灰色表示されます。

   - 脆弱性のリストで解決された脆弱性についてのエントリを非表示にするには、［**修正済み**］をオフにします。

5. 脆弱性のリストを「非表示」のステータスでフィルタリングするには、次のいずれかの手順を実行します：

   - 脆弱性のリストで非表示の脆弱性についてのエントリを表示するには、［**非表示**］をオンにします。脆弱性リストでは、非表示の脆弱性に関するエントリは灰色表示されます。

   - 脆弱性のリストで非表示の脆弱性についてのエントリを非表示にするには、［**非表示**］をオフにします。

指定した脆弱性エントリのフィルター条件は、［**保管領域**］ウィンドウを閉じた後は保存されません。

# ソフトウェアモジュールの整合性の確認

このセクションでは、整合性チェックタスクの詳細と設定について説明します。

## 整合性チェックタスクの概要

Kaspersky Endpoint Security は、アプリケーション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。

脆弱性スキャンタスクを開始すると、進捗状況が、Kaspersky Endpoint Security メインウィンドウにある［**プロテクションとコントロール**］タブの、［**タスク**］セクションの［**脆弱性スキャン**］タスク名の横のフィールドに表示されます。

整合性チェックタスクの結果はレポートに記録されます。

## 整合性チェックタスクの開始または停止

整合性チェックタスクは、選択したタスク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。

*整合性チェックタスクを開始または停止するには：*

1. メインウィンドウを開きます。
2. ［**プロテクションとコントロール**］タブを選択します。
3. ［**タスク**］セクションを開きます。
4. 右クリックして、整合性チェックタスク名が含まれる行のコンテキストメニューを表示します。
5. 次のいずれかの手順を実行します：

   - 整合性チェックタスクを開始するには、コンテキストメニューで［**スキャンの開始**］を選択します。
     このタスクの名前を持つボタンの右側に表示されるタスク進捗ステータスが［*実行中*］に変わります。
   - 整合性チェックタスクを停止する場合は、メニューから［**スキャンの停止**］を選択します。
     このタスクの名前を持つボタンの右側に表示されるタスク進捗ステータスが［*停止*］に変わります。

## 整合性チェックタスクの実行方法の選択

*整合性チェックタスクの実行方法を選択するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**スケジュールされているタスク**］セクションで、［**整合性チェック**］を選択します。

   ウィンドウの右側に、整合性チェックタスク設定が表示されます。

3. ［**実行方法**］セクションで、次のいずれかを選択します：

   - 整合性チェックタスクを手動で開始するには、［**手動開始**］を選択します。
   - 整合性チェックタスクの開始スケジュールを設定するには、［**カスタム**］を選択します。

4. 前の手順で［**カスタム**］を選択した場合は、タスクの実行スケジュールの設定を指定します。次の手順に従います：

   a. ［**頻度**］で、整合性チェックタスクの開始スケジュールを指定します。次のいずれかのオプションを選択します：［**分ごと**］、［**時間ごと**］、［**日ごと**］、［**毎週**］、［**1回のみ**］、［**毎月**］、［**本製品の起動後**］

   b. ［**頻度**］で選択した項目に応じて、タスクの開始時間を定義する設定値を指定します。

   c. スキップされた整合性チェックタスクをできるだけ早く開始するには、［**スキップしたスケジュールタスクを後で実行する**］をオンにします。

   > ［**頻度**］で［**時間ごと**］、［**分ごと**］、または［**本製品の起動後**］を選択した場合、［**スキップしたスケジュールタスクを後で実行する**］は無効になります。

   d. コンピューターのリソースが制限されている場合にタスクを一時停止するには、［**コンピューターを使用していないときのみ実行**］をオンにします。

   このスケジュールオプションは、コンピューターの資源の節約に役立ちます。

5. ［**OK**］をクリックします。

6. 変更を保存するには［**保存**］をクリックします。

# レポートの管理

このセクションでは、レポートの設定と管理の方法について説明します。

## レポート管理の原則

レポートには、Kaspersky Endpoint Security の各コンポーネントの動作、各スキャンタスク、アップデートタスク、整合性チェックタスク、脆弱性スキャンタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

レポートのデータは、イベントのリストを含むテーブルの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。詳細属性を表示するには、グラフの名前の横にある をクリックします。各種コンポーネントの動作中に記録されるイベントや各種タスクの実行結果には、さまざまな属性があります。

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。
- ［**すべての保護コンポーネント**］レポート。次の Kaspersky Endpoint Security コンポーネントの処理過程で記録されたイベントに関する情報が含まれます：
  - ファイルアンチウイルス
  - メールアンチウイルス
  - ウェブアンチウイルス
  - メッセンジャーアンチウイルス
  - システムウォッチャー
  - ファイアウォール
  - ネットワーク攻撃防御
  - 有害 USB 攻撃ブロック
- Kaspersky Endpoint Security コンポーネントの操作またはタスクの実行に関するレポート。
- 「**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**。アイコン：通常は重要な情報が含まれていない形式的なイベントです。
- **重要イベント**。アイコン：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**。アイコン：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。
- イベントフィルターによってイベントのグループ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 は最も古いエントリから現時点にいたるまで、選択されたレポートのすべてのエントリを削除します。

## レポート設定の指定

次のような方法で、レポートを設定することができます：

- レポート最長保管期間を設定する

  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。レポートの最長保管期間は変更できます。また、期間ベースの制約を無効にすることもできます。

- レポートファイルの最大サイズを設定する

  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サイズの制限をキャンセルしたり、サイズに別の値を設定したりすることができます。

## レポート最長保管期間の設定

*レポート最長保管期間を変更するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
3. ウィンドウの右側にある［**レポート**］セクションで、次のいずれかを実行します：
   - レポート保管期間を制限するには、［**保存期間**］をオンにします。［**保存期間**］の横にあるフィールドに、レポートの最長保管期間を指定します。

既定の最長レポート保管期間は 30 日です。

- レポート保管期間の制限を取り消すには、［**保存期間**］をオフにします。

レポート保管期間の制限は、既定では有効です。

4. 変更を保存するには［**保存**］をクリックします。

## レポートファイルの最大サイズの設定

*レポートファイルの最大サイズを設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
3. ウィンドウの右側にある［**レポート**］セクションで、次のいずれかを実行します：
   - レポートファイルのサイズを制限するには、［**最大サイズ**］をオンにします。［**最大サイズ**］の右側のフィールドで、レポートファイルの最大サイズを指定します。
     既定では、レポートの最大ファイルサイズは 1024 MB に制限されています。
   - レポートファイルのサイズの制限を解除するには、［**最大サイズ**］をオフにします。

   レポートファイルのサイズ制限は、既定では有効になっています。
4. 変更を保存するには［**保存**］をクリックします。

## レポートの表示

*レポートを表示するには、次の手順を実行します：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**レポート**］をクリックして、［**レポート**］ウィンドウを開きます。
3. すべての保護コンポーネントのレポートを生成するには、［**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［**すべての保護コンポーネント**］を選択します。
   すべての保護コンポーネントの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、Kaspersky Endpoint Security の保護コンポーネントの動作中に発生したイベントがリスト表示されます。
4. コンポーネントの操作あるいはタスクに関するレポートを生成するには、［**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。
   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。

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。

## レポートでのイベント情報の表示

各イベントの詳細なサマリーをレポートに表示できます。

*各イベントの詳細なサマリーをレポートに表示するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**レポート**］をクリックして、［**レポート**］ウィンドウを開きます。
3. ウィンドウの左側で、必要なコンポーネントまたはタスクのレポートを選択します。

   レポートの範囲に含まれるイベントが、ウィンドウの右側のテーブルに表示されます。レポートの中で特定のイベントを探すには、フィルタリング、検索、およびソート機能を使用します。
4. レポートの中で必要な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。

## レポートのファイルへの保存

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. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**レポート**］をクリックして、［**レポート**］ウィンドウを開きます。
3. 次のいずれかの手順を実行します：

   - すべての保護コンポーネントのレポートを生成するには、コンポーネントとタスクのリストで［**すべての保護コンポーネント**］を選択します。

     すべての保護コンポーネントの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、すべての保護コンポーネントの処理におけるイベントがリスト表示されます。

   - 特定のコンポーネントまたはタスクの動作に関するレポートを生成するには、リストから目的の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、選択したコンポーネントまたはタスクの動作中のイベントがリスト表示されます。
4. 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

5. 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。
   コンテキストメニューが開きます。
6. コンテキストメニューで、レポートファイルを保存するエンコーディングを［**ANSI で保存**］または［**Unicode で保存**］から選択します。
   Microsoft Office の標準の［**名前を付けて保存**］ウィンドウが開きます。
7. ［**名前を付けて保存**］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。
8. ［**ファイル名**］にレポートファイル名を入力します。
9. ［**ファイルの種類**］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：
10. ［**保存**］をクリックします。

## レポートの削除

*レポートから情報を削除するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
3. ウィンドウの右側にある［**レポート**］セクションで、［**レポートの削除**］をクリックします。
   ［**レポートの削除**］ウィンドウが開きます。
4. 情報を削除したいレポートのチェックボックスをオンにします。
   - **すべてのレポート**
   - **プロテクションのレポート**：次の Kaspersky Endpoint Security コンポーネントの運用に関する情報が含まれています：
     - ファイルアンチウイルス
     - メールアンチウイルス
     - ウェブアンチウイルス
     - メッセンジャーアンチウイルス
     - システムウォッチャー
     - ファイアウォール
     - ネットワーク攻撃防御
     - 有害 USB 攻撃ブロック

- **スキャンタスクのレポート**：完了したスキャンタスクに関する情報が含まれています：
  - 完全スキャン
  - 簡易スキャン
  - オブジェクトスキャン
  - 整合性チェック
- **アップデートタスクのレポート**：完了したアップデートタスクに関する情報が含まれています。
- **ファイアウォールのレポート**：ファイアウォールの運用に関する情報が含まれています。
- **管理コンポーネントのレポート**：次の Kaspersky Endpoint Security コンポーネントの運用に関する情報が含まれています：
  - アプリケーション起動コントロール
  - アプリケーション権限コントロール
  - 脆弱性モニター
  - デバイスコントロール
  - ウェブコントロール
- **データ暗号化レポート**

5. ［OK］をクリックします。

# 通知サービス

このセクションでは、Kaspersky Endpoint Security の動作時にイベントをユーザーに通知する通知サービスおよび通知のパラメータの設定方法について説明します。

## Kaspersky Endpoint Security の通知の概要

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 taskbar 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。

## 通知サービスの設定

通知サービスの設定では、次の操作を実行できます：

- Kaspersky Endpoint Security がイベントを記録するイベントログを設定する。
- 画面上に通知を表示する方法を設定する。
- メール通知の配信を設定する。

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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
   ウィンドウの右側に、レポートと保管領域の設定が表示されます。

3. ［**通知**］セクションの［**設定**］をクリックします。
   ［**通知**］ウィンドウが開きます。
   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。

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. ［**ローカルログに保存**］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、［**アプリケーションとサービス ログ**］の［**Kaspersky Event Log**］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**］の順にクリックします。

6. ［**OK**］をクリックします。

7. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
   ウィンドウの右側に、レポートと保管領域の設定が表示されます。

3. ［**通知**］セクションの［**設定**］をクリックします。
   ［**通知**］ウィンドウが開きます。
   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。

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. ［**メールアカウント設定**］をクリックします。
   ［**メールアカウント設定**］ウィンドウが開きます。

8. ［**イベント通知を送信する**］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。

9. メール通知の配信設定を指定してください。
10. ［**OK**］をクリックします。
11. ［**メールアカウント設定**］ウィンドウで［**OK**］をクリックします。
12. 変更を保存するには［**保存**］をクリックします。

## 製品のステータスに関する通知領域での警告の表示を設定

*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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**インターフェイス**］を選択します。
   Kaspersky Security Network のインターフェイスの設定が、ウィンドウの右側に表示されます。
3. ［**警告**］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. 変更を保存するには［**保存**］をクリックします。

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。

# 隔離とバックアップの管理

このセクションでは、隔離とバックアップの設定および管理の方法について説明します。

## 隔離とバックアップの概要

*隔離*は、感染の可能性があるファイルのリストです。*感染の可能性があるファイル*とは、ウイルスなどの脅威またはその亜種に感染している可能性があるファイルのことです。

Kaspersky Endpoint Security が感染している可能性があるファイルを隔離するときには、ファイルをコピーせずに移動します。ファイルをハードディスクまたはメールから削除し、そのファイルを特別なデータ保管領域に保存します。隔離されたファイルは特別な形式で保存され、脅威となることはありません。

Kaspersky Endpoint Security は、ウイルススキャンの実行時や、ファイルアンチウイルス、メールアンチウイルス、システムウォッチャーの各コンポーネントの動作時に、感染している可能性があるファイルを検知して隔離できます。

Kaspersky Endpoint Security は次の場合にファイルを隔離します：

- ファイルコードが既知の悪意のあるプログラムを部分的に修正したものに類似しているか、悪意のあるソフトウェアに近い構造をしており、Kaspersky Endpoint Security の定義データベースのリストにはない。この場合、ファイルアンチウイルスとメールアンチウイルスによるヒューリスティック分析の後に、またはスキャン中に、ファイルが隔離されます。ヒューリスティック分析が誤検知をすることはほとんどありません。

- ファイルが実行する処理のシーケンスが危険である。この場合、システムウォッチャーが動作を分析した後に、ファイルが隔離されます。

*バックアップ*は、感染駆除のプロセス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のリストです。*バックアップコピー*とは、このファイルの感染駆除または削除を最初に試みる際に作成されるファイルコピーのことです。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。

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、駆除されたファイルのコピーを元のフォルダーに復元することができます。

定義データベースまたはソフトウェアモジュールのアップデート後、Kaspersky Endpoint Security が脅威を特定し、処理できることがあります。このため、定義データベースまたはソフトウェアモジュールのアップデート後には、隔離されたファイルをスキャンしてください。

## 隔離とバックアップの設定

データ保管領域は、隔離とバックアップで構成されています。隔離とバックアップは、次のように設定できます：

- 隔離ファイルとバックアップファイルコピーの最長保管期間を設定します。

  既定では、隔離ファイルとバックアップファイルコピーの最長保管期間は 30 日間です。最長保管期間が経過すると、Kaspersky Endpoint Security によってデータ保管領域から最も古いファイルが削除されます。ファイルの最長保管期間は変更できます。また、期間ベースの制約を無効にすることもできます。

- 隔離とバックアップの最大サイズを設定できます。

既定では、隔離とバックアップの最大サイズは 100 MB です。データ保管領域が最大サイズに到達すると、データの最大保管サイズを超えないように、Kaspersky Endpoint Security により、隔離とバックアップから最も古いファイルが自動的に削除されます。隔離とバックアップの最大サイズをキャンセルまたは変更することができます。

## 隔離ファイルとバックアップファイルコピーの最長保管期間の設定

*隔離ファイルとバックアップファイルコピーの最長保管期間を設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
3. 次のいずれかの手順を実行します：
   - 隔離とバックアップファイルの保管期間を制限するには、ウィンドウの右側にある［**隔離とバックアップの設定**］セクションで、［**保存期間**］をオンにします。［**保存期間**］の右側のフィールドで、隔離のファイルとバックアップファイルコピーの最長保管期間を指定します。既定では、隔離ファイルとバックアップファイルコピーの保管期間は 30 日間に制限されています。
   - 隔離とバックアップファイルの保管期間の制限を取り消すには、ウィンドウの右側にある［**隔離とバックアップの設定**］セクションで、［**保存期間**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## 隔離とバックアップの最大サイズの設定

*隔離とバックアップの最大サイズを設定するには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
3. 次のいずれかの手順を実行します：
   - 隔離とバックアップの合計サイズを制限する場合は、ウィンドウ右側の［**隔離とバックアップの設定**］セクションにある［**保存サイズ**］をオンにし、**保存サイズ**］の横にあるフィールドで隔離とバックアップの最大サイズを指定します。

     既定では、隔離とバックアップにあるファイルから成るデータの最大保存サイズは 100 MB です。
   - 隔離とバックアップの制限を解除するには、ウィンドウの右側にある［**隔離とバックアップの設定**］セクションで、［**保存サイズ**］をオフにします。

   既定では、隔離とバックアップのサイズは制限されません。
4. 変更を保存するには［**保存**］をクリックします。

# 隔離の管理

Kaspersky Endpoint Security は、設定で定義した保管期間を過ぎると、ファイルのステータスに関係なく、隔離から自動的にファイルを削除します。

隔離の管理時には、次のファイル操作が可能です：

- Kaspersky Endpoint Security によって隔離されたファイルを表示する。
- 現在のバージョンの Kaspersky Endpoint Security の定義データベースとモジュールを使用して、感染の可能性があるファイルをスキャンする。
- 隔離から元のフォルダーにファイルを復元する。
- 隔離からファイルを削除する。
- ファイルが保存されていた元のフォルダーを開く。

隔離されたファイルはテーブル形式で表示されます。

テーブルのデータを管理しながら、次の処理も実行できます：

- 隔離されたファイルを列の値またはカスタムフィルタリング条件でフィルタリングする。
- 隔離されたファイルの検索機能を使用する。
- 隔離されたイベントを並べ替える。
- 隔離されたファイルのテーブルに表示される列とその順番を変更する。

選択した隔離イベントをクリップボードにコピーすることができます。複数の隔離されたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

# アップデート後の隔離ファイルのスキャンの有効化と無効化

Kaspersky Endpoint Security でのファイルのスキャン中に感染の兆候が検知された一方で、そのファイルに影響を与えている悪意のあるプログラムが判別できない場合、感染の可能性があるファイルは隔離に移動します。その後、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た後に、Kaspersky Endpoint Security において脅威が特定され無力化されることがあります。自動スキャンを有効化して、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るたびに、隔離内のファイルを自動的にスキャンすることができます。

隔離内のファイルを定期的にスキャンしてください。スキャンによってファイルのステータスが変わることがあります。その後、ファイルによってはウイルスを駆除して元の場所に復元し、引き続き使用できる場合があります。

*隔離されたファイルのアップデート後のスキャンを有効にするには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側の［**詳細設定**］セクションで、［**レポートと保管領域**］を選択します。
   ウィンドウの右側に、レポートと保管領域の管理設定が表示されます。

3. ［**隔離とバックアップの設定**］セクションで、次のいずれかの手順を実行します：

   - Kaspersky Endpoint Security のアップデートのたびに隔離されたファイルをスキャンする場合は、［**アップデート後に隔離されているファイルをスキャン**］をオンにします。

   - Kaspersky Endpoint Security のアップデートのたびに隔離されたファイルをスキャンしない場合は、［**アップデート後に隔離されているファイルをスキャン**］をオフにします。

4. 変更を保存するには［**保存**］をクリックします。

## 隔離にあるファイルに対するオブジェクトスキャンタスクの開始

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後、Kaspersky Endpoint Security は、隔離されたファイルに含まれる脅威の種類を特定し、処理できることがあります。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るたびに、隔離されたファイルが自動的にスキャンされるように製品を設定していない場合は、隔離されたファイルに対してオブジェクトスキャンタスクを手動で開始することができます。

*隔離されたファイルに対してオブジェクトスキャンタスクを開始するには：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
   ［**保管領域**］ウィンドウに［**隔離**］タブが表示されます。

3. ［**隔離**］タブで、感染の可能性がありスキャンしたいファイルを1つ以上選択します。
   複数の隔離されたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

4. 次のいずれかの方法で、オブジェクトスキャンタスクを開始します：

   - ［**再スキャン**］をクリックします。

   - 右クリックしてコンテキストメニューを表示し、［**再スキャン**］を選択します。

スキャンの完了後、スキャンされたファイルの数、および検知された脅威の数を示す通知が表示されます。

## 隔離からのファイルの復元

*隔離からファイルを復元するには：*

1. メインウィンドウを開きます。

2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
   ［**保管領域**］ウィンドウに［**隔離**］タブが表示されます。

3. すべての隔離されたファイルを復元するには、任意のファイルのコンテキストメニューで［**すべて復元**］を選択します。

隔離のすべてのファイルが元のフォルダーに復元されます。

4. 1つ以上の隔離ファイルを復元するには、次の手順に従います：

   a. ［**隔離**］タブで、隔離から復元したいファイルを1つ以上選択します。

   複数の隔離されたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

   b. ファイルを次のいずれかの方法で復元します：

   - ［**復元**］をクリックします。
   - 右クリックしてコンテキストメニューを表示し、［**復元**］を選択します。

選択したファイルが元のフォルダーに復元されます。

## 隔離からのファイルの削除

*隔離からファイルを削除するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。

   ［**保管領域**］ウィンドウに［**隔離**］タブが表示されます。
3. すべての隔離されたファイルを削除するには、任意のファイルのコンテキストメニューで［**すべて削除**］を選択します。

   すべてのファイルが隔離から削除されます。
4. 1つ以上の隔離ファイルを削除するには：

   a. ［**隔離**］タブで、隔離から削除する、感染の可能性があるファイルを1つ以上選択します。

   複数の隔離されたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

   b. 次のいずれかの方法で、ファイルを削除します：

   - [**削除**］をクリックします。
   - 右クリックしてコンテキストメニューを表示し、［**削除**］を選択します。

選択されたファイルが隔離から削除されます。

## バックアップの管理

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、ファイルの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。

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）。

Kaspersky Endpoint Security は、設定で定義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、バックアップから自動的にファイルのバックアップコピーを削除します。

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。

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。

バックアップを管理しながら、ファイルのバックアップコピーを使用して次の処理を実行できます：

- ファイルのバックアップコピーを表示する。
- 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。
- 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。

テーブルのデータを管理しながら、次の処理も実行できます：

- 列やカスタムのフィルタリング条件でバックアップコピーをフィルタリングする。
- バックアップコピーの検索機能を使用する。
- バックアップコピーを並べ替える。
- バックアップコピーのテーブルに表示される列とその順番を変更する。

選択したバックアップイベントをクリップボードにコピーすることができます。複数のバックアップされたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

## バックアップからのファイルの復元

*バックアップからファイルを復元するには：*

1. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**バックアップ**］タブを選択します。

4. すべてのバックアップされたファイルを復元するには、任意のファイルのコンテキストメニューで［**すべて復元**］を選択します。

   バックアップコピーのすべてのファイルが元のフォルダーに復元されます。

5. バックアップから1つ以上のファイルを復元するには、次の手順に従います：

   a. テーブルの［**バックアップ**］タブで、バックアップされたファイルを1つ以上選択します。

      複数の隔離されたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

   b. ファイルを次のいずれかの方法で復元します：

      - ［**復元**］をクリックします。
      - 右クリックしてコンテキストメニューを表示し、［**復元**］を選択します。

   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

*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. メインウィンドウを開きます。
2. メインウィンドウの上部にある［**隔離**］をクリックして、［**保管領域**］ウィンドウを開きます。
3. ［**保管領域**］ウィンドウで、［**バックアップ**］タブを選択します。
4. ［バックアップ］内のファイルをすべて削除する場合は、次のいずれかを実行します：

   - 任意のファイルのコンテキストメニューで、［**すべて削除**］を選択します。
   - ［**保管領域のクリア**］をクリックします。

   すべてのバックアップされたファイルがバックアップから削除されます。

5. バックアップから1つ以上のファイルを削除するには：

   a. テーブルの［**バックアップ**］タブで、バックアップされたファイルを1つ以上選択します。

      複数のバックアップされたファイルを選択するには、任意のファイルを右クリックしてコンテキストメニューを表示し、［**すべて選択**］を選択します。スキャンしないファイルの選択を解除するには、**CTRL** キーを押しながらクリックします。

   b. 次のいずれかの方法で、ファイルを削除します：

      - [**削除**］をクリックします。
      - 右クリックしてコンテキストメニューを表示し、［**削除**］を選択します。

   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。

# 製品の詳細設定

このセクションでは、Kaspersky Endpoint Security の詳細設定とその設定方法について説明します。

## 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、設定ファイルを配信キット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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. ［**設定の管理**］セクションで、［**エクスポート**］をクリックします。
   Microsoft Windows 標準の［**設定ファイルを選択してください**］ウィンドウが開きます。
4. 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. ［**設定の管理**］セクションで、［**インポート**］をクリックします。
   Microsoft Windows 標準の［**設定ファイルを選択してください**］ウィンドウが開きます。
4. 設定ファイルのパスを指定します。
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。

# 信頼ゾーン

このセクションでは、信頼ゾーンの情報、および信頼するオブジェクトの設定方法と信頼するアプリケーションのリストの作成方法について説明します。

## 信頼ゾーンの概要

*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。つまり、信頼ゾーンとはスキャンを除外する項目のグループです。

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。

次のオブジェクトをスキャンから除外できます：

- 特定の形式のファイル
- マスクによって選択されたファイル
- 選択されているファイル
- フォルダー
- アプリケーションプロセス

### 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 がオブジェクトのウイルスなどの脅威のスキャンを実行しないときに適用される条件グループです。

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。このようなアプリケーションには悪意のある機能は一切ありませんが、マルウェアの補助コンポーネントとして使用することができます。このようなアプリケーションの例としては、リモート管理ツール、IRC クライアント、FTP サーバー、一時停止 / 隠蔽プロセス用の各種ユーティリティ、キーロガー、パスワードクラッカー、オートダイヤラーがあります。このようなアプリケーションは、ウイルスには分類されません。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合法的なソフトウェアについては、カスペルスキーのウイルス百科事典（https://encyclopedia.kaspersky.com/knowledge/riskware/）で確認することができます。

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、リモート管理プログラムを使用する頻度が多い場合を考えてみます。これは、リモートコンピューターを管理するためのリモートアクセスアプリケーションです。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、ここで説明する方法で 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：

- ファイルアンチウイルス
- メールアンチウイルス
- ウェブアンチウイルス
- アプリケーション権限コントロール
- スキャンタスク
- システムウォッチャー

### 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 はすべてのプログラム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。Kaspersky Endpoint Security は、信頼するアプリケーションのリストにあるアプリケーションをスキャンから除外します。

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の間の競合（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。

## 信頼するオブジェクトを作成する

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。

*信頼するオブジェクトを作成する*

1. ［設定］ウィンドウを開きます。

2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開き、［**信頼するオブジェクト**］タブが表示されます。

4. ［**追加**］をクリックします。
   ［**信頼するオブジェクト**］ウィンドウが開きます。このウィンドウの［**プロパティ**］セクションで、スキャンから除外する条件を1つ以上作成できます。

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。

   ファイルまたはフォルダーの名前マスクに、アスタリスク（「*」）を使用して、ファイル名の任意の文字を指定できます。

   たとえば、マスクを使用して、次のようなパスを追加できます：

   - 任意のフォルダー中に配置されたファイルのパス：
     - マスク「*.exe」は、拡張子 が EXE であるファイルのパスすべてを含みます。
     - マスク「*.test」は、「test」という名前のファイルのパスすべてを含みます。
   - 特定のフォルダー中に配置されたファイルのパス：
     - マスク「C:\dir*.*」は、フォルダー「C:\dir\」に配置されたファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
     - マスク「C:\dir*」は、フォルダー「C:\dir\」に配置されたファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
     - マスク「C:\dir\」は、フォルダー「C:\dir\」に配置されたファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
     - マスク「C:\dir*.exe」は、フォルダー「C:\dir\」に配置された拡張子が EXE であるファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
     - マスク「C:\dir\test」は、フォルダー「C:\dir\」に配置された名前が「test」であるファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
     - マスク「C:\dir*\test」は、フォルダー「C:\dir\」に配置された名前が「test」であるファイルすべてのパスを含みますが、「C:\dir\」のサブフォルダー中のファイルは含まれません。
   - 特定の名前を持つすべてのフォルダー中に配置されたファイルのパス：

- マスク「dir*.*」は、名前が「dir」のフォルダー中のファイルすべてのパスを含みますが、サブフォルダーの中のファイルは含まれません。
- マスク「dir*」は、名前が「dir」のフォルダー中のファイルすべてのパスを含みますが、サブフォルダーの中のファイルは含まれません。
- マスク「dir\」は、名前が「dir」のフォルダー中のファイルすべてのパスを含みますが、サブフォルダーの中のファイルは含まれません。
- マスク「dir*.exe」は、名前が「dir」のフォルダーの拡張子が EXE であるファイルすべてのパスを含みますが、サブフォルダー中のファイルは含まれません。
- マスク「dir\test」は、名前が「dir」のフォルダー中の名前が「test」であるファイルすべてのパスを含みますが、サブフォルダーの中のファイルは含まれません。

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。

6. 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. カスペルスキーのウイルス百科事典の分類に従って、オブジェクト名またはオブジェクト名マスクを入力します。

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。

7. 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。

8. 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［**すべての保護コンポーネント**］をクリックすると、［**設定**］が表示されます。

b. ［**設定**］をクリックして［**保護コンポーネント**］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. ［**保護コンポーネント**］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。

9. ［**信頼するオブジェクト**］ウィンドウで［OK］をクリックします。

追加した信頼するオブジェクトが、［**信頼ゾーン**］ウィンドウの［**信頼するオブジェクト**］タブに表示されます。この信頼するオブジェクトに指定された設定が［**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。

10. ［**信頼ゾーン**］ウィンドウで［**OK**］をクリックします。

11. 変更を保存するには［**保存**］をクリックします。

## 信頼するオブジェクトを変更する

*信頼するオブジェクトを変更するには、次の操作を行います：*

1. ［設定］ウィンドウを開きます。

2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開き、［**信頼するオブジェクト**］タブが表示されます。

4. 変更したい信頼するオブジェクトを、リストから選択します。

5. 次のいずれかの方法で、スキャンからの除外の設定を変更します：

   - ［**編集**］をクリックします。
     ［**信頼するオブジェクト**］ウィンドウが開きます。

   - ［**信頼するオブジェクトの説明**］にあるリンクをクリックして、変更する必要のある設定のウィンドウを開きます。

6. 前の手順で［**編集**］を選択した場合、［**信頼するオブジェクト**］ウィンドウで［**OK**］をクリックします。
   この信頼するオブジェクトの変更された設定が［**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。

7. ［**信頼ゾーン**］ウィンドウで［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## 信頼するオブジェクトを削除する

*信頼するオブジェクトを削除するには、次の操作を行います：*

1. ［設定］ウィンドウを開きます。

2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開き、［**信頼するオブジェクト**］タブが表示されます。

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. [**削除**］をクリックします。

削除された信頼するオブジェクトが、リストから表示されなくなります。

6. ［**信頼ゾーン**］ウィンドウで［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開き、［**信頼するオブジェクト**］タブが表示されます。
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. 次のいずれかの手順を実行します：
   - 信頼するオブジェクトを有効にするには、信頼するオブジェクト名の隣にあるチェックボックスをオンにします。
   - 信頼するオブジェクトを無効にするには、信頼するオブジェクト名の隣にあるチェックボックスをオフにします。
6. ［**OK**］をクリックします。
7. 変更を保存するには［**保存**］をクリックします。

## 信頼するアプリケーションのリストの編集

*信頼するアプリケーションのリストを編集するには：*

1. ［設定］ウィンドウを開きます。
2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開きます。
4. ［**信頼ゾーン**］ウィンドウで、［**信頼するアプリケーション**］タブを選択します。
5. 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、次の手順に従います：
   a. ［**追加**］をクリックします。

b. 表示されるコンテキストメニューで、次のいずれかを実行します：

- 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リストからアプリケーションを見つけるには、メニューの［**アプリケーション**］項目を選択します。

  ［**アプリケーションの選択**］ウィンドウが開きます。

- 目的のアプリケーションの実行ファイルのパスを指定するには、［**参照**］を選択します。

  Microsoft Windows 標準の［**開く**］ウィンドウが開きます。

c. 次のいずれかの方法でアプリケーションを選択します：

- 前の手順で［**アプリケーション**］を選択した場合、［**アプリケーションの選択**］ウィンドウで、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リストからアプリケーションを選択して［OK］をクリックします。

- 前の手順で［**参照**］を選択した場合、Microsoft Windows 標準の［開く］ウィンドウで、目的のアプリケーションの実行ファイルのパスを指定して［**開く**］をクリックします。

この処理を実行すると、［**信頼するアプリケーション**］ウィンドウが開きます。

a. 選択したアプリケーションに対する信頼ゾーンルールの横にあるチェックボックスをオンにします：

- **開いたファイルをスキャンしない**
- **アプリケーションの動作を監視しない**
- **親プロセス（親アプリケーション）の制限を継承しない**
- **子アプリケーションの動作を監視しない**
- **アプリケーションインターフェイスとの相互作用をブロックしない**
- **ネットワークトラフィックをスキャンしない**

b. ［**信頼するアプリケーション**］ウィンドウで、［OK］をクリックします。

追加した信頼するアプリケーションが信頼するアプリケーションのリストに表示されます。

6. 信頼するアプリケーションの設定を編集するには、次の手順に従います：

a. 信頼するアプリケーションのリストで、信頼するアプリケーションを選択します。

b. ［**編集**］をクリックします。

c. ［**信頼するアプリケーション**］ウィンドウが開きます。

d. 選択したアプリケーションに対する信頼ゾーンルールの横にあるチェックボックスをオンまたはオフにします：

> ［**信頼するアプリケーション**］ウィンドウで信頼ゾーンルールがすべてオフになっている場合、信頼するアプリケーションはスキャン対象に含まれます。この場合、信頼するアプリケーションは信頼するアプリケーションのリストから除外されませんが、そのチェックボックスはオフにされます。

e. ［**信頼するアプリケーション**］ウィンドウで、［OK］をクリックします。

7. 信頼するアプリケーションのリストから信頼するアプリケーションを削除するには、次の手順に従います：

   a. 信頼するアプリケーションのリストで、信頼するアプリケーションを選択します。

   b. [**削除**］をクリックします。

8. ［**信頼ゾーン**］ウィンドウで［**OK**］をクリックします。

9. 変更を保存するには［**保存**］をクリックします。

## 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対する信頼ゾーンルールを有効または無効にする

*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. ［設定］ウィンドウを開きます。

2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開きます。

4. ［**信頼ゾーン**］ウィンドウで、［**信頼するアプリケーション**］タブを選択します。

5. 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。

6. 次のいずれかの手順を実行します：

   - 信頼するアプリケーションを Kaspersky Endpoint Security によるスキャンから除外するには、そのアプリケーション名の横にあるチェックボックスをオンにします。

   - 信頼するアプリケーションを Kaspersky Endpoint Security によるスキャンに含めるには、そのアプリケーション名の横にあるチェックボックスをオフにします。

7. ［**OK**］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

## 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「*許可*」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. ［設定］ウィンドウを開きます。

2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開きます。

4. ［**信頼ゾーン**］ウィンドウで、［**信頼するシステム証明書ストア**］タブを選択します。

5. ［**信頼するシステム証明書ストアを使用**］をオンにします。

6. ［**信頼するシステム証明書ストア**］ドロップダウンリストで、Kaspersky Endpoint Security が信頼する必要があるシステムストアを選択します。

7. ［**信頼ゾーン**］ウィンドウで［OK］をクリックします。

8. 変更を保存するには［**保存**］をクリックします。

# Kaspersky Endpoint Security セルフディフェンス

このセクションでは、Kaspersky Endpoint Security のセルフディフェンス機構とリモートコントロールディフェンス機構の情報と、これらの機構の設定方法について説明します。

# Kaspersky Endpoint Security セルフディフェンスの概要

Kaspersky Endpoint Security は、Kaspersky Endpoint Security の処理をブロックしたり、Kaspersky Endpoint Security をコンピューターから削除したりしようとするマルウェアなどの悪意のあるプログラムからコンピューターを保護します。

コンピューターのセキュリティシステムの安定性は、Kaspersky Endpoint Security のセルフディフェンス機構およびリモートコントロールディフェンス機構によって維持されます。

セルフディフェンス機構は、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。

リモートコントロールディフェンスは、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管理の試みをすべてブロックします。

64 ビット版オペレーティングシステムで稼働するコンピューターでは、ハードディスク上のアプリケーションファイルとシステムレジストリのエントリの改竄および削除を防止するセルフディフェンス機能のみが使用可能です。

# セルフディフェンスの有効化または無効化

既定では、Kaspersky Endpoint Security のセルフディフェンス機構は有効です。必要に応じて、セルフディフェンスを無効にすることができます。

*セルフディフェンスを有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. 次のいずれかの手順を実行します：
   - 製品のセルフディフェンス機構を有効にするには、［**セルフディフェンスを有効にする**］をオンにします。
   - 製品のセルフディフェンス機構を無効にするには、［**セルフディフェンスを有効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## リモートコントロールディフェンスの有効化または無効化

リモートコントロールディフェンス機構は、既定では有効です。必要に応じて、リモートコントロールディフェンスを無効にすることができます。

*リモートコントロールディフェンス機構を有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. 次のいずれかの手順を実行します：
   - リモートコントロールディフェンス機構を有効にするには、［**システムサービスの外部からの管理を無効にする**］をオンにします。
   - リモートコントロールディフェンス機構を無効にするには、［**システムサービスの外部からの管理を無効にする**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## リモート管理アプリケーションのサポート

外部のコントロールプロテクションが有効のとき、リモート管理アプリケーションが必要と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. ［設定］ウィンドウを開きます。
2. 左にある［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。

3. ［**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。
   ［**信頼ゾーン**］ウィンドウが開きます。

4. ［**信頼ゾーン**］ウィンドウで、［**信頼するアプリケーション**］タブを選択します。

5. ［**追加**］をクリックします。

6. 表示されるコンテキストメニューで、次のいずれかを実行します：

   - 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リストからリモート管理アプリケーションを見つけるには［**アプリケーション**］項目を選択します。
     ［**アプリケーションの選択**］ウィンドウが開きます。

   - 目的のリモート管理アプリケーションの実行ファイルのパスを指定するには、［**参照**］を選択します。
     Microsoft Windows 標準の［**開く**］ウィンドウが開きます。

7. 次のいずれかの方法でアプリケーションを選択します：

   - 前の手順で［**アプリケーション**］を選択した場合、［**アプリケーションの選択**］ウィンドウで、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リストからアプリケーションを選択して［**OK**］をクリックします。

   - 前の手順で［**参照**］を選択した場合、Microsoft Windows 標準の［開く］ウィンドウで、目的のアプリケーションの実行ファイルのパスを指定して［**開く**］をクリックします。

   この処理を実行すると、［**信頼するアプリケーション**］ウィンドウが開きます。

8. ［**アプリケーションの動作を監視しない**］をオンにします。

9. ［**信頼するアプリケーション**］ウィンドウで、［**OK**］をクリックします。
   追加した信頼するアプリケーションが信頼するアプリケーションのリストに表示されます。

10. 変更を保存するには［**保存**］をクリックします。

# 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

このセクションでは、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について説明します。また、検知可能なオブジェクトの種類と Kaspersky Endpoint Security の動作モードを選択するためのガイドラインも提供します。

# 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の概要

## 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種別のうち検知できるものの数に関係します。

## 検知可能なオブジェクトの選択

Kaspersky Endpoint Security では、コンピューターのプロテクションを詳細に調整し、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強化するために、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可能にして、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、ポータブルコンピューター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
- 脆弱性スキャンタスク
- 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、ポータブルコンピューター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。ポータブルコンピューター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の同時操作の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

最近の悪意のあるプログラムは、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すで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プログラム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おそれがあります。

ワークステーション用 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。

サーバー用 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再起動プロンプトは表示できません。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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ［**オブジェクト**］セクションの［**設定**］をクリックします。
   ［**検知するオブジェクト**］ウィンドウが表示されます。
4. 以下のチェックボックスを使用して、Kaspersky Endpoint Security に検知させるオブジェクトの種類を選択します：
   - **悪意のあるツール**
   - **アドウェア**
   - **オートダイヤラー**
   - **その他の脅威**
   - **損害を与える可能性がある圧縮ファイル**
   - **多重圧縮ファイル**
5. ［OK］をクリックします。
   ［**検知するオブジェクト**］ウィンドウが閉じます。［**オブジェクト**］セクションの［**次のオブジェクト種別の検知が有効です**］の下に、選択したオブジェクトの種類が表示されます。

6. 変更を保存するには［**保存**］をクリックします。

## ワークステーション向けの特別な駆除の有効化または無効化

*ワークステーション向けの特別な駆除を有効または無効にするには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**プロテクション**］セクションを選択します。
   ウィンドウの右側に、プロテクション設定が表示されます。
3. ウィンドウの右側で、次のいずれかの手順を実行します：
   - ［**特別な駆除を有効にする**］をオンにし、特別な駆除を有効にします。
   - ［**特別な駆除を有効にする**］をオフにし、特別な駆除を無効にします。
4. 変更を保存するには［**保存**］をクリックします。

［特別な駆除］タスクを Kaspersky Security Center から開始すると、ユーザーがオペレーティングシステムの機能の大部分を使用できなくなります。タスクが完了すると、ワークステーションが再起動します。

## サーバー向けの特別な駆除の有効化または無効化

*サーバーで特別な駆除技術を有効にするには、次のいずれかの手順を実行します：*

- アクティブな Kaspersky Security Center ポリシーのプロパティで、特別な駆除技術を有効化します。次の手順に従います：
  a. ポリシーのプロパティウィンドウで［**全般的なプロテクション設定**］セクションを開きます。
  b. ［**特別な駆除を有効にする**］をオンにします。
  c. 変更を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。
- Kaspersky Security Center のウイルススキャングループタスクのプロパティで、［**すぐに特別な駆除を実行する**］をオンにします。

*サーバーで特別な駆除技術を無効にするには、次のいずれかの手順を実行します。*

- Kaspersky Security Center ポリシーのプロパティで、特別な駆除技術を有効化します。次の手順に従います：
  a. ポリシーのプロパティウィンドウで［**全般的なプロテクション設定**］セクションを開きます。
  b. ［**特別な駆除を有効にする**］をオフにします。
  c. 変更を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

- Kaspersky Security Center のウイルススキャングループタスクのプロパティで、［**すぐに特別な駆除を実行する**］をオフにします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. ［**動作方法**］セクションで、［**設定**］をクリックします。
   ［**動作方法**］ウィンドウが開きます。
4. ［**動作方法**］ウィンドウで次の処理を実行します：
   - 省エネモードを有効にするには、［**バッテリー使用中はスケジュールタスクを延期する**］をオンにします。
     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
     - 脆弱性スキャンタスク
     - 整合性チェックタスク
   - 省エネモードを無効にするには、［**バッテリー使用中はスケジュールタスクを延期する**］をオフにします。この場合、Kaspersky Endpoint Security はコンピューターの電源にかかわらず、スケジュールされているタスクを実行します。
5. 変更を保存するには［**保存**］をクリックします。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. ［**動作方法**］セクションで、［**設定**］をクリックします。

［**動作方法**］ウィンドウが開きます。

4. ［**動作方法**］ウィンドウで次の処理を実行します：

   - リソースを他のアプリケーションに割り当てるモードを有効にするには、［**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**］をオンにします。

     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
     - 脆弱性スキャンタスク
     - 整合性チェックタスク

   - リソースを他のアプリケーションに割り当てるモードを無効にするには、［**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**］をオフにします。この場合、Kaspersky Endpoint Security は他のアプリケーションの動作にかかわらず、スケジュールされているタスクを実行します。

   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。

5. 変更を保存するには［**保存**］をクリックします。

# パスワードによる保護

このセクションでは、パスワードを使用して Kaspersky Endpoint Security へのアクセスを制限する方法について説明します。

## Kaspersky Endpoint Security へのアクセス制限の概要

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されていない場合、コンピューター保護の全体のレベルが低下することがあります。

Kaspersky Endpoint Security へのアクセスを制限するには、ユーザー名とパスワードを設定し、それらの認証情報の入力をユーザーに求める製品の操作を指定します。

本製品の以前のバージョンを Kaspersky Endpoint Security 10 Service Pack 2 for Windows にアップグレードする場合、設定されていたパスワードは保存されません。パスワードによる保護の設定を初めて編集する際は、既定のユーザー名 KLAdmin を使用します。

# パスワードによる保護の有効化と無効化

パスワードを使用して本製品へのアクセスを制限する場合は、注意してください。パスワードを忘れた場合は、カスペルスキーのテクニカルサポートに、パスワードによる保護の解除方法を問い合わせてください。

*パスワードによる保護を有効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   アプリケーションの設定が、ウィンドウの右側に表示されます。
3. ［**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**］ウィンドウが開きます。
4. ［**パスワードによる保護を有効にする**］をオンにします。
5. ［**ユーザー名**］に、パスワードで保護された操作の実行時に［**パスワードの確認**］ウィンドウで指定するユーザー名を入力します。
6. ［**新しいパスワード**］に、本製品にアクセスする際のパスワードを入力します。
7. ［**新しいパスワードの確認**］でパスワードを確認します。
8. 本製品のすべての操作に対するアクセスを制限するには、［**パスワードを要求する操作**］セクションで［**すべて選択**］をクリックします。
9. ユーザーアクセスの制限を選択するには、［**パスワードを要求する操作**］セクションで、該当する操作の横にあるチェックボックスをオンにします：
   - **本製品の設定**
   - **本製品の終了**
   - **保護コンポーネントの停止**
   - **管理コンポーネントの停止**
   - **ライセンスの削除**
   - **本製品の削除 / 変更 / 修復**
   - **暗号化されたドライブ上のデータへのアクセスの復元**
   - **レポートの表示**
10. ［**OK**］をクリックします。
    製品は次のように入力されたパスワードを確認します：パスワードが一致する場合、そのパスワードが適用されます。パスワードが一致しないと、［**パスワードの確認**］にパスワードを再入力するよう求められます。

パスワードによる保護が有効になると、パスワードの範囲に含まれる操作が実行されるたびにパスワードの入力が求められる。現在のセッション中にパスワードで保護された操作を再度試行するたびにパスワードの入力を求められないようにする場合は、［**パスワードの確認**］ウィンドウで［**現在のセッションでパスワードを保存する**］をオンにしてください。

［**現在のセッションでパスワードを保存する**］をオフにすると、パスワードで保護された操作を試みるたびに、パスワードの入力が求められます。

*パスワードによる保護を無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   アプリケーションの設定が、ウィンドウの右側に表示されます。
3. ［**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**］ウィンドウが開きます。
4. ［**パスワードによる保護を有効にする**］をオフにします。

   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。

5. ［OK］をクリックします。

パスワードによる保護が無効になると、Kaspersky Endpoint Security の次回起動時に本製品へのアクセス制限がキャンセルされます。

## Kaspersky Endpoint Security のアクセスパスワードの変更

*Kaspersky Endpoint Security のアクセスパスワードを変更するには、次の手順を実行します：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
3. ［**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**］ウィンドウが開きます。
4. ［**ユーザー名**］にユーザー名を入力します。
5. ［**新しいパスワード**］に、製品にアクセスするための新しいパスワードを入力します。
6. ［**パスワードの確認**］に、新しいパスワードを再度入力します。
7. ［OK］をクリックします。
   製品は次のように入力されたパスワードを確認します：パスワードが一致すると、新しいパスワードが適用され、［**パスワードによる保護**］ウィンドウが閉じます。パスワードが一致しないと、［**パスワードの確認**］にパスワードを再入力するよう求められます。

8. 変更内容を保存するには、［設定］ウィンドウの［**保存**］をクリックします。

## 一時パスワードの使用について

Kaspersky Security Center のポリシーで管理されているクライアントコンピューターで作業しているユーザーが、ポリシーレベルでパスワードによって保護されている Kaspersky Endpoint Security の操作を実行する必要がある場合があります。パスワードによる保護が有効な場合、パスワードの範囲で指定された操作は、Kaspersky Security Center 管理者のみが実行できます。ただし、Kaspersky Security Center との接続が失われた場合（ユーザーが企業ネットワークの外にいる場合など）、Kaspersky Security Center のローカルインターフェイスで作業する機能が制限されます。

ユーザーに対し、ポリシー設定で設定されているパスワードを渡さずに必要な操作を実行できるようにするには、Kaspersky Security Center 管理者が一時パスワードを作成します。一時パスワードは、有効期間と操作の範囲が限定されます。ユーザーが本製品のローカルインターフェイスに一時パスワードを入力すると、Kaspersky Security Center 管理者が許可した操作が使用可能になります。

一時パスワードの有効期間が終了すると、Kaspersky Endpoint Security は、Kaspersky Security Center ポリシーの設定に従って動作します。ポリシーレベルでパスワードによって保護されている動作は、ユーザーが実行できなくなります。

## Kaspersky Security Center 管理コンソールを使用した一時パスワードの作成

*一時パスワードを作成してユーザーに送信するには：*

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、一時パスワードを要求しているユーザーのコンピューターが属してい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. 一時パスワードを要求しているユーザーのコンピューターのコンテキストメニューで、［**プロパティ**］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。
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. ［Kaspersky Endpoint Security Service Pack 2 for Windows］を選択し、次のいずれかの方法でアプリケーションのプロパティウィンドウを開きます。

   - 画面下部の［**プロパティ**］をクリックします。
   - 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。

   アプリケーションの設定ウィンドウが開きます。
7. アプリケーションの設定ウィンドウの［**詳細設定**］セクションで、［**アプリケーション設定**］サブセクションを選択します。
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**］ウィンドウが開きます。

9. ［**パスワードによる保護**］ウィンドウの［**一時パスワード**］セクションで、［**設定**］をクリックします。

このボタンは、コンピューターで動作している Kaspersky Security Center ポリシーで Kaspersky Security Center のパスワードによる保護が有効な場合に使用できます。

［**一時パスワードを作成**］ウィンドウが開きます。

10. ［**有効期限**］で、一時パスワードを使用できなくなる日を指定します。

一時パスワードは、表示されている日に無効になります。Kaspersky Endpoint Security のローカルインターフェイスで操作を実行する権限を付与するには、新しい一時パスワードを作成する必要があります。

11. ［**一時パスワードの範囲**］テーブルで、一時パスワードが有効なあいだにユーザーが使用でき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。

［**一時パスワード**］が開き、暗号化パスワードが表示されます。

13. パスワードと適用手順をコピーし、ユーザーに送信します。

## Kaspersky Endpoint Security のインターフェイスでの一時パスワードの適用

以下の手順は、Kaspersky Endpoint Security がインストールされているクライアントコンピューターのユーザー向けです。

*一時パスワードを適用するには：*

1. ［設定］ウィンドウを開きます。

2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。

アプリケーションの設定が、ウィンドウの右側に表示されます。

3. ［**パスワードによる保護**］セクションで、［**一時パスワード**］をクリックします。

［**一時パスワード**］ウィンドウが開きます。

4. ［**一時パスワードを有効にする**］をオンにします。

5. 入力フィールドに、Kaspersky Security Center の管理者から送信されたパスワードを入力します。

6. ［**OK**］をクリックして、変更内容を保存します。

一時パスワードを適用すると、Kaspersky Security Center 管理者が許可した操作が使用可能になります。［**一時パスワード**］ウィンドウには、一時パスワードの有効期限と許可された操作が表示されます。

# Kaspersky Security Center からの製品のリモート管理

このセクションでは、Kaspersky Security Center を使用した Kaspersky Endpoint Security の管理方法について説明します。

## Kaspersky Security Center からの製品の管理について

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を、リモートで実行できます。

Kaspersky Security Center を使用した本製品の管理についてのより詳しい情報は、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

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。

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。

## 異なるバージョンの管理プラグインを使用する場合の考慮事項

次を変更するために管理プラグインを使用できます：

- ポリシー
- ポリシーのプロファイル
- グループタスク
- ローカルタスク
- Kaspersky Endpoint Security のローカル設定

管理プラグインのバージョンが、Kaspersky Endpoint Security と管理プラグインの互換性に関する情報で示されているバージョン以上である場合のみ、Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理できます。必要な管理プラグインの最小バージョンは、配布キットにある installer.ini ファイルで確認できます。

コンポーネントが起動されると、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、そのコンポーネント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コンポーネント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グレードしてください。

### 以前指定された設定を新しいバージョンの管理プラグインで変更する

新しいバージョンの管理プラグインを使用して、以前指定されたすべての設定を変更し、以前使用していたバージョンの管理プラグインにはなかった新しい設定を指定できます。

新しいバージョンの管理プラグインは、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、新しい設定に規定値を割り当てます。

新しいバージョンの管理プラグインを使用して、ポリシー、ポリシーのプロファイル、グループタスクの設定を変更すると、コンポーネントは以前のバージョンの管理プラグインでは使用できなくなります。Kaspersky Endpoint Security のローカル設定とローカルタスクの設定は、以前のバージョンの管理プラグインで引き続き使用できます。

## クライアントコンピューター上の Kaspersky Endpoint Security の起動と終了

*クライアントコンピューター上で本製品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。

   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 10 for Windows］を選択します。
8. 次の手順に従います：

   - 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 ボタンをクリックするか、次の操作を行います：

     a. Kaspersky Endpoint Security のコンテキストメニューで［**プロパティ**］を選択するか、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 10 for Windows の設定ウィンドウが開きます。

     b. ［**全般**］セクションで、ウィンドウの右側にある［**開始**］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 ボタンをクリックするか、次の操作を行います：

a. Kaspersky Endpoint Security のコンテキストメニューで［**プロパティ**］を選択するか、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 10 for Windows の設定ウィンドウが開きます。

b. ［**全般**］セクションで、ウィンドウの右側にある［**停止**］をクリックします。

## Kaspersky Endpoint Security の設定

*Kaspersky Endpoint Security 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、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. アプリケーション「Kaspersky Endpoint Security 10 for Windows」を選択します。
8. 次のいずれかの手順を実行します：

   - Kaspersky Endpoint Security 10 for Windows のコンテキストメニューで［**プロパティ**］を選択します。
   - 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 10 for Windows の設定ウィンドウが開きます。
9. ［**詳細設定**］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 10 for Windows の設定**ウィンドウの残りのセクションは、Kaspersky Security Center の標準的なアプリケーション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 管理者用ガイド*』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、［**詳細**］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 10 for Windows の設定ウィンドウで［**OK**］をクリックします。

# タスクの管理

このセクションでは、Kaspersky Endpoint Security のタスクを管理する方法について説明します。Kaspersky Security Center を介したタスク管理の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

## Kaspersky Endpoint Security のタスクの概要

Kaspersky Security Center は、タスクを使用して、クライアントコンピューターにおけるカスペルスキー製品のアクティビティを管理します。タスクによって、ライセンスのインストール、コンピューターのスキャン、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といった基本的な管理機能が実装されます。

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
- 管理グループに属していないコンピューターグループ向けのタスク

> 管理グループに属していないコンピューターグループ向けのタスクは、タスク設定で指定されているクライアントコンピューターだけに適用されます。タスクが設定されているコンピューターグループに新しいクライアントコンピューターを追加しても、そのタスクは追加された新しいコンピューターには適用されません。追加された新しいコンピューターにタスクを適用するには、新しいタスクを作成するか、既存タスクの設定を編集します。

Kaspersky Endpoint Security をリモートで管理するには、次に挙げる種別のタスクを使用できます：

- **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。
- **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または削除します。
- **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収集されます。

  DLL モジュールとスクリプトファイルのインベントリを有効化できます。その場合、Kaspersky Security Center は、Kaspersky Endpoint Security がインストールされたコンポーネントで読み込まれた DLL モジュールの情報と、スクリプトを含むファイルの情報を受け取ります。

  > DLL モジュールとスクリプトファイルのインベントリを有効にすると、インベントリタスクの実行時間とデータベースのサイズが大幅に増加します。

- **アップデート**：アップデート設定に応じて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。
- **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。

- **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。
- **KSN との接続の確認**：KSN サーバーに対して使用可能性を問い合わせ、KSN 接続ステータスを更新します。
- **整合性チェック**：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ソフトウェアモジュールに関するデータを取得し、各モジュールの電子証明書をスキャンします。
- **認証エージェントアカウントの管理**：タスクの実行中に、認証エージェントアカウントを削除、追加、編集するコマンドを生成します。

タスクでは、次の操作を実行できます：

- タスクの開始、停止、一時停止、および再開
- 新しいタスクの作成
- タスク設定の編集

Kaspersky Endpoint Security のタスク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、Kaspersky Endpoint Security の各機能範囲に対するアクセス設定によって定義されます。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。

## タスク管理モードの設定

*Kaspersky Endpoint Security のローカルインターフェイスで、タスクの作業方法を設定するには：*

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、Kaspersky Endpoint Security のローカルインターフェイスでタスクの作業方法を設定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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. ［**詳細設定**］セクションで［**アプリケーション設定**］サブセクションを選択します。
7. ［**動作方法**］セクションで次の操作を実行します：
   - Kaspersky Endpoint Security のインターフェイスとコマンドラインを使用したローカルタスクの作業をユーザーに許可するには、［**ローカルタスクの使用を許可する**］をオンにします。

このチェックボックスをオフにすると、ローカルタスクの機能が停止します。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やコマンドラインでのローカルタスクの開始や編集もできなくなります。

- グループタスクのリストの表示をユーザーに許可するには、［**グループタスクの表示を許可する**］をオンにします。
- グループタスクの設定の編集をユーザーに許可するには、［**グループタスクの管理を許可する**］をオンにします。

8. ［**OK**］をクリックして、変更内容を保存します。
9. ポリシーを適用します。

   Kaspersky Security Center ポリシーの適用の詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

## ローカルタスクの作成

*ローカルタスクを作成するには：*

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、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. ローカルタスクを作成するコンピューターを選択します。
5. 次のいずれかの手順を実行します：
   - 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［**すべてのタスク**］ - ［**タスクの作成**］を選択します。
   - クライアントコンピューターのコンテキストメニューで［**プロパティ**］を選択し、表示されるコンピューターのプロパティウィンドウの［**タスク**］タブで［**追加**］をクリックします。
   - ［**処理を実行**］で［**タスクの作成**］を選択します。

   タスクウィザードが起動します。
6. タスクウィザードの指示に従います。

## グループタスクの作成

*グループタスクを作成するには：*

1. Kaspersky Security Center の管理コンソールを開きます。

2. 次のいずれかの手順を実行します：

   - コンソールツリーで、［**管理対象デバイス**］フォルダーを選択して、Kaspersky Security Center が管理するすべてのコンピューターを対象にしたグループタスクを作成します。
   - コンソールツリーの［**管理対象デバイス**］フォルダーで、該当するクライアントコンピューターを含む管理グループの名前のフォルダーを選択します。

3. 作業領域で［**タスク**］タブを選択します。
4. ［**タスクの作成**］をクリックします。
   タスクウィザードが起動します。
5. タスクウィザードの指示に従います。

## デバイスの抽出タスクの作成

*デバイスを抽出するタスクを作成するには、次の手順を実行します：*

1. Kaspersky Security Center の管理コンソールを開きます。
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. ［**タスクの作成**］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。
5. ［**タスクを割り当てるデバイスの選択**］ウィンドウで、［**デバイスの抽出にタスクを割り当てる**］を選択します。
6. ウィザードの次のウィンドウで［**参照**］をクリックします。
   ［**デバイスの抽出**］ウィンドウが開きます。
7. 必要なデバイスを選択します。
8. ［**デバイスの抽出**］ウィンドウで［**OK**］をクリックします。
9. タスクウィザードの指示に従います。

## タスクの開始、終了、一時停止、再開

クライアントコンピューターで Kaspersky Endpoint Security アプリケーションが実行中の場合、Kaspersky Security Center を使用してこのクライアントコンピューターのタスクを開始、停止、一時停止、再開できます。Kaspersky Endpoint Security が一時停止している場合、タスクの実行も一時停止し、Kaspersky Security Center を使用してタスクを開始、停止、一時停止、再開することはできなくなります。

*ローカルタスクを開始、停止、一時停止、再開するには：*

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. ローカルタスクの開始、停止、一時停止、再開を実行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。

   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. ［**タスク**］セクションを選択します。

   ウィンドウの右側に、ローカルタスクのリストが表示されます。
7. 開始、停止、一時停止、再開するローカルタスクを選択します。
8. 次のいずれかの方法で、タスクに対して必要な処理を実行します：

   - ローカルタスクを右クリックしてコンテキストメニューを表示し、［**開始**］、［**停止**］、［**一時停止**］、［**再開**］を選択します。
   - ローカルタスクを開始または停止するには、ローカルタスクリストの右側にある / をクリックします。
   - 次の手順に従います：

     a. ローカルタスクのリストの下にある［**プロパティ**］をクリックするか、タスクのコンテキストメニューで［**プロパティ**］を選択します。

     タスクのプロパティウィンドウが開きます。

     b. ［**全般**］タブで、［**開始**］、［**停止**］、［**一時停止**］、［**再開**］をクリックします。

*グループタスクを開始、停止、一時停止、再開するには：*

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、グループタスクの開始、停止、一時停止、または再開の対象に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［**タスク**］タブを選択します。

   グループタスクが、ウィンドウの右側に表示されます。
4. 開始、停止、一時停止、再開するグループタスクを選択します。
5. 次のいずれかの方法で、タスクに対して必要な処理を実行します：

   - グループタスクのコンテキストメニューで［**開始**］、［**停止**］、［**一時停止**］、［**再開**］を選択します。
   - ウィンドウの右側の / をクリックして、グループタスクを開始または停止します。
   - 次の手順に従います：

a. 管理コンソールの作業領域の右側にある［**タスクの設定**］をクリックするか、タスクのコンテキストメニューで［**プロパティ**］を選択します。

タスクのプロパティウィンドウが開きます。

b. ［**全般**］タブで、［**開始**］、［**停止**］、［**一時停止**］、［**再開**］をクリックします。

*選択されたコンピューターのタスクを開始、停止、一時停止、再開するには：*

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［**タスク**］フォルダーで、開始、停止、一時停止、再開する選択されたコンピューターのタスクを選択します。
3. 次のいずれかの手順を実行します：

- タスクのコンテキストメニューで［**開始**］、［**停止**］、［**一時停止**］、［**再開**］を選択します。
- ウィンドウの右側の / をクリックして、選択されたコンピューターのタスクを開始または停止します。
- 次の手順に従います：

a. 管理コンソールの作業領域の右側にある［**タスクの設定**］をクリックするか、タスクのコンテキストメニューで［**プロパティ**］を選択します。

タスクのプロパティウィンドウが開きます。

b. ［**全般**］タブで、［**開始**］、［**停止**］、［**一時停止**］、［**再開**］をクリックします。

## タスク設定の編集

*ローカルタスクの設定を編集するには：*

1. Kaspersky Security Center の管理コンソールを開きます。
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。

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. ［**タスク**］セクションを選択します。

ウィンドウの右側に、ローカルタスクのリストが表示されます。

7. ローカルタスクのリストから必要なローカルタスクを選択してください。
8. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：

- ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
- 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

9. ローカルタスクのプロパティウィンドウで、設定するセクションを選択します。
10. ローカルタスク設定を編集します。
11. 変更内容を保存するには、ローカルタスクのプロパティウィンドウで［OK］をクリックします。
12. 変更内容を保存するには、コンピューターのプロパティウィンドウで［OK］をクリックします。

*グループタスクの設定を編集するには：*

1. Kaspersky Security Center の管理コンソールを開きます。
2. ［**管理対象デバイス**］フォルダーで、必要な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［**タスク**］タブを選択します。
   グループタスクが、管理コンソールの作業領域に表示されます。
4. 必要なグループタスクを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
6. グループタスクのプロパティウィンドウで、設定するセクションを選択します。
7. グループタスク設定を編集します。
8. 変更内容を保存するには、グループタスクのプロパティウィンドウで［OK］をクリックします。

*コンピューターの抽出に対するタスク設定を編集するには：*

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［**タスク**］フォルダーで、設定を編集するコンピューターの抽出のタスクを選択します。
3. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。
4. コンピューターの抽出に対するタスクのプロパティウィンドウで、設定するセクションを選択します。
5. コンピューターの抽出に対するタスクの設定を編集します。
6. 変更内容を保存するには、コンピューターの抽出に対するタスクのプロパティウィンドウで［OK］をクリックします。

タスクプロパティウィンドウの［**プロパティ**］セクション以外のセクションはすべて、Kaspersky Security Center で使用されているセクションと同じです。詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。［**設定**］セクションには、Kaspersky Endpoint Security 10 for Windows 固有の設定が含まれます。その内容は、選択するタスクまたはタスク種別によって異なります。

# ポリシーの管理

このセクションでは、Kaspersky Endpoint Security のポリシーの作成と設定について説明します。Kaspersky Security Center のポリシーを使用した Kaspersky Endpoint Security の管理についてのより詳しい情報は、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

# ポリシーの概要

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 Endpoint Security を使用して、管理グループ内の個々のコンピューターに対してポリシーによって指定された設定値をローカルに変更できます。ポリシーによって変更がブロックされていない設定のみ、ローカルで変更できます。

クライアントコンピューター上の製品設定を編集できるかどうかは、ポリシー内の設定の「ロック」ステータスによって異なります：

- 設定が「ロック」（）されている場合は、その設定の値はローカルで編集できません。ポリシーで指定された設定値が、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で使用されます。
- 設定の「ロックが解除」（）されている場合は、ローカルで編集できます。ローカルで構成された設定は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されます。ポリシーで構成された設定は適用されません。

ポリシーが最初に適用される際に、ローカルアプリケーションの設定がそのポリシー設定に従って変更されます。

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。

Kaspersky Endpoint Security の機能の範囲には、以下があります：

- プロテクション：この機能の範囲には、ファイルアンチウイルス、メールアンチウイルス、ウェブアンチウイルス、メッセンジャーアンチウイルス、脆弱性スキャン、スキャンタスクが含まれます。
- アプリケーション起動コントロールこの機能の範囲には、アプリケーション起動コントロールが含まれます。
- デバイスコントロールデバイスコントロールが含まれます。
- 暗号化：この機能の範囲には、ハードディスク、ファイル、フォルダーの暗号化が含まれます。
- 信頼ゾーン：この機能の範囲には、信頼ゾーンが含まれます。

- ウェブコントロールウェブコントロールが含まれます。
- 侵入防止この機能の範囲には、アプリケーション動作モニター、脆弱性モニター、ファイアウォール、ネットワーク攻撃防御、アプリケーション権限コントロールが含まれます。
- 基本的なプロテクション：この機能の範囲には、他の機能の範囲で指定されない全般的なアプリケーション設定が含まれます。ライセンス、KSN 設定、インベントリタスク、定義データベースとモジュールのアップデートタスク、セルフディフェンス、詳細アプリケーション設定、レポートと保管領域、パスワードによる保護の設定、アプリケーションインターフェイス設定が含まれます。

ポリシーでは、次の操作を実行できます：

- ポリシーの作成
- ポリシー設定の編集

  管理サーバーにアクセスするために使用したユーザーアカウントに、特定の機能の範囲の設定を編集する権限がない場合、その機能の範囲の設定を変更することはできません。

- ポリシーの削除
- ポリシーステータスの変更

Kaspersky Endpoint Security との相互作用と関連しないポリシーの使用については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

## ポリシーの作成

*ポリシーを作成するには：*

1. Kaspersky Security Center の管理コンソールを開きます。
2. 次のいずれかの手順を実行します：
   - Kaspersky Security Center が管理するすべてのコンピューターを対象にしたポリシーを作成する場合、コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。
   - コンソールツリーの［**管理対象デバイス**］フォルダーで、該当するクライアントコンピューターを含む管理グループの名前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. 次のいずれかの手順を実行します：
   - ［**ポリシーの作成**］をクリックします。
   - 右クリックしてコンテキストメニューを表示し、［**作成**］ - ［ポリシー］を選択します。

   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。

## ポリシー設定の編集

*ポリシー設定を編集するには、次の手順を実行します：*

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、ポリシー設定の編集対象に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、［**ポリシー**］タブを選択します。
4. 必要なポリシーを選択します。
5. 次のいずれかの方法で、ポリシーのプロパティウィンドウを開きます：
   - ポリシーのコンテキストメニューから［**プロパティ**］を選択します。
   - 管理コンソールの作業領域の右側にある［**ポリシーの設定**］をクリックします。

   Kaspersky Endpoint Security 10 for Windows のポリシー設定には、コンポーネントの設定と本製品の設定があります。ポリシーのプロパティウィンドウの［**プロテクション**］セクションと［**エンドポイントコントロール**］セクションには、保護コンポーネントと管理コンポーネントの設定が表示されます。［**データ暗号化**］セクションには、ファイルやフォルダーの暗号化設定が表示されます。［**詳細設定**］セクションには、製品の設定が表示されます。

   ポリシーの設定でデータ暗号化設定と管理コンポーネント設定の表示を有効にするには、Kaspersky Security Center の［**インターフェイスの設定**］ウィンドウで、対応するチェックボックスをオンにする必要があります。
6. ポリシー設定を編集します。
7. 変更内容を保存するには、ポリシーのプロパティウィンドウで［**OK**］をクリックします。

## Kaspersky Security Center ポリシーで表示される設定の選択

*Kaspersky Security Center のポリシーで表示される設定を選択するには：*

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 – <コンピューター名>**］のコンテキストメニューで、［表示］ - ［**インターフェイスの設定**］の順に選択します。

   ［**インターフェイスの設定**］ウィンドウが開きます。
3. ［**インターフェイスの設定**］ウィンドウで、Kaspersky Security Center のポリシー作成設定とポリシーのプロパティで表示する設定の横にあるチェックボックスをオンにします。
   - Kaspersky Security Center の新規ポリシーウィザードのウィンドウおよびポリシープロパティで管理コンポーネント設定の表示を有効にするには、［**エンドポイントコントロール設定の表示**］をオンにします。
   - Kaspersky Security Center の新規ポリシーウィザードのウィンドウおよびポリシープロパティでデータ暗号化設定の表示を有効にするには、［**データ暗号化と保護機能の表示**］をオンにします。

4. ［OK］をクリックします。

## Kaspersky Security Center サーバーへのユーザーメッセージの送信

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。

- アプリケーション起動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［アプリケーション起動コントロール］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にて 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にて 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。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にて 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メッセージの表示

アプリケーション起動コントロール、デバイスコントロール、ウェブコントロールでは、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。

ユーザーが管理者にメッセージを送信する方法は 2 つあります：

- Kaspersky Security Center イベント保管領域のイベント

  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 がアクティブポリシーの下で動作している場合、ユーザーのイベントが Kaspersky Security Center のイベント保管領域に送信されます。

- メール

  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 がポリシーの下で動作していない場合やモバイルポリシーの下で動作している場合、ユーザーの情報がメールで送信されます。

*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、［**抽出イベント**］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. 次のいずれかの方法で［**イベント設定**］ウィンドウを開きます：

   - イベントを右クリックします。表示されるコンテキストメニューで、［**プロパティ**］を選択します。
   - 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。

# Kaspersky Security Network への参加

このセクションでは、Kaspersky Security Network への参加に関する情報を提供し、Kaspersky Security Network の使用を有効または無効にする手順を説明しています。

# Kaspersky Security Network への参加の概要

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収集されたデータを使用しています。*Kaspersky Security Network* は、そのようなデータを収集するように設計されています。

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。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、一部の保護コンポーネントの効果が高まり、誤検知の可能性が低減されます。

インフラストラクチャの場所に応じて、グローバル KSN サービス（インフラストラクチャがカスペルスキーのサーバーによってホストされている）とプライベート KSN サービス（インフラストラクチャがインターネットサービスプロバイダーなど、サードパーティのサーバーによってホストされている）があります。

プライベート KSN を使用するには、ライセンスを変更した場合、新しいライセンスの詳細をサービスプロバイダーに提出します。そうしないと、KSN とのデータ交換ができません。

KSN に参加するユーザーのおかげで、カスペルスキーは脅威の種類とソースに関する情報を迅速に取得し、このような脅威を無効にするためのソリューションを開発し、本製品のコンポーネントにより表示される誤検知数を最小限に抑えることができます。

KSN に参加している間、製品の操作中に生成された統計情報が自動的に KSN に送信されます。コンピューターやデータに損害を与える目的で悪用される可能性がある特定のファイル（またはファイルの一部）をカスペルスキーに送信することもできます。

個人データは収集、処理、保存されません。KSN に参加している間に生成されたカスペルスキーの統計情報の送信や、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、カスペルスキーは 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を公開することがあります。この場合、KSN への接続ステータスは「*制限付きで有効*」になります。

Kaspersky Security Center 管理サーバーによって管理されるユーザーコンピューターは、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：

- ユーザーの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、外部ネットワーク接続への負荷を軽減し、ユーザーの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 プロキシサービスの詳細については、『*Kaspersky Security Center 管理者用ガイド*』を参照してください。

KSN プロキシサービスは、Kaspersky Security Center のポリシーのプロパティで設定できます。

Kaspersky Security Network への参加は任意です。本製品の初期設定中に、KSN への参加について案内されます。KSN への参加はいつでも開始または中止できます。

## 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. ［設定］ウィンドウを開きます。
2. ウィンドウの左側の［**詳細設定**］セクションで、［**KSN 設定**］サブセクションを選択します。
   Kaspersky Security Network の設定が、ウィンドウの右側に表示されます。
3. 次のいずれかの手順を実行します：
   - Kaspersky Security Network の使用を有効にするには、［**KSN 声明および参加条件に同意する**］をオンにします。
   - Kaspersky Security Network の使用を無効にするには、［**KSN 声明および参加条件に同意する**］をオフにします。
4. 変更を保存するには［**保存**］をクリックします。

## Kaspersky Security Network への接続の確認

*Kaspersky Security Network への接続を確認するには：*

1. メインウィンドウを開きます。
2. ウィンドウ上部の［**Kaspersky Security Network**］をクリックします。
   ［**Kaspersky Security Network**］ウィンドウが開きます。
   ［**Kaspersky Security Network**］ウィンドウの左側には、Kaspersky Security Network への接続モードが円形の **KSN** ボタンの形式で示されます：
   - Kaspersky Endpoint Security が Kaspersky Security Network に接続していない場合、**KSN** ボタンが灰色になります。この場合、**KSN** ボタンで示されるステータスは［*無効*］です。
   - Kaspersky Endpoint Security が Kaspersky Security Network に接続しており、KSN サーバーが使用可能な場合、**KSN** ボタンが緑になります。次の情報が、［**KSN**］の下に表示されます：［*有効*］ステータス、使用中の KSN の種別（［**プライベート KSN**］または［**グローバル KSN**］）、KSN サーバーと前回同期した日時。ウィンドウの右側に、ファイル、Web リソース、ソフトウェアの評価に関する統計情報が表示されます。

Kaspersky Endpoint Security は、ユーザーが［**Kaspersky Security Network**］ウィンドウを開く際に、KSN の使用状況に関する統計データを収集します。統計は、リアルタイムにアップデートされません。

- Kaspersky Endpoint Security が Kaspersky Security Network に接続しているが、KSN サーバーが使用できない場合、**KSN** ボタンが赤になります。**KSN** ボタンで示されるステータスは［*有効*］です。

  KSN サーバーと前回同期した時間が 15 分よりも前の場合、またはステータスが［*不明*］の場合、KSN サーバーが使用できないことを意味します。このような場合は、テクニカルサポート、またはサービスプロバイダーに問い合わせてください。

  次のような理由で、Kaspersky Security Network サーバーに接続できないことがあります：

  - コンピューターがインターネットに接続されていない。
  - 製品がアクティベートされていないか、ライセンスの有効期間が切れている。
  - ライセンス関連の問題が検知された（例：ライセンスがブラックリストに登録されている）。

## Kaspersky Security Network でのファイルの評価の確認

KSN サービスでは、カスペルスキーの評価データベースにあるアプリケーションに関する情報を取得できます。これにより、企業レベルでアプリケーション起動ポリシーを柔軟に管理し、犯罪者がコンピューターや個人情報に損害を与えるために使用する可能性のあるアドウェアなどのプログラムの起動を防止できます。

*Kaspersky Security Network でのファイルの評価を確認するには：*

1. 評価を確認するファイル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. ［**KSN のレピュテーションをチェック**］を選択します。

このオプションは、Kaspersky Security Network 声明の条項に同意している場合に使用できます。

［**<ファイル名> - KSN の評価**］ウィンドウが開きます。［**<ファイル名> - KSN の評価**］ウィンドウに、確認したファイルに関する以下の情報が表示されます：

- **パス**：ファイルが保存されているディスク上のパス
- **バージョン**：アプリケーションのバージョン（実行ファイルでのみ表示されます）
- **デジタル署名**：ファイルのデジタル署名の有無
- **署名日時**：証明書がデジタル署名で署名された日時
- **作成日時**：ファイルの作成日時
- **更新日時**：ファイルが前回変更された日時
- **サイズ**：ファイルがディスク上で占めている領域

- ファイルを信頼またはブロックしているユーザーの数に関する情報

## Kaspersky Security Network の強化された保護

Kaspersky Security Network は、ユーザーを高いレベルで保護します。保護の方法は、絶え間なく発生する高度な脅威やゼロデイ攻撃に対抗する目的で設計されています。クラウド技術と、カスペルスキーのウイルスアナリストの専門技術を統合することにより、ネットワーク上の最も高度な脅威に対する最高の保護が、本製品によって実現されます。

本製品の保護で強化された点の詳細は、カスペルスキーの Web サイトを参照してください。

# 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。

## カスペルスキーのフォーラム

特に緊急の対応が必要ではない場合は、カスペルスキーのWebフォーラムをご利用ください。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。

このフォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

# テクニカルサポートへのお問い合わせ

このセクションでは、テクニカルサポートの利用方法と利用条件について説明しています。

## テクニカルサポートの利用方法

製品のドキュメントや製品の情報源で問題の解決法が見つからない場合、テクニカルサポートに問い合わせてください。テクニカルサポート担当者が、製品のインストール方法や使用方法についてのお問い合わせに回答いたします。

テクニカルサポートは、製品版ライセンスを購入した場合にのみ利用できます。試用版ライセンスでは、テクニカルサポートは提供されません。

テクニカルサポートにご連絡いただく前に、「カスペルスキーのサポートサービス規約」をお読みください。

テクニカルサポートへの連絡方法は、次のとおりです：

- 電話によるテクニカルサポート
- カスペルスキーカンパニーアカウントのポータルを通じて、カスペルスキーテクニカルサポートにリクエストを送信

## テクニカルサポートの連絡先

テクニカルサポートを受ける方法は、カスペルスキーのテクニカルサポートサイトに記載されています。

テクニカルサポートにご連絡いただく前に、「カスペルスキーのサポートサービス規約」をお読みください。

## カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品を使用する企業向けのポータルです。このポータルは、オンラインリクエストを通じてユーザーとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストのステータスを追跡でき、リクエストの履歴を保存できます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語

- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語
- 日本語

カスペルスキーカンパニーアカウントについて詳しくは、テクニカルサポートサイトをご覧ください。

## テクニカルサポート用の情報収集

カスペルスキーのテクニカルサポートのスペシャリストに問題を報告した後で、*トレースファイル*の作成を要請される場合があります。このトレースファイルを使用して、アプリケーションコマンドの実行プロセスを順を追って追跡し、エラーが発生した製品動作の段階を特定することができます。

また、テクニカルサポートのスペシャリストから、オペレーティングシステムの詳細な情報や、コンピューターで実行中のプロセス、コンポーネントの動作に関する詳細なレポート、製品のクラッシュダンプを求められる場合があります。

必要な情報は、Kaspersky Endpoint Security で集めることができます。収集された情報は、ハードディスクに保存して、後から都合のよいときにアップロードできます。

診断の実行中、テクニカルサポートの担当者から次の製品設定を変更するよう求められる場合があります：

- 詳細な診断情報を収集する機能の有効化
- 標準のユーザーインターフェイスでは設定できない、個別の製品コンポーネントの設定の調整
- 収集される診断情報を保存および送信する設定の変更
- ネットワークトラフィックの取得およびログの設定

テクニカルサポートの担当者は、これらの操作に必要なすべての情報（操作の順番に関する詳細、変更する設定、設定ファイル、スクリプト、追加のコマンドライン機能、デバッグモジュール、特定の目的のためのユーティリティなど）を提供し、デバッグ用に収集されるデータの範囲についてお知らせします。収集された詳細な診断情報は、ユーザーのコンピューターに保存されます。収集されたデータがカスペルスキーに自動送信されることはありません。

ダンプファイルをカスペルスキーに送信するためのダンプサーバーのアドレスを決定するために用いられた設定は、ユーザーのコンピューターに保存されます。必要に応じて、この設定の値を、オペレーティングシステムのレジストリキー `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"` で編集できます。

上記の操作は、テクニカルサポートのスペシャリストによる監督下でのみ、指示に従って実行する必要があります。管理者用ガイドに記載されている以外の方法や、テクニカルサポートのスペシャリストに指示された以外の方法で本製品の設定を独自に変更すると、オペレーティングシステムが低速になったり、クラッシュしたり、コンピューターのセキュリティに影響したり、処理されるデータの可用性や完全性が損なわれたりする可能性があります。

## トレースファイルの作成

*トレースファイルを作成するには：*

1. メインウィンドウを開きます。
2. 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。
3. ［**サポート**］ウィンドウで、［**システムトレース**］をクリックします。
   ［**テクニカルサポート用の情報**］ウィンドウが開きます。
4. トレースプロセスを開始するには、［**トレースを有効にする**］をオンにします。
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. 問題が発生した状況を再現します。
7. トレースプロセスを停止するには、［**テクニカルサポート用の情報**］ウィンドウに戻り、［**トレースを有効にする**］をオフにします。

トレースファイルを作成したら、カスペルスキーのサーバーにトレース結果をアップロードする操作に進みます。

## トレースファイルの内容と保存場所

収集したデータの安全性の確保はユーザー個人に責任があります。コンピューターに保存されている収集したデータがカスペルスキーに送信されるまでは、そのデータの監視とアクセスの制限に留意してください。

本製品を使用している限り、トレースファイルは読めないように変更された形式で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恒久的に削除されます。

トレースファイルは、フォルダー <ドライブ名>\ProgramData\Kaspersky Lab に保存されます。

トレースファイルの名前は次のような形式になります：`KES<version number_dateXX.XX_timeXX.XX_pidXXX.><トレースファイルの種別>.log.enc1`

認証エージェントのトレースファイルは、次の名前で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`

トレースファイルに保存されたデータを確認できます。データの確認方法については、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。

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

## 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。
- 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。トラフィックは、trafmon2.ppl からのみトレースファイルに記録されます。
- 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機能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。

## 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。

### プラグインのトレースファイルの内容

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：

- コンテキストメニューからスキャンタスクを起動するプラグインの shellex.dll.log トレースファイルには、スキャンタスクの実行に関する情報およびプラグインのデバッグに必要なデータが含まれます。
- メールアンチウイルスプラグインの mcou.OUTLOOK.EXE トレースファイルには、メールアドレスを含め、メールメッセージの一部が含まれることがあります。

### 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。

## カスペルスキーへのダンプファイルとトレースファイルの送信を有効または無効にする

*カスペルスキーへのダンプファイルとトレースファイルの送信を有効または無効にするには：*

1. ［設定］ウィンドウを開きます。
2. ウィンドウの左側で、［**詳細設定**］セクションを選択します。
   製品の詳細設定が、ウィンドウの右側に表示されます。
3. ［**動作方法**］セクションで、［**設定**］をクリックします。
   ［**動作方法**］ウィンドウが開きます。
4. ［**動作方法**］ウィンドウで［**ダンプ書き出しを有効にする**］をオンにすると、本製品のダンプファイルの書き出しが有効になります。
5. 次のいずれかの手順を実行します：
   - 本製品の次の起動時に製品のクラッシュの原因を分析するためのダンプファイルとトレースファイルをカスペルスキーに送信するための通知を［**テクニカルサポート用の情報のサーバーへのアップロード**］ウィンドウに表示するには、［**ダンプファイルとトレースファイルを Kaspersky Lab に送信する**］をオンにします。

- そうしない場合、［**ダンプファイルとトレースファイルを Kaspersky Lab に送信する**］をオフにします。

6. ［**動作方法**］ウィンドウで［**OK**］をクリックします。

7. 変更を保存するには、メインウィンドウで［**保存**］をクリックします。

## ファイルをテクニカルサポートサーバーに送信する

オペレーティングシステム、トレースファイル、ダンプファイルに関する情報を含むファイルをカスペルスキーのテクニカルサポートの担当者に送信する必要があります。

*ファイルをテクニカルサポートサーバーに送信するには：*

1. Kaspersky Endpoint Security の動作異常の後で、Kaspersky Endpoint Security を再起動します。
   ［**直前のアプリケーションの起動が失敗しました**］ウィンドウが開きます。

   ダンプファイルまたはトレースファイルをテクニカルサポートに送信するまで、または［**キャンセル**］をクリックするまで、Kaspersky Endpoint Security を起動するたびに（コンピューターの再起動後も含め）［**直前のアプリケーションの起動が失敗しました**］ウィンドウが開きます。

2. ［**直前のアプリケーションの起動が失敗しました**］ウィンドウで［**詳細**］をクリックして、生成されたファイルのリストを開きます。

3. テクニカルサポートに送信するファイルの横のチェックボックスをオンにします。

4. ［**規約の表示**］をクリックします。
   ［**データ提供規約**］ウィンドウが表示されます。

5. データ提供規約のテキストを読んで、［**閉じる**］をクリックします。

6. ［**直前のアプリケーションの起動が失敗しました**］ウィンドウで、［**データ提供規約に同意する**］をオンにします。

7. ［**送信**］をクリックします。
   ［**リクエスト番号**］ウィンドウが開きます。

8. ［**リクエスト番号**］ウィンドウで、カスペルスキーカンパニーアカウントを通じてテクニカルサポートに問い合わせたときにリクエストに割り当てられた番号を指定します。

9. ［**OK**］をクリックします。

選択したデータファイルが圧縮され、テクニカルサポートのサーバーに送信されます。

## ダンプファイルとトレースファイルの保護の有効化または無効化

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とユーザーの個人情報が含まれます。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. ［設定］ウィンドウを開きます。
2. 左にある［**詳細設定**］セクションを選択します。
   アプリケーションの設定が、ウィンドウの右側に表示されます。
3. ［**動作方法**］セクションで、［**設定**］をクリックします。
   ［**動作方法**］ウィンドウが開きます。
4. 次のいずれかの手順を実行します：
   - 保護を有効にする場合は［**ダンプファイルとトレースファイルの保護を有効にする**］をオンにします。
   - 保護を無効にする場合は［**ダンプファイルとトレースファイルの保護を有効にする**］をオフにします。
5. ［**動作方法**］ウィンドウで［OK］をクリックします。
6. 変更を保存するには、メインウィンドウで［**保存**］をクリックします。

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。

## 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。

## 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、システムの他のコンポーネントとハードウェアバスを経由して通信します。

## 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（HTTP 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。

アンチウイルスによる保護では、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、カスペルスキーのスペシャリストによって作成されます。定期的にアップデートされ、カスペルスキー製品の配布キットに含まれています。

## アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を置換または追加する処理。

## アドレスのブラックリスト

カスペルスキー製品によって、メッセージの内容とは関係なくすべての受信メッセージがブロックされるメールアドレスのリスト。

## エクスプロイト

システムまたはソフトウェアの何らかの脆弱性を利用するプログラムコード。ユーザーの知らないうちにコンピューターにマルウェアをインストールさせる目的でよく使用されます。

## 隔離

Kaspersky Endpoint Security は、感染の可能性があるファイルをこのフォルダーに配置します。隔離されたファイルは暗号化された形式で保存されます。

## 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「コンテナー」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。これらは、悪意のあるコードが侵入する危険性がかなり高いファイルです。

## 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、既知の悪意のあるソフト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、使用を推奨しません。

## 感染の可能性があるファイル

既知のウイルスの修正されたコードまたはウイルスのコードに類似したコードを含むファイルのうち、カスペルスキーがまだ特定していないもの。感染の可能性があるファイルは、ヒューリスティック分析によって検知されます。

## 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。

## 管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center のコンポーネント。製品の管理にも使用できます。

## 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

ファイルのシグネチャがウイルスと似ているために、感染していないファイルが感染していると報告された場合に、誤検知になります。

## シグネチャ分析

Kaspersky Endpoint Security の定義データベースを使用する脅威の検知テクノロジー。定義データベースには、既知の脅威の説明と脅威を駆除する方法が登録されています。シグネチャ分析を使用する保護では、許容可能な最小限のセキュリティを実行します。カスペルスキーのエキスパートの提案に基づいて、この方法は常に有効になっています。

## 証明書

秘密鍵とその鍵の所有者および範囲に関する情報を含み、公開鍵が所有者のものであることを確認する電子文書。証明書は、それを発行した認証局によって署名されている必要があります。

## 証明書の件名

証明書に結び付けられている秘密鍵の所有者。オブジェクトには、ユーザーやアプリケーション、あらゆる仮想オブジェクト、コンピューター、またはサービスを設定できます。

## 証明書の発行元

証明書を発行した認証局。

## 証明書のハッシュ値

証明書の暗号鍵を特定するために使用される情報。ハッシュ値は、暗号鍵の値に暗号学的ハッシュ関数を適用することで生成されます。

## 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。

## 製品設定

あらゆる種類のタスクに共通していて、製品の動作全体を管理する製品設定（製品パフォーマンス設定、レポート設定、バックアップ設定など）。

## ソフトウェアモジュール

アプリケーションセットアップファイルに含まれていて、製品のコア機能を実装するファイル。製品が実行するそれぞれのタスクの種別に対応する独立した実行可能モジュール（リアルタイム保護、オンデマンドスキャン、アップデート）。メインウィンドウからコンピューターの完全スキャンを開始する場合は、そのタスクのモジュールを起動します。

## タスク

カスペルスキー製品によって実行される機能。ファイルのリアルタイム保護、デバイスの完全スキャン、定義データベースのアップデートなどがあります。

## タスク設定

各種のタスクに固有の製品設定。

## 定義データベース

定義データベースの公開日時点でカスペルスキーが認識している、コンピューターセキュリティの脅威に関する情報を含むデータベース。定義データベースのシグネチャは、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

システムのハードディスクが暗号化された後で認証プロセスを経て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。

## ネットワークエージェントコネクター

製品とネットワークエージェントを接続するアプリケーションの機能。ネットワークエージェントを使用すると、Kaspersky Security Center を通して製品をリモートで管理できます。

## ネットワークサービス

ネットワークアクティビティを定義するパラメータのセット。このネットワークアクティビティに対し、ファイアウォールの動作を規定するネットワークルールを作成できます。

## バックアップ

駆除または削除を試みる前に、作成されたファイルをバックアップコピーする特殊な保管領域。

## パッチ

製品の操作中やアップデートのインストール中に発見されたバグを修正するための製品への小さな追加事項。

## ヒューリスティック分析

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。

## ファイルの隔離への移動

感染の可能性があるファイルの処理方法の1つ。この方法によって、ファイルへのアクセスがブロックされ、ファイルは元の位置から隔離に移されます。このフォルダーでは、感染の脅威を取り除くために、ファイルは暗号化された状態のまま保管されます。

## ファイルマスク

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：

- ***** – 任意のゼロ文字以上の文字を置き換えます。
- **?** – 任意の1文字を置き換えます。

ファイル名と拡張子は、必ずピリオドで区切られていることに注意してください。

## フィッシング

機密情報を盗む目的のメールが送信されるインターネット詐欺の一種。多くの場合、金融関連のデータが標的になります。

## フィッシングサイトの URL のデータベース

カスペルスキーのエキスパート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。定義データベースデータベースは定期的にアップデートされ、カスペルスキー製品の配布キットの一部です。

## 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

プロテクション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。

## 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。

# 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

登録商標およびサービスマークは、それぞれ対応する所有者の所有財産です。

Adobe、Acrobat および Shockwave は米国 Adobe Systems Incorporated の米国およびその他の国における商標または登録商標です。

Mac、FireWire は米国 Apple の米国およびその他の国における登録商標です。

AutoCAD は、米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 の米国およびその他の国における商標または登録商標です。

Citrix および Citrix Provisioning Services は、米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。

dBase は dataBased Intelligence, Inc. の商標です。

EMC および SecurID は、EMC Corporation の米国およびその他の国における商標または登録商標です。

ICQ は ICQ LLC の商標および登録商標です。

Intel および Pentium は米国 Intel Corporation の米国およびその他の国における登録商標です。

Logitech は Logitech Company の米国および他の国における登録商標または商標です。

Mail.ru は Mail.Ru, LLC. の登録商標です。

Microsoft、Windows、Internet Explorer、Access、Excel、PowerPoint、Outlook、Outlook Express、Windows Server、Visual Basic、Visual FoxPro、BitLocker、LifeCam Cinema、PowerShell、Surface は Microsoft Corporation の米国およびその他の国における登録商標です。

Mozilla および Thunderbird は Mozilla Foundation の商標です。

Novell は Novell Inc. の米国およびその他の国における登録商標です。

Java および JavaScript は Oracle Corporation およびその子会社の登録商標です。

SafeNet は SafeNet, Inc. の登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited のライセンス契約の下で使用されています。