kaspersky

Kaspersky Endpoint Security 12.12 for Windows

© 2026 AO Kaspersky Lab

目次

Kaspersky Endpoint Security for Windows のヘルプ
- 新機能
- よくある質問（FAQ）

Kaspersky Endpoint Security for Windows
- 製品のモード：スタンダード、EDR Agent、Light Agent
- 製品の購入
- システム要件
- オペレーティングシステムの種別に応じて利用できる本製品の機能の比較
- 管理用コンソールの種別に応じて利用できる製品機能の比較表
- 他のアプリケーションとの互換性情報

本製品のインストールと削除
- Kaspersky Security Center による導入
  - 製品の標準インストール
  - インストールパッケージの作成
  - インストールパッケージ内の定義データベースのアップデート
  - リモートインストールタスクの作成
- ウィザードを使用したローカルへの製品のインストール
- System Center Configuration Manager を使用しての製品のリモートインストール
- ファイル setup.ini のインストール設定の説明
- コンポーネントの変更
- 旧バージョンの製品のアップグレード
  - 再起動せずに本製品をアップデートする
  - 本製品の SMU アップデート
- 本製品の削除

製品のライセンス
- 使用許諾契約書について
- ライセンスの概要
- ライセンスの証明書について
- 月額制サービスについて
- ライセンスについて
- アクティベーションコードの概要
- ライセンス情報ファイルについて
- ワークステーション向けのライセンス種別による製品機能の比較
- サーバー向けのライセンス種別による製品機能の比較
- 製品のアクティベーション
- ライセンスの削除
- ライセンス情報の表示
- ライセンスの更新または購入
- 月額制サービスの更新

データ提供
- 使用許諾契約書におけるデータ提供
- Kaspersky Security Network 使用時のデータ提供

Detection and Response ソリューション使用中のデータ提供
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform (EDR)
欧州連合の規則（GDPR）の順守
使用開始時に行う設定
Kaspersky Endpoint Security for Windows の管理プラグインについて
異なるバージョンの管理プラグインを使用する場合の留意点
外部サービスと相互作用する暗号化プロトコルを使用する場合の留意点
製品のインターフェイス
タスクバーの通知領域の製品アイコン
簡略化したアプリケーションインターフェイス
製品インターフェイスの表示の設定
本製品の使用準備
ポリシーの管理
ポリシーの作成
セキュリティレベルインジケーター
タスクの管理
個別のローカル環境用の製品設定
Kaspersky Endpoint Security の起動と終了
プロテクションとコントロールの一時停止と再開
設定ファイルの作成と使用
既定の設定の復元
Kaspersky Endpoint Security のパフォーマンスと他のアプリケーションとの互換性
省エネモードの有効化または無効化
他のアプリケーションへのリソースの供与の有効化または無効化
Kaspersky Endpoint Security のパフォーマンス最適化のためのベストプラクティス
マルウェアのスキャン
コンピューターのスキャン
コンピューターに接続されたリムーバブルドライブのスキャン
バックグラウンドスキャン
コンテキストメニューからのスキャン
アプリケーション整合性チェック
スキャン範囲の編集
スケジュールされたスキャンの実行
異なるユーザーとしてスキャンの実行
スキャンの最適化
定義データベースとソフトウェアモジュールのアップデート
データベースと製品機能のアップデートシナリオ
サーバーリポジトリからアップデート
共有フォルダーからアップデート
Kaspersky Update Utility を使用してのアップデート
モバイルモードでのアップデート
アップデートタスクの開始と停止
別のユーザーアカウントの権限でのアップデートタスクの開始
アップデートタスクの実行方法の選択
アップデート元の追加

製品機能のアップデート
プロキシサーバーを使用してのアップデート
前回のアップデートのロールバック
特別な駆除の技術
ワークステーションにおけるアクティブな脅威の駆除
サーバーにおけるアクティブな脅威の駆除
処理されていない脅威の排除
コンピューターの保護
ファイル脅威対策
ファイル脅威対策の有効化と無効化
ファイル脅威対策の自動的な一時停止
感染したファイルに対してファイル脅威対策が行う処理の変更
ファイル脅威対策の保護範囲の設定
スキャン方法の使用
ファイル脅威対策で使用するスキャン技術の設定
スキャンの最適化
複合ファイルのスキャン
スキャン方法の変更
コンテナスキャン
ホスト侵入防止
ホスト侵入防止の有効化と無効化
アプリケーションの信頼グループの管理
アプリケーションの信頼グループを変更する
信頼グループの権限の設定
Kaspersky Endpoint Security の前に起動したアプリケーションの信頼グループを選択する
不明なアプリケーションに信頼グループを選択する
デジタル署名されたアプリケーションに信頼グループを選択する
アプリケーション権限の管理
オペレーティングシステムのリソースと個人データの保護
未使用のアプリケーションに関する情報の削除
ホスト侵入防止の監視
音声、映像へのアクセスの保護
有害 USB 攻撃ブロック
有害 USB 攻撃ブロックの有効化と無効化
USB デバイスの認証時のセキュリティキーボードの使用
バーコードスキャナー認証
AMSI 保護
AMSI 保護の有効化と無効化
AMSI 保護によるファイルスキャンの最適化
ウェブ脅威対策
ウェブ脅威対策の有効化と無効化
悪意のある Web アドレスの検知方法
フィッシング対策
信頼する URL のリストの作成
信頼する URL のリストのエクスポート / インポート

メール脅威対策
- メール脅威対策の有効化と無効化
- 感染したメールに対する処理の変更
- メール脅威対策の保護範囲の設定
- メールに添付されている複合ファイルのスキャン
- メール添付ファイルのフィルター
- 添付ファイルのフィルターの拡張子のエクスポートおよびインポート
- Microsoft Office Outlook におけるメールのスキャン
- Thunderbird、MyOffice、R7-Office におけるメールのスキャン

ネットワーク脅威対策
- ネットワーク脅威対策の有効化と無効化
- 攻撃元コンピューターのブロック
- ブロックから除外するアドレスの設定
- ブロックの除外対象のリストのエクスポート / インポート
- 種別ごとのネットワーク脅威対策の設定

ファイアウォール
- ファイアウォールの有効化または無効化
- ネットワーク接続種別の変更
- ネットワークパケットルールの管理
  - ネットワークパケットルールの作成
  - ネットワークパケットルールの有効化または無効化
  - ネットワークパケットルールに対するファイアウォール処理の変更
  - ネットワークパケットルールの優先順位の変更
  - ネットワークパケットルールのエクスポートおよびインポート
  - XML でのネットワークパケットルールの定義
- アプリケーションネットワークルールの管理
  - アプリケーションネットワークルールの作成
  - アプリケーションネットワークルールの有効化と無効化
  - アプリケーションネットワークルールのファイアウォール処理の変更
  - アプリケーションネットワークルールの優先度の変更
- ネットワークモニター

脆弱性攻撃ブロック
- 脆弱性攻撃ブロックの有効化と無効化
- システムプロセスのメモリ保護

ふるまい検知

アンチクリプター
- 外部からの暗号化に対する共有フォルダーの保護の有効化または無効化
- 信頼できないコンピューターのブロック期間の設定
- 保護範囲の編集
- 外部データ暗号化用の信頼できるコンピューターの追加
- 外部からの暗号化に対する共有フォルダーの保護の除外リストのエクスポートおよびインポート

修復エンジン

Kaspersky Security Network
- Kaspersky Security Network の使用の有効化と無効化
- Kaspersky Private Security Network
- 保護機能のクラウドモードの有効化と無効化

KSN プロキシ設定
Kaspersky Security Network でのファイルの評価の確認
暗号化された接続のスキャン
暗号化された接続のスキャンの有効化
信頼するルート証明書のインストール
信頼されていない証明書を持つ暗号化された接続のスキャン
独自の証明書ストアにカスペルスキーの証明書を追加する
暗号化された接続をスキャンから除外する
データの消去
コンピューターのコントロール
ウェブコントロール
Web リソースへのアクセスルールの追加
Web リソースアドレスによるフィルター
Web リソースコンテンツによるフィルター
Web リソースへのアクセスルールのテスト
ウェブコントロールルールのエクスポートおよびインポート
ウェブコントロールルールの Web リソースアドレスのエクスポートおよびインポート
ユーザーが行っているインターネット活動の監視
ウェブコントロールメッセージのテンプレートの編集
Web リソースアドレスマスクの編集
仮想マシンのウェブコントロール
ウェブコントロールのメッセージテンプレートの変数
デバイスコントロール
アクセスルールの概要
種別ごとのデバイスへのアクセスの管理
接続バスによるデバイスへのアクセスの管理
デバイスに対するユーザーアクセス権の区別
モバイルデバイスへのアクセスの管理
Bluetooth デバイスへのアクセスの管理
プリンターのコントロール
Wi-Fi 接続の制御
リムーバブルドライブの使用状況の監視
キャッシュ期間の変更
信頼するデバイスを使用した処理
アプリケーションインターフェイスから信頼リストへのデバイスの追加
Kaspersky Security Center から信頼リストへのデバイスの追加
信頼するデバイスのリストのエクスポート / インポート
ブロックされたデバイスへのアクセスの取得
オンラインモードでのアクセス権の付与
オフラインモードでのアクセス権の付与
デバイスコントロールメッセージのテンプレートの編集
アンチブリッジ
アンチブリッジを有効にする
接続ルールのステータスの変更
接続ルールの優先度の変更

アダプティブアノマリーコントロール
アダプティブアノマリーコントロールのトレーニング
アダプティブアノマリーコントロールルールの有効化と無効化
アダプティブアノマリーコントロールルールが適用されたときに実行する処理の変更
アダプティブアノマリーコントロールルールの除外の作成
アダプティブアノマリーコントロールルールの除外のエクスポートとインポート
アダプティブアノマリーコントロールルールへのアップデートの適用
アダプティブアノマリーコントロールのメッセージテンプレートの編集
アダプティブアノマリーコントロールの動作の監視
アプリケーションコントロール
アプリケーションコントロールの機能の制限
クライアントコンピューターにインストールされたアプリケーションについての情報の取得
ブロック対象のアプリケーションモードを有効にする方法
ベースラインコンピューターに基づくアプリケーションコントロール
アプリケーションコントロールルールの管理
アプリケーションコントロールルールの適用条件の追加
実行ファイルフォルダーからアプリケーションカテゴリへの実行ファイルの追加
イベントに関連した実行ファイルのアプリケーションカテゴリへの追加
アプリケーションコントロールルールを追加する
Kaspersky Security Center を使用したアプリケーションコントロールルールのステータス変更
アプリケーションコントロールルールのエクスポートおよびインポート
アプリケーションコントロールの動作によるイベントの表示
ブロックされたアプリケーションに関するレポートの表示
アプリケーションコントロールルールのテスト
アプリケーションコントロールルールのテストを有効または無効にする
テストモードでのブロック対象アプリケーションのレポートの表示
アプリケーションコントロールのテスト動作によるイベントの表示
アプリケーション動作モニター
ファイルまたはフォルダーの名前のマスクの作成
アプリケーションコントロールのメッセージテンプレートの編集
アプリケーションコントロールのメッセージテンプレートの変数
許可されるアプリケーションのリストの実装のベストプラクティス
アプリケーションの許可リストモードの設定
許可リストモードのテスト
許可リストモードのサポート
ネットワークポートの監視
すべてのネットワークポートの監視の有効化
監視対象ネットワークポートのリストの作成
すべてのネットワークポートを監視するアプリケーションのリストの作成
監視対象のポートのリストのエクスポートまたはインポート
Windows イベントログ監視
事前定義済みのルールの設定
カスタムルールの追加
システム変更監視
システム変更監視ルールについて
リアルタイムシステム変更監視
オンデマンドのシステム変更チェック

- システム変更監視ルールのエクスポートとインポート
- システム変更監視レポートの表示
- システム変更ステータスのリセット
- Cloud Discovery

信頼ゾーン
- 信頼するオブジェクトの作成
- 検知したオブジェクトの種別による除外リストの作成
- 信頼するアプリケーションのリストの編集
- ローカルの信頼ゾーンの作成
- 信頼ゾーンでのエクスポート / インポート
- 信頼できるデジタル署名によるアプリケーションの処理
- 補足資料：設定済みの信頼するオブジェクトとアプリケーション
  - SQL サーバー
  - Microsoft Exchange サーバー
  - System Center Configuration Manager
  - Citrix
  - VMware

バックアップの管理
- バックアップファイルの最大保管期間の設定
- バックアップの最大サイズの設定
- バックアップからのファイルの復元
- バックアップからのファイルのバックアップコピーの削除

通知サービス
- イベントログ設定の指定
- 通知の表示と配信の設定
- 製品のステータスに関する通知領域での警告の表示設定
- ユーザーと管理者間のメッセージ

レポートの管理
- レポートの表示
- レポート最長保管期間の設定
- レポートファイルの最大サイズの設定
- レポートのファイルへの保存
- レポートの消去

Kaspersky Endpoint Security セルフディフェンス
- セルフディフェンスの有効化と無効化
- AM-PPL のサポートの有効化と無効化
- 外部からの管理に対するアプリケーションサービスの保護
- リモート管理アプリケーションのサポート
- パスワードによる保護
  - パスワードによる保護を有効にする
  - 個別のユーザーまたはグループへの権限付与
  - 一時パスワードを使用した権限の付与
  - 一時パスワードの取り消し
  - パスワードによる保護で付与する権限に関する留意事項
  - KLAdmin パスワードのリセット
- 管理サーバーの接続の保護

データ暗号化
暗号化機能の制限
暗号鍵（AES56 / AES256）の鍵長の変更
Kaspersky Disk Encryption
SSD ドライブ暗号化の特別な機能
Kaspersky Disk Encryption の開始
暗号化から除外するハードディスクのリスト作成
暗号化から除外するハードディスクのリストのエクスポートおよびインポート
シングルサインオン（SSO）技術の有効化
認証エージェントアカウントの管理
認証エージェントでのトークンまたはスマートカードの使用
ハードディスクの復号化
Kaspersky Disk Encryption 技術で保護されたドライブへのアクセスの復元
認証エージェントのサービスアカウントを使用したログイン
オペレーティングシステムのアップデート
暗号化機能のアップデートのエラーの解決
認証エージェントのトレース
認証エージェントのヘルプテキストの編集
認証エージェントの動作テスト後に残存するオブジェクトとデータの削除
BitLocker の管理
BitLocker ドライブ暗号化の開始
BitLocker で保護されたハードドライブの復号化
BitLocker で保護されたハードドライブへのアクセスの復元
ソフトウェアアップデート時の BitLocker 保護の一時停止
ローカルコンピュータードライブでのファイルレベルの暗号化
ローカルコンピュータードライブのファイルの暗号化
アプリケーションを対象にした暗号化ファイルへのアクセスルールの策定
特定のアプリケーションによって作成または変更されたファイルの暗号化
復号化ルールの作成
ローカルコンピュータードライブでのファイルの復号化
暗号化されたパッケージへの追加
暗号化されたファイルへのアクセスの復元処理
オペレーティングシステム障害が発生した後の暗号化されたデータへのアクセスの復元
暗号化ファイルアクセスメッセージのテンプレートの編集
リムーバブルドライブの暗号化
リムーバブルドライブの暗号化の開始
リムーバブルドライブの暗号化ルールの追加
リムーバブルドライブの暗号化ルールのリストのエクスポートまたはインポート
リムーバブルドライブ上の暗号化ファイルにアクセスするためのポータブルモード
リムーバブルドライブの復号化
データ暗号化の詳細の表示
暗号化ステータスの表示
Kaspersky Security Center ダッシュボードで暗号化の統計情報の表示
ローカルコンピュータードライブでのファイル暗号化エラーの表示
データ暗号化レポートの表示

暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用
FDERT 復元ツールを使用してデータを復元する
オペレーティングシステムのレスキューディスクの作成
Detection and Response ソリューション
MDR および EDR Optimum のライセンス管理
Kaspersky Endpoint Agent
［KES + KEA］構成からの［KES + 組み込みエージェント］構成への移行
Kaspersky Endpoint Agent のポリシーとタスクの移行
Endpoint Detection and Response Agent (EDR Agent)
EDR Agent のインストール
EDR Agent と MDR の統合
EDR Agent と EDR (KATA) の統合
EDR Agent と NDR (KATA) の統合
EDR Agent と EDR Expert（オンプレミス）の連携
サードパーティ製の EPP 製品との互換性
Managed Detection and Response
組み込みエージェントと MDR の連携
MDR の KEA から KES への移行ガイド
Endpoint Detection and Response
組み込みエージェントと EDR Optimum / EDR Expert の連携
セキュリティ侵害インジケーター（IOC）のスキャン
IOC スキャンの拡張テレメトリ
ファイルを隔離する
ファイルを取得する
ファイルを削除する
プロセスの開始
プロセスの終了
実行防止
コンピューターのネットワーク分離
Cloud Sandbox
EDR Optimum の KEA から KES への移行ガイド
Kaspersky Sandbox
組み込みエージェントと Kaspersky Sandbox の連携
セキュリティ侵害インジケーターのスキャン（スタンドアロンタスク）
Kaspersky Sandbox の KEA から KES への移行ガイド
Kaspersky Anti Targeted Attack Platform
組み込みエージェントと EDR / NDR (KATA) の連携
EDR (KATA) テレメトリの設定
EDR (KATA) テレメトリの除外リスト
例 1。除外されるプロセス
例 2。除外されるネットワークコミュニケーション
例 3。除外されるファイル操作
例 4。除外されるレジストリ変更
KATA Sandbox
組み込みエージェントと KATA Sandbox の連携
Threat Response 処理の設定
EDR の KEA から KES への移行ガイド（KATA）

- Endpoint Detection and Response Expert（オンプレミス）
  - 組み込みエージェントと EDR Expert（オンプレミス）の連携
  - EDR Expert（オンプレミス）のテレメトリ設定
  - EDR Expert（オンプレミス）のテレメトリ除外
  - EDR Expert（オンプレミス）のイベントフィルターのエクスポートとインポート
- 隔離の管理
  - 隔離フォルダーの最大サイズの設定
  - 隔離されたファイルの Kaspersky Security Center への送信
  - 隔離からのファイルの復元
- EDR 処理の監視

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Kaspersky Endpoint Security と KUMA の連携
- KUMA に送信するイベントのフィルタリング
- KUMA イベントフィルターのエクスポートとインポート

KSWS から KES への移行ガイド
- KSWS と KES のコンポーネントの対応
- KSWS と KES の設定の対応
- KSWS コンポーネントの移行
- KSWS のタスクとポリシーの移行
- KSWS の信頼ゾーンの移行
- KSWSのアプリケーション起動コントロールルールの移行
- KSWS の代替としての KES のインストール
- 「KSWS + KEA」構成からの「KES + 組み込みエージェント」構成への移行
- Kaspersky Security for Windows Server が正常に削除されたことの確認
- KSWS のライセンスでの KES のアクティベート
- 高負荷のサーバーを移行する際の留意点
- Server Core モードのサーバーでの本製品の管理
- 「KSWS + KEA」から「KES + 組み込みエージェント」への移行

仮想マシンを保護する Light Agent モード
- Light Agent モードに関する特別な考慮事項
- 仮想マシンの予備設定
  - Citrix App Layering テクノロジーとの互換性
  - Citrix Provisioning（Citrix Provisioning Services）テクノロジーとの互換性
  - Omnissa App Volumes テクノロジーとの互換性
- Light Agent のインストール
- Light Agent と SVM の接続
  - SVM 検出
  - Light Agent の SVM 選択アルゴリズムの設定
  - 複数の SVM に対する複数の Light Agent の接続の分散（タグ）
  - Light Agent と SVM の間の接続の保護
- Light Agent のアクティベーション
- KSVLA Light Agent から KES Light Agent への移行ガイド
  - KSVLA Light Agent の代替として KES Light Agent のインストール
  - KSVLA Light Agent と KES Light Agent のコンポーネントの対応
  - KSVLA Light Agent のタスクとポリシーの移行
  - [KSVLA Light Agent+KEA] 設定から [KES Light Agent+組み込みエージェント] への移行

コマンドラインを使用しての製品の管理
- Setup：本製品のインストール
- Setup /x：本製品の削除
- msiexec /i：本製品の復元
- AVP コマンド
  - SCAN：マルウェアのスキャン
  - UPDATE：定義データベースとソフトウェアモジュールのアップデート
  - ROLLBACK：前回のアップデートのロールバック
  - TRACES：トレース
  - START：プロファイルの起動
  - STOP：プロファイルの停止
  - STATUS：プロファイルのステータス
  - STATISTICS：プロファイルの動作の統計情報
  - RESTORE：バックアップからのファイルの復元
  - EXPORT：本製品の設定のエクスポート
  - IMPORT：本製品の設定のインポート
  - ADDKEY：ライセンス情報ファイルの適用
  - LICENSE：ライセンス管理
  - RENEW：ライセンスの更新または購入
  - PBATESTRESET：暗号化前のディスクチェックの結果のリセット
  - EXIT：本製品の終了
  - EXITPOLICY：ポリシーの無効化
  - STARTPOLICY：ポリシーの有効化
  - DISABLE：保護の無効化
  - SPYWARE：スパイウェアの検知の切り替え
  - KSN：KSN / KPSN の切り替え
  - SERVERBINDINGDISABLE：サーバー接続の保護の無効化
- KESCLI コマンド
  - Scan：マルウェアのスキャン
  - GetScanState：スキャン完了のステータス
  - GetLastScanTime：スキャン完了時刻の判断
  - GetThreats：検知した脅威に関するデータの取得
  - UpdateDefinitions：定義データベースとソフトウェアモジュールのアップデート
  - GetDefinitionState：データベースの前回のアップデート日時の決定
  - EnableRTP：保護の有効化
  - GetRealTimeProtectionState：ファイル脅威対策のステータス
  - GetEncryptionState：ディスク暗号化のステータス
  - Version：本製品のバージョンの識別
- Detection and Response 管理コマンド
  - SANDBOX：Sandbox の管理
  - PREVENTION：実行防止の管理
  - ISOLATION：ネットワーク分離の管理
  - RESTORE：隔離からのファイルの復元
  - IOCSCAN：セキュリティ侵害インジケーター（IOC）のスキャン
  - MDRLICENSE：MDR のアクティベーション
  - EDRKATA：EDR (KATA) との連携
  - KUMA：KUMA との連携

YARA：YARA スキャンの実行
TELEMETRYFILTERS：KUMA に送信するイベントのフィルタリング
Light Agent 管理コマンド
KSVLAINFO：Light Agent モードの特定
VIISINFO：Light Agent と Integration Server との接続のステータス
SVMINFO：Light Agent と Protection Server との接続のステータス
エラーコード
補足資料：製品プロファイル
REST API を使用した製品の管理
REST API の使用を有効にしての本製品のインストール
API の使用
製品の情報源
テクニカルサポートへのお問い合わせ
トレースファイルの内容と保存場所
アプリケーションの動作のトレース
製品のパフォーマンスのトレース
ダンプ書き込み
ダンプファイルとトレースファイルの保護
OS データの取得（Kaspersky Get System Info）
制限と警告
用語解説
Cloud Discovery
Integration Server
IOC
IOC ファイル
Kerberos 認証
Light Agent
OLE オブジェクト
OpenIOC
SVM
Trusted Platform Module
Web リソースアドレスの正規化された形式
アーカイブ
悪意のある URL のデータベース
感染可能なファイル
感染したファイル
管理グループ
駆除
現在のライセンス
誤検知
証明書の発行元
スキャン範囲
タスク
定義データベース
認証エージェント
ネットワークエージェント
フィッシングサイトの URL のデータベース

ポータブルファイルマネージャー
保護範囲
マスク
ライセンス証明書
補足資料
補足資料 1：製品設定
ファイル脅威対策
ウェブ脅威対策
メール脅威対策
ネットワーク脅威対策
ファイアウォール
有害 USB 攻撃ブロック
AMSI 保護
脆弱性攻撃ブロック
ふるまい検知
ホスト侵入防止
修復エンジン
Kaspersky Security Network
Windows イベントログ監視
アンチクリプター
ウェブコントロール
デバイスコントロール
アプリケーションコントロール
アダプティブアノマリーコントロール
システム変更監視
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert（オンプレミス）
Network Detection and Response (KATA)
KUMA との連携
ディスク全体の暗号化
ファイルレベルの暗号化
リムーバブルドライブの暗号化
テンプレート（データの暗号化）
除外リスト
製品設定
レポートと保管領域
ネットワークの設定
インターフェイス
設定の管理
定義データベースとソフトウェアモジュールのアップデート
補足資料 2：アプリケーションの信頼グループ
補足資料 3：リムーバブルドライブの簡易スキャンのファイル拡張子
補足資料 4：メール脅威対策用の添付ファイルフィルターのファイル種別
補足資料 5：外部サービスとの相互作用のためのネットワーク設定

補足資料 6：アプリケーションイベント
緊急
機能エラー
警告
情報メッセージ
補足資料 7：実行防止でサポートされるファイルの拡張子
補足資料 8：実行防止でサポートされるスクリプトインタープリター
補足資料 9：レジストリ内の IOC スキャン範囲（RegistryItem）
補足資料 10：IOC ファイルの要件
補足資料 11：アプリケーションコンポーネントルールのユーザーアカウント
補足資料 12：EDR Threat Response 用 API
サードパーティ製のコードに関する情報
商標に関する通知

Kaspersky Endpoint Security for Windows のヘルプ

12.12 の新機能

- 共有フォルダの保護は、アンチクリプターという独立したコンポーネントになりました。
- 遡及的スキャン機能が *IOC スキャンタスク*に追加されました。
- Kaspersky Endpoint Security for Windows の各バージョンの新機能

使用開始時に行う設定

- Kaspersky Endpoint Security for Windows の導入
- Kaspersky Endpoint Security for Windows の初期設定
- 製品のパフォーマンスの最適化
- Kaspersky Endpoint Security for Windows のライセンス

脅威の駆除

- ワークステーション
- サーバー
- 侵害インジケーターの検知時の対処（ネットワーク分離 → 隔離 → 実行防止）

その他のソリューションの一部としての KES の使用

- Kaspersky EDR
- Kaspersky Sandbox
- Kaspersky MDR

データ提供

- 使用許諾契約書におけるデータ提供
- Kaspersky Security Network 使用時のデータ提供
- 欧州連合の規則（GDPR）の順守

新機能

12.12 のアップデート

Kaspersky Endpoint Security 12.12 for Windows では、次の新機能と改良点が導入されました：

1. 以前はふるまい検知コンポーネントの一部であった外部からの暗号化に対する共有フォルダの保護は、現在は独立したコンポーネント（アンチクリプター）になっています。
2. インターネットアクセス用のプロキシサーバーを介して本製品を認証するための Kerberos プロトコルのサポートが追加されました。
3. 信頼するアプリケーションに対して、完全パスだけではなくファイルハッシュを指定できるようになりました。
4. Endpoint Detection and Response (EDR) ソリューションのユーザーが、追加の *IOC* スキャンタスク機能を使用できるようになりました。遡及的 IOC スキャン機能が使用可能になりました。*遡及的 IOC スキャン* は、Kaspersky Endpoint Security が一定期間のデータを使用してセキュリティ侵害インジケーターをスキャンする *IOC* スキャンタスクのモードです。このモードは、コンピューターのネットワーク動作のデータ内のセキュリティ侵害インジケーターを検知することを目的としています。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムのログとブラウザーのログ内のデータを分析します。
5. カスペルスキーの Endpoint Detection and Response (EDR) のユーザーは、隔離のサイズ制限を解除できます。本製品はサイズの大きいメモリダンプファイルを保存する可能性があるため、YARA スキャンでこれが必要になる場合があります。これで、ディスクの空き容量をすべて隔離に使用できるようになります。

6. Kaspersky Unified Monitoring and Analysis Platform (KUMA) へのイベントのエクスポートを最適化するために HTTPS 圧縮がサポートされるようになりました。これにより、送信トラフィック量を減らすことができます。

7. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF22004、PF22008、PF22014 に含まれる変更を組み込みました。

12.11 のアップデート

Kaspersky Endpoint Security 12.11 for Windows の新機能と改良点は次の通りです：

1. 本製品は、設定を保存する前に、管理コンポーネントの設定を確認します。アプリケーションコントロール、デバイスコントロール、システム変更監視のコンポーネントのチェックが追加されました。管理コンポーネントの現在の設定によってコンピューターの負荷が増加したり、システム障害が発生したりする可能性がある場合に、本製品で警告が表示されるようになりました。たとえば、アプリケーションコントロールで、許可されたアプリケーションを除くすべてのアプリケーションをブロックするモードを選択し、許可ルールを追加していないと、このような設定ではシステム障害が発生する可能性があるため、本製品で警告が表示されます。

2. KATA Sandbox に確認用ファイルを自動送信するサポートが追加されました。*KATA Sandbox* は、Kaspersky Anti Targeted Attack Platform のコンポーネントの 1 つで、オペレーティングシステムの仮想イメージ上でファイルを実行します。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。KATA Sandbox を自動モードで動作させるには、Kaspersky Anti Targeted Attack Platform 8.0 以降を導入する必要があります。

3. EDR テレメトリの送信が最適化されました。最大パケット長を指定できるようになりました。

4. Kaspersky Security Network への接続診断が改善されました。潜在的な問題を解決するために、Kaspersky Security Network の接続エラーの詳細が拡張されました。

5. Kaspersky Unified Monitoring and Analysis Platform (KUMA) に送信するイベントリストを設定するためのサポートが追加されました。KUMA の設定済みのイベントリストに加えて、テレメトリにイベントを手動で追加したり、Windows イベントログで ID によってイベントを除外したりできるようになりました。

6. Web コンソールのポリシーインターフェイスが更新されました。重要な機能に素早くアクセスできるように、ポリシーセクションのレイアウトが変更されました。

7. Windows 11 25H2 のサポート。

8. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF22004、PF22008、PF22014 に含まれる変更を組み込みました。

12.10 のアップデート

Kaspersky Endpoint Security 12.10 for Windows の新機能と改良点は次の通りです：

1. 有害 USB 攻撃ブロックに、画面からバーコードを読み取ってバーコードスキャナーを認証するオプションが追加されました。バーコードスキャナーを認証するために、セキュリティキーボードを使用してコードを入力する必要がなくなりました。

2. カスペルスキーの Endpoint Detection and Response (EDR) ソリューションのユーザー向けの新機能と改善点は次の通りです。

   - アラートの詳細でネットワーク分離を管理できるようになりました。さらに、アラートの詳細で、コンピューターのネットワーク分離期間を指定したり除外リストを追加できます。

   - アラートの詳細に新しいデータを追加できるようになりました。アラートの詳細に、EDR で脅威に対応中にアプリケーションがどのように動作したかを含む、脅威に関する情報を含めることができるようになりました。

   - IOC ファイルの処理が改善されました。Kaspersky Security Center Web コンソールのインターフェイスで IOC ファイルの内容を表示および編集できるようになりました。IOC ファイルを読み込むと、IOC タームアプリケーションにレポートが表示されます。

   - 検知された IOC への対応が改善されました。*IOC スキャンタスク*で検知されたファイルを、タスクのプロパティの IOC 検知結果で直接隔離できるようになりました。タスクのプロパティでコンピューターをネットワークから分離することもできます。

   - TXT ファイルで生成されたファイルハッシュ、IP アドレス、DNS 名のリストに基づいて *IOC スキャンタスク*のプロパティで IOC ファイルを直接作成できるようになりました。

   - *IOC スキャンタスク*のスキャン範囲が拡大されました。レジストリの IOC スキャンの範囲を定義できるようになりました（[**Windows レジストリ - RegistryItem**]）。本製品の以前のバージョンで使用できたのは、レジストリ内の設定済みの IOC スキャン範囲のみでした。

3. パスワードによる保護の新しい権限（*設定のエクスポート*）が追加されました。既定では、KLAdmin ユーザーのみが、製品インターフェイスで Kaspersky Endpoint Security の設定を含む設定ファイルを作成できます。他のユーザーにアクセスを許可するには、対応する権限を付与する必要があります。

4. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF13120、PF13123、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF15062、PF16052、PF16053、PF16055、PF16056、PF16057、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF21007 に含まれる変更を組み込みました。

12.9 のアップデート

Kaspersky Endpoint Security 12.9 for Windows の新機能と改良点は次の通りです：

1. *一時パスワードを管理* するための新しい機能が追加されました。一時パスワードを使用すると、別のコンピューターで、パスワードによる保護を有効にした Kaspersky Endpoint Security にアクセスできるようになります。一時パスワードの管理では、パスワード履歴を保存したり（最大 30 日間）、一時パスワードのステータス（*使用中*、*有効期間終了*、*失効*）を監視したり、一時パスワードを取り消したりできます。

2. ウェブコントロールルールで禁止された Web リソースへの接続をポリシーの適用直後に終了する オプションが追加されました。本製品の以前のバージョンでは、ウェブコントロールによって、禁止された Web リソースへの新しい接続しか制限されませんでした。

3. Kaspersky Anti Targeted Attack Platform ユーザー向けに、コンピューター上でローカルに YARA チェックを実行する オプションが追加されました。これを実行するには、YARA ルールを含むファイルをダウンロードし、CMD でコマンドを実行する必要があります。

4. サードパーティ製ツールを使用してドライブが既に BitLocker で保護されている コンピューターで BitLocker が有効になっている場合の本製品の動作が修正されました。Kaspersky Endpoint Security は復元手順を開始して、回復キーを Kaspersky Security Center に送信します。このため、BitLocker の管理は、Kaspersky Security Center コンソールに転送されます。

5. カスペルスキーの Detection and Response ソリューションのユーザー向けに、新しいセクション［**応答履歴**］が利用できるようになりました。このセクションには、コンピューターで実行された脅威の対応処理に関する情報が含まれます。処理には、［*プロセスの終了*］タスクやネットワークからのコンピューターの隔離などが含まれます。応答履歴は、次のカスペルスキーソリューション（MDR、EDR、KATA）のユーザーのみ使用できます。

6. Kaspersky Unified Monitoring and Analysis Platform ユーザーに、EDR の脅威対応処理のサポートが提供されるようになりました。脅威への応答の際に、KUMA は対応する EDR タスクを作成するスクリプトを実行します。EDR タスクを実行するには、KUMA コンソールでカスタムスクリプト向けの応答ルールを作成し、イベントを選択する必要があります。

7. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF20011、PF20016、PF20017、PF20020、PF20021 に含まれる変更を組み込みました。

12.8 のアップデート

Kaspersky Endpoint Security 12.8 for Windows の新機能と改良点は次の通りです：

1. 仮想環境を保護する Light Agent モードがサポートされるようになりました。Kaspersky Security for Virtualization Light Agent 6.2 ソリューションの一部として、本製品を Light Agent として導入できるようになりました。

2. サーバー上での Docker コンテナー内のファイル操作の傍受がサポートされるようになりました。コンテナーは、アプリケーションがオペレーティングシステムと直接やり取りすることなく実行できる分離された環境です。Kaspersky Endpoint Security は、ユーザーがアクセスするコンテナ内のファイルをスキャンします。脅威が検知されると、本製品はこのアクティビティをブロックし、コンテナー内のファイルの駆除を試みます。ファイルを駆除できない場合、本製品はコンテナーを停止します。

3. 外部からの暗号化に対する共有フォルダーの保護の保護範囲を定義できるようになりました（ふるまい検知コンポーネント）。本製品がファイルの動作を監視する必要がある共有フォルダーを指定できるようになりました。保護範囲からファイルを除外することもできます。本製品の以前のバージョンでは、ふるまい検知コンポーネントはすべての共有フォルダーのファイルの動作を監視していました。

4. インストールパッケージで、オペレーティングシステムの種別ごとに異なるコンポーネントのセットを設定できるようになりました。つまり、同じインストールパッケージを使用して、本製品をワークステーションとサーバーに導入できます。特定のオペレーティングシステムの種別で使用できないコンポーネントは、インストールパッケージのプロパティで自動的に除外されます。

5. 設定済みの信頼するオブジェクトとアプリケーションを選択するためのオプションが追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、仮想環境（Citrix、VMware）における本製品の信頼ゾーンを迅速に設定できます。このような信頼するオブジェクトには、仮想マシンファイル VHD や VHDX が含まれます。信頼するオブジェクトは、アプリケーションインストールパッケージの作成時、ポリシーの作成時、または Kaspersky Endpoint Security のインストール時に追加できます。

6. EDR テレメトリに、USB 接続デバイスでの操作のイベントが含まれるようになりました。これらのイベントを EDR テレメトリから除外リストに追加することもできます。

7. 古い TLS 1.0 プロトコル経由のネットワーク接続をブロックするオプションが追加されました。TLS 1.0 はセキュリティ レベルが低いため、このプロトコルを無効にして、新しい TLS 1.2 または TLS 1.3 バージョンを使用することをお勧めします。既定では、 Kaspersky Endpoint Security は TLS 1.0 接続をブロックします。製品のバージョンを更新すると、TLS 1.0 プロトコルを使用するサードパーティのサービスの動作が失敗する可能性があります。サードパーティのサービス運用における問題を回避するため、製品のバージョンを更新する前にグループポリシーで TLS 1.0 プロトコルの使用を許可することができます。

8. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ PF10053、PF10054、PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018 に含まれる変更を組み込みました。

12.7 のアップデート

Kaspersky Endpoint Security 12.7 for Windows の新機能と改良点は次の通りです：

1. マルウェアのスキャンタスクの CPU リソース使用率を制限できるようになりました。これを行うには、アプリケーション設定で、コンピューターのスキャン中に利用できるすべてのコアにかかる最大 CPU 負荷率を指定します。

2. 手動で KATA Sandbox でのスキャン用にファイルを送信できるようになりました。*KATA Sandbox* は、Kaspersky Anti Targeted Attack Platform のコンポーネントの 1 つで、オペレーティングシステムの仮想イメージ上でファイルを実行します。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。スキャンするファイルを KATA Sandbox に送信するには、ファイルのコンテキストメニューで関連するコマンドを選択します。

3. 企業 LAN を保護するソリューション、*Kaspersky Network Detection and Response* との連携を設定できるようになりました。Kaspersky Network Detection and Response (NDR) は、Kaspersky Anti Targeted Attack Platform の一部です。NDR との連携は、標準モードおよび EDR Agent モードで設定できます。

4. メール脅威対策拡張機能に、Microsoft Office Outlook メールクライアントのバージョン 2021 のサポートが追加されました。この機能拡張により、プロトコルレベルではなく、メールクライアントのレベルでメッセージをスキャンすることができます。この機能拡張では、メッセージに加えて、Microsoft Exchange のリポジトリから MAPI インターフェイスを通じて受信したオブジェクト（たとえば、カレンダー内のオブジェクト）をスキャンすることができます。このスキャンは、メールクライアントで行われます。

5. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ PF10049、PF10355、PF12114、PF13109、PF14056、PF15038、PF15045、PF16037、PF16042、PF16047、PF17014、PF17018、PF17021、PF17024、PF18006、PF18007 に含まれる変更を組み込みました。

12.6 のアップデート

Kaspersky Endpoint Security 12.6 for Windows の新機能と改良点は次の通りです：

1. カスペルスキーの SIEM ソリューションとの連携用機能（*Kaspersky Unified Monitoring and Analysis Platform (KUMA)*）が追加されました。Windows イベントログから KUMA コレクターにイベントを送信できるようになりました。これにより、KUMA エージェントをインストールすることなく、Kaspersky Endpoint Security がインストールされているすべてのコンピューターから Windows イベント（サポートされる EventIDs は限定されます）を KUMA で受信できます。

2. *システム変更監視*という新しいコンポーネントがファイル変更監視コンポーネントの代わりに追加されました。システム変更監視コンポーネントには、ファイル変更監視のすべての機能が含まれており、さらにレジストリの変更や外部デバイスの接続を監視することもできます。システム変更監視コンポーネントは、コンピューターのセキュリティ侵害を示す可能性のあるオペレーティングシステムの変更を監視します。そのような変更を検知すると、Kaspersky Endpoint Security は対応するイベントを生成し、管理者に警告します。ファイル変更監視は本製品の一部ではなくなりました。本製品をアップデートすると、ファイル変更監視の設定がシステム変更監視に自動的に移行されます。システム変更監視を正しく動作させるには、Kaspersky Endpoint Security のアプリケーションと管理プラグインの両方をバージョン 12.6 にアップデートする必要があります。

3. インストールされた組み込みの EDR エージェント（KATA）のステータスが、Kaspersky Security Center コンソールのコンピューターのプロパティに追加されました。組み込みの EDR エージェント（KATA）がインストールされている場合、［**Endpoint Sensor status**］列にはコンポーネントの現在のステータスが表示されます（例：*実行中*、*停止中*、*ライセンスが対応していない*など）。

4. 設定済みの信頼するオブジェクトとアプリケーションを選択するためのオプションが追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で本製品を使用する際の信頼ゾーンを迅速に設定できます。このような信頼するオブジェクトには、データベースファイル MDF や LDF が含まれます。信頼するオブジェクトは、新しいポリシーの作成時、既存のポリシーの変更時、または Kaspersky Endpoint Security のインストール時に追加できます。

5. Kaspersky Endpoint Detection and Response Optimum の警告の詳細の表示が、Kaspersky Endpoint Security 管理プラグインから個別の Kaspersky Endpoint Detection and Response 管理プラグインに移動されました。EDR 管理プラグインは、Windows、Mac、Linux オペレーティングシステム上のエージェントを操作するための単一のプラグインです。今後、EDR Optimum を使用する場合は、*脅威の対応タスク*の作成には Kaspersky Endpoint Security 管理プラグインが、アラートの詳細の表示には EDR 管理プラグインが必要になります。

6. Windows 11 24H2 のサポート。

7. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ pf10048、pf10353、pf12106、pf12107、pf12108、pf13090、pf13100、pf15031、pf15034、pf15036、pf16021、pf16023、pf16029、pf17002 に含まれる変更を組み込みました。

12.5 のアップデート

Kaspersky Endpoint Security 12.5 for Windows の新機能と改良点は次の通りです：

1. テレメトリの除外リストを設定するオプションが追加されました。*テレメトリ*とは、保護対象コンピューター上で発生したイベントのリストです。テレメトリデータは、組織の IT インフラストラクチャを監視および保護するために、Kaspersky Anti Targeted Attack Platform (EDR) で使用されます。テレメトリの除外リストを設定すると、コンピューターのパフォーマンスを向上し、テレメトリ収集サーバーへのデータ転送を最適化することができます。

2. 本製品の信頼ゾーンのインターフェイスが改善されました。管理者が、ユーザーによる独自（ローカル）の信頼するオブジェクトとアプリケーションの追加を禁止している場合、信頼ゾーンのオブジェクトがユーザーに対して非表示にされるようになりました。これにより、侵入者による信頼ゾーンへの不正アクセスが防止され、コンピューターのセキュリティレベルが向上します。

3. MyOffice Mail および R7-Office Organizer メールクライアントのトラフィックをスキャンするオプションが追加されました。メール脅威対策コンポーネントにより、ダウンロード時にメッセージの添付ファイルだけでなく、送受信されたメッセージもスキャンされるようになりました。

4. Web リソースの新規カテゴリ「*生成 AI ツール*」が追加されました。ウェブコントロールを使用して、新規カテゴリから Web サイトへのアクセスを設定できます。

5. ファイアウォールリストでネットワークパケットルールの場所を選択できるようになりました。リスト内のネットワークパケットルールの位置によって、そのルールの優先順位が決まります。以前のバージョンでは、新しいルールはリストの最後にのみ追加できました。追加後にリスト内でルールを手動で移動して優先度を設定する必要がありました。新たに、ルールを追加するときに、ルールをリストの先頭に配置するか、リストの最後に配置するか、選択されたルールの横に配置するかを選択できるようになりました。

6. Kaspersky Endpoint Security コンポーネントのルールで、Active Directory のユーザーだけでなく、Kaspersky Security Center のユーザーリストのユーザーも選択できるようになりました。また、ローカルユーザーアカウントデータを手入力することもできます。この機能は、次のコンポーネントのルールに追加されました：アプリケーションコントロール、デバイスコントロール、ウェブコントロール、アダプティブアノマリーコントロール、および Windows イベントログ監視。

7. ネットワーク攻撃検知レポートに、攻撃元コンピューターの MAC アドレスの列が追加されました（ネットワーク脅威対策コンポーネント）。これで、IP アドレスに加え、攻撃元のコンピューターの MAC アドレスもレポートに表示されるようになりました。これは、インシデントの調査に役立ちます。Kaspersky Security Center Linux コンソールのバージョン 15.1 以降では、攻撃元コンピューターの MAC アドレスを含むレポートも使用できます。

8. コンピューターの保護要件のレベルが引き上げられました。保護レベル「高」の場合、外部からの管理に対するアプリケーションサービスの保護を有効にすることが必要になりました。ポリシーウィンドウの上部で、セキュリティレベルインジケーターを確認してください。セキュリティレベルが「中」または「低」の場合、セキュリティレベルのインジケーターの推奨ウィンドウで外部からの管理に対するアプリケーションサービスの保護を有効にすることができます。

9. Endpoint Detection and Response Agent (EDR Agent) 構成で本製品を実行しているときのオブジェクト検知に、新しいイベントのサポートが追加されました。これらのイベントは、[KES+組み込みエージェント] の構成では既にサポートされていました。

10. このバージョンの Kaspersky Endpoint Security for Windows の開発にあたり、プライベートパッチ pf9640、pf9830、pf9831、pf10047、pf10351、pf12102、pf12105、pf13084、pf13089、pf14040、pf14047、pf15026、pf15028、pf16013 に含まれる変更を組み込みました。

12.4 のアップデート

Kaspersky Endpoint Security 12.4 for Windows の新機能と改良点は次の通りです：

1. Kaspersky Security Center へのコンピューターの接続を保護する新機能が追加されました。新しい［*管理サーバーの接続の保護*］タスクにより、信頼済みのサーバーに接続するためのパスワードを設定することができます。つまり、このパスワードがないと、コンピューターに再接続することも、別のサーバーからコマンドを実行することもできません。

2. パスワードによる保護機能に、Active Directory 以外からも手動でユーザーを選択できる機能が追加されました。つまり、ユーザー名とパスワードを手動で指定して、そのアカウントに Kaspersky Endpoint Security へのアクセス権限を割り当てることができます。これにより、KLAdmin パスワードを他のユーザーと共有したり、本製品へのアクセスを制御するために新しい Active Directory アカウントを作成したりする必要がなくなります。

3. Windows 11 23H2 のサポート。

12.3 のアップデート

Kaspersky Endpoint Security 12.3 for Windows の新機能と改良点は次の通りです：

1. Endpoint Detection and Response Agent 設定に本製品をインストールできるようになりました。この設定により、カスペルスキーの Detection and Response ソリューションである Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform (EDR) が必要とするコンポーネントセットとともに本製品をインストール可能です。この設定に、サードパーティソリューション（Dr.Web、Dallas Lock、ESET など）と並べて本製品をインストールできます。これにより、カスペルスキーの Detection and Response と同時にサードパーティのインフラストラクチャセキュリティツールを使用できるようになります。

2. Bluetooth デバイス での Kaspersky Endpoint Security の操作を改善しました。除外の設定を行い、入力デバイス（ワイヤレスキーボード、マウスなど）を除くすべての Bluetooth デバイスへのアクセスを制限できるようになりました。

3. 実行ファイルのデータベースに対するアプリケーションコントロールコンポーネントの動作が最適化されました。ファイルがコンピューターから削除された場合に、Kaspersky Endpoint Security がそのファイルの情報をデータベースから自動的に削除するようになりました。これにより、データベースを最新の状態に保ち、Kaspersky Security Center のリソースを節約できます。

4. コンピューターの保護要件のレベルが引き上げられました。保護レベル「高」の場合、パスワードによる保護を有効にする ことが必要になりました。ポリシーウィンドウの上部 で、保護レベルのインジケーターを確認してください。保護レベルが「中」または「低」の場合、セキュリティレベルのインジケーターの推奨ウィンドウでパスワード保護を有効にすることができます。

5. アプリケーションが Kaspersky Security Network との連携を有効にするため、HTTPS プロトコルのサポートが追加されました。KSN プロキシサーバー設定の管理サーバーのプロパティで、HTTPS の使用を有効にします。

12.2 のアップデート

Kaspersky Endpoint Security 12.2 for Windows の新機能と改良点は次の通りです：

1. Wi-Fi ネットワークへの接続を制御する（デバイスコントロール）ために、WPA3 プロトコルのサポートを追加しました。信頼する Wi-Fi ネットワークの設定で WPA3 プロトコルを選択して、安全性の低いプロトコルを使用したネットワークへの接続をブロックすることができるようになりました。

2. ネットワーク脅威対策の除外対象として、プロトコルやポートを選択できるようになりました。信頼するデバイスの IP アドレスの指定に加え、ポートやプロトコルも選択できるようになりました。これにより、個々のデータストリームを除外し、信頼する IP アドレスからのネットワーク攻撃を防止することができます。

3. コンピューターにポリシーが適用されている場合、ローカルの*定義データベースと製品機能のアップデートタスク* のアップデート元の順序が異なります。最初のアップデート元として、カスペルスキーのサーバーではなく、Kaspersky Security Center サーバーが既定で使用されるようになりました。これにより、ユーザーがローカルで*定義データベースと製品機能のアップデート*タスクを実行する際のトラフィックを節約することができます。

12.1 のアップデート

Kaspersky Endpoint Security 12.1 for Windows の新機能と改良点は次の通りです：

1. Kaspersky Anti Targeted Attack Platform ソリューション用の組み込みエージェントが追加されました。EDR (KATA) を使用する際に Kaspersky Endpoint Agent が不要になりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。Kaspersky Endpoint Agent のポリシーを移行するには、移行ウィザードを使用してください。本製品のアップデート後、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。互換性のないソフトウェアの一覧に Kaspersky Endpoint Agent が追加されました。Kaspersky Endpoint Security にはすべての Detection and Response ソリューション向けの組み込みエージェントが含まれているため、ソリューションとの連携のために Kaspersky Endpoint Agent をインストールする必要はなくなりました。

2. Azure WVD 互換性モードがサポートされるようになりました。この機能により、Kaspersky Anti Targeted Attack Platform コンソールに Azure 仮想マシンの状態が正しく表示されるようになります。Azure WVD 互換モードはこれらの仮想マシンに永続的に一意な Sensor ID を割り当てることができます。

3. iTunes または類似のアプリケーションで、モバイルデバイスのユーザーアクセスを設定できるようになりました。例えばモバイルデバイスを iTunes でのみ使用できるように設定し、リムーバブルドライブとしての使用をブロックすることができます。本製品は Android Debug Bridge (ADB) アプリケーション向けのこれらのルールもサポートします。

4. Kaspersky Security Center バージョン 11 はサポートされません。Kaspersky Security Center を最新のバージョンにアップグレードしてください。

12.0 のアップデート

Kaspersky Endpoint Security 12.0 for Windows の新機能と改良点は次の通りです：

1. サーバーの Kaspersky Endpoint Security の操作が改善されました。Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows に移行して、ワークステーションおよびサーバーを保護する単一のソリューションを使用できるようになりました。製品設定を移行するには、ポリシーとタスクの一括変換ウィザードを実行します。KSWS のライセンスは KES のアクティベートに使用できます。KES への移行後、サーバーを再起動する必要はありません。KES への移行について詳しくは、移行ガイドを参照してください。

2. Amazon Machine Image (AMI) 内の有料版の仮想マシンイメージの一部としての本製品のライセンスに関する操作が改善されました。本製品を個別にアクティベートする必要はありません。この場合、Kaspersky Security Center は本製品に事前に追加されている、クラウド環境に対するライセンスを使用します。

3. デバイスコントロールが改善されました：

   - ポータブルデバイス（MTP）に対して、アクセスルール（読み取り/書き込み）の設定、デバイスにアクセスできるユーザーまたはユーザーグループの選択、デバイスアクセススケジュールの設定ができるようになりました。リムーバブルドライブと同様の方法で、ポータブルデバイスにアクセスルールを作成できるようになりました。

   - Android Debug Bridge (ADB) または類似のアプリケーションで、モバイルデバイスのユーザーアクセスを設定できるようになりました。例えばモバイルデバイスを ADB でのみ使用できるように設定し、リムーバブルドライブとしての使用をブロックすることができます。

- モバイルデバイスへのアクセスがブロックされている場合でも、モバイルデバイスをコンピューターのUSB ポートに接続して再充電できるようになりました。

- プリンターについて、ユーザーの印刷権限を設定できるようになりました。Kaspersky Endpoint Security はローカルおよびネットワークプリンターへのアクセスのコントロールをサポートします。個別のユーザーに対して、ローカルまたはネットワークプリンターでの印刷を許可したりブロックしたりできるようになりました。

- WPA3 プロトコルのサポートが Wi-Fi ネットワークへの接続のコントロールに追加されました。信頼する Wi-Fi ネットワークの設定で WPA3 プロトコルを使用するよう選択して、安全性の低いプロトコルを使用したネットワークへの接続をブロックすることができるようになりました。

11.11.0 のアップデート

1. サーバー向けの Windows イベントログ監視が追加されました。Windows イベントログ監視は Windows イベントログの分析結果に基づいて保護対象環境の整合性を監視します。通常と異なるふるまいを検知した場合、本製品は管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。

2. サーバー向けのファイル変更監視が追加されました。ファイル変更監視は指定した監視範囲内でのオブジェクト（ファイルおよびフォルダー）に対する変更を検知します。これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。オブジェクトの変更が検知されると、本製品は管理者に通知します。

3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) のアラートの詳細インターフェイスが改善されました。脅威の活動連鎖の要素が調整され、連鎖内のプロセス間のリンクがオーバーラップすることがなくなりました。これにより、進化する脅威をより分析しやすくなりました。

4. 製品のパフォーマンスが向上しました。パフォーマンス向上のため、ネットワーク脅威対策機能により処理されるネットワークトラフィックが最適化されました。

5. 再起動せずに Kaspersky Endpoint Security をアップグレードするオプションが追加されました。これにより、製品のアップグレード時にもサーバーの動作が中断されることがありません。バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることもできるようになりました。

6. Kaspersky Security Center コンソール内でのスキャンタスクの名前が変更されました。タスクはマルウェアのスキャンと呼ばれるようになりました。

11.10.0 のアップデート

Kaspersky Endpoint Security 11.10.0 for Windows の新機能と改良点は次の通りです：

1. カスペルスキーのディスク全体の暗号化のシングルサインオンに、サードパーティの資格情報プロバイダーのサポートが追加されました。Kaspersky Endpoint Security は ADSelfService Plus のユーザーのパスワードを監視し、ユーザーがパスワードを変更した際などに認証エージェントのデータを更新します。

2. Cloud Sandbox により検知された脅威を表示できるオプションが追加されました。この技術は Endpoint Detection and Response ソリューション（EDR Optimum または EDR Expert）のユーザーが利用できます。*Cloud Sandbox* はコンピューター上のより高度な脅威を検知する技術です。Kaspersky Endpoint Security は、検知したファイルを自動的に Cloud Sandbox に送って分析します。Cloud Sandbox はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してそのファイルの評価を決定します。

3. EDR Optimum のユーザー向けに、アラートの詳細にファイルの追加情報が表示されるようになりました。アラートの詳細に、信頼グループ、デジタル署名およびファイルの配信その他の情報が含まれるようになりました。アラートの詳細から直接 Kaspersky Threat Intelligence Portal（KL TIP）の詳細なファイルの説明にジャンプできるようになりました。

4. 製品のパフォーマンスが向上しました。パフォーマンス向上場を実現するため、バックグラウンドスキャンの動作を最適化し、スキャンが既に実行されている場合はスキャンタスクをキューに追加する機能を追加しました。

11.9.0 のアップデート

Kaspersky Endpoint Security 11.9.0 for Windows の新機能と改良点は次の通りです：

1. Kaspersky Disk Encryption を使用した場合、認証エージェントのサービスアカウントを作成することができるようになりました。サービスアカウントは、ユーザーがパスワードを忘れたときなどにコンピューターへのアクセス権を取得するために必要です。このサービスアカウントは予備のアカウントとして使用することもできます。

2. Kaspersky Endpoint Agent 配布パッケージは製品の配信キットに含まれなくなりました。Kaspersky Endpoint Security の組み込みエージェントを使用して Detection and Response ソリューションをサポートできます。必要に応じて、Kaspersky Endpoint Agent 配布パッケージは Kaspersky Anti Targeted Attack Platform の配信キットからダウンロードできます。

3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) のアラートの詳細インターフェイスが改善されました。脅威への対応機能にツールチップが実装されました。セキュリティ侵害インジケーターが検知された場合に、企業インフラストラクチャのセキュリティ確保のための手順が表示されるようになりました。

4. Kaspersky Hybrid Cloud Security のライセンスで Kaspersky Endpoint Security for Windows をアクティベートできるようになりました。

5. 信頼されていない証明書を持つドメインとの接続の確立および暗号化された接続のスキャンエラーに関する新しいイベントが追加されました。

11.8.0 のアップデート

Kaspersky Endpoint Security 11.8.0 for Windows の新機能と改良点は次の通りです：

1. Kaspersky Endpoint Detection and Response Expert ソリューションの操作をサポートする組み込みエージェントが追加されました。*Kaspersky Endpoint Detection and Response Expert* は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。EDR Expert は EDR Optimum に比べ、より多くの脅威監視および応答機能を備えています。このソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

2. ネットワークモニターのインターフェイスが改善されました。ネットワークモニターには TCP に加えて UDP プロトコルが表示されるようになりました。

3. スキャンタスクが改善されました。スキャン中にコンピューターを再起動すると、Kaspersky Endpoint Security は自動的にスキャンが中断された箇所からタスクを継続して実行します。

4. タスクの実行時間に制限を設定できるようになりました。スキャンおよび*IOC* スキャンタスクに対して実行時間を制限できます。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。スキャンタスクの実行時間を短縮するため、スキャン範囲を設定したり、スキャンを最適化したりすることができます。

5. Windows 10 Enterprise マルチセッションに本製品がインストールされた場合、サーバープラットフォームの制限事項は解消されます。Kaspersky Endpoint Security は Windows 10 Enterprise のマルチセッションを、サーバーオペレーティングシステムではなくワークステーションのオペレーティングシステムとして認識するようになりました。それに応じて、サーバープラットフォームの制限事項は Windows 10 Enterprise のマルチセッションにインストールされた本製品には適用されなくなりました。また、サーバー用のライセンスではなく、ワークステーション用のライセンスがアクティベーションに使用されます。

11.7.0 のアップデート

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

1. Kaspersky Endpoint Security for Windows のインターフェイスが更新されました。

2. Windows 11、Windows Server 10 21H2 および Windows Server 2022 をサポートするようになりました。

3. 追加された新機能：

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

     Kaspersky Sandbox を使用する際に Kaspersky Endpoint Agent が不要になりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。Kaspersky Endpoint Agent のポリシーを移行するには、移行ウィザードを使用してください。Kaspersky Sandbox のすべての機能が動作するためには Kaspersky Security Center 13.2 が必要です。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行に関して詳しくは、製品のヘルプを参照してください。

   - Kaspersky Endpoint Detection and Response Optimum ソリューションの操作をサポートする組み込みエージェントが追加されました。*Kaspersky Endpoint Detection and Response Optimum* は、高度なサイバー脅威から組織の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。

     Kaspersky Endpoint Detection and Response を使用する際に Kaspersky Endpoint Agent が不要になりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。Kaspersky Endpoint Agent のポリシーおよびタスクを移行するには、移行ウィザードを使用してください。Kaspersky Endpoint Detection and Response Optimum のすべての機能を使用するには、Kaspersky Security Center 13.2 が必要です。Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行に関して詳しくは、製品のヘルプを参照してください。

4. Kaspersky Endpoint Agent のポリシーおよびタスクを移行する移行ウィザードが追加されました。移行ウィザードは、Kaspersky Endpoint Security for Windows の新しく統合されたポリシーおよびタスクを作成します。ウィザードを使用すると、Detection and Response ソリューションを Kaspersky Endpoint Agent から Kaspersky Endpoint Security に移行できます。Detection and Response solutions には、Kaspersky Sandbox、Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) および Kaspersky Managed Detection and Response (MDR) が含まれます。

5. 配信キットに含まれている Kaspersky Endpoint Agent がバージョン 3.11 にアップデートされました。

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

6. BitLocker 暗号化機能が改善されました：

   - BitLocker ドライブ暗号化で拡張 PIN が使用できるようになりました。*拡張 PIN* を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります。

   - オペレーティングシステムのアップグレードやアップグレードパッケージのインストール用に BitLocker 認証を無効にする機能が追加されました。アップデートのインストールには、コンピューターの再起動が複数回必要になることがあります。正常にアップデートをインストールするために一時的に BitLocker 認証をオフにして、アップデートのインストール後に再度認証を有効にすることができます。

   - BitLocker 暗号化パスワードまたは PIN に有効期限を設定できるようになりました。パスワードまたは PIN の有効期間が終了すると、Kaspersky Endpoint Security はユーザーに新しいパスワードの入力を要求します。

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

8. ファイアウォール機能が改善されました：

   - ファイアウォールのパケットルールの IP アドレスの範囲を設定できるようになりました。アドレスの範囲は IPv4 または IPv6 形式で入力できます。例：`192.168.1.1-192.168.1.100` または `12:34::2-12:34::99`。

   - ファイアウォールのパケットルールに IP アドレスの代わりに DNS 名を入力できるようになりました。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。

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

10. スキャンタスクが改善されました：

    - コンピューターのアイドル状態でのスキャンタスクが*改善されました*。スキャン中にコンピューターを再起動すると、Kaspersky Endpoint Security は自動的にスキャンが中断された箇所からタスクを継続して実行します。

    - スキャンタスクが最適化されました。既定では、Kaspersky Endpoint Security はコンピューターが使用されていないときにのみスキャンを実行します。タスクのプロパティからコンピューターのスキャンをいつ実行するか設定できます。

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

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

11.6.0 のアップデート

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

1. Windows 10 21H1 のサポート。Microsoft Windows 10 オペレーティングシステムのサポートについては、テクニカルサポートサイトのナレッジベースの記事を参照してください。

2. Managed Detection and Response が追加されました。この機能は、Kaspersky Managed Detection and Response と呼ばれるソリューションとのやり取りをサポートします。Kaspersky Managed Detection and Response (MDR) は、24 時間体制で日々増加していく脅威に対抗する保護を提供します。企業側で専門知識や技術を確保するために限られたリソースの時間や労力を費やす必要はありません。ソリューションについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

3. 配信キットに含まれている Kaspersky Endpoint Agent がバージョン 3.10 にアップデートされました。Kaspersky Endpoint Agent 3.10 は新機能を実装し、また一部の既知の問題を修正し、安定性が向上しました。製品の詳細については、Kaspersky Endpoint Agent をサポートするカスペルスキー製品のガイドを参照してください。

4. ネットワーク脅威対策の設定で、ポートのスキャンおよびネットワークフラッディングのような攻撃に対する保護を管理する機能を提供できるようになりました。

5. ファイアウォールのネットワークルールを作成する方法が新しく追加されました。ネットワークモニターウィンドウで表示される接続のパケットルールおよびアプリケーションルールを追加できます。ネットワークルールの接続設定は自動で設定されます。

6. ネットワークモニターのインターフェイスが改善されました。ネットワークでの操作に関する次の情報を追加しました：ネットワーク操作を開始したプロセス ID、ネットワーク種別（ローカルネットワークまたはインターネット）、ローカルポート。既定では、ネットワーク種別に関する情報は非表示です。

7. 新規 Windows ユーザーに対して自動で認証エージェントアカウントを作成できるようになりました。エージェントを使用して、ユーザーがKaspersky Disk Encryption 技術を使用して暗号化されたドライブにアクセスするための認証を完了し、オペレーティングシステムを読み込むことができます。本製品はコンピューター上の Windows ユーザーアカウントに関する情報を確認します。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。そのため、すでに暗号化されたドライブを持つコンピューター用に認証エージェントを手動で追加する必要はありません。

8. ユーザーのコンピューター上の製品インターフェイスでディスクの暗号化プロセスを確認できるようになりました（Kaspersky Disk Encryption および BitLocker）。暗号化モニターツールは製品のメインウィンドウから実行できます。

11.5.0 のアップデート

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

1. Windows 10 20H2 のサポート。Microsoft Windows 10 オペレーティングシステムのサポートについては、テクニカルサポートサイトのナレッジベースの記事を参照してください。

2. 製品インターフェイスのアップデート。また、通知エリアの製品アイコン、製品の通知、ダイアログボックスもアップデートされました。

3. アプリケーションコントロール、デバイスコントロール、アダプティブアノマリーコントロールの Web プラグインのインターフェイスの向上。

4. ルールおよび除外リストの一覧を XML 形式でインポートおよびエクスポートする機能の追加。エクスポート後に XML 形式のリストを編集できます。Kaspersky Security Center コンソールでのみリストを管理できます。次のリストのエクスポートおよびインポートが可能です：

   - ふるまい検知（除外リスト）
   - ウェブ脅威対策（信頼する URL のリスト）
   - メール脅威対策（添付ファイルの拡張子のフィルターのリスト）
   - ネットワーク脅威対策（除外リスト）
   - ファイアウォール（ネットワークパケットルールのリスト）
   - アプリケーションコントロール（ルールのリスト）
   - ウェブコントロール（ルールのリスト）
   - ネットワークポートの監視（Kaspersky Endpoint Security の監視対象のポートおよびアプリケーションのリスト）
   - Kaspersky Disk Encryption（除外リスト）
   - リムーバブルドライブの暗号化（ルールのリスト）

5. 脅威の検知レポートにオブジェクトの MD5 情報が追加されました。以前のバージョンの Kaspersky Endpoint Security では、オブジェクトの SHA256 のみが表示されていました。

6. デバイスコントロールの設定で、デバイスアクセスルールに優先度を割り当てられるようになりました。優先度を割り当てることにより、ユーザーのデバイスへのアクセスをより柔軟に設定できるようになりました。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 0 を設定し、Everyone グループには 1 を設定します。優先度は、ファイルシステムを持つデバイスにのみ設定できます。これには、ハードディスク、リムーバブルドライブ、フロッピーディスク、CD/DVD ドライブ、およびポータブルデバイス（MTP）が含まれます。

7. 追加された新機能：

   - サウンドの管理。
   - ネットワークにかかる費用の対策で、モバイル接続時などインターネット接続が制限されている場合に Kaspersky Endpoint Security のネットワークトラフィックを制限します。

- 信頼するリモートアクセスアプリケーションでの Kaspersky Endpoint Security 設定の管理（TeamViewer、LogMeIn Pro および Remotely Anywhere など）。リモート管理アプリケーションを使用して Kaspersky Endpoint Security を開始したり製品インターフェイスで Kaspersky Endpoint Security 設定を管理できます。

- Firefox および Thunderbird で保護されたトラフィックのスキャン設定の管理。Mozilla により使用される証明書ストアを選択できます：Windows 証明書ストアまたは Mozilla 証明書ストア。この機能はポリシーが適用されていないコンピューターのみに利用可能です。ポリシーがコンピューターに適用されていた場合、Kaspersky Endpoint Security は Firefox および Thunderbird に対して自動的に Windows 証明書ストアの使用を有効にします。

8. 保護されたトラフィックのスキャンモードを設定できるようになりました： 保護機能が無効になった場合でも常にトラフィックをスキャンする、または保護機能が要求したときにのみトラフィックをスキャンします。

9. レポートの情報を削除する手順を見直しました。ユーザーはすべてのレポートを削除することのみ可能です。以前のバージョンでは、ユーザーはレポートからその情報を削除されるアプリケーションコンポーネントを選択していました。

10. Kaspersky Endpoint Security の設定を含む設定ファイルのインポートの手順および製品設定の復元の手順を見直しました。インポートまたは復元前に、Kaspersky Endpoint Security は警告のみを表示します。以前のバージョンでは、新しい設定が適用される前に新しい設定の値を表示できました。

11. BitLocker により暗号化されたドライブへのアクセスの復元の手順を簡素化しました。アクセス復元の手順の完了後、Kaspersky Endpoint Security は新しいパスワードまたは PIN コードを設定するよう通知します。新しいパスワードの設定後、BitLocker はドライブを暗号化します。以前のバージョンでは、ユーザーは BitLocker の設定で手動でパスワードをリセットする必要がありました。

12. ユーザーは特定のコンピューターにローカルの信頼ゾーンを作成することができるようになりました。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。管理者はローカルの除外リストまたはローカルの信頼するアプリケーションの使用を許可またはブロックできます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

13. 信頼するアプリケーションのプロパティにコメントを入力できるようになりました。コメントは信頼するアプリケーションの検索や並べ替えに役に立ちます。

14. REST API を使用した製品の管理：

    - メール脅威対策の Outlook 用機能拡張を設定できるようになりました。

    - ウイルスやワーム、トロイの木馬の検出を無効にすることは禁止されています。

11.4.0 のアップデート

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

1. タスクバーの通知エリアの製品アイコンのデザインが新しくなりました。古いアイコン（）の代わりに新しいアイコン（）が表示されます。本製品のアップデート後に再起動が必要な場合など、ユーザーが操作を実行する必要がある場合はアイコンが に変わります。本製品の保護機能が無効になっている、または問題がある場合はアイコンが または に変わります。アイコンにマウスオーバーすると、コンピューターの保護についての説明が表示されます。

2. 配信キットに含まれている Kaspersky Endpoint Agent がバージョン 3.9 にアップデートされました。Kaspersky Endpoint Agent 3.9 は新しい Kaspersky ソリューションとの統合をサポートします。製品の詳細については、Kaspersky Endpoint Agent をサポートするカスペルスキー製品のガイドを参照してください。

3. Kaspersky Endpoint Security コンポーネントのステータスに「*ライセンスが対応していない*」が追加されました。メインアプリケーションウィンドウのコンポーネントのリストで機能の状態を表示できます。

4. 脆弱性攻撃ブロックからの新しいイベントがレポートに追加されました。

5. 暗号化が開始されると、Kaspersky Disk Encryption技術向けのドライバーが自動的に Windows 回復環境（WinRE）に追加されるようになりました。以前のバージョンの Kaspersky Endpoint Security では、本製品のインストール時にドライバーが追加されていました。WinRE へのドライバーの追加により、Kaspersky Disk Encryption 技術で保護されたコンピューターのオペレーティングシステムの回復時に、アプリケーションの動作がより安定します。

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

よくある質問（FAQ）

全般

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

以前のバージョンと比べて、どのような機能が追加されたり変更されましたか？

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

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

製品の導入

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

コマンドラインを使用したインストールではどのような設定を指定できますか？

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

アップデート

定義データベースをアップデートするにはどのような方法がありますか？

アップデートの実行後に問題が発生したら、どのように対応すればよいですか？

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

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

セキュリティ

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

信頼できるファイルをスキャン対象から除外するにはどうすればよいですか？

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

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

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

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

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

インターネット

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

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

SNS へのアクセスをブロックするにはどうすればよいですか？

アプリケーション

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

コンピューターゲームの実行を禁止するにはどうすればよいですか？

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

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

デバイス

外付けドライブの使用をブロックするにはどうすればよいですか？

信頼リストにデバイスを追加するにはどうすればよいですか？

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

暗号化

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

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

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

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

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

サポート

レポートファイルはどこに保存されていますか？

トレースファイルを作成するにはどうすればよいですか？

ダンプの書き込みを有効にするにはどうすればよいですか？

Kaspersky Endpoint Security for Windows

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

本製品は、自動制御システムを伴う技術プロセスでの使用を想定していません。そのようなシステムで端末を保護するには、Kaspersky Industrial CyberSecurity for Nodes 製品の使用を推奨します。

脅威検知技術

機械学習

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

クラウド分析

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

エキスパートによる分析

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

ふるまい分析

リアルタイムでオブジェクトの活動を分析します。

自動分析

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

Sandbox

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

Cloud Sandbox

Kaspersky Endpoint Security は、カスペルスキーの提供する隔離された環境でオブジェクトをスキャンします。Cloud Sandbox 技術は、使用しているライセンス種別にかかわらずすべての Kaspersky Security Network ユーザーに対して有効で使用可能です。Endpoint Detection and Response ソリューションを導入済みの場合は、Cloud Sandbox で検知された脅威向けの個別のカウンターを有効にすることができます。

選択ツリー

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

セクション	コンポーネント
脅威対策	**ファイル脅威対策** ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターの RAM に常駐し、開いたファイル、保存したファイル、実行されたファイルのすべてをリアルタイムでスキャンします。このコンポーネントは、接続されているドライブを含むすべてのコンピュータードライブ上のファイルをスキャンします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。 **ウェブ脅威対策** ウェブ脅威対策は、インターネットからの悪意のあるファイルのダウンロードを防ぎ、悪意のある Web サイトやフィッシングサイトをブロックします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。 **メール脅威対策** メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。 メール脅威対策は、受信メッセージと送信メッセージの両方をスキャンすることができます。製品は、以下のメールクライアントの POP3、SMTP、IMAP、NNTP をサポートしています。 • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Mozilla Thunderbird、MyOffice Mail、R7-Office Organizer の各メールクライアントでトラフィックをスキャンするには、証明書ストアにカスペルスキーの証明書を追加し、独自の証明書ストアを選択する必要があります。 メール脅威対策は、他のプロトコルやメールクライアントをサポートしていません。 メール脅威対策は、メッセージに*プロトコルレベル*でアクセスできるとは限りません（たとえば、Microsoft Exchange ソリューションを使用する場合）。このため、メール脅威対策には、Microsoft Office Outlook 用の機能拡張が含まれています。この機能拡張により、*メールクライアントレベル*でメッセージをスキャンすることができます。メール脅威対策の機能拡張は Outlook 2010、2013、2016、2019 および 2021 の操作をサポートします。 **ネットワーク脅威対策** *ネットワーク脅威対策*コンポーネント（侵入検知システム、IDS とも呼ばれます）は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視します。本製品は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、定義データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、定義データベースと製品機能のアップデート時にアップデートされます。 **ファイアウォール** ファイアウォールは、インターネットまたはローカルネットワークでの作業中に、コンピューターへの不正な接続をブロックします。ファイアウォールは、コンピューター上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義された*ネットワークルール*を使用してコンピューターを保護します。 **有害 USB 攻撃ブロック** 有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。 **AMSI 保護** AMSI 保護コンポーネントは、Microsoft の Antimalware Scan Interface をサポートする目的で設計されています。*AMSI（Antimalware Scan Interface）*により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト（たとえば、PowerShell スクリプトなど）のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。

セクション	コンポーネント
先進の脅威対策 	**Kaspersky Security Network** *KSN（Kaspersky Security Network）*はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。 **ふるまい検知** ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures（BSS）を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。 さらに、ふるまい検知は、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。 **アンチクリプター** アンチクリプターコンポーネントは共有フォルダ内の動作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。 **脆弱性攻撃ブロック** 脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとすると、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。 さらに、脆弱性攻撃ブロックは、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。 **ホスト侵入防止** ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。 **修復エンジン** 修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。
セキュリティコントロール 	**アプリケーションコントロール** アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。 **デバイスコントロール** デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。 **ウェブコントロール** ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します。 **アダプティブアノマリーコントロール** アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「*Office アプリケーションによる Microsoft PowerShell の起動*」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートするのと同様に、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。 **Windows イベントログ監視** Windows イベントログ監視は Windows イベントログの分析に基づいて保護対象環境の整合性を監視します。通常と異なるふるまいを検知した場合、本製品は管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。 **システム変更監視** システム変更監視コンポーネントは、コンピューターのセキュリティ侵害を示す可能性のあるオペレーティングシステムの変更を監視します。そのような変更を検知すると、Kaspersky Endpoint Security は対応するイベントを生成し、管理者に警告します。

セクション	コンポーネント
タスク 	**マルウェアのスキャン** Kaspersky Endpoint Security はコンピューターのウイルスやその他の脅威をスキャンします。マルウェアのスキャンを実行することにより、セキュリティレベルが低く設定されていたなどの理由でマルウェアが保護機能によって検知されなくても、マルウェアを拡散してしまわずにすみます。 **定義データベースと製品機能のアップデート** アップデートされた定義データベースおよび製品機能をダウンロードします。アップデートにより、コンピューターは新しいウイルスや脅威から保護されます。製品は既定で自動的にアップデートされますが、必要に応じて、定義データベースと製品機能を手動でアップデートすることができます。 **前回のアップデートのロールバック** 前回アップデートした定義データベースと製品機能を元に戻します。これにより、必要に応じて、定義データベースと製品機能を前のバージョンにロールバックすることができます。この機能は、たとえば新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。 **アプリケーション整合性チェック** Kaspersky Endpoint Security は、製品のインストールフォルダーにある製品機能に破損や変更がないかチェックします。製品機能のデジタル署名が正しくない場合、そのモジュールは破損していると考えられます。
データ暗号化 	**ファイルレベルの暗号化** この機能を使用してファイルの暗号化ルールを作成できます。暗号化のための事前定義されたフォルダーを指定したり、手動でフォルダーを指定したり、または拡張子で個別のファイルを指定したりできます。 **ディスク全体の暗号化** この機能を使用すると、Kaspersky Disk Encryption または BitLocker ドライブ暗号化を使用してハードドライブを暗号化できます。 **リムーバブルドライブの暗号化** この機能を使用してリムーバブルドライブのデータを保護します。ディスク全体の暗号化（FDE）またはファイルレベルの暗号化（FLE）を使用できます。

セクション	コンポーネント
Detection and Response 	**Endpoint Detection and Response Optimum** Kaspersky Endpoint Detection and Response Optimum ソリューション（以降「EDR Optimum」とします）の組み込みエージェントです。*Kaspersky Endpoint Detection and Response* は、高度なサイバー脅威から企業の IT インフラストラクチャを保護するソリューションです。Kaspersky Endpoint Detection and Response は、高度なサイバー脅威から企業の IT インフラストラクチャを保護するソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。このソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。 **Endpoint Detection and Response Expert** Kaspersky Endpoint Detection and Response Expert ソリューション（以降「EDR Expert」とします）の組み込みエージェントです。EDR Expert は EDR Optimum に比べ、より多くの脅威監視および応答機能を備えています。このソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。 **Endpoint Detection and Response Expert（オンプレミス）**および**Network Detection and Response (KATA)** Kaspersky Anti Targeted Attack Platform ソリューションの一部である Endpoint Detection and Response および Network Detection and Response コンポーネントの管理用の組み込みエージェントです。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています： • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。 **Sandbox** Sandbox の組み込みエージェント*Sandbox* コンポーネントはコンピューター上の高度な脅威を検知し、自動的にブロックします。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。ソリューションについて詳しくは、Kaspersky Sandbox のヘルプおよび Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。 **Managed Detection and Response** Kaspersky Managed Detection and Response ソリューションの操作をサポートする組み込みエージェントです。*Kaspersky Managed Detection and Response (MDR)* ソリューションはお客様のインフラストラクチャ内のセキュリティインシデントを自動で検知し分析します。MDR はエンドポイントから取得する遠隔測定したデータと機械学習を使用します。MDR はカスペルスキーのエキスパートにインシデントのデータを送信します。エキスパートはインシデントを処理し、新しい項目を定義データベースに追加するなどの対応をします。また、エキスパートたちはインシデントの処理に対して、コンピューターをネットワークから分離するなど、推奨事項を提示することもあります。ソリューションについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

製品のモード：スタンダード、EDR Agent、Light Agent

Kaspersky Endpoint Security for Windows は、多くのカスペルスキーのソリューションの一部です。ソリューションに応じて、製品のモードを選択する必要があります。



標準モード

これは本製品のメインのモードであり、既定のモードとなります。Kaspersky EPP（Endpoint Protection Platform）ソリューションの一部として、このモードで本製品をインストールできます。たとえば、標準モードの Kaspersky Endpoint Security は、Kaspersky Endpoint Security for Business の一部です。Kaspersky Endpoint Security は、様々な脅威、ネットワーク攻撃、詐欺からワークステーションとサーバーを包括的に保護します。



EDR Agent

このモードでは、Kaspersky Detection and Response ソリューションをサードパーティ製 EPP ソリューションとともに導入できます。Detection and Response ソリューションには、Kaspersky Managed Detection and Response（MDR）と Kaspersky Anti Targeted Attack Platform（KATA）が含まれます。EDR Agent は、カスペルスキーの SIEM ソリューションである Kaspersky Unified Monitoring and Analysis Platform（KUMA）もサポートします。

このモードでは、ファイル脅威対策やウェブ脅威対策などの標準の保護機能は使用できません。コンピューターの標準の保護は、サードパーティ製 EPP ソリューションにより提供されます。EDR Agent は、これらのコンピューターで実行されているプロセス、開かれているネットワーク接続、変更されているファイルを継続的に監視し、Detection and Response ソリューションと連携します。



Light Agent

このモードは仮想環境を保護するために使用されます。Light Agent モードの Kaspersky Endpoint Security は、Kaspersky Hybrid Cloud Security ソリューションの一部です。Light Agent は、ワークステーション用およびサーバー用のゲストオペレーティングシステムを搭載した仮想マシンを保護します。このモードでは、標準モードと同じ保護機能および管理コンポーネントを使用できます。違いは、個別の仮想マシンである SVM（Secure Virtual Machine）にインストールされた特別なソリューションのコンポーネントによって、オブジェクトがスキャンされてウイルスやその他のマルウェアが検知されることです。したがって、Light Agent は仮想マシンのリソースではなく、SVM のリソースを使用してインフラストラクチャのセキュリティを確保します。

製品の購入

配信キットには、次の配布パッケージが含まれています：

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

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

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

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

各配布パッケージには次のファイルが含まれています：

`kes_win.msi`	Kaspersky Endpoint Security のインストールパッケージ。
`setup_kes.exe`	いずれの製品インストールの方法でも必要となるファイル。
`kes_win.kud`	Kaspersky Endpoint Security のインストールパッケージの作成で必要となるファイル。

klcfginst.msi	Kaspersky Security Center 管理コンソールのアプリケーション管理プラグインのインストールパッケージ。
bases.cab	インストール中に使用されるアップデートパッケージファイル。
cleaner_v2.cab cleanerapi_v2.cab	競合するソフトウェアをアンインストールするためのファイル。
incompatible.txt	Kaspersky Endpoint Security と互換性の問題が発生する可能性のあるソフトウェアのリストを含むファイル。カスペルスキーは、Kaspersky Endpoint Security とリストにあるソフトウェアとの互換性を保証しません。
ksn_<language ID>.txt	Kaspersky Security Network への参加条件が記載されたファイル。
license.txt	使用許諾契約書とプライバシーポリシーの内容が記載されたファイル。
installer.ini	配信キットの内部設定を含むファイル。
kes.cab	製品のグラフィカルインターフェイス用ファイル。
aes256.cab/aes56.cab	AES 暗号アルゴリズム用ファイル。
package.kcat	製品の配信キットの署名が含まれるファイル。デジタル署名は、製品の配信キットの信頼性と整合性を保証するものです。

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

システム要件

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

全般的な最小要件：

- 2 GB 以上のディスク空き容量
- CPU：
  - ワークステーション：1 GHz
  - サーバー：1.4 GHz
  - SSE2 命令のサポート

  Arm アーキテクチャはサポートされていません。
- メモリ：
  - ワークステーション（x86）：1 GB
  - ワークステーション（x64）：2 GB
  - サーバー：2 GB
  - Kaspersky Anti Targeted Attack Platform との連携用の組み込みエージェント付きでアプリケーションをインストールするサーバー：8 GB

- Microsoft .NET Framework 4 以降
- 本製品をインストールするには、コンピューターの管理者権限が必要です。

ワークステーション

サポート対象のワークステーション用オペレーティングシステム：

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 以降
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise マルチセッション
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

Windows オペレーティングシステムのバージョン 11 24H2 以降では、UDP Receive Segment Coalescing Offload（URO）テクノロジーがサポートされます。互換性のあるネットワークカードとドライバーがコンピューターにインストールされている場合、この技術は既定で有効になります。ユーザーのコンピューターで URO を無効にすると、アプリケーションのパフォーマンスが大幅に低下する可能性があります。

Kaspersky Endpoint Security の適切な動作を確保するには、ユーザーのコンピューターで Windows セキュリティセンター（Windows Security Center、wscsvc）のサービスが実行されている必要があります。

オペレーティングシステムの更新 KB4490628（2019 年 3 月 12 日）および KB4474419（2019 年 9 月 23 日）がインストールされていない場合、Microsoft Windows 7 に Kaspersky Endpoint Security をインストールできません。詳細な情報については、テクニカルサポートのナレッジベースを参照してください。

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

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

サーバー

Kaspersky Endpoint Security では、サーバー向けの Windows オペレーティングシステムを実行しているコンピューター上での本製品の主要機能がサポートされるようになりました。サーバーおよび組織のクラスターで、Kaspersky Security for Windows Server の代わりに Kaspersky Endpoint Security for Windows を使用できます（クラスターモード、Cluster Mode）。本製品は Server Core Mode もサポートします（「既知の問題」を参照してください）。

サポート対象のサーバー用オペレーティングシステム：

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

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

- Windows MultiPoint Server 2011（64 ビット）
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 以降
- Windows Web Server 2008 R2 Service Pack 1 以降
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2016 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2019 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition （Server Core モードを含む）
- Windows Server 2025 Standard / Datacenter

オペレーティングシステムの更新 KB4490628（2019 年 3 月 12 日）および KB4474419（2019 年 9 月 23 日）がインストールされていない場合、Microsoft Windows Server 2008 R2 に Kaspersky Endpoint Security をインストールできません。

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

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

サポート対象外のサーバー用オペレーティングシステム：

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Standard / Enterprise / Datacenter SP2 以降
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 以降
- Microsoft Small Business Server 2008 Standard / Premium SP2 以降

仮想プラットフォーム

標準モードでの製品の動作を保証する、サポートされている仮想プラットフォーム：

- VMware Workstation Pro 17.6.4
- VMware ESXi 8.0 Update 3g
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

Light Agent をインストールする仮想マシン

仮想マシンの BIOS は、SMBIOS 仕様バージョン 2.1 以降をサポートしている必要があります。

仮想マシンには次のパッケージとユーティリティをインストールする必要があります。

- Microsoft Hyper-V を使用する場合 – Integration Services パッケージ。
- VMware vSphere を使用する場合 – VMware Tools パッケージ。
- XenServer を使用する場合 – XenTools パッケージ。
- HUAWEI FusionSphere を使用する場合 – HUAWEI Tools パッケージ。
- KVM ベースのハイパーバイザーを使用する場合 – QEMU Guest Agent。

製品を Light Agent モードで実行するための仮想インフラストラクチャ要件については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

アプリケーションが正しく動作するため、少なくとも 100 Mbit/s の帯域幅を持つ仮想化ネットワークインターフェイスを使用してください。

ターミナルサーバー

サポートされるターミナルサーバーの種別：

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

- Windows Server 2012 R2 の Microsoft Remote Desktop Services
- Windows Server 2016 の Microsoft Remote Desktop Services
- Windows Server 2019 の Microsoft Remote Desktop Services
- Windows Server 2022 の Microsoft Remote Desktop Services
- Windows Server 2025 の Microsoft Remote Desktop Services
- Citrix Virtual Apps and Desktops 7 2507 LTSR に含まれる Citrix RDSH

Kaspersky Security Center のサポート

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

- Kaspersky Security Center 14
- Kaspersky Security Center 14.1
- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1

オペレーティングシステムの種別に応じて利用できる本製品の機能の比較

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

Kaspersky Endpoint Security 12.8 for Windows 以降では、インストールパッケージで、オペレーティングシステムの種別ごとに異なるコンポーネントのセットを設定できます。つまり、同じインストールパッケージを使用して、本製品をワークステーションとサーバーに導入できます。

機能	ワークステーション	サーバー	Server Core モード
先進の脅威対策			
Kaspersky Security Network	✓	✓	✓
ふるまい検知	✓	✓	✓
アンチクリプター	✓	✓	✓
脆弱性攻撃ブロック	✓	✓	✓
ホスト侵入防止	✓	–	–
修復エンジン	✓	✓	✓
脅威対策			
ファイル脅威対策	✓	✓	✓
ウェブ脅威対策	✓	✓	–
メール脅威対策	✓	✓	–
ファイアウォール	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓
有害 USB 攻撃ブロック	✓	✓	–
AMSI 保護	✓	✓	✓
セキュリティコントロール			
Windows イベントログ監視	–	✓	–
アプリケーションコントロール	✓	✓	✓
デバイスコントロール	✓	✓	✓
ウェブコントロール	✓	✓	–
アダプティブアノマリーコントロール	✓	–	–
システム変更監視	–	✓	–
Cloud Discovery	✓	–	–
データ暗号化			
Kaspersky Disk Encryption	✓	–	–
BitLocker ドライブ暗号化	✓	✓	✓
ファイルレベルの暗号化	✓	–	–
リムーバブルドライブの暗号化	✓	–	–
Detection and Response			
Endpoint Detection and Response Optimum	✓	✓	✓
Endpoint Detection and Response Expert	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓
Sandbox	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓
KUMA 連携	✓	✓	✓

管理用コンソールの種別に応じて利用できる製品機能の比較表

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

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

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

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

Kaspersky Endpoint Security は、Kaspersky Next Pro View ソリューションの一部です。このソリューションの一部として動作する場合の利用可能な製品機能の詳細については、Kaspersky Next のヘルプを参照してください。

Kaspersky Endpoint Security の機能の比較表

機能	Kaspersky Security Center		Kaspersky Security Center
	管理コンソール	Web コンソール	Cloud コンソール
先進の脅威対策			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
ふるまい検知	✓	✓	✓
アンチクリプター			
脆弱性攻撃ブロック	✓	✓	✓
ホスト侵入防止	✓	✓	✓
修復エンジン	✓	✓	✓
脅威対策			
ファイル脅威対策	✓	✓	✓
ウェブ脅威対策	✓	✓	✓
メール脅威対策	✓	✓	✓
ファイアウォール	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓
有害 USB 攻撃ブロック	✓	✓	✓
AMSI 保護	✓	✓	✓
セキュリティコントロール			

機能	Kaspersky Security Center		Kaspersky Security Center
	管理コンソール	Web コンソール	Cloud コンソール
Windows イベントログ監視	✓	✓	✓
アプリケーションコントロール	✓	✓	✓
デバイスコントロール	✓	✓	✓
ウェブコントロール	✓	✓	✓
アダプティブアノマリーコントロール	✓	✓	✓
システム変更監視	✓	✓	✓
Cloud Discovery	–	–	✓
データ暗号化			
Kaspersky Disk Encryption	✓	✓	–
BitLocker ドライブ暗号化	✓	✓	✓
ファイルレベルの暗号化	✓	✓	–
リムーバブルドライブの暗号化	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA 連携	✓	✓	✓
タスク			
ライセンスの追加	✓	✓	✓
コンポーネントの変更	✓	✓	✓
インベントリ	✓	✓	✓
アップデート	✓	✓	✓
アップデートのロールバック	✓	✓	✓
マルウェアのスキャン	✓	✓	✓
アプリケーション整合性チェック	✓	✓	–
データの消去	✓	✓	✓
認証エージェントアカウントの管理（Kaspersky Disk Encryption）	✓	✓	–
IOC スキャン (EDR)	–	✓	✓
ファイルの隔離 (EDR)	–	✓	✓
ファイルの取得 (EDR)	–	✓	✓
ファイルの削除 (EDR)	–	✓	✓
プロセスの開始 (EDR)	–	✓	✓
プロセスの終了 (EDR)	–	✓	✓

他のアプリケーションとの互換性情報

Kaspersky Endpoint Security は、一部のカスペルスキー製品および一部のサードパーティ製品と共存できないことがあります。そのため、インストール前、製品バージョンのアップデート前、製品コンポーネントの変更前に、Kaspersky Endpoint Security はコンピューターをスキャンして、そのようなアプリケーションが存在するかどうかを確認します。

サードパーティ製品との互換性情報

Kaspersky Endpoint Security は、サードパーティのエンドポイント保護システム (Endpoint Protection Platform、EPP) の一部であるアプリケーションとは互換性がありません。Kaspersky Endpoint Security では、他のアプリケーションと互換性の問題が発生することもあります。互換性を判断するために、Kaspersky Endpoint Security は、カスペルスキーが用意したソフトウェアのリストを参照します。このリストは incompatible.txt ファイルに含まれています。このファイルは配信キットに含まれています。

カスペルスキーは、Kaspersky Endpoint Security とリストにあるソフトウェアとの互換性を保証しません。リスト内のソフトウェアが検出されると、インストーラーは Kaspersky Endpoint Security の導入を停止します。インストーラーはリストにある一部のアプリケーションを自動的に削除する場合があります。リスクに関係なく Kaspersky Endpoint Security とリストにあるソフトウェアを同じコンピューターにインストールする場合は、コンピューターのチェックを省略できます（以下の手順を参照）。

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

カスペルスキー製品との互換性情報

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

- カスペルスキー スタンダード | プラス | プレミアム
- カスペルスキー スモール オフィス セキュリティ
- カスペルスキー インターネット セキュリティ
- Kaspersky Anti-Virus
- Kaspersky Total Security
- カスペルスキー セーフキッズ
- カスペルスキー フリー
- Kaspersky Anti-Ransomware Tool
- Kaspersky Anti Targeted Attack Platform および Kaspersky Endpoint Detection and Response ソリューションの一部としての Endpoint Sensor。

- カスペルスキーの Detection and Response ソリューションの一部としての Kaspersky Endpoint Agent。

  カスペルスキーは、すべての Detection and Response が Kaspersky Endpoint Agent ではなく、Kaspersky Endpoint Security の組み込みエージェントと連携するよう切り替えています。バージョン 12.1 から、本製品はすべての Detection and Response ソリューションがサポートされるようになりました。

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

  Kaspersky Endpoint Security 12.0 より、Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows に移行して、ワークステーションおよびサーバーを保護する同一のソリューションを使用できるようになりました。

- Kaspersky Embedded Systems Security

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

互換性の問題が発生する可能性のあるソフトウェアのチェックを省略する

Kaspersky Endpoint Security が incompatible.txt リストに記載のあるソフトウェアを検出した場合、製品のインストールは終了します。インストールを続行するには、そのソフトウェアを削除する必要があります。しかし、サードパーティ製品のマニュアルに、その製品がエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）と互換性があると記載がある場合は、Kaspersky Endpoint Security をその製造元の製品がインストールされているコンピューターにインストールすることが可能です。例えば、Endpoint Detection and Response (EDR) ソリューションのプロバイダーがサードパーティの EPP システムとその製品の互換性があると記載している場合などです。このような場合は、インストール済みのソフトウェアのチェックを実行せずに Kaspersky Endpoint Security のインストールを開始する必要があります。このためには、インストーラーに次のパラメータを渡す必要があります。

- `SKIPPRODUCTCHECK=1`：インストール済みのソフトウェアのチェックの実行を無効にします。互換性の問題が発生する可能性のあるソフトウェアのリストは、配信キットに含まれている incompatible.txt ファイルで参照できます。このパラメータの値が指定されておらず、リストに記載されている製品が検知された場合、Kaspersky Endpoint Security のインストールは終了します。
- `SKIPPRODUCTUNINSTALL=1`：incompatible.txt リストに記載されたソフトウェアが検知された場合の自動削除を無効にします。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security は互換性の問題が発生する可能性のあるソフトウェアの削除を試みます。
- `CLEANERSIGNCHECK=0`：チェックによって見つかったソフトウェアのデジタル署名検証を無効にします。このパラメータが設定されていない場合、Kaspersky Security Center 経由でアプリケーションを配布する際のデジタル署名の検証は無効にされます。アプリケーションがローカルでインストールされる場合、デジタル署名の検証は既定で有効になります。

ローカルで本製品をインストールする場合、コマンドラインでパラメータを渡すことができます。

インストールプロセス中に互換性の問題を引き起こす可能性のあるソフトウェアのスキャンをスキップした場合、製品コンポーネントが変更されたときに、Kaspersky Endpoint Security はこのチェックを再度実行できます。インストールされたソフトウェアのスキャンをスキップするには、*コンポーネントの変更*タスクを設定する必要があります。

例：

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

リモートから Kaspersky Endpoint Security をインストールする場合は、インストールパッケージ生成ファイル（`kes_win.kud`）の`[Setup]`に適切なパラメータを追加する必要があります（以下を参照）。`kes_win.kud` ファイルは配信キットに含まれています。

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

本製品のインストールと削除

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

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

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

1. ファイル「setup.ini」で指定した設定。
2. ファイル「installer.ini」で指定した設定。
3. コマンドラインで指定した設定。
4. 設定ファイル（install.cfg）で指定した設定。

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

Kaspersky Endpoint Security のインストール時に、オペレーティングシステムが独自のメッセージを表示する場合があります。製品のインストール中に、ネットワークおよびインターネット接続が中断される場合もあります。

Kaspersky Endpoint Security のインストール、アップデート、アンインストール時に、エラーが発生することがあります。これらのエラーの解決方法については、テクニカルサポートのナレッジベースを参照してください。

Kaspersky Security Center による導入

企業ネットワーク内のコンピューターへの Kaspersky Endpoint Security の導入には、複数の方法を使用できます。組織のニーズに最適な導入シナリオを選択するか、いくつかの導入シナリオを同時に組み合わせて使用できます。本製品のインストール前に、Kaspersky Security Center ネットワークエージェントがコンピューターにインストールされていることを確認する必要があります。*ネットワークエージェント*は、管理サーバーとクライアントコンピューターのやり取りをサポートします。

Kaspersky Security Center は、次の主要な導入方法をサポートしています：

- 製品導入ウィザードを使用した製品のインストール

  Kaspersky Endpoint Security の既定の設定で組織のニーズを満たすことができ、組織のインフラストラクチャの構成もシンプルで特別な設定が必要ない場合、標準インストールでの導入が便利です。

- リモートインストールタスクを使用した製品のインストール

  Kaspersky Endpoint Security 設定を指定し、リモートインストールタスク自体にも柔軟に管理設定を行える一般的なインストール方法です。Kaspersky Endpoint Security をインストールするには、次の手順を実行します：

  1. インストールパッケージの作成
  2. リモートインストールタスクの作成

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

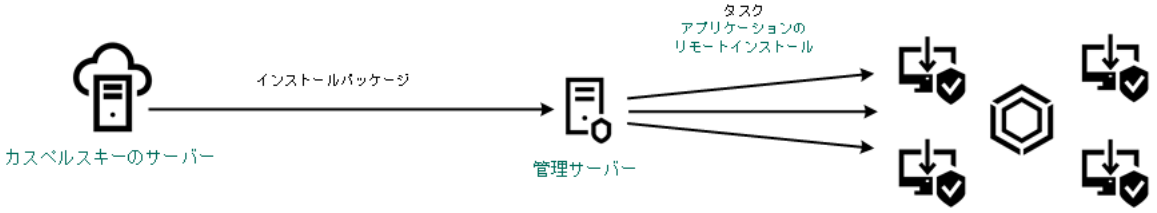
製品の標準インストール

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

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

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

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



Kaspersky Endpoint Security の導入

管理コンソール（MMC）で製品導入ウィザードを実行する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**リモートインストール**］を選択します。
3. ［**管理対象デバイス（ワークステーション）にインストールパッケージを配布**］リンクをクリックします。

製品導入ウィザードが開始されます。ウィザードの指示に従います。

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

ステップ 1：インストールパッケージの選択

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

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

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

ステップ 2：インストールパッケージのソースの選択

［**Kaspersky Security Center パッケージを配信**］のソースを選択します。

ステップ 3：インストール先のデバイスの選択

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

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

ステップ 4：リモートインストールタスク設定の定義

次の追加のアプリケーション設定を設定します：

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

ステップ 5：ライセンスの選択

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

ステップ 6：オペレーティングシステムの再起動設定の選択

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

ステップ 7：製品のインストール前の互換性のない製品の削除

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

ステップ 8：コンピューターへのアクセス用のアカウントの選択

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

ステップ 9：インストールの開始

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

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

Web コンソールのメインウィンドウで、［**検出と製品の導入**］→［**導入と割り当て**］→［**製品導入ウィザード**］をクリックします。

製品導入ウィザードが開始されます。ウィザードの指示に従います。

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

ステップ 1：インストールパッケージの選択

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

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

ステップ 2：ライセンスの選択

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

ステップ 3：ネットワークエージェントの選択

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

ステップ 4：インストール先のデバイスの選択

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

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

ステップ 5：詳細設定

次の追加のアプリケーション設定を設定します：

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

ステップ 6：オペレーティングシステムの再起動設定の選択

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

ステップ 7：製品のインストール前の互換性のない製品の削除

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

ステップ 8：管理グループへの割り当て

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

ステップ 9：コンピューターへのアクセス用のアカウントの選択

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

ステップ 10：インストールの開始

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

インストールパッケージの作成

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

管理コンソール（MMC）でインストールパッケージを作成する方法

1. 管理コンソールで、［**管理サーバー**］→［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に移動します。

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

2. ［**インストールパッケージの作成**］をクリックします。

新規パッケージウィザードが表示されます。ウィザードの指示に従います。

ステップ1：インストールパッケージの種別の選択

［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。

ステップ2：インストールパッケージ名の定義

Kaspersky Endpoint Security for Windows 12.12 などのインストールパッケージの名前を入力します。

ステップ3：インストールする配布パッケージの選択

［**参照**］をクリックし、配布キットに含まれている `kes_win.kud` ファイルを選択します。

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

ステップ4：使用許諾契約書とプライバシーポリシー

使用許諾契約書およびプライバシーポリシーの条項を読んで同意します。

インストールパッケージが作成され、Kaspersky Security Center に追加されます。インストールパッケージを使用して、組織ネットワーク内のコンピューターへの Kaspersky Endpoint Security のインストールまたはインストール済みの製品のバージョンのアップデートを実行できます。

インストールパッケージの設定では、オペレーティングシステムの種別ごとに製品コンポーネントを選択できます。つまり、インストールパッケージには、ワークステーション用とサーバー用の 2 セットのコンポーネントが含まれています。インストールパッケージを導入する前に、インストーラーはオペレーティングシステムの種別を検出し、そのオペレーティングシステムの種別に対して選択した製品コンポーネントのみをインストールします。この方法では、ワークステーションとサーバーに同じインストールパッケージを使用できます。

インストールパッケージには、管理サーバーリポジトリの定義データベースが含まれます。インストールパッケージのデータベースをアップデートすることで、Kaspersky Endpoint Security をインストールした後にデータベースをアップデートすることにより生じるトラフィック量を削減できます。

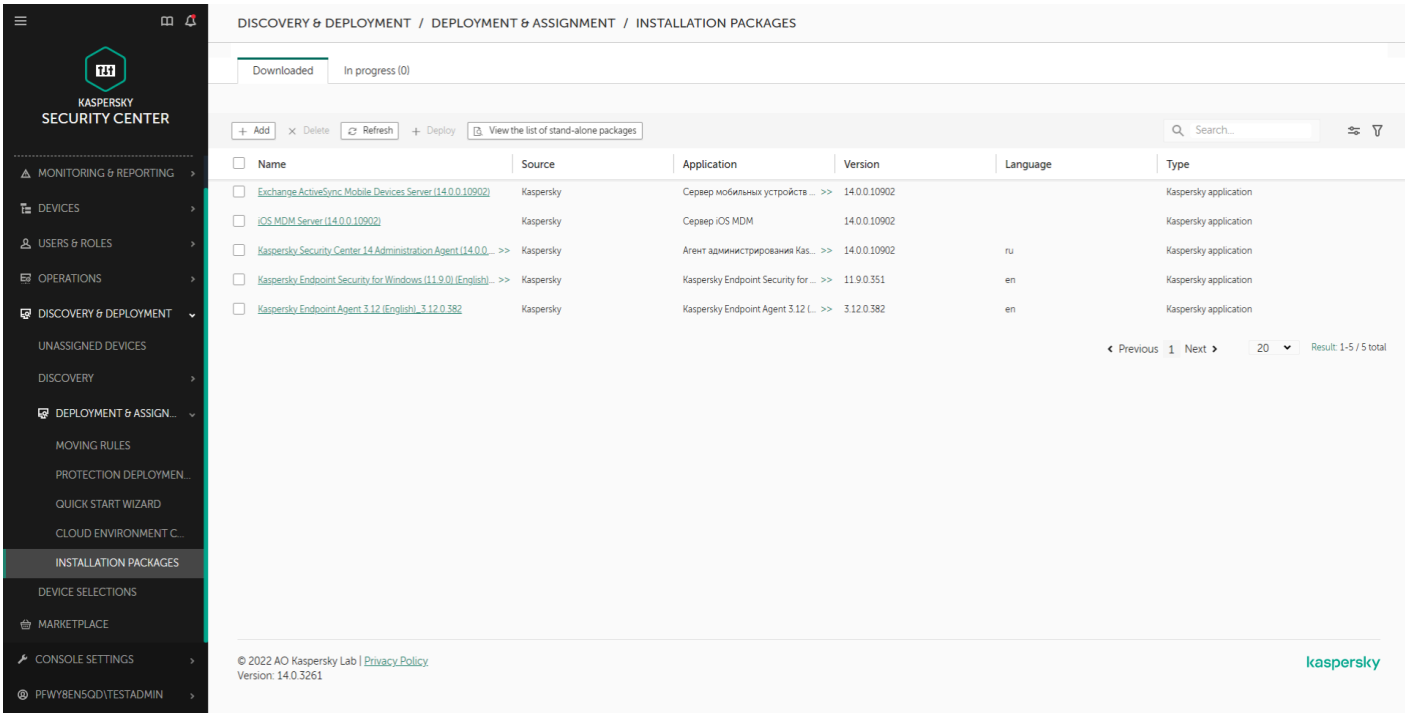
Web コンソールと Cloud コンソールでインストールパッケージを作成する方法

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

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

2. ［**追加**］をクリックします。

新規パッケージウィザードが表示されます。ウィザードの指示に従います。



インストールパッケージのリスト

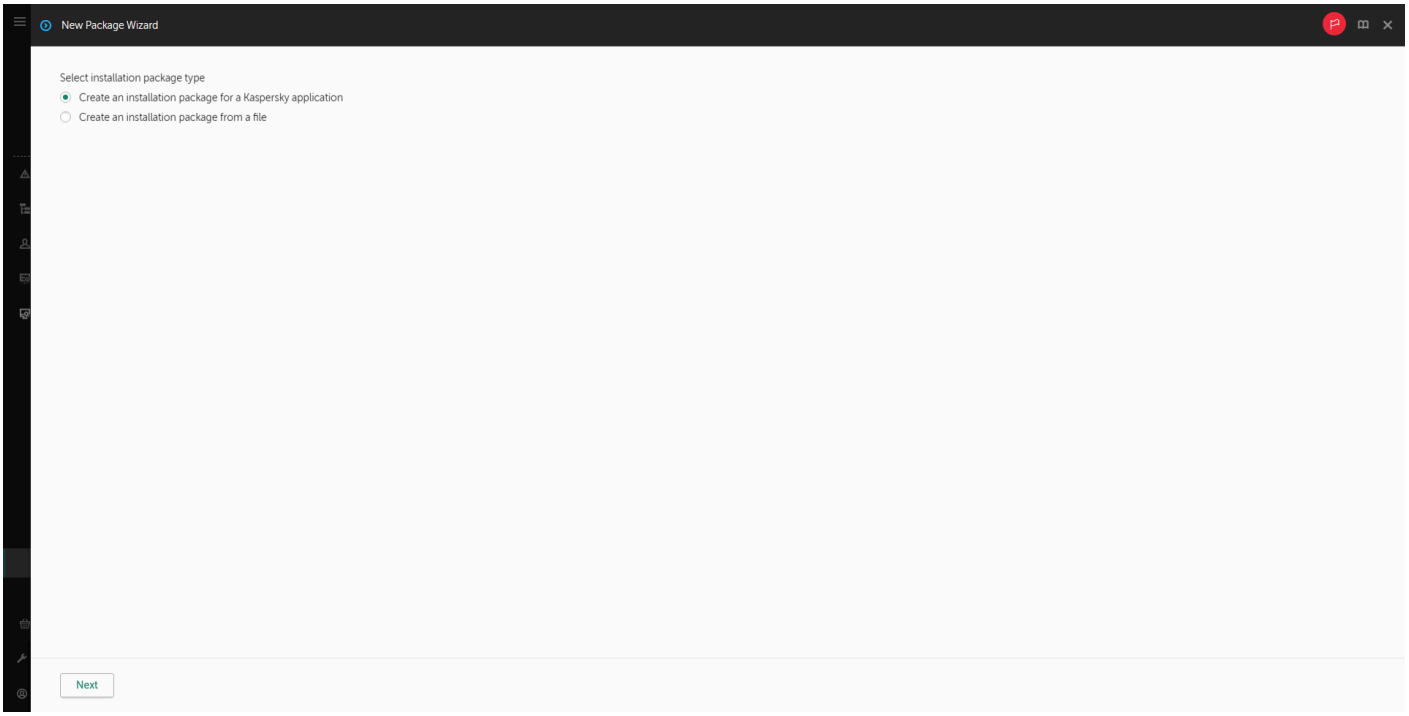
ステップ1：インストールパッケージの種別の選択

［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。

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

インストールパッケージをファイルから作成することもできます。

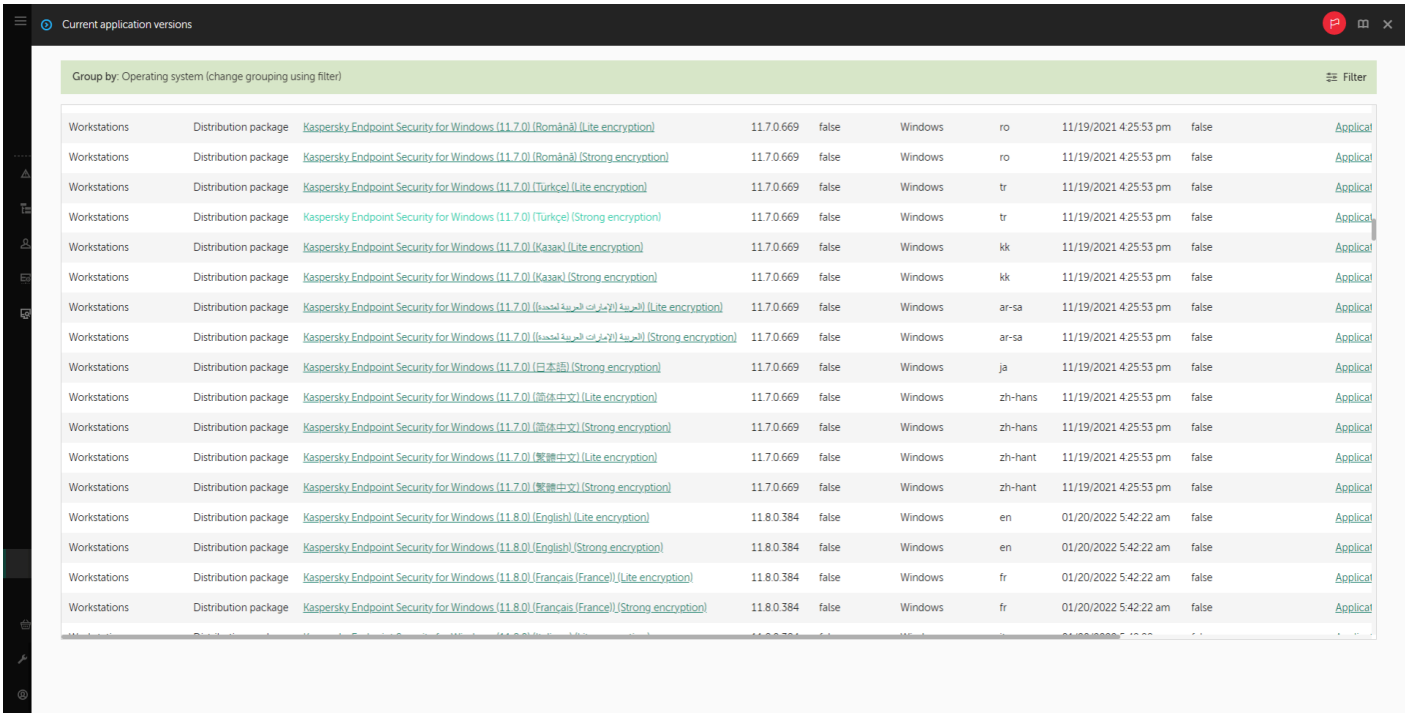
ファイルからの Kaspersky Endpoint Security 向けのインストールパッケージの作成は、Kaspersky Security Center Web コンソールでのみ可能です。



インストールパッケージの種別

ステップ 2：インストールパッケージ

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

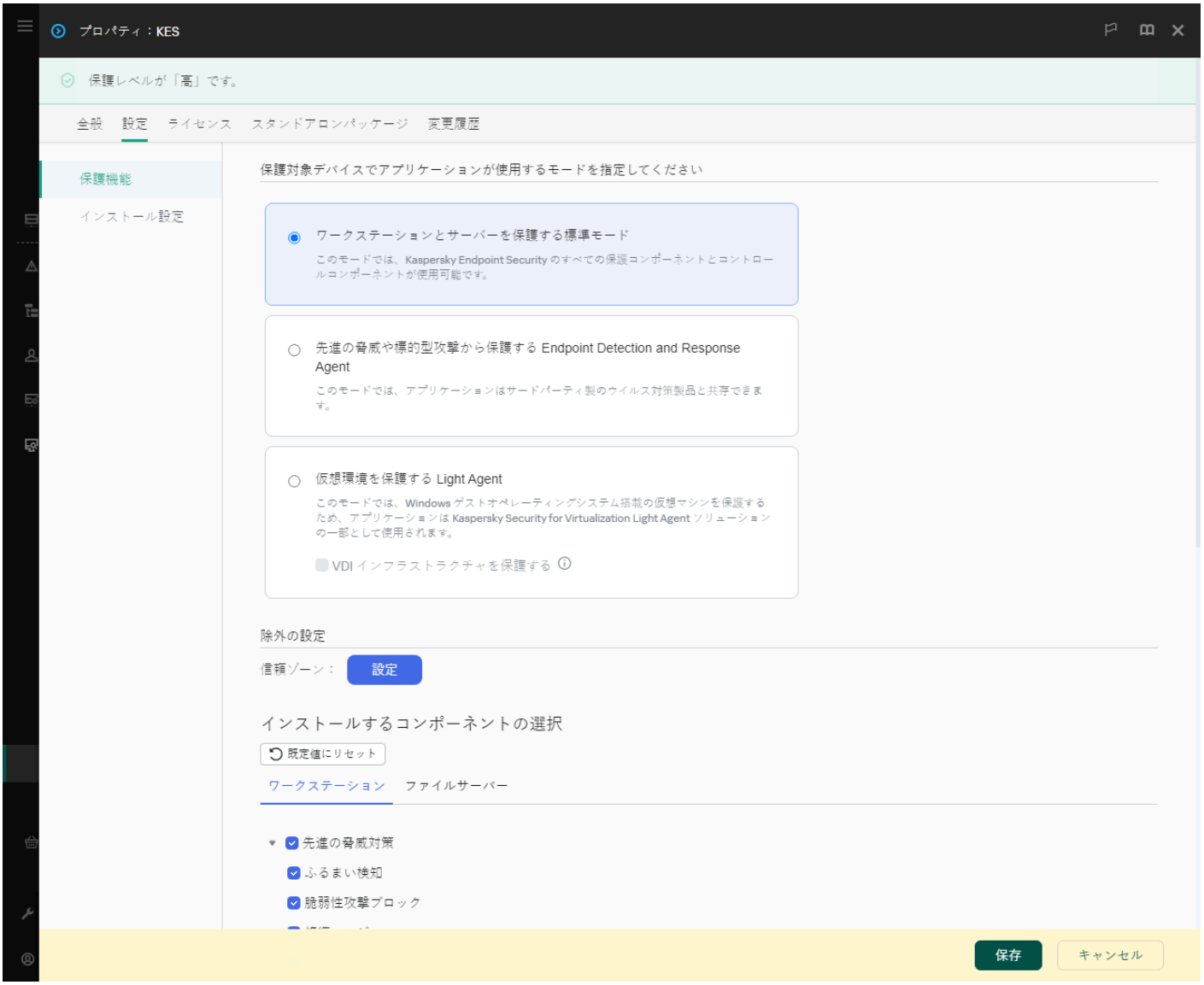


カスペルスキーのサーバーのインストールパッケージのリスト

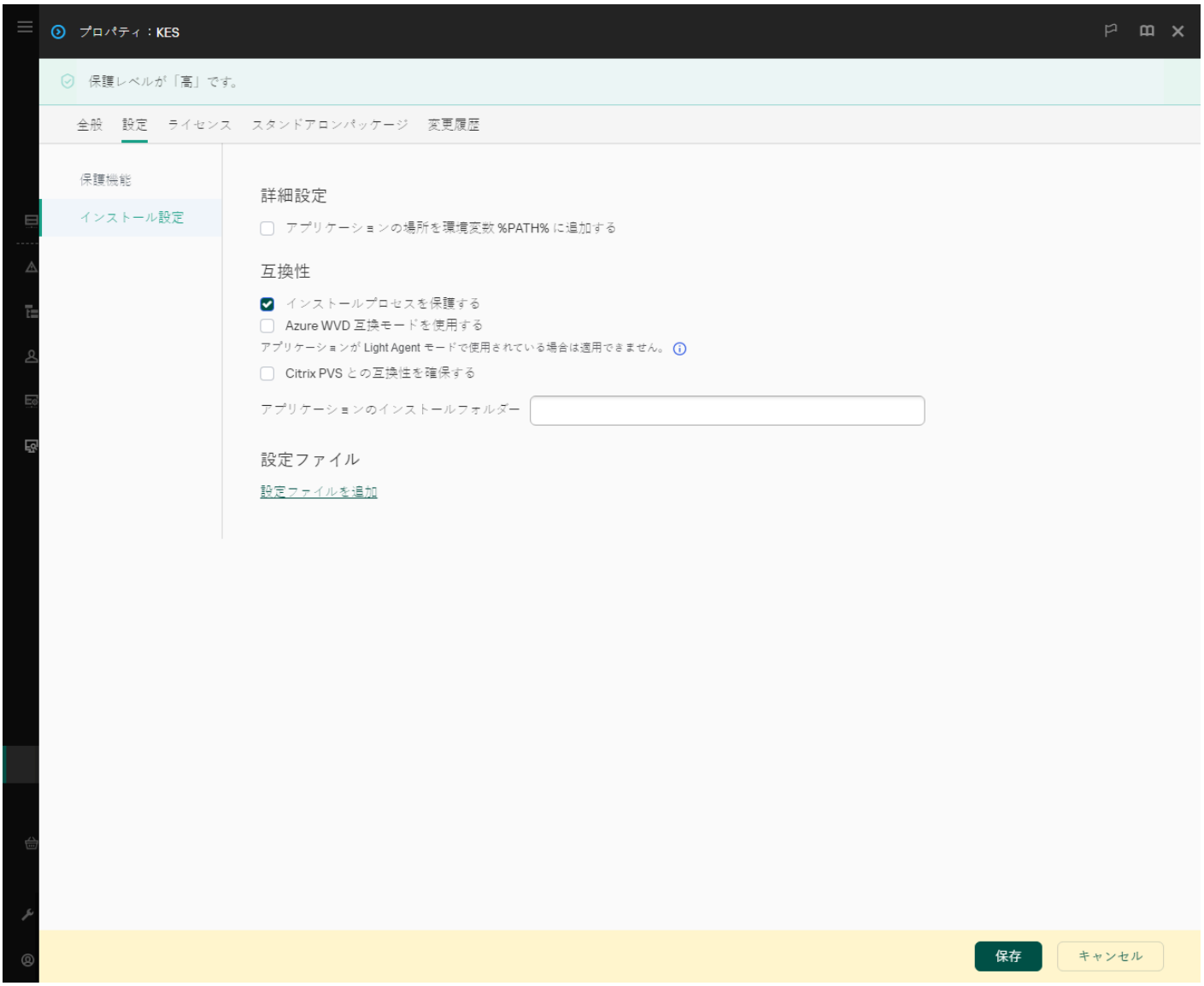
インストールパッケージが作成され、Kaspersky Security Center に追加されます。インストールパッケージを使用して、組織ネットワーク内のコンピューターへの Kaspersky Endpoint Security のインストールまたはインストール済みの製品のバージョンのアップデートを実行できます。

インストールパッケージの設定では、オペレーティングシステムの種別ごとに製品コンポーネントを選択できます。つまり、インストールパッケージには、ワークステーション用とサーバー用の 2 セットのコンポーネントが含まれています。インストールパッケージを導入する前に、インストーラーはオペレーティングシステムの種別を検出し、そのオペレーティングシステムの種別に対して選択した製品コンポーネントのみをインストールします。この方法では、ワークステーションとサーバーに同じインストールパッケージを使用できます。

インストールパッケージには、管理サーバーリポジトリの定義データベースが含まれます。インストールパッケージのデータベースをアップデートすることで、Kaspersky Endpoint Security をインストールした後にデータベースをアップデートすることにより生じるトラフィック量を削減できます。



インストールパッケージに含まれるコンポーネント



インストールパッケージのインストール設定

インストールパッケージの設定

セクション	説明
保護機能	**標準モード**：既定の設定。この設定では、Detection and Response ソリューションのサポートを提供するコンポーネントを含め、アプリケーションのすべてのコンポーネントを使用できます。この設定は、さまざまな脅威、ネットワーク攻撃、詐欺からコンピューターを包括的に保護するために使用されます。 **Endpoint Detection and Response Agent**：この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。 **仮想環境を保護する Light Agent**：この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。
除外リスト	Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。 Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。 信頼ゾーンは、後でポリシープロパティの［信頼するオブジェクトとアプリケーション］で設定することもできます。

セクション	説明
インストールするコンポーネントの選択	このセクションでは、ユーザーに提供する製品コンポーネントを選択できます。［*コンポーネントの変更*］タスクを使用して、後からコンポーネントのセットを変更できます。 ワークステーション用とサーバー用に別のコンポーネントのセットを作成できます。インストールパッケージを導入する前に、インストーラーはオペレーティングシステムの種別を検出し、そのオペレーティングシステムの種別に対して選択した製品コンポーネントのみをインストールします。この方法では、ワークステーションとサーバーに同じインストールパッケージを使用できます。 使用可能なコンポーネントセットは、製品の設定により異なります： **標準モード** 既定の設定では、有害 USB 攻撃ブロック、Detection and Response、データ暗号化はインストールされません。これらのコンポーネントは、インストールパッケージの設定で追加できます。 **Endpoint Detection and Response Agent** この設定では、Kaspersky Detection and Response ソリューションの組み込みエージェントのみ使用可能です。 **仮想環境を保護する Light Agent** この設定では、データ暗号化コンポーネントとアダプティブアノマリーコントロールを除くほぼすべての［**標準モード**］設定で使用可能な製品コンポーネントを使用できます。
識別 ID	このセクションでは、本製品をアクティベートできます。本製品をアクティベートするには、ライセンスを選択する必要があります。その前に、管理サーバーにライセンスを追加しておく必要があります。Kaspersky Security Center 管理サーバーへのライセンスの追加について詳しくは、Kaspersky Security Center ヘルプを参照してください。
競合アプリケーション	互換性のない製品のリストを注意深く読んで、これらの製品の削除を許可してください。コンピューターに競合するアプリケーションがインストールされていると、Kaspersky Endpoint Security のインストールはエラーで終了します。
インストール設定	**avp.com ファイルのパスをシステム変数 %PATH% に追加する**：コマンドラインインターフェイスの使用で便利なように、%PATH% 変数にインストール先のパスを追加できます。 **インストールプロセスを保護する**：インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Endpoint Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります（たとえば、Windows Remote Desktop でリモートインストールを実行するとき）。 **Citrix PVS との互換性を確保する**：Kaspersky Endpoint Security を仮想マシンにインストールするために、Citrix Provisioning Services のサポートを有効にすることができます。 **Azure WVD 互換モードを使用する**：この機能により、Kaspersky Anti Targeted Attack Platform コンソールに Azure 仮想マシンの状態が正しく表示されるようになります。コンピューターのパフォーマンスを監視するため、Kaspersky Endpoint Security はテレメトリを KATA サーバーに送信します。テレメトリにはコンピューターの ID（Sensor ID）が含まれます。Azure WVD 互換モードはこれらの仮想マシンに永続的に一意な Sensor ID を割り当てることができます。互換モードがオフになっている場合、Azure 仮想マシンの仕組みにより、コンピューターが再起動した後に Sensor ID が変更されることがあります。このため、コンソール上で仮想マシンが重複して表示されることがあります。 **アプリケーションのインストールフォルダー**：クライアントコンピューター上での Kaspersky Endpoint Security のインストール先のパスを変更できます。既定では、アプリケーションは `%ProgramFiles(x86)%\Kaspersky Lab\KES.12.12` フォルダーにインストールされます。 **設定ファイル**：定義済みの設定で本製品をインストール。これには、Kaspersky Endpoint Security の設定を定義した設定ファイルをアップロードする必要があります。製品のローカルインターフェイスで、設定ファイルを作成できます。

インストールパッケージ内の定義データベースのアップデート

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

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

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

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

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

   これにより、Kaspersky Security Center にダウンロードされたインストールパッケージのリストが開きます。
3. インストールパッケージのプロパティを開きます。
4. ［**全般**］セクションで、［**定義データベースのアップデート**］をクリックします。

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

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

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

   Web コンソールにダウンロードされたインストールパッケージのリストが表示されます。
2. 定義データベースをアップデートする Kaspersky Endpoint Security のインストールパッケージの名前をクリックします。

   インストールパッケージのプロパティウィンドウが表示されます。
3. ［**一般情報**］タブで［**定義データベースのアップデート**］をクリックします。

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

リモートインストールタスクの作成

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

管理コンソール（MMC）でリモートインストールタスクを作成する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
3. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

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

ステップ 2：インストールパッケージの選択

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

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

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

ステップ 3：追加

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

ステップ 4：設定

次の追加のアプリケーション設定を設定します：

- **インストールパッケージの強制ダウンロード**：製品インストールの方法を選択します：
  - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。
  - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、Kaspersky Security Center ヘルプを参照してください。
  - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。
- **別の管理サーバーの管理対象デバイスに対する処理**：Kaspersky Endpoint Security のインストール方法を選択します。ネットワーク内に複数の管理サーバーがインストールされている場合、同じクライアントコンピューターが複数の管理サーバーで可視になる場合があります。これにより、たとえば同じクライアントコンピューターへの同じ製品のリモートインストールが複数の管理サーバーから重複して実行されるなどの競合が発生する場合があります。
- **アプリケーションが既にインストールされている場合は再インストールしない**：古いバージョンの製品をインストールする場合などには、このオプションをオフにします。

ステップ 5：オペレーティングシステムの再起動設定の選択

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

ステップ 6：タスクを割り当てるデバイスの選択

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

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

ステップ 7：タスクを実行するアカウントの選択

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

ステップ 8：タスク開始スケジュールの設定

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

ステップ 9：タスク名の定義

タスクの名前を入力します。たとえば、*Kaspersky Endpoint Security for Windows 12.12 のインストール*など。

ステップ 10：タスク作成の終了

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

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

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

ステップ 2：インストール先のコンピューターの選択

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

ステップ 3：インストールパッケージの設定

インストールパッケージを設定します：

1. Kaspersky Endpoint Security for Windows (12.12) インストールパッケージを選択します。
2. ネットワークエージェントのインストールパッケージを選択します。
   選択したバージョンのネットワークエージェントが Kaspersky Endpoint Security と合わせてインストールされます。*ネットワークエージェント*は、管理サーバーとクライアントコンピューターのやり取りをサポートします。ネットワークエージェントが既にコンピューター上にインストールされている場合、再インストールは行われません。

3. ［**インストールパッケージの強制ダウンロード**］ブロックで、製品のインストール方法を選択します。

   - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントを使用して Kaspersky Endpoint Security がインストールされます。

   - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：インストールパッケージが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

   - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ファイルが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。

4. ［**同時ダウンロード数の上限**］で、管理サーバーに送信されるインストールパッケージのダウンロード要求数の上限を設定します。要求数の上限を設定することで、ネットワークに過剰な負荷を与えずにすみます。

5. ［**インストール試行回数の上限**］フィールドで、インストールの試行回数に制限を設定します。Kaspersky Endpoint Security のインストールがエラーで終了した場合、タスクは自動的にインストールをもう一度開始します。

6. 必要に応じて、［**アプリケーションが既にインストールされている場合は再インストールしない**］をオフにします。これにより、以前のバージョンの製品をインストールすることなどが可能になります。

7. 必要に応じて、［**ダウンロード前に OS の種別を確認する**］をオフにします。このオプションがオンの場合、コンピューターのオペレーティングシステムが製品のインストール要件を満たさないのに製品の配布パッケージを誤ってダウンロードしてしまうことを防ぐことができます。コンピューターのオペレーティングシステムが製品のインストール要件を確実に満たしている場合は、この検証をスキップできます。

8. 必要に応じて、［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］をオンにします。Kaspersky Endpoint Security はネットワークエージェントを使用して、あるいは Active Directory を使用して手動でインストールされます。ネットワークエージェントをインストールするには、リモートインストールタスクはドメイン管理者権限で実行する必要があります。

9. 必要に応じて、［**実行中のアプリケーションを終了するよう通知する**］をオンにします。Kaspersky Endpoint Security のインストールはコンピューターのリソースを消費します。このオプションをオンにすると、ユーザーの利便性のために、製品のインストールウィザードで、インストールを開始する前に実行中のアプリケーションを終了するようにメッセージが表示されます。これにより、他のアプリケーションの動作でのエラーやコンピューターでのエラーの発生を防ぐことができます。

10. ［**別の管理サーバーの管理対象デバイスに対する処理**］ブロックで、Kaspersky Endpoint Security のインストール方法を選択します。ネットワーク内に複数の管理サーバーがインストールされている場合、同じクライアントコンピューターが複数の管理サーバーで可視になる場合があります。これにより、たとえば同じクライアントコンピューターへの同じ製品のリモートインストールが複数の管理サーバーから重複して実行されるなどの競合が発生する場合があります。

ステップ 4：タスクを実行するアカウントの選択

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

ステップ 5：タスク作成の完了

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

ウィザードを使用したローカルへの製品のインストール

インストールウィザードのインターフェイスは、製品のインストール手順に対応した一連のウィンドウで構成されています。インストールウィザードを実行しているユーザーアカウントが管理者グループに属していることを確認してください。

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

1. ユーザーのコンピューターに配信キットフォルダーをコピーします。
2. Setup_kes.exe を実行します。

   インストールウィザードが起動します。

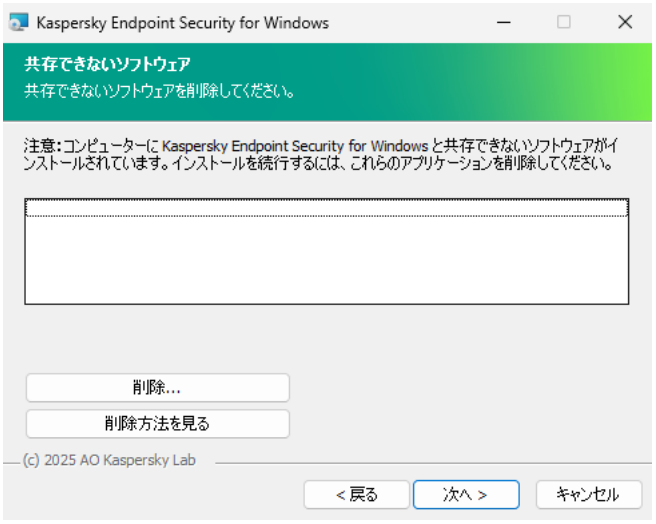
インストールの準備

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

- Kaspersky Endpoint Security と互換性の問題が発生する可能性のあるソフトウェアがあるかどうか（ソフトウェアのリストは、配信キットに含まれる incompatible.txt に記載されています）
- システム要件が満たされているかどうか

- Microsoft .NET Framework が存在するかどうか
- ユーザーがソフトウェア製品をインストールできる権限を持っているかどうか

上記のいずれかの要件が満たされていない場合は、該当する通知が画面に表示されます。たとえば、共存できないソフトウェアに関する通知（下図を参照）などが表示されます。



共存できないソフトウェアを削除する

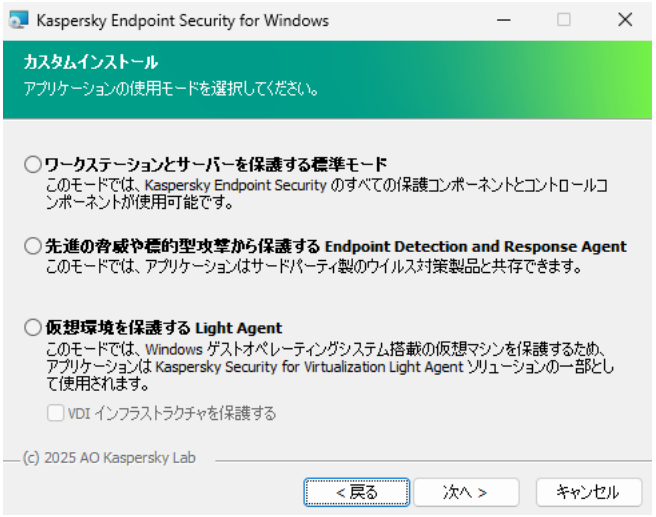
コンピューターが上記の要件を満たしている場合、インストールウィザードは、インストールする製品と同時に実行されたときに競合する可能性があるカスペルスキー製品がないか検索します。このようなアプリケーションが見つかった場合は、手動で削除するよう要求されます。

検出されたアプリケーションに以前のバージョンの Kaspersky Endpoint Security が含まれている場合、移行可能なすべてのデータ（アクティベーションのデータ、製品設定など）は保持され、Kaspersky Endpoint Security 12.12 for Windows のインストール時に使用されます。本製品の以前のバージョンは自動的に削除されます。該当する製品バージョンは次の通りです：

- Kaspersky Endpoint Security 11.10.0 for Windows（ビルド 11.10.0.399）
- Kaspersky Endpoint Security 11.11.0 for Windows（ビルド 11.11.0.452）
- Kaspersky Endpoint Security 12.0 for Windows（ビルド 12.0.0.465）
- Kaspersky Endpoint Security 12.1 for Windows（ビルド 12.1.0.506）
- Kaspersky Endpoint Security 12.2 for Windows（ビルド 12.2.0.462）
- Kaspersky Endpoint Security 12.3 for Windows（ビルド 12.3.0.493）
- Kaspersky Endpoint Security 12.4 for Windows（ビルド 12.4.0.467）
- Kaspersky Endpoint Security 12.5 for Windows（ビルド 12.5.0.539）
- Kaspersky Endpoint Security 12.6 for Windows（ビルド 12.6.0.438）
- Kaspersky Endpoint Security 12.7 for Windows（ビルド 12.7.0.533）
- Kaspersky Endpoint Security 12.8 for Windows（ビルド 12.8.0.505）
- Kaspersky Endpoint Security 12.9 for Windows（ビルド 12.9.0.384）

- Kaspersky Endpoint Security 12.10 for Windows（ビルド 12.10.0.466）
- Kaspersky Endpoint Security 12.11 for Windows（ビルド 12.11.0.637）

Kaspersky Endpoint Security の設定



アプリケーションの設定の選択

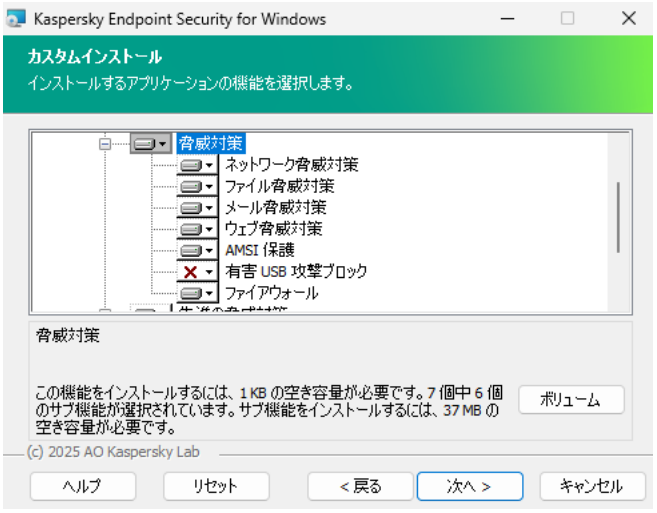
標準モード既定の設定。この設定では、Detection and Response ソリューションのサポートを提供するコンポーネントを含め、アプリケーションのすべてのコンポーネントを使用できます。この設定は、さまざまな脅威、ネットワーク攻撃、詐欺からコンピューターを包括的に保護するために使用されます。

Endpoint Detection and Response Agentこの設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。

仮想環境を保護する Light Agentこの設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。

Kaspersky Endpoint Security の各コンポーネント

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



インストールする製品コンポーネントの選択

既定では、以下を除くすべてのコンポーネントが選択されています：

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

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

Detection and Response コンポーネントをインストールする必要がある場合、Kaspersky Endpoint Security は次の構成をサポートします：

- Endpoint Detection and Response Optimum のみ
- Endpoint Detection and Response Expert のみ
- Endpoint Detection and Response (KATA) のみ
- Network Detection and Response (KATA) のみ
- Sandbox のみ
- Endpoint Detection and Response Optimum と Sandbox
- Endpoint Detection and Response Expert と Sandbox
- Endpoint Detection and Response (KATA) と Sandbox

- Network Detection and Response (KATA) と Endpoint Detection and Response (KATA)
- Network Detection and Response (KATA) と Managed Detection and Response

Kaspersky Endpoint Security は、本製品のインストール前に選択されたコンポーネントを検証します。選択した Detection and Response コンポーネントの構成がサポートされない場合は、Kaspersky Endpoint Security はインストールされません。

本製品をインストールするフォルダーの選択

クライアントコンピューター上での Kaspersky Endpoint Security のインストール先のパスを変更できます。既定では、アプリケーションは `%ProgramFiles(x86)%\Kaspersky Lab\KES.12.12` フォルダーにインストールされます。

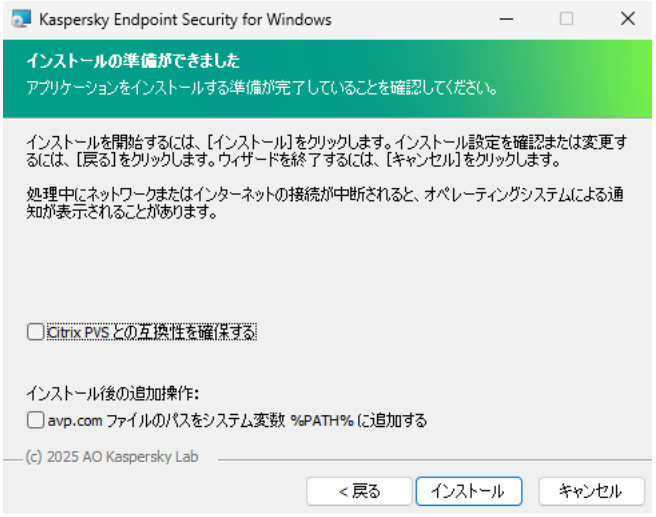
信頼ゾーンの設定

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。

信頼ゾーンは、後でポリシープロパティの［信頼するオブジェクトとアプリケーション］で設定することもできます。

詳細設定



詳細な製品のインストール設定

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

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

avp.com ファイルのパスをシステム変数 %PATH% に追加するコマンドラインインターフェイスの使用で便利なように、%PATH% 変数にインストール先のパスを追加できます。

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

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

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

1. Configuration Manager コンソールを開きます。
2. コンソールの右側の［**アプリケーション管理**］ブロックで、［**パッケージ**］を選択します。
3. コンソール上部のコントロールパネルで［**パッケージの作成**］をクリックします。
   *パッケージとプログラムの作成ウィザード*が開始します。
4. パッケージとプログラムの作成ウィザードで、次の操作を実行します：
   a. ［**パッケージ**］セクションで次の操作を実行します：
      - ［**名前**］にインストールパッケージの名前を入力します。
      - ［**ソースフォルダー**］で、Kaspersky Endpoint Security の配布パッケージを含むフォルダーのパスを指定します。
   b. ［**アプリケーション種別**］セクションで［**標準プログラム**］を選択します。
   c. ［**標準プログラム**］セクションで次の操作を実行します：
      - ［**名前**］に、インストールパッケージの一意の名前（たとえばアプリケーション名とバージョン）を入力します。
      - ［**コマンドライン**］で、コマンドラインから Kaspersky Endpoint Security をインストールする際のオプションを指定します。
      - ［**参照**］をクリックして、製品の実行ファイルのパスを指定します。
      - ［**実行方法**］リストで［**管理者の権限で実行**］が選択されていることを確認してください。

d. ［**要件**］セクションで次の操作を実行します：

- Kaspersky Endpoint Security をインストールする前に別のアプリケーションを起動するには、［**別のプログラムを最初に実行**］をオンにします。

  ［**アプリケーション**］からアプリケーションを選択するか、［**参照**］をクリックしてアプリケーションの実行ファイルのパスを指定します。

- 製品を特定のオペレーティングシステムにのみインストールするには、［**プラットフォームの要件**］ブロックで［**このプログラムは、指定したプラットフォームでのみ実行できます**］をオンにします。

  下のリストで、Kaspersky Endpoint Security をインストールするオペレーティングシステムの横にあるチェックボックスをオンにします。

この手順は省略可能です。

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

作成されたインストールパッケージが、［**パッケージ**］セクションの使用可能なインストールパッケージのリストに表示されます。

5. インストールパッケージのコンテキストメニューから［**展開**］を選択します。

*展開ウィザード*が開始します。

6. 展開ウィザードで次の操作を実行します：

a. ［**全般**］セクションで次の操作を実行します：

- ［**ソフトウェア**］にインストールパッケージの一意の名前を入力するか、［**参照**］をクリックしてリストからインストールパッケージを選択します。

- ［**コレクション**］に製品をインストールするコンピューターのコレクションの名前を入力するか、［**参照**］をクリックしてコレクションを選択します。

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

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

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

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

ファイル setup.ini のインストール設定の説明

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

本製品をサイレントモードでインストールする場合にのみ、setup.ini ファイルを使用します。

ファイル setup.ini の設定ファイル install.cfg にパスを追加することはできません。また、Kaspersky Endpoint Security の配信キットと同じフォルダーにこのファイルを配置するだけでは、設定ファイル install.cfg はスキップされます。install.cfg ファイルの設定を適用するには、アプリケーションのインストールコマンドで次のようにパスを指定する必要があります：`CONFIGPATH=<path to the configuration file>`

こちらのリンクから setup.ini ファイルをダウンロードできます

setup.ini ファイルには次のセクションが含まれています：

- `[Setup]`：製品のインストールの全般設定。
- `[Components]`：標準モードでインストールするコンポーネントの選択。コンポーネントが1つも指定されていない場合は、オペレーティングシステムで利用できるコンポーネントがすべてインストールされます。ファイル脅威対策は必須のコンポーネントです。このセクションで表示される設定に関係なくコンピューターにインストールされます。
- `[Tasks]`：Kaspersky Endpoint Security タスクのリストに含まれるタスクを選択します。タスクが1つも指定されていない場合は、すべてのタスクが Kaspersky Endpoint Security のタスクリストに含まれます。

`1` を設定する代わりに `yes`、`on`、`enable`、`enabled`、`true` も指定できます。`0` を設定する代わりに `no`、`off`、`disable`、`disabled`、`false` も指定できます。

setup.ini ファイルの設定

セクション	パラメータ	説明
`[Setup]`	`InstallDir`	アプリケーションのインストールフォルダーのパス。
	`ActivationCode`	Kaspersky Endpoint Security のアクティベーションコード
	`EULA=1`	使用許諾契約書の条項に同意する。使用許諾契約書のテキストは、Kaspersky Endpoint Security の配信キットに含まれています。 製品をインストールまたはアップグレードするには、使用許諾契約書に同意する必要があります。

セクション	パラメータ	説明
	`PrivacyPolicy=1`	プライバシーポリシーに同意する。プライバシーポリシーのテキストは、Kaspersky Endpoint Security の配信キットに含まれています。 本製品のインストールおよびバージョンのアップグレードには、プライバシーポリシーに同意する必要があります。
	`KSN`	Kaspersky Security Network (KSN) への参加に同意するかどうか。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security を最初に起動したときに、KSN への参加に同意するかどうかの確認画面が表示されます。次の値を設定できます： • `1`：KSN への参加に同意する • `0`：KSN への参加に同意しない（既定値） Kaspersky Endpoint Security の配布パッケージは、Kaspersky Security Network とともに使用するように最適化されています。Kaspersky Security Network に参加しない場合、インストール後すぐに Kaspersky Endpoint Security をアップデートしてください。
	`Login`	Kaspersky Endpoint Security の機能と設定にアクセスできるユーザー名の指定（パスワードによる保護機能）。ユーザー名は、「`Password`」および「`PasswordArea`」の設定と合わせて指定します。既定では、ユーザー名 KLAdmin が使用されます。
	`Password`	Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワード（パスワードは「`Login`」および「`PasswordArea`」パラメータと合わせて指定します）。 「`Login`」パラメータでユーザー名を指定せずにパスワードを指定した場合、KLAdmin が既定のユーザー名として使用されます。
	`PasswordArea`	Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワードが必要になる操作の範囲。この範囲内に含まれている操作をユーザーが実行しようとした場合、Kaspersky Endpoint Security でアカウントの認証情報の入力を要求されます（「`Login`」と「`Password`」パラメータ）。複数の値を指定するには、区切り文字として`;`を使用してください。 次の値を設定できます： • `SET`：製品設定の変更 • `EXIT`：製品の終了 • `DISPROTECT`：保護機能の停止とスキャンタスクの停止 • `DISPOLICY`：Kaspersky Security Center ポリシーの無効化 • `UNINST`：コンピューターからの製品の削除 • `DISCTRL`：管理コンポーネントの停止 • `REMOVELIC`：ライセンスの削除 • `REPORTS`：レポートの表示 • `EXPORT`：本製品の設定のエクスポート 例：「`PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`」。
	`SelfProtection`	製品のインストール保護メカニズムを有効にするかどうか。次の値を設定できます： • `1`：製品のインストール保護メカニズムを有効にする（既定値） • `0`：製品のインストール保護メカニズムを無効にする インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Endpoint Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります（たとえば、Windows Remote Desktop でリモートインストールを実行するとき）。
	`PROTECTOSSERVICES`	オペレーティングシステムのサービスの保護機能。オペレーティングシステムのサービスの保護は、サードパーティ製アプリケーションによってオペレーティングシステムのサービスの処理が妨げられるのを防止します。こうしたサービスには、アプリケーションの自動起動サービスなどがあります。 • `1`：オペレーティングシステムのサービスの保護は有効です（既定値）。 • `0`：オペレーティングシステムのサービスの保護は無効です。

セクション	パラメータ	説明
	EnableAzureSupport	Azure WVD 互換モードを有効または無効にします。次の値を設定できます： • 1：Azure WVD 互換モードを有効にする • 0：Azure WVD 互換モードを無効にする（既定値） この機能により、Kaspersky Anti Targeted Attack Platform コンソールに Azure 仮想マシンの状態が正しく表示されるようになります。コンピューターのパフォーマンスを監視するため、Kaspersky Endpoint Security はテレメトリを KATA サーバーに送信します。テレメトリにはコンピューターの ID（Sensor ID）が含まれます。Azure WVD 互換モードはこれらの仮想マシンに永続的に一意な Sensor ID を割り当てることができます。互換モードがオフになっている場合、Azure 仮想マシンの仕組みにより、コンピューターが再起動した後に Sensor ID が変更されることがあります。このため、コンソール上で仮想マシンが重複して表示されることがあります。
	Reboot=1	製品のインストール後またはアップグレード後にコンピューターの再起動が必要な場合に自動再起動を行うかどうか。このパラメータの値が指定されていない場合、コンピューターの自動再起動はブロックされます。 Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。
	AddEnvironment	%PATH% システム変数に、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスを追加するかどうか。次の値を設定できます： • 1：%PATH% システム変数を、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスで補完する • 0：%PATH% システム変数を、Kaspersky Endpoint Security セットアップフォルダーにある実行ファイルのパスで補完しない
	AMPPL	AM-PPL 技術（Antimalware Protected Process Light）を使用した Kaspersky Endpoint Security プロセスの保護を有効にするかどうか。AM-PPL 技術について詳しくは、Microsoft の Web サイトの情報を参照してください。 AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。 次の値を設定できます： • 1：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を有効にする • 0：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を無効にする
	UPGRADEMODE	アプリケーションのアップグレードモード： • Seamless はコンピューターを再起動してアプリケーションをアップグレードすることを意味します（既定値）。 • Force はコンピューターを再起動せずにアプリケーションをアップグレードすることを意味します。 バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。これより前のバージョンのアプリケーションをアップグレードする場合は、コンピューターを再起動する必要があります。バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることもできるようになりました。 Kaspersky Endpoint Security のインストールでは再起動は必要ありません。従って、アプリケーションのアップグレードモードはアプリケーション設定で指定されます。アプリケーション設定またはポリシーでこのパラメータを変更できます。 既にインストールされている製品をアップグレードする場合、setup.ini ファイルで指定されたパラメータの優先度は、製品設定またはコマンドラインで指定されたパラメータよりも高くなります。たとえば、Force アップグレードモードが setup.ini ファイルで指定されていて、Seamless モードが製品設定で指定されている場合、再起動せずにアップグレードをインストールします（Force）。UPGRADEMODE パラメータが指定されていない setup.ini ファイルを使用している場合、インストーラーは既定値（Seamless）を使用して、コンピューターを再起動してアップグレードをインストールします。
	SetupReg	setup.reg ファイルに含まれるレジストリキーをレジストリに書き込む。SetupReg: setup.reg パラメータ値。
	EnableTraces	本製品のトレース記録を有効にするかどうか。Kaspersky Endpoint Security は、起動後にトレースファイルを「%ProgramData%\Kaspersky Lab\KES.12.12\Traces」フォルダーに保存します。次の値を設定できます： • 1：トレース記録をオンにする • 0：トレース記録をオフにする（既定値）

セクション	パラメータ	説明
	TracesLevel	トレース記録の詳細度。次の値を設定できます： • 100（緊急）：深刻なエラーに関するメッセージのみ。 • 200（高）：深刻なエラーを含めたすべてのエラーに関するメッセージ。 • 300（診断）：すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。 • 400（重要）：すべてのエラーに関するメッセージとすべての警告および詳細情報。 • 500（通常）：すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ（既定値）。 • 600（低）：すべてのメッセージ。
	RESTAPI	REST API を使用した製品の管理。REST API を使用して製品を管理するには、ユーザー名（RESTAPI_User パラメータ）を指定する必要があります。 次の値を設定できます： • 1 – REST API による管理を許可する • 0 – REST API による管理をブロックする（既定値） REST API を使用して製品を管理するには、管理システムを使用した管理を許可する必要があります。許可するには、AdminKitConnector=1 パラメータを設定します。REST API を使用して製品を管理する場合、カスペルスキーの管理システムを使用して製品を管理することはできません。
	RESTAPI_User	REST API による製品の管理に使用する Windows ドメインアカウントのユーザー名。REST API による製品の管理はこのユーザーのみ実行できます。ユーザー名は、<DOMAIN>\<UserName> の形式で入力します（例：RESTAPI_User=COMPANY\Administrator）。REST API を利用するユーザーは1人しか選択できません。 REST API を使用して製品を管理するには、ユーザー名の追加は必須です。
	RESTAPI_Port	REST API による製品の管理に使用するポート。既定ではポート 6782 が使用されます。ポートが使用されていないことを確認してください。
	RESTAPI_Certificate	リクエストを識別するための証明書（例：RESTAPI_Certificate=C:\cert.pem）。REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。
	StandaloneMode	Endpoint Detection and Response Agent (EDR Agent) モードでアプリケーションをインストールします。*Endpoint Detection and Response Agent* は、Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform ソリューションをサポートするために、組織の IT インフラストラクチャ内の個々のワークステーションやサーバーにインストールされるアプリケーションです。EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。これにより、カスペルスキーの Detection and Response と同時にサードパーティのインフラストラクチャセキュリティツールを使用できるようになります。 EDR Agent をインストールするには、[Components] セクションで、StandaloneKATA、StandaloneNDR、StandaloneMDR のいずれかのコンポーネントを選択します。EDR Agent は他の製品コンポーネントをサポートしません。 次の値を設定できます： • 1：EDR Agent モードでアプリケーションをインストールする • 0：アプリケーションを標準モード（既定）でインストールする
	KSVLAMode	Light Agent モードでアプリケーションをインストールします。この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。 次の値を設定できます： • 1：Light Agent モードでアプリケーションをインストールする • 0：アプリケーションを標準モード（既定）でインストールする
	InstallOnVDI	Light Agent モードでアプリケーションをインストールする場合（KSVLAMode=1）に VDI 保護モードを有効にします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。 次の値を設定できます： • 1：VDI 保護モードを有効にする • 0：VDI 保護モードを無効にする（既定）

セクション	パラメータ	説明
	KESExclusions	本製品をサーバーにインストールする場合に、設定済みの信頼するオブジェクトとアプリケーションを追加します。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。例えば、SQL サーバーの設定済みの信頼するオブジェクトには、データベースファイル MDF や LDF が含まれます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。 次の値を設定できます： • 1：設定済みの信頼するオブジェクトとアプリケーションを有効にする • 0：設定済みの信頼するオブジェクトとアプリケーションを無効にする（既定）
	LAExclusions	本製品を仮想マシンにインストールする場合（Light Agent モード）に、設定済みの信頼するオブジェクトとアプリケーションを追加します。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。 次の値を設定できます： • 1：設定済みの信頼するオブジェクトとアプリケーションを有効にする • 0：設定済みの信頼するオブジェクトとアプリケーションを無効にする（既定）
	EnableUniqueSensorID	本製品のインストール中またはアップデート中に、一意のコンピューター識別子（Sensor ID）を作成します。Sensor ID は、サーバーにテレメトリを送信するコンピューターを識別するために、Kaspersky Anti Targeted Attack Platform ソリューションで使用されます。本製品は、Sensor ID の作成時に、マザーボードのシリアル番号などのコンピューターの設定を考慮するアルゴリズムを使用します。本製品を仮想環境で使用する場合など、いくつかのケースでは、Sensor ID が重複する場合があります。その結果、Kaspersky Anti Targeted Attack Platform がテレメトリの送信元コンピューターを識別できなくなります。一意の Sensor ID を作成するには、パラメータ EnableUniqueSensorID=1 を設定する必要があります。これにより、本製品が、コンピューターに関する他のデータを考慮する別のアルゴリズムを使用して Sensor ID を作成するようになります。これにより、一意の Sensor ID が確保されます。 既定では、パラメータは設定されていません。本製品は次の場合に Sensor ID を継承します： • 製品バージョンのアップデート • ［KES + KEA］設定からの［KES + 組み込みエージェント］設定への移行 インストーラーは、アプリケーション修復の一環として、Sensor ID を継承しようとします。Sensor ID を復元できない場合は、新しい Sensor ID が作成されます。
[Components]	ALL	すべてのコンポーネントのインストール。このパラメータの値を 1 に設定すると、個々のコンポーネントのインストール設定にかかわらず、すべてのコンポーネントがインストールされます。 Detection and Response ソリューションをサポートする方法により、Endpoint Detection and Response Optimum および Kaspersky Sandbox コンポーネントがコンピューターにインストールされます。Endpoint Detection and Response コンポーネントはこの構成と互換性がありません。
	MailThreatProtection	メール脅威対策
	WebThreatProtection	ウェブ脅威対策
	AMSI	AMSI 保護
	HostIntrusionPrevention	ホスト侵入防止
	BehaviorDetection	ふるまい検知
	ExploitPrevention	脆弱性攻撃ブロック
	RemediationEngine	修復エンジン
	Firewall	ファイアウォール：
	NetworkThreatProtection	ネットワーク脅威対策
	WebControl	ウェブコントロール：
	DeviceControl	デバイスコントロール
	ApplicationControl	アプリケーションコントロール
	AdaptiveAnomaliesControl	アダプティブアノマリーコントロール

セクション	パラメータ	説明
	`CloudDiscovery`	Cloud Discovery
	`LogInspector`	Windows イベントログ監視
	`AntiCryptor`	アンチクリプター
	`SystemIntegrityMonitor`	システム変更監視
	`FileEncryption`	ファイルレベルの暗号化ライブラリ
	`DiskEncryption`	ディスク全体の暗号化ライブラリ
	`BadUSBAttackPrevention`	有害 USB 攻撃ブロック
	`EDR`	Endpoint Detection and Response Optimum (EDR Optimum) このコンポーネントは EDR Expert（`EDRCloud`）および EDR (KATA)（`EDRKATA`） コンポーネントと互換性がありません。
	`EDRCloud`	Kaspersky Endpoint Detection and Response Expert (EDR Optimum) このコンポーネントは EDR Optimum（`EDR`）および EDR (KATA)（`EDRKATA`）コンポーネントとは互換性がありません。
	`AntiAPT`	Endpoint Detection and Response (KATA) このコンポーネントは EDR Expert (`EDRCloud`) および EDR Optimum (`EDR`) コンポーネントとは互換性がありません。
	`SB`	Kaspersky Sandbox または KATA Sandbox。 *Kaspersky Sandbox* は、カスペルスキーによるスタンドアロンの Detection and Response ソリューションです。*KATA Sandbox* は、Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントの 1 つです。
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) このコンポーネントは EDR Expert (`EDRCloud`) および EDR Optimum (`EDR`) コンポーネントとは互換性がありません。
	`AdminKitConnector`	管理システムを使用した製品管理。管理システムには、Kaspersky Security Center などが含まれます。カスペルスキーの管理システムに加えて、サードパーティ製ソリューションを使用することもできます。Kaspersky Endpoint Security はそのための API を提供します。 次の値を設定できます： • `1` – 管理システムを利用した製品管理を許可する（既定値） • `0` – ローカルインターフェイスを利用した製品管理のみを許可する
	`KUMAIntegration`	KUMA との連携
	`StandaloneKATA`	Kaspersky Anti Targeted Attack Platform (EDR) との連携のために、Endpoint Detection and Response Agent (EDR Agent) モードで本製品をインストールします。
	`StandaloneMDR`	Kaspersky Managed Detection and Response との連携のために、Endpoint Detection and Response Agent (EDR Agent) モードで本製品をインストールします。
	`StandaloneNDR`	Kaspersky Anti Targeted Attack Platform (NDR) との連携のために、Endpoint Detection and Response Agent (EDR Agent) モードで本製品をインストールします。

セクション	パラメータ	説明
[Tasks]	ScanMyComputer	完全スキャンタスク。次の値を設定できます： • 1：タスクを Kaspersky Endpoint Security のタスクリストに含める • 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない
	ScanCritical	簡易スキャンタスク。次の値を設定できます： • 1：タスクを Kaspersky Endpoint Security のタスクリストに含める • 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない
	Updater	アップデートタスク。次の値を設定できます： • 1：タスクを Kaspersky Endpoint Security のタスクリストに含める • 0：タスクを Kaspersky Endpoint Security のタスクリストに含めない

コンポーネントの変更

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

- クライアントデバイスのローカルで、インストールウィザードを使用する。

  製品コンポーネントは、Windows オペレーティングシステムの通常の方法で、コントロールパネルを使用して変更されます。インストールウィザーを実行して、利用可能な製品コンポーネントを変更するオプションを選択します。画面に表示される指示に従って操作します。

  > Kaspersky Security Center 経由で本製品をインストールした場合、この方法は使用できません。コントロールパネルで選択した製品コンポーネントを変更できるのは、製品をローカルにインストールした後のみです。

- Kaspersky Security Center を使用してリモートで実行。

  ［*コンポーネントの変更*］タスクを使用すると、インストール後でも Kaspersky Endpoint Security のコンポーネントを変更できます。

製品コンポーネントを変更する際は、次の事項に留意してください：

- Windows Server を実行しているコンピューターでは、Kaspersky Endpoint Security のすべてのコンポーネントをインストールできません（たとえば、アダプティブアノマリーコントロールコンポーネントは使用できません）。

- コンピューターのハードディスクがディスク全体の暗号化（FDE）で保護されている場合、ディスク全体の暗号化コンポーネントは削除できません。ディスク全体の暗号化コンポーネントを削除するには、コンピューターのすべてのハードディスクを復号してください。

- コンピューターに暗号化されたファイル（FLE で暗号化）があるか、ユーザーが暗号化されたリムーバブルドライブ（FDE または FLE で暗号化）を使用している場合、データ暗号化コンポーネントを削除すると、これらのファイルやリムーバブルドライブにアクセスできなくなります。データ暗号化コンポーネントを再インストールすると、これらのファイルやリムーバブルドライブにアクセスできるようになります。

- 本製品が Light Agent モードで VDI インフラストラクチャにインストールされている場合、設定されたコンポーネントの変更はサポートされません。

管理コンソール（MMC）で製品コンポーネントを追加または削除する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**インストールするコンポーネントの選択**］の順に選択します。

ステップ 2：製品コンポーネントの変更のタスク設定

製品の設定を選択します：

- **ワークステーションとサーバーを保護する標準モード**：既定の設定。この設定では、Detection and Response ソリューションのサポートを提供するコンポーネントを含め、アプリケーションのすべてのコンポーネントを使用できます。この設定は、さまざまな脅威、ネットワーク攻撃、詐欺からコンピューターを包括的に保護するために使用されます。
- **先進の脅威や標的型攻撃から保護する Endpoint Detection and Response Agent**：この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。

  EDR エージェントが MDR と連携するように製品の構成を変更する場合は、テレメトリの受信を担当するコンポーネントが有効になっていることを確認してください。

- **仮想環境を保護する Light Agent**：この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。

ユーザーのコンピューターで使用できる製品コンポーネントを選択します。

ステップ 3：詳細設定

タスクの詳細設定を指定します（下の表を参照ください）。

ステップ 4：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 5：タスク開始スケジュールの設定

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

ステップ 6：タスク名の定義

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

ステップ 7：タスク作成の完了

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

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
2. ［**タスク種別**］から［**コンポーネントの変更**］を選択します。
3. ［**タスク名**］に「*アプリケーションコントロールコンポーネントの追加*」などの簡潔な名前を付けます。
4. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

ステップ2：タスクを割り当てるデバイスの選択

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

ステップ3：タスク作成の完了

［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにしてウィザードを終了します。

タスクのプロパティで、［**アプリケーション設定**］セクションを選択します。次に、製品の設定を選択します：

- **ワークステーションとサーバーを保護する標準モード**：既定の設定。この設定では、Detection and Response ソリューションのサポートを提供するコンポーネントを含め、アプリケーションのすべてのコンポーネントを使用できます。この設定は、さまざまな脅威、ネットワーク攻撃、詐欺からコンピューターを包括的に保護するために使用されます。
- **先進の脅威や標的型攻撃から保護する Endpoint Detection and Response Agent**：この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。

EDR エージェントが MDR と連携するように製品の構成を変更する場合は、テレメトリの受信を担当するコンポーネントが有効になっていることを確認してください。

- **仮想環境を保護する Light Agent**：この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。

ユーザーのコンピューターで使用できる製品コンポーネントを選択します。タスクの詳細設定を指定します（下の表を参照ください）。

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

Kaspersky Endpoint Security のインストール、アップデート、アンインストール時に、エラーが発生することがあります。これらのエラーの解決方法については、テクニカルサポートのナレッジベースを参照してください。

タスクの詳細設定

パラメータ	説明
タスク設定	**共存できないサードパーティ製品を確認する**：既定では、Kaspersky Endpoint Security は、インストールされているアプリケーションの互換性をチェックします。互換性の問題が発生する可能性のあるソフトウェアのリストは、incompatible.txt ファイルで参照できます。このファイルは配信キットに含まれています。インストールされているソフトウェアのスキャンが有効になっている場合、リスト内のアプリケーションが検知されると、Kaspersky Endpoint Security はタスクを停止します。サードパーティ製ソフトウェアのベンダードキュメントに、Endpoint Protection Platform（EPP）との互換性が記載されている場合は、インストールされたソフトウェアのスキャンを無効にすることができます。 **共存できないサードパーティ製品を削除する**：コンポーネントセットを変更する前に incompatible.txt ファイルに記載のあるアプリケーションを自動的に削除します。この機能を有効にすると、Kaspersky Endpoint Security はタスクを続行するために互換性の問題を引き起こす可能性のあるアプリケーションを削除しようとします。 **Azure WVD 互換モードを使用する**：この機能により、Kaspersky Anti Targeted Attack Platform コンソールに Azure 仮想マシンの状態が正しく表示されるようになります。コンピューターのパフォーマンスを監視するため、Kaspersky Endpoint Security はテレメトリを KATA サーバーに送信します。テレメトリにはコンピューターの ID（Sensor ID）が含まれます。Azure WVD 互換モードはこれらの仮想マシンに永続的に一意な Sensor ID を割り当てることができます。互換モードがオフになっている場合、Azure 仮想マシンの仕組みにより、コンピューターが再起動した後に Sensor ID が変更されることがあります。このため、コンソール上で仮想マシンが重複して表示されることがあります。
除外リスト	Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。 Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。 信頼ゾーンは、後でポリシープロパティの［信頼するオブジェクトとアプリケーション］で設定することもできます。

パラメータ	説明
分離モード / 複合モード	ワークステーション用とサーバー用に別のコンポーネントのセットを作成できます（[**分離モード**]）。インストールパッケージを導入する前に、インストーラーはオペレーティングシステムの種別を検出し、そのオペレーティングシステムの種別に対して選択した製品コンポーネントのみをインストールします。この方法では、ワークステーションとサーバーに同じインストールパッケージを使用できます。 ［**複合モード**］では、ワークステーションとサーバーの共通のコンポーネントリストが提供されます。個々のコンポーネントが使用可能かどうかは、オペレーティングシステムの種別によって異なります。このモードでは、ワークステーション用とサーバー用に別のインストールパッケージを作成することを推奨します。インストールパッケージ内の共通のコンポーネントリストは、標準モードでのみ設定できます。
製品コンポーネントの構成の変更に対してパスワードを使用する	Kaspersky Endpoint Security へのアクセスを制限するために、管理者がパスワードによる保護を有効にしているケースが多くあります。つまり、製品コンポーネントの選択を変更するには、［**本製品の削除 / 変更 / 修復**］権限を持つユーザーの資格情報を入力する必要があります。例としては、KLAdmin アカウントを使用することができます。
Kaspersky Endpoint Agent および Kaspersky Security for Windows Server のアンインストールにパスワードを使用する	Kaspersky Endpoint Agent (KEA) および Kaspersky Security for Windows Server (KSWS) へのアクセスを制限するため、管理者がこれらのタスクの設定に対してパスワード保護を有効にしているケースが多くあります。つまり、[KES+KEA] 設定を [KES+組み込みエージェント] に移行する場合、または KSWS から KES に移行する場合は、これらの製品をアンインストールするためにパスワードを入力する必要があるということになります。

旧バージョンの製品のアップグレード

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

- 新しいバージョンの Kaspersky Endpoint Security の言語は、インストールされているバージョンの製品の言語と同じものである必要があります。アプリケーションの言語が一致しない場合、製品のアップグレードはエラーで終了します。
- アップグレードを開始する前に、アクティブなアプリケーションをすべて終了してください。
- アップデートプロセスの最初に、Kaspersky Endpoint Security はディスク全体の暗号化機能が動作しないようにロックします。ディスク全体の暗号化機能をロックできない場合、アップデートのインストールは開始されません。アップデートが完了すると、ディスク全体の暗号化機能を再び使用できるようになります。

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

- Kaspersky Endpoint Security 11.10.0 for Windows（ビルド 11.10.0.399）
- Kaspersky Endpoint Security 11.11.0 for Windows（ビルド 11.11.0.452）
- Kaspersky Endpoint Security 12.0 for Windows（ビルド 12.0.0.465）
- Kaspersky Endpoint Security 12.1 for Windows（ビルド 12.1.0.506）
- Kaspersky Endpoint Security 12.2 for Windows（ビルド 12.2.0.462）
- Kaspersky Endpoint Security 12.3 for Windows（ビルド 12.3.0.493）
- Kaspersky Endpoint Security 12.4 for Windows（ビルド 12.4.0.467）
- Kaspersky Endpoint Security 12.5 for Windows（ビルド 12.5.0.539）
- Kaspersky Endpoint Security 12.6 for Windows（ビルド 12.6.0.438）
- Kaspersky Endpoint Security 12.7 for Windows（ビルド 12.7.0.533）

- Kaspersky Endpoint Security 12.8 for Windows（ビルド 12.8.0.505）
- Kaspersky Endpoint Security 12.9 for Windows（ビルド 12.9.0.384）
- Kaspersky Endpoint Security 12.10 for Windows（ビルド 12.10.0.466）
- Kaspersky Endpoint Security 12.11 for Windows（ビルド 12.11.0.637）

Kaspersky Endpoint Security のインストール、アップデート、アンインストール時に、エラーが発生することがあります。これらのエラーの解決方法については、テクニカルサポートのナレッジベースを参照してください。

アプリケーションのアップグレード方法

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

- Kaspersky Update サービス（Seamless Update – SMU）を使用。
- クライアントデバイスのローカルで、インストールウィザードを使用。
- クライアントデバイスのローカルで、コマンドラインを使用。
- Kaspersky Security Center を使用してリモートで実行。
- Microsoft Windows のグループポリシー管理エディターを使用してリモートで実行（詳しい手順については、Microsoft のテクニカルサポートサイトを参照してください）。
- System Center Configuration Managerを使用してリモートで実行。

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

- Kaspersky Security Center Web コンソール または Kaspersky Security Center Cloud コンソール

  本製品の新しいバージョンの既定のセットでインストールパッケージを作成した場合は、ユーザーのコンピューターのコンポーネントのセットは変更されません。既定のコンポーネントのセットの Kaspersky Endpoint Security を使用するには、インストールパッケージのプロパティを開いて、コンポーネントのセットを変更してから元の機能のセットに戻して変更を保存します。

- Kaspersky Security Center の管理コンソール

  アップデート後、アプリケーションコンポーネントのセットはインストールパッケージのコンポーネントのセットと一致します。本製品の新しいバージョンに既定のコンポーネントのセットを含めた場合、既定のセットに含まれない機能（有害 USB 攻撃ブロック機能など）はコンピューターから削除されます。アップデート前と同じコンポーネントのセットの使用を続けるには、インストールのパッケージの設定で必要なコンポーネントを選択してください。

再起動せずに本製品をアップデートする

再起動せずに本製品をアップデートすると、製品のバージョンがアップデートされた場合にもサーバーの動作を妨げることがありません。

再起動せずに本製品をアップデートする場合、次の制限事項があります：

- バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。これより前のバージョンのアプリケーションをアップグレードする場合は、コンピューターを再起動する必要があります。
- バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることができるようになりました。本製品の以前のバージョンにパッチをインストールするには、コンピューターの再起動が必要になる場合があります。
- 本製品の再起動なしのアップデートは、データ暗号化（カスペルスキーの暗号化（FDE）、BitLocker、ファイルレベルの暗号化（FLE））が有効になっているコンピューターでは利用できません。データ暗号化が有効になっているコンピューターで本製品をアップグレードするには、コンピューターを再起動する必要があります。
- 再起動せずに仮想マシン上で本製品をアップグレードすることはできません。仮想マシン上で本製品をアップグレードするには、仮想マシンを再起動する必要があります。

本製品のアップグレード、パッチのインストール、製品コンポーネントのセットの変更、または復元を行うと、Kaspersky Endpoint Security が再起動し、新しいバージョンの使用を開始します。Kaspersky Endpoint Security の再起動には最大で 1 分かかる場合があります。その間、コンピューターの保護レベルが低下します。本製品を再起動すると、コンピューターの保護レベルが元に戻ります。

管理コンソール（MMC）で製品のアップグレードモードを選択する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. 製品のアップグレードモードを設定するには、［**アプリケーションのアップデートの設定**］ブロックで、［**再起動せずに製品アップデートをインストールする**］を選択します。
6. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。

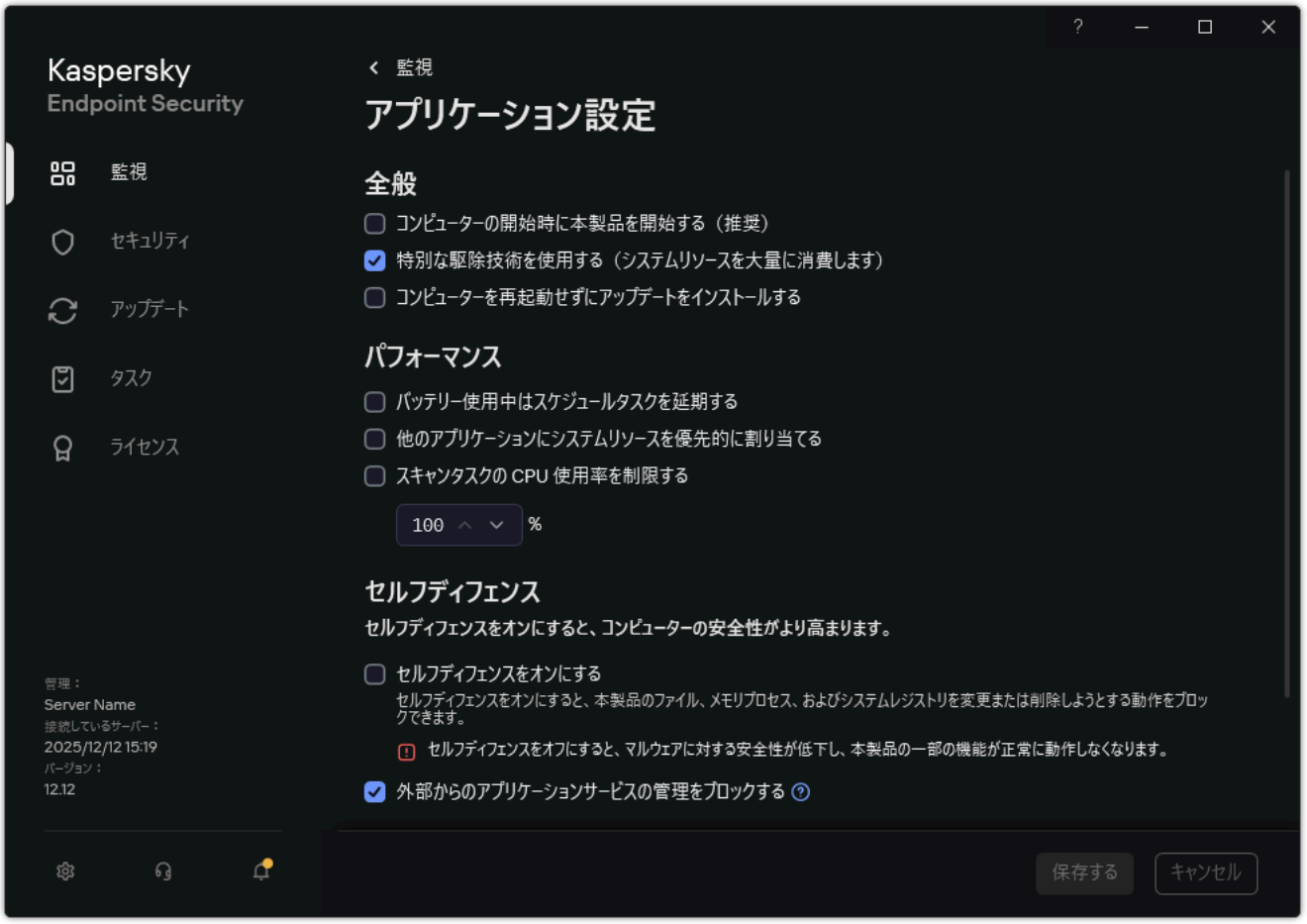
4. 製品のアップグレードモードを設定するには、［**詳細設定**］ブロックで、［**再起動せずに製品アップデートをインストールする**］を選択します。

5. 変更内容を保存します。

製品インターフェイスで製品のアップグレードモードを選択する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. 製品のアップグレードモードを設定するには、［**全般**］ブロックで、［**コンピューターを再起動せずにアップデートをインストールする**］を選択します。

4. 変更内容を保存します。

結果、再起動せずに本製品をアップグレードした後に 2 つのバージョンの製品がコンピューターにインストールされることになります。インストーラーは Program Files および Program Data フォルダーの個別のサブフォルダーに新しいバージョンの製品をインストールします。インストーラーは新しいバージョンの製品に対して個別のレジストリキーを作成します。以前のバージョンの製品を手動で削除する必要はありません。コンピューターが再起動されると、古いバージョンの製品は自動的に削除されます。

Kaspersky Endpoint Security のアップグレードは、Kaspersky Security Center のコンソールのカスペルスキー製品のバージョンレポートを使用して確認することができます。

本製品の SMU アップデート

カスペルスキーのアップデートサービス（Seamless Update、SMU）を使用して製品をアップデートする場合、その他のアップデート方法とは異なり、インストーラを実行する必要はありません。Kaspersky Endpoint Security は本製品の新しいバージョンと定義データベースをを同じソースから取得します。

SMU アップデートにより、組織内のすべてのコンピューター上の本製品を最新バージョンに更新できます。SMU アップデートを適用する前に、一部のコンピューターで本製品の新しいバージョンをテストすることをお勧めします。テストする場合、テストするコンピュータ上の本製品を手動で更新する必要があります（たとえば、ローカルでセットアップウィザードを使用するなど）。SMU アップデートを実行するときに個別のコンピュータを選択することはできません。

製品のアップデートのスケジュールは、 カスペルスキーによって決定されます。新しいバージョンの製品がスムーズに実行できるよう、 カスペルスキー は段階的にアップデートを提供しています。このため、SMU アップデートは、新しいバージョンがリリースされてから最大 2 か月遅れて提供される可能性があります。

本製品の SMU アップデートは、［*定義データベースと製品機能のアップデート*］タスクを使用して管理できます。本製品の新しいバージョンを定義データベースと同じパッケージに含めるには、*製品機能*のアップデートを［*定義データベースと製品機能のアップデート*］タスクの設定で許可する必要があります。また、［*定義データベースと製品機能のアップデート*］タスクの設定で、再起動せずに製品をアップデートできるよう許可することができます。

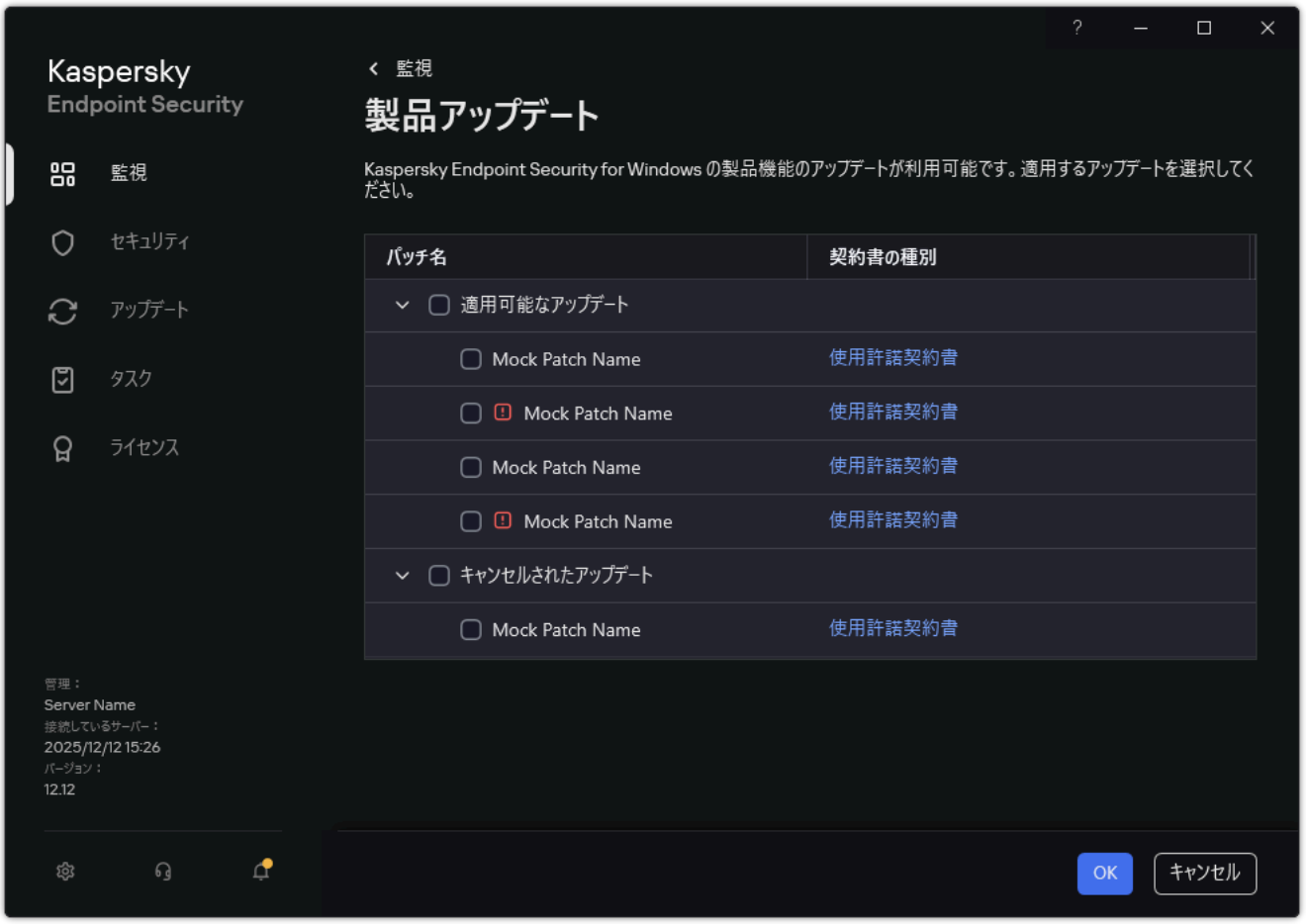
本製品の SMU アップデートの手順

1. **本製品の新しいバージョンがリリースされると、 カスペルスキー はアップデートを配布します。**
2. **ユーザーが本製品のアップデートを承認します。**

   コンピュータが Kaspersky Security Center に接続されている場合、アップデートは Kaspersky Security Center の［**定義データベースと製品機能のアップデート**］セクションで利用できます。アップデートの承認について詳しくは、Kaspersky Security Center のヘルプを参照してください。

   コンピューターが Kaspersky Security Center に接続されていない場合は、製品インターフェイスの通知セクションでアップデートを利用できます。アップデートを承認するには、製品のバージョンを選択し、利用規約の条項に同意します（下の図を参照）。
3. **Kaspersky Endpoint Security は、設定されたスケジュールに従って［*定義データベースと製品機能のアップデート*］タスクを実行します。**

Kaspersky Endpoint Security がコンピューター上で製品をサイレントモードでアップデートします。



利用可能な製品アップデート

本製品の削除

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

Kaspersky Endpoint Security のインストール、アップデート、アンインストール時に、エラーが発生することがあります。これらのエラーの解決方法については、テクニカルサポートのナレッジベースを参照してください。

Kaspersky Security Center を使用して本製品をリモートで削除する

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

管理コンソール（MMC）からアプリケーションを削除する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
3. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

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

ステップ 2：削除するアプリケーションの選択

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

ステップ 3：アプリケーションのアンインストールのタスク設定

Kaspersky Endpoint Security for Windows (12.12) を選択します。

ステップ 4：アンインストールユーティリティの設定

次の追加のアプリケーション設定を設定します：

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

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

1. ［**アンインストール用パスワードを使用する**］チェックボックスをオンにします。
2. ［**編集**］をクリックします。
3. KLAdmin アカウントのパスワードを入力します。

ステップ 5：オペレーティングシステムの再起動設定の選択

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

ステップ 6：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 7：タスクを実行するアカウントの選択

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

ステップ 8：タスク開始スケジュールの設定

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

ステップ 9：タスク名の定義

タスクの名前を入力します。たとえば、*Kaspersky Endpoint Security 12.12 のアンインストール*など。

ステップ 10：タスク作成の終了

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

本製品がサイレントモードでアンインストールされます。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

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

ステップ 2：タスクを割り当てるデバイスの選択

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

ステップ 3：本製品のアンインストール設定の指定

本製品のアンインストール設定を指定します：

1. **管理対象アプリケーションをアンインストールする**の種別を選択します。
2. **Kaspersky Endpoint Security for Windows** を選択します。

3. **アンインストールユーティリティの強制ダウンロード**ユーティリティの配布方法を選択します：

   - **ネットワークエージェントを使用する**：コンピューター上にネットワークエージェントがインストールされていない場合、オペレーティングシステムの共有フォルダーを使用して先にネットワークエージェントがインストールされます。その後、ネットワークエージェントのツールを使用して Kaspersky Endpoint Security がアンインストールされます。

   - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、管理サーバー経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。クライアントコンピューターにネットワークエージェントがインストールされていないが、クライアントコンピューターが管理サーバーと同じネットワーク内に存在する場合にこのオプションを選択できます。

   - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**：ユーティリティが、ディストリビューションポイント経由でオペレーティングシステムの共有フォルダーを使用してクライアントコンピューターに配布されます。ネットワーク内に1つ以上のディストリビューションポイントがある場合にこのオプションを選択できます。ディストリビューションポイントについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

4. ［**同時ダウンロード数の上限**］で、管理サーバーに送信されるアンインストールユーティリティのダウンロード要求数の上限を設定します。要求数の上限を設定することで、ネットワークに過剰な負荷を与えずにすみます。

5. ［**アンインストール試行回数の上限**］で、製品のアンインストールの試行を繰り返す回数の上限を設定します。Kaspersky Endpoint Security のアンインストールがエラーで終了した場合、タスクは自動的にアンインストールをもう一度開始します。

6. 必要に応じて、［**ダウンロード前に OS の種別を確認する**］をオフにします。このオプションがオンの場合、コンピューターのオペレーティングシステムが製品のインストール要件を満たさないのにアンインストールユーティリティを誤ってダウンロードしてしまうことを防ぐことができます。コンピューターのオペレーティングシステムが製品のインストール要件を確実に満たしている場合は、この検証をスキップできます。

ステップ 4：タスクを実行するアカウントの選択

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

ステップ 5：タスク作成の完了

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

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

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

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Security Center の **アプリケーションのリモートアンインストール**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**アンインストール用パスワードを使用する**］チェックボックスをオンにします。
5. KLAdmin アカウントのパスワードを入力します。
6. 変更内容を保存します。

アンインストールを完了するには、コンピューターを再起動してください。再起動するために、ネットワークエージェントはポップアップウィンドウを表示します。

Active Directory を使用して本製品をリモートで削除する

Microsoft Windows のグループポリシーを使用して本製品をリモートで削除することができます。本製品をアンインストールするには、グループポリシー管理コンソール（gpmc.msc）を開いて、グループポリシーエディターを使用してアプリケーションの削除タスクを作成してください（詳細については、Microsoft のテクニカルサポートサイトを参照してください）。

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

1. 次の内容の BAT ファイルを作成します：

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   <GUID> は、アプリケーションの固有の識別子です。テクニカルサポートのナレッジベースで、または次のコマンドを使用して、アプリケーションの GUID を確認できます：

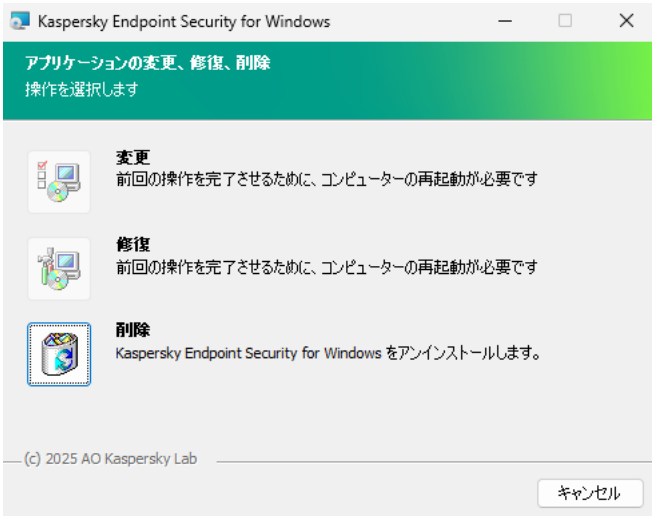
   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
   IdentifyingNumber
   ```

   例：
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. グループ ポリシー管理コンソール（gpmc.msc）でコンピューターの Microsoft Windows ポリシーを新規作成します。
3. 新しいポリシーを使用してコンピューター上に作成した BAT ファイルを実行します。

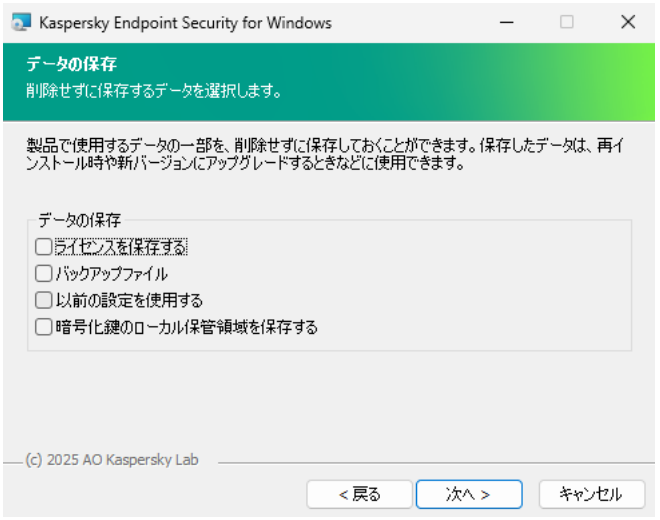
ローカルでの製品の削除

インストールウィザードを使用して本製品をローカルで削除することができます。Kaspersky Endpoint Security は、Windows オペレーティングシステムでその他のアプリケーションをアンインストールするときと同じように、コントロールパネルを使用してアンインストールされます。インストールウィザードが起動します。画面に表示される指示に従って操作します。



本製品の削除操作の選択

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



本製品の削除後のデータ保存

次のデータを保存できます：

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

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

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

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

Kaspersky Endpoint Security はデータを `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` フォルダーに保存します。

ローカルでコマンドラインを使用して製品を削除することもできます。

製品のライセンス

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

使用許諾契約書について

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

製品を使用する前に、使用許諾契約書の条件をよくお読みください。

使用許諾契約書の条件は、次のような方法で確認できます：

- Kaspersky Endpoint Security を対話モードでインストールする場合。
- ファイル license.txt を読む：このドキュメントは、製品配信キットに含まれています。また、製品のインストールフォルダー `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES` にもあります。

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

ライセンスの概要

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

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

次の種類のライセンスが提供されています：

- *試用版* - 製品を試用するための無償ライセンス

  通常、試用版ライセンスには短い有効期間が設定されています。試用版ライセンスの有効期間が終了すると、すべての Kaspersky Endpoint Security 機能が無効になります。製品を引き続き使用するには、製品版ライセンスを購入してください。

  試用版ライセンスでアプリケーションをアクティベートできるのは一度だけです。本製品は、製品版ライセンスでアクティベートされた後は、試用版ライセンスでアクティベートすることはできません。

- *製品版* - Kaspersky Endpoint Security の購入時に提供される有償ライセンス

  製品版ライセンスで使用できる製品の機能は、選択する製品によって異なります。選択した製品は、ライセンス証書に表示されます。利用可能な製品に関する情報については、カスペルスキーの Web サイトを参照してください。

  製品版のライセンスの有効期間が終了すると、本製品の主要な機能が無効になります。製品を引き続き使用するには、ライセンスを更新してください。ライセンスを更新する予定がない場合は、コンピューターから本製品を削除してください。

ライセンスの証明書について

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

ライセンスの証明書に含まれるライセンス情報は次のとおりです：

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

月額制サービスについて

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

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

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

月額制サービスで Kaspersky Endpoint Security を使用するには、サービスプロバイダーから受け取ったアクティベーションコードを適用する必要があります。アクティベーションコードの適用後、アクティブキーが追加されます。現在のライセンスは、月額制サービスでアプリケーションを使用するためのライセンスを決定します。ライセンス情報ファイルを使用して本製品を定額制サービスでアクティベートすることはできません。サービスプロバイダーが提供するのは、アクティベーションコードのみです。月額制サービスで予備のライセンスを追加することはできません。

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

ライセンスについて

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

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

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

使用許諾契約書の条項に違反すると、カスペルスキーによってライセンスがブロックされる場合があります。ライセンスがブロックされている場合、アプリケーションの使用を継続するには、別のライセンスを追加する必要があります。

ライセンスには、現在と予備の 2 種類があります。

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

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

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

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

アクティベーションコードの概要

*アクティベーションコード*は、20 文字からなる一意の英数字列です。アクティベーションコードを入力して、Kaspersky Endpoint Security をアクティベートするライセンスを追加します。Kaspersky Endpoint Security の購入後に指定したメールアドレスで、アクティベーションコードを受け取ります。

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

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

製品のアクティベーション後にアクティベーションコードを紛失した場合、アクティベーションコードを復元できます。たとえば、カスペルスキーカンパニーアカウントの登録に、アクティベーションコードが必要となる場合があります。本製品のアクティベーション後にアクティベーションコードを紛失した場合は、ライセンスを購入したカスペルスキーの代理店にお問い合わせください。

ライセンス情報ファイルについて

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

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

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

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

ライセンス情報ファイルを復元するには：

- ご購入元の販売代理店へ問い合わせる
- 既存のアクティベーションコードに基づき、カスペルスキーの Web サイトでライセンス情報ファイルを取得する
- 別の管理サーバーからライセンス情報ファイルを取得する

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

ワークステーション向けのライセンス種別による製品機能の比較

ワークステーション向けの Kaspersky Endpoint Security で利用できる機能の組み合わせはライセンス種別により異なります（下の表を参照）。

サーバー向けの製品機能比較も参照してください。

Kaspersky Next のライセンスタイプ別のアプリケーション機能の比較は、Kaspersky Next のヘルプをご覧ください。

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
先進の脅威対策								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
ふるまい検知	✓	✓	✓	✓	✓	✓	✓	✓
アンチクリプター	✓	✓	✓	✓	✓	✓	✓	✓
脆弱性攻撃ブロック	✓	✓	✓	✓	✓	✓	✓	✓
ホスト侵入防止	✓	✓	✓	✓	✓	✓	✓	✓
修復エンジン	✓	✓	✓	✓	✓	✓	✓	✓
脅威対策								
ファイル脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
ウェブ脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
メール脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
ファイアウォール	✓	✓	✓	✓	✓	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
有害 USB 攻撃ブロック	✓	✓	✓	✓	✓	✓	✓	✓
AMSI 保護	✓	✓	✓	✓	✓	✓	✓	✓
セキュリティコントロール								
Windows イベントログ監視	–	–	–	–	–	–	–	–
アプリケーションコントロール	✓	✓	✓	✓	✓	✓	✓	✓
デバイスコントロール	✓	✓	✓	✓	✓	✓	✓	✓
ウェブコントロール	✓	✓	✓	✓	✓	✓	✓	✓
アダプティブアノマリーコントロール	–	✓	✓	✓	✓	✓	–	✓
システム変更監視	–	–	–	–	–	–	–	–
データ暗号化								
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
BitLocker ドライブ暗号化	–	✓	✓	✓	✓	✓	–	✓
ファイルレベルの暗号化	–	✓	✓	✓	✓	✓	–	✓
リムーバブルドライブの暗号化	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *（Kaspersky Sandbox のライセンスは別途購入する必要があります）*	✓	✓	✓	✓	✓	✓	✓	✓
KUMA との連携 *（KUMA 連携のライセンスは別途購入する必要があります）*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent モード *（本製品をアクティベートするには、Light Agent が接続されている SVM にライセンスを追加する必要があります）*	–	–	–	–	–	–	✓	✓

サーバー向けのライセンス種別による製品機能の比較

サーバー向けの Kaspersky Endpoint Security で利用できる機能の組み合わせはライセンス種別により異なります（下の表を参照）。

ワークステーション向けの製品機能比較も参照してください。

Kaspersky Next のライセンスタイプ別のアプリケーション機能の比較は、Kaspersky Next のヘルプをご覧ください。

Kaspersky Endpoint Security の機能の比較表

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
先進の脅威対策								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
ふるまい検知	✓	✓	✓	✓	✓	✓	✓	✓
アンチクリプター	✓	✓	✓	✓	✓	✓	✓	✓
脆弱性攻撃ブロック	✓	✓	✓	✓	✓	✓	✓	✓

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
ホスト侵入防止	–	–	–	–	–	–	–	–
修復エンジン	✓	✓	✓	✓	✓	✓	✓	✓
脅威対策								
ファイル脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
ウェブ脅威対策	–	✓	✓	✓	✓	✓	✓	✓
メール脅威対策	–	✓	✓	✓	✓	✓	✓	✓
ファイアウォール	✓	✓	✓	✓	✓	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓	✓	✓	✓	✓	✓
有害 USB 攻撃ブロック	✓	✓	✓	✓	✓	✓	✓	✓
AMSI 保護	✓	✓	✓	✓	✓	✓	✓	✓
セキュリティコントロール								
Windows イベントログ監視	–	–	–	–	–	–	–	✓
アプリケーションコントロール	–	✓	✓	✓	✓	✓	–	✓
デバイスコントロール	–	✓	✓	✓	✓	✓	✓	✓
ウェブコントロール	–	✓	✓	✓	✓	✓	✓	✓
アダプティブアノマリーコントロール	–	–	–	–	–	–	–	–
システム変更監視	–	–	–	–	–	–	–	✓
データ暗号化								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
BitLocker ドライブ暗号化	–	✓	✓	✓	✓	✓	–	✓
ファイルレベルの暗号化	–	–	–	–	–	–	–	–
リムーバブルドライブの暗号化	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *（Kaspersky Sandbox のライセンスは別途購入する必要があります）*	✓	✓	✓	✓	✓	✓	✓	✓

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
KUMA との連携 *（KUMA 連携のライセンスは別途購入する必要があります）*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent モード *（本製品をアクティベートするには、Light Agent が接続されている SVM にライセンスを追加する必要があります）*	–	–	–	–	–	–	✓	✓

製品のアクティベーション

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

次のいずれかの方法で製品をアクティベートすることができます：

- 製品インターフェイスから、アクティベーションウィザードを使用して、ローカルで行う方法。この方法で、現在のライセンスと予備のライセンスの両方を追加できます。
- Kaspersky Security Center の機能を使用して、リモートで行う方法。
  - ［*ライセンスの追加*］タスクを使用

    この方法を使用すると、特定のコンピューターまたは単一の管理グループに属するコンピューターにライセンスを追加できます。この方法で、現在のライセンスと予備のライセンスの両方を追加できます。
  - Kaspersky Security Center 管理サーバーに保存されているライセンスをコンピューターに配信

    この方法を使用すると、Kaspersky Security Center に既に接続されているコンピューターと新しく検出されたコンピューターに自動的にライセンスを追加できます。この方法を使用するには、最初にライセンスを Kaspersky Security Center 管理サーバーに追加する必要があります。Kaspersky Security Center 管理サーバーへのライセンスの追加について詳しくは、Kaspersky Security Center ヘルプを参照してください。

    定額制サービスで購入したアクティベーションコードが優先的に配信されます。

- Kaspersky Endpoint Security のインストールパッケージにライセンスを追加する

  この方法を使用すると、Kaspersky Endpoint Security の導入中にインストールパッケージのプロパティにライセンスを追加することができます。本製品はインストール後に自動的にアクティベートされます。

- コマンドラインを使用。

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

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、製品を個別にアクティベートする必要はありません。

製品のアクティベーション

管理コンソール（MMC）で製品をアクティベートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**ライセンスの追加**］の順に選択します。

ステップ 2：ライセンスの追加

アクティベーションコードを入力するか、ライセンス情報ファイルを選択します。

Kaspersky Security Center のリポジトリへのライセンスの追加について詳しくは、Kaspersky Security Center ヘルプを参照してください。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスク開始スケジュールの設定

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

ステップ 5：タスク名の定義

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

ステップ 6：タスク作成の完了

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

Web コンソールおよび Cloud コンソールで製品をアクティベートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
2. ［**タスク種別**］から［**ライセンスの追加**］を選択します。
3. ［**タスク名**］に「*マネージャー用の Kaspersky Endpoint Security for Windows のアクティベーション*」などの簡潔な名前を付けます。
4. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。次の手順に進みます。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：ライセンスの選択

製品のアクティベーションに使用するライセンスを選択します。次の手順に進みます。

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

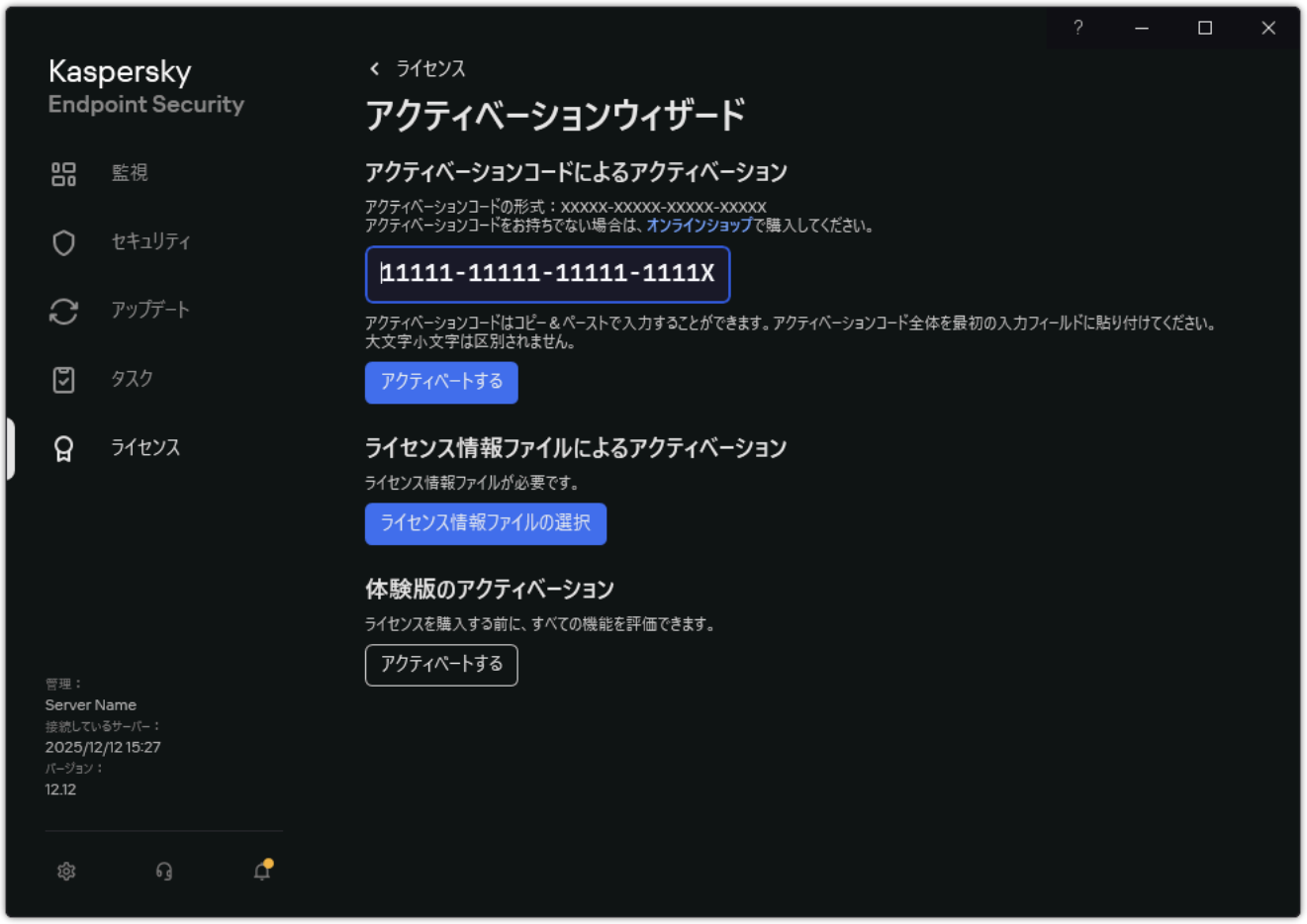
ステップ 4：タスク作成の完了

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

製品インターフェイスで製品をアクティベートする方法

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

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



製品のアクティベーション

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

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

1. 管理コンソールで、［**カスペルスキーのライセンス**］のフォルダーに移動します。

   ライセンスのリストが開きます。

2. ライセンスのプロパティを開きます。

3. ［**全般**］セクションで、［**管理対象デバイスにライセンスを自動的に配信する**］をオンにします。

4. 変更内容を保存します。

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

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

1. Web コンソールのメインウィンドウで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］をクリックします。

   ライセンスのリストが開きます。

2. ライセンスのプロパティを開きます。

3. ［**全般**］タブで、［**管理対象デバイスにライセンスを自動的に配信する**］を有効にします。

4. 変更内容を保存します。

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

*アクティベーションコード*を使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーへのインターネット接続が必要です。*ライセンス情報ファイル*を使用して製品をアクティベートする場合、インターネット接続は必要ありません。コンピューターがインターネットに接続できない分離されたネットワークセグメントにある場合、コードを使用して製品をアクティベートするには、Kaspersky Security Center 管理サーバーのプロキシサーバーとしての使用を許可する必要があります。つまり、製品はインターネットにアクセスできる管理サーバーを介してアクティベーションサーバーにアクセスできます。

管理コンソール（MMC）で、製品をアクティベートするためのプロキシサーバーとして管理サーバーを使用することを許可する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。

4. ［**アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する**］チェックボックスをオンにします。

5. 変更内容を保存します。

Web コンソールと Cloud コンソールで、製品をアクティベートするためのプロキシサーバーとして管理サーバーを使用することを許可する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**KSC 連携**］に移動します。

5. ［**アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する**］チェックボックスをオンにします。

6. 変更内容を保存します。

*アクティベーションコード*を使用して製品をアクティベートできない場合、カスペルスキーのソリューション を使用して*ライセンス情報ファイル*を入手し、別の方法で製品のアクティベーションを再度試みることができます。

ライセンス使用状況の監視

ライセンスの使用状況を次の方法を使用して監視できます：

- 組織のインフラストラクチャの *ライセンス使用レポート*（[**監視とレポート**] → [**レポート**]）を表示する。
- [**管理対象デバイス**] → [**デバイス**] タブでコンピューターのステータスを表示する。製品がアクティベートされていない場合、コンピューターには ⚠「*アクティベートされていません*」というステータスが表示されます。
- コンピューターのプロパティでライセンス情報を表示する。
- 主要なプロパティを表示します（[**操作**] → [**ライセンス管理**]）。

Kaspersky Security Center Cloud コンソールの一部として製品をアクティベートする場合の詳細

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

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

ライセンスの削除

ライセンスを削除するには、コンピューター上で特別なタスクを実行する必要があります。たとえば、ライセンスユニットを再編成するために、ライセンスを削除できます。また、ライセンスの有効期限が終了すると、ユーザーに通知されます。製品を試用するために短期間のライセンスを追加した場合（EDR Optimum アドオンなど）、通知を除去するためにこのライセンスを削除して、コンピューターの状態を修正できます。

*ライセンスの削除*タスクを実行して、コンピューターからライセンスを削除することができます。有効なライセンスと予備のライセンスを削除できます。Kaspersky Endpoint Security のアクティベーションライセンスに加えて、Kaspersky Detection and Response ソリューションの個々のライセンス（EDR Optimum アドオンなど）を削除できます。

管理コンソール（MMC）でライセンスを削除する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**ライセンスの削除**］の順に選択します。

ステップ 2：ライセンスの選択

削除するライセンスを選択します。Kaspersky Security Center のライセンスストアからライセンスを選択することも、ライセンス情報ファイルを選択することもできます。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスク開始スケジュールの設定

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

ステップ 5：タスク名の定義

タスクの名前を入力します（たとえば、「*ベータ版のライセンスの削除*」など）。

ステップ 6：タスク作成の完了

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

Web コンソールでライセンスを削除する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
2. ［**タスク種別**］から［**ライセンスの削除**］を選択します。
3. ［**タスク名**］フィールドに「*ベータ版のライセンスの削除*」などの短く分かりやすい名前を付けます。
4. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。次の手順に進みます。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：ライセンスの選択

削除するライセンスを選択します。Kaspersky Security Center のライセンスストアからライセンスを選択することも、ライセンス情報ファイルを選択することもできます。次の手順に進みます。

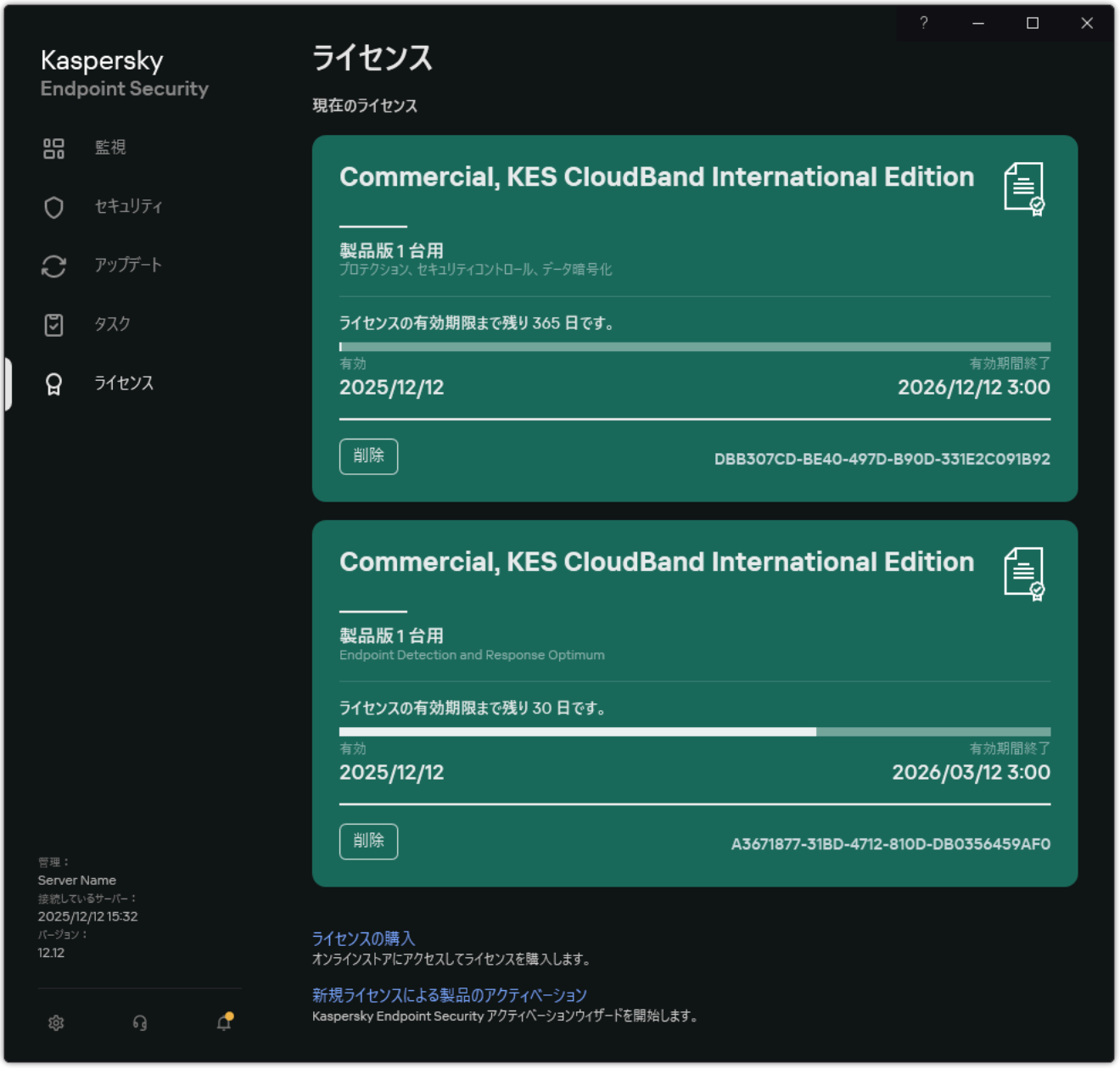
ステップ 4：タスク作成の完了

［**終了**］をクリックして、ウィザードを終了します。タスクのリストに新しいタスクが表示されます。タスクを実行するには、タスクのチェックボックスをオンにし、［**開始**］をクリックします。

製品インターフェイスでライセンスを削除する方法

1. メインウィンドウで、［**ライセンス**］をクリックします。

2. 削除するライセンスを選択して［**削除**］をクリックします。



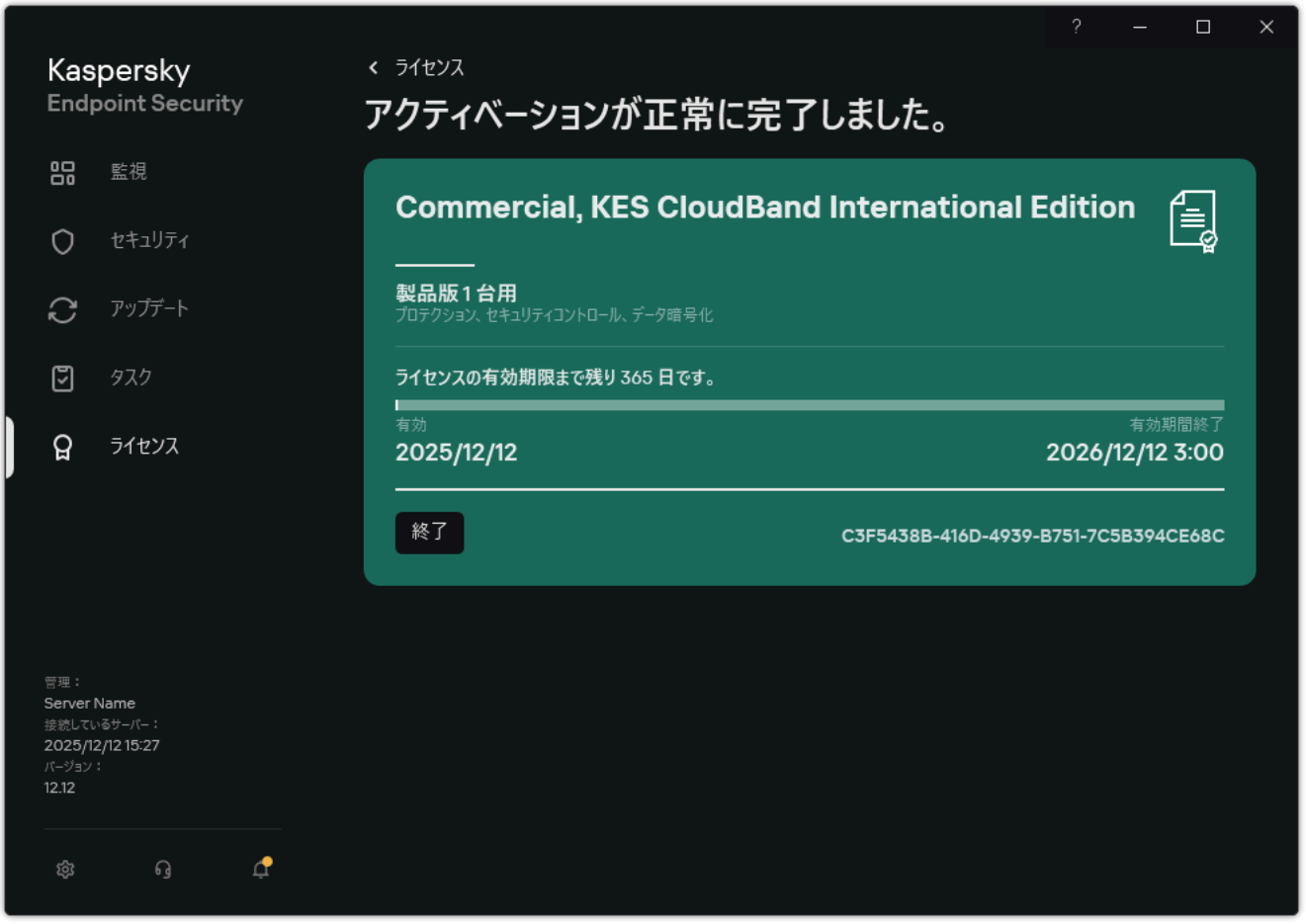
［ライセンス］ウィンドウ

コマンドラインでライセンスを削除することもできます。

ライセンス情報の表示

ライセンスの情報を確認するには：

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



［ライセンス］ウィンドウ

このセクションには次の内容が表示されます：

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

- *ライセンスに関する追加情報*：ライセンスの有効期間の開始日時および終了日時（現在のライセンスのみ）およびライセンスの有効期間の残り日数です。

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

- *識別 ID*：識別 ID はアクティベーションコードまたはライセンス情報ファイルから生成される一意の英数字列です。

［ライセンス］ウィンドウで、次の操作も実行できます：

- **ライセンスの購入 / ライセンスの更新**：ライセンスを購入または更新できる Web サイトが開きます。購入または更新するには、企業の情報を入力して注文に対する支払いを行ってください。

- **新規ライセンスによる製品のアクティベーション**：アクティベーションウィザードが起動します。ウィザードでアクティベーションコードまたはライセンス情報ファイルを使用してライセンスを追加できます。アクティベーションウィザードでは、現在のライセンスを 1 つと予備のライセンスを 1 つのみ追加できます。

ライセンスの更新または購入

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

ライセンスを購入するには、次の手順を実行します：

1. メインウィンドウで、［**ライセンス**］をクリックします。
2. 次のいずれかの手順を実行します：

   - ライセンスが追加されていない場合または試用版ライセンスが追加されている場合は、［**ライセンスの購入**］をクリックします。
   - 製品版ライセンスが追加されている場合は、［**ライセンスの更新**］をクリックします。

   ライセンス購入用の Web サイトが表示されます。

月額制サービスの更新

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

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

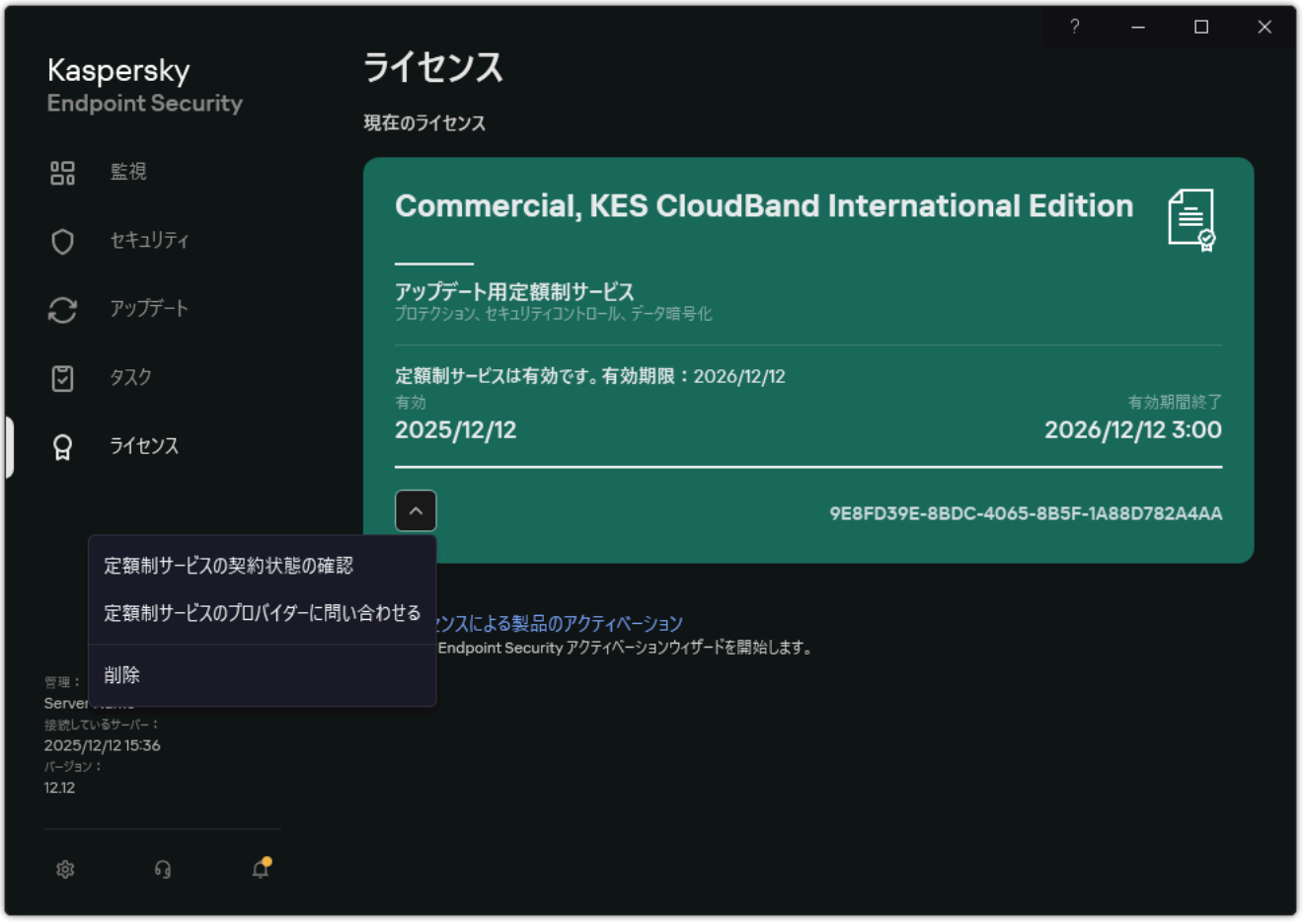
本製品を期限付き月額制サービスで使用している場合、月額制サービスの有効期間（または月額制サービスの更新猶予期間）が終了する日に、Kaspersky Endpoint Security が通知を表示して、月額制サービスの自動更新を停止します。この場合、Kaspersky Endpoint Security は製品版ライセンスの期限切れのときと同じ動作をします。つまり、製品はアップデートなしで動作し、Kaspersky Security Network サービスが利用できなくなります。

月額制サービスは、サービスプロバイダーの Web サイトで更新できます。

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

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

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



月額制サービスの更新

データ提供

使用許諾契約書におけるデータ提供

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

- Kaspersky Endpoint Security の種別、バージョン、ローカリゼーション
- Kaspersky Endpoint Security のインストールされたアップデートのバージョン
- コンピューターの識別子およびそのコンピューターにインストールされた Kaspersky Endpoint Security の識別子
- シリアル番号と現在のライセンスの識別子
- オペレーティングシステムの種別、バージョンおよびビット数、および仮想環境の名前（Kaspersky Endpoint Security が仮想環境にインストールされている場合）
- 権利者のサービスの一意な要求の識別子
- 情報の送信時に使用中である Kaspersky Endpoint Security コンポーネントの識別子

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

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

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

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

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

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

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

Kaspersky Security Network 使用時のデータ提供

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

4 台以下のコンピューター用のライセンスでの KSN の使用

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

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

5 台以上のコンピューター用のライセンスでの KSN の使用

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

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

- KSN 設定のアップデートに関する情報：使用中の設定情報の識別子、受信した設定情報の識別子、設定情報のアップデートのエラーコード。

- スキャンされるファイルと URL アドレスに関する情報：スキャンされたファイルのチェックサム（MD5、SHA2-256、SHA1）およびファイルパターンのチェックサム（MD5）、パターンのサイズ、検知した脅威の種別および権利者の分類に基づく名前、定義データベースの識別子、評価が要求されている URL アドレスおよび参照元の URL アドレス、接続プロトコルの識別子および使用しているポートの番号。

- 脅威を検知したスキャンタスクの識別子。

- 認証を検証するために使用されたデジタル署名に関する情報：スキャンされたオブジェクトの署名に使用された証明書および証明書の公開鍵のチェックサム（SHA256）。

- スキャンを実行している本ソフトウェアのコンポーネントのタスク識別子。

- 定義データベースの識別子および定義データベースのレコードの識別子。

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

- 権利者の本ソフトウェアに関する情報：バージョンの詳細、種別、Kaspersky サービスへの接続に使用されるプロトコルのバージョン。

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

- 要求された Web リソースの分類結果に関する情報：処理された URL およびホストの IP アドレス、分類を実行した本ソフトウェアのコンポーネントのバージョン、分類方法および Web リソースに定義された一連のカテゴリ。

- 端末にインストールされた本ソフトウェアに関する情報：ソフトウェアおよびその開発元の名前、レジストリキーおよびその値、インストールされたソフトウェアコンポーネントのファイルに関する情報（チェックサム（MD5、SHA2-256、SHA1）、名前、コンピューター上のパス、サイズ、バージョンおよびデジタル署名）。

- コンピューターのウイルス対策の状態に関する情報：使用中の定義データベースのバージョンおよび公開のタイムスタンプ、タスクの識別子およびスキャンを実行したソフトウェアの識別子。

- エンドユーザーによってダウンロードされているファイルに関する情報：ダウンロードファイルおよびダウンロードページの URL および IP アドレス、ダウンロードプロトコルの識別子および接続先ポート番号、URL の状態（悪意があるかどうか）、ファイルの属性、サイズおよびチェックサム（MD5、SHA2-256、SHA1）、ファイルをダウンロードしたプロセスに関する情報（チェックサム（MD5、SHA2-256、SHA1）、作成日時、ビルド日時、自動実行の状態、属性、圧縮プログラムの名前、署名に関する情報、実行ファイルのフラグ、形式の識別子、情報量）、ファイル名および端末上のパス、ファイルのデジタル署名とその生成のタイムスタンプ、検知した URL アドレス、疑わしいまたは悪意があると判明したページのスクリプトの数、生成された HTTP リクエストおよびリクエストへのレスポンスに関する情報。

- 実行中のアプリケーションおよびそれらのモジュールに関する情報：システム上で実行されているプロセスに関するデータ（プロセスの識別子（PID）、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、信頼済みプログラムまたはプロセスの署名、プロセスのファイルとそのチェックサム（MD5、SHA2-256、SHA1）の完全パスおよび起動したコマンドライン、プロセスの整合性レベル、プロセスが属するアプリケーションの説明（アプリケーション名および製造元の情報）、使用されるデジタル署名の信頼性を検証するための情報、またはファイルのデジタル署名が存在しない場合は存在しないことを示す情報）、プロセスに読み込まれたモジュールに関する情報（名前、サイズ、種別、作成日時、属性、チェックサム（MD5、SHA2-256、SHA1）、コンピューター上のパス）、PE ファイルヘッダー情報、圧縮プログラムの名前（ファイルが圧縮されている場合）。

- 悪意のある可能性のあるオブジェクトおよび活動に関する情報：検知したオブジェクトの名前およびコンピューター上の完全パス、処理されたファイルのチェックサム（MD5、SHA2-256、SHA1）、検知した日時、感染したファイルの名前およびサイズおよびそのパス、パステンプレートコード、実行ファイルのフラグ、オブジェクトがコンテナーであるかどうかを示すフラグ、圧縮プログラムの名前（ファイルが圧縮されている場合）、ファイル種別コード、ファイル形式の識別子、マルウェアが実行した処理のリストおよびそれに対応したソフトウェアとユーザーの判定、判定に使用された定義データベースの識別子および定義データベースのレコードの識別子、悪意のある可能性があるオブジェクトであることを示すフラグ、権利者の分類による検知された脅威の名前、危険度レベル、検知ステータスおよび検知方法、解析されたコンテキストに含めた理由およびコンテキスト内のファイルのシーケンス番号、チェックサム（MD5、SHA2-256、SHA1）、感染したメッセージまたはリンクの送信に使用されたアプリケーションの実行ファイルの名前と属性、ブロックされたオブジェクトのホストの匿名化した IP アドレス（IPv4 および IPv6）、ファイルの情報量、ファイルの自動実行のフラグ、システム内でファイルが最初に検知された時刻、前回統計情報が送信されてからファイルが実行された回数、悪意のあるオブジェクトを受信したメールクライアントの名前とチェックサム（MD5、SHA2-256、SHA1）およびサイズに関する情報、スキャンを実行したソフトウェアのタスクの識別子、ファイルの評価または署名がチェックされたかどうかのフラグ、ファイルの処理結果、当該オブジェクトに対して収集されたパターンのチェックサム（MD5）、サイズおよびパターン（バイト）、適用された検知技術の技術仕様。

- スキャンしたオブジェクトに関する情報：ファイルの移動先の信頼グループおよび移動元の信頼グループ、当該カテゴリに分類された理由、カテゴリの識別子、元のカテゴリおよびカテゴリデータベースのバージョンに関する情報、ファイルの信頼済み証明書のフラグ、ファイルの製造元、ファイルのバージョン、ファイルが含まれているアプリケーションの名前およびバージョン。

- 検知された脆弱性に関する情報：脆弱性データベース内の脆弱性の識別子、脆弱性の危険度。

- 実行ファイルのエミュレーションに関する情報：ファイルのサイズおよびチェックサム（MD5、SHA2-256、SHA1）、エミュレーションコンポーネントのバージョン、エミュレーション深度、エミュレーション中に取得された論理ブロックのプロパティの配列および論理ブロック内の関数の配列、実行ファイルの PE ヘッダーのデータ。

- 攻撃元コンピューターの IP アドレス（IPv4 および IPv6）、攻撃の標的となったコンピューターのポート番号、攻撃に使用された IP パケットのプロトコルの識別子、攻撃対象（組織名、Web サイト）、攻撃への対処のフラグ、攻撃の重み、信頼度。

- ネットワークリソースの偽装に関連した攻撃に関する情報：閲覧した Web サイトの DNS および IP アドレス（IPv4 および IPv6）。

- 要求された Web リソースの DNS アドレスおよび IP アドレス（IPv4 または IPv6）、Web リソースにアクセスしているファイルおよび Web クライアントに関する情報、ファイルの名前とサイズおよびチェックサム（MD5、SHA2-256、SHA1）、ファイルの完全パスとパステンプレートコード、デジタル署名の確認結果、KSN のステータス。

- マルウェアの処理のロールバックに関する情報：動作がロールバックされたファイルのデータ（ファイル名、ファイルの完全パス、サイズおよびチェックサム（MD5、SHA2-256、SHA1））、成功または失敗した削除処理に関するデータ、ファイルの名前変更とコピーおよびレジストリ内の値の復元（レジストリキーの名前およびその値）、マルウェアによって変更されたシステムファイルに関するロールバック実施前後の情報。

- アダプティブアノマリーコントロールコンポーネントの実行セットに関する情報：トリガーされたルールの識別子とステータス、ルールがトリガーされたときに本ソフトウェアにより実行された処理、プロセスまたはスレッドが疑わしい動作を実行しているユーザーアカウントの種別および疑わしい動作の影響を受けたプロセスに関する情報（スクリプト識別子またはプロセスファイル名、プロセスファイルへの完全パス、パステンプレートコード、プロセスファイルのチェックサム（MD5、SHA2-256、SHA1））。疑わしい動作を実行したオブジェクトおよび疑わしい動作の影響を受けたオブジェクトに関する情報（レジストリキー名またはファイル名、ファイルへの完全パス、パステンプレートコード、およびファイルのチェックサム（MD5、SHA2-256、SHA1））。

- 読み込まれたソフトウェアの機能に関する情報。モジュールファイルの名前、サイズおよびチェックサム（MD5、SHA2-256、SHA1）、完全パスおよびパステンプレートコード、モジュールファイルのデジタル署名設定、署名の作成日時、モジュールファイルに署名した発行先および組織名、モジュールが読み込まれたプロセスの識別子、モジュールの供給元の名前、読み込み列内のモジュールのシーケンス番号。

- 本ソフトウェアと KSN サービスとの通信品質に関する情報：統計が生成された期間の開始日時と終了日時、リクエストの品質および使用されている各 KSN サービスの接続に関する情報、（KSN サービス識別子、成功したリクエストの数、キャッシュからの応答があったリクエストの数、失敗したリクエストの数（ネットワークの問題、KSN が本ソフトウェアの設定で無効、誤ったルーティング）、成功したリクエストの時間範囲、キャンセルされたリクエストの時間範囲、制限時間を超えたリクエストの時間範囲、キャッシュから取得された KSN への接続の数、成功した KSN への接続の数、失敗した KSN への接続の数、成功したトランザクションの数、失敗したトランザクションの数、成功した KSN への接続の時間範囲、失敗した KSN への接続の時間範囲、成功したトランザクションの時間範囲、失敗したトランザクションの時間範囲）。

- 悪意のある可能性のあるオブジェクトが検知された場合に、プロセスのメモリ内のデータに関して提供される情報：システムのオブジェクト階層（ObjectManager）の要素、UEFI BIOS メモリのデータ、レジストリキーの名前とその値。

- システムログのイベントに関する情報。イベントのタイムスタンプ、イベントが見つかったログの名前、イベントの種別およびカテゴリ、イベントの発生元の名前およびイベントの説明。

- ネットワーク接続に関する情報。ポートを開いたプロセスを開始したファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、プロセスファイルのパスおよびデジタル署名、ローカルおよびリモートの IP アドレス、ローカルおよびリモートの接続ポート番号、接続状態、ポートが開かれたときのタイムスタンプ

- コンピューター上の本ソフトウェアのインストールおよびアクティベーションの日付に関する情報：ライセンスを購入した代理店の識別子、ライセンスのシリアル番号、アクティベーションサービスからのチケットの署名済みヘッダー（地域の本ソフトウェアのアクティベーションセンターの識別子、アクティベーションコードのチェックサム、チケットのチェックサム、チケットの作成日、チケットの一意な識別子、チケットのバージョン、ライセンスの状態、チケットの有効期間の開始日時と終了日時、ライセンスの一意な識別子、ライセンスのバージョン）、チケットのヘッダーの署名に使用されている証明書のハッシュ、ライセンス情報ファイルのチェックサム（MD5）、コンピューターにインストールされたソフトウェアの一意な識別子、アップデートされるアプリケーションの種別および識別子、アップデートタスクの識別子。

- インストールされているすべてのアップデート一式に関する情報、および最後にインストールまたは削除されたアップデート一式に関する情報、アップデート情報の送信を発生させたイベントの種別、最後にアップデートをインストールしてからの経過時間、現在インストールされている定義データベースに関する情報。

- コンピューター上のソフトウェアの処理に関する情報：CPU の使用に関するデータ、メモリの使用（プライベートバイト、非ページプール、ページプール）に関するデータ、ソフトウェアのプロセス中のアクティブなスレッド数および保留中のプロセス数、エラーが発生する前のソフトウェアの処理時間。

- 本ソフトウェアインストール後および前回のアップデート適用後に発生したソフトウェアダンプおよびシステムダンプ（BSOD）の数、クラッシュしたソフトウェアモジュールの識別子とバージョン、ソフトウェアプロセスのメモリスタック、およびクラッシュ時の定義データベースに関する情報。

- システムダンプ（BSOD）のデータ：コンピューターで BSOD が発生したことを示すフラグ、BSOD の原因となったドライバーの名前、ドライバーのアドレスおよびメモリスタック、BSOD が発生するまでのセッションの時間を示すフラグ、クラッシュしたドライバーのメモリスタック、保管されたメモリダンプの種別、BSOD が 10 分以上継続する前の OS セッションのフラグ、ダンプの一意な識別子、BSOD のタイムスタンプ。

- 本ソフトウェアのコンポーネントの操作中に発生したエラーまたはパフォーマンスの問題に関する情報：本ソフトウェアのステータスの識別子、エラー種別、エラーが発生したときのコードと原因および時刻、コンポーネントの識別子、エラーが発生した製品のモジュールおよびプロセス、エラー発生中のタスクまたはアップデートカテゴリの識別子、本ソフトウェアが使用するドライバーのログ（エラーコード、モジュール名、ソースファイル名およびエラーが発生した行）

- 定義データベースおよび本ソフトウェアのコンポーネントのアップデートに関する情報：最後のアップデート中および現在のアップデート中にダウンロードされたインデックスファイルの名前と日時。

- 本ソフトウェアの操作の異常終了に関する情報：ダンプファイルの生成日時、種別、本ソフトウェアの操作の異常終了の起因となったイベントの種別（予期しない電源の切断、サードパーティ製アプリケーションのクラッシュ）、予期しない電源の切断が発生した日時。

- ソフトウェアドライバーとハードウェアおよびソフトウェアとの互換性に関する情報：ソフトウェアコンポーネントの機能を制限する OS のプロパティに関する情報（セキュアブート、KPTI、WHQL エンフォース、BitLocker、大文字と小文字の区別）、インストールされたダウンロードソフトウェアの種別（UEFI、BIOS）、Trusted Platform Module（TPM）の識別子、TPM 仕様のバージョン、コンピューターに組み込まれている CPU に関する情報、Code Integrity と Device Guard の操作モードとパラメータ、ドライバーの操作モードおよび現在のモードの使用理由、ソフトウェアドライバーのバージョン、コンピューターにおけるソフトウェアとハードウェアの仮想化サポート状況。

- エラーの発生原因となったサードパーティ製アプリケーションに関する情報：名前、バージョンおよび言語、エラーコードおよびアプリケーションのシステムログに含まれるエラーに関する情報、該当するサードパーティ製アプリケーションのエラーのアドレスおよびメモリスタック、ソフトウェアのコンポーネント内でエラーが発生したことを示すフラグ、エラーが発生するまでサードパーティ製アプリケーションが動作していた時間、エラーが起きたアプリケーションプロセスイメージのチェックサム（MD5、SHA2-256、SHA1）、アプリケーションプロセスイメージのパスおよびパスのテンプレートコード、アプリケーションに関連付けられたエラー記述を含むシステムログからの情報、エラーが起きたアプリケーションモジュールに関する情報（例外の識別子、アプリケーションモジュールのオフセットとしてのクラッシュメモリアドレス、モジュールの名前とバージョン、権利者のプラグインで発生したアプリケーションクラッシュの識別子およびクラッシュのメモリスタック、クラッシュ発生までのアプリケーションセッションの時間）。

- 本ソフトウェアのアップデーターコンポーネントのバージョン、コンポーネントが動作中のアップデートタスク実行中にアップデーターコンポーネントがクラッシュした回数、アップデートタスク種別の識別子、アップデーターコンポーネントがアップデートタスクを完了させようとして失敗した回数。

- 本ソフトウェアのシステム監視コンポーネントの動作に関する情報：コンポーネントの詳細バージョン、イベントキューをオーバーフローさせたイベントのコードおよび該当するイベントの数、キューがオーバーフローしたイベントの総数、イベントを開始したプロセスのファイルに関する情報（ファイル名およびコンピューター上のパス、ファイルパスのテンプレートコード、ファイルに関連付けられたプロセスのチェックサム（MD5、SHA2-256、SHA1））、発生したイベント遮断の識別子、遮断フィルターのバージョン、遮断されたイベントの種別の識別子、キュー内の最初のイベントと現在のイベント間におけるイベントキューのサイズとイベントの数、キュー内の期限切れイベントの数、現在のイベントを開始したプロセスのファイルに関する情報（ファイル名およびコンピューター上のパス、ファイルパスのテンプレートコード、ファイルに関連付けられたプロセスのチェックサム（MD5、SHA2-256、SHA1））、イベントの処理時間、イベントの処理時間の上限、統計を送信する確率、処理時間制限を超えた OS イベントに関する情報（イベントの日時、定義データベースの初期化繰り返しの回数、定義データベースのアップデート後に最後の初期化繰り返しが実行された日時、各システム監視コンポーネントのイベント処理遅延時間、キューにあるイベントの数、処理されたイベントの数、現在の種別の遅延イベントの数、現在の種別のイベントの合計遅延時間、すべてのイベントの合計遅延時間）。

- ソフトウェアパフォーマンスの問題が発生した場合に SysConfig / SysConfigEx / WinSATAssessment イベントが出力される Microsoft の Windows イベントトレースツール（ETW：Event Tracing for Windows）からの情報：コンピューターに関する情報（機種、製造元、筐体のフォームファクター、バージョン）、Windows パフォーマンスメトリックスに関する情報（WinSAT 評価、Windows パフォーマンスインデックス）、ドメイン名、物理プロセッサおよび論理プロセッサに関する情報（物理プロセッサおよび論理プロセッサの数、製造元、モデル、ステッピングレベル、コア数、クロック周波数、CPUID、キャッシュ特性、論理プロセッサ特性、サポートされるモードと命令を示すフラグ）、RAM モジュールに関する情報（種別、フォームファクター、製造元、モデル、容量、メモリ割り当ての細分性）、ネットワークインターフェイスに関する情報（IP アドレスおよび MAC アドレス、名前、説明、ネットワークインターフェイスの設定、種別ごとのネットワークパッケージの数とサイズの内訳、ネットワーク通信速度、種別ごとのネットワークエラー数の内訳）、IDE コントローラーの設定、DNS サーバーの IP アドレス、ビデオカードに関する情報（モデル、説明、製造元、互換性、ビデオメモリ容量、画面許可、ピクセルあたりのビット数、BIOS バージョン）、プラグアンドプレイのデバイスに関する情報（名前、説明、デバイス識別子［PnP、ACPI］）、ディスクおよびストレージデバイスに関する情報（ディスクまたはフラッシュデバイスの数、製造元、モデル、ディスク容量、シリンダー数、シリンダーあたりのトラック数、トラックあたりのセクター数、セクター容量、キャッシュ特性、シーケンシャル番号、パーティション数、SCSI コントローラーの設定）、論理ディスクに関する情報（シーケンシャル番号、パーティション容量、ボリューム容量、ボリューム文字、パーティション種別、ファイルシステム種別、クラスター数、クラスターのサイズ、クラスターあたりのセクター数、空のクラスターと占有されているクラスターの数、起動可能ボリュームの文字、ディスクの先頭に関するパーティションのオフセットアドレス）、BIOS マザーボードに関する情報（製造元、発売日、バージョン）、マザーボードに関する情報（製造元、モデル、タイプ）物理メモリに関する情報（共有されている容量およびフリーの容量）、オペレーティングシステムのサービスに関する情報（名前、説明、ステータス、タグ、プロセスに関する情報［名前および PID］）、コンピューターの電力消費のパラメータ、割り込みコントローラーの設定、Windows システムフォルダーのパス（Windows および System32）、OS に関する情報（バージョン、ビルド、発売日、名前、種別、インストール日）、ページファイルのサイズ、モニターに関する情報（番号、製造元、画面許可、解像度の容量、種別）ビデオカードドライバーに関する情報（製造元、発売日、バージョン）。

- EventTrace / EventMetadata イベントが出力される Microsoft の ETW からの情報：システムイベントのシーケンスに関する情報（種別、時間、日付、タイムゾーン）、トレース結果を含むファイルに関するメタデータ（名前、構造、トレースパラメータ、種別ごとのトレース操作数の内訳）、OS に関する情報（名前、種別、バージョン、ビルド、リリース日、開始時刻）。

- Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power イベントが出力される Microsoft の ETW からの情報：開始および完了したプロセスに関する情報（名前、PID、開始パラメータ、コマンドライン、リターンコード、電力管理パラメータ、開始および完了した時刻、アクセストークン種別、SID、セッション識別子、インストールされている記述子の数）、スレッドの優先順位の変更に関する情報（TID、優先順位、時間）、プロセスのディスク操作に関する情報（種別、時刻、容量、数）、使用可能なメモリプロセスの構造と容量に対する変更履歴。

- StackWalk / Perfinfo イベントが出力される Microsoft の ETW からの情報：パフォーマンスカウンターに関する情報（個々のコードセクションのパフォーマンス、関数呼び出しのシーケンス、PID、TID、ISR および DPC のアドレスと属性）。

- KernelTraceControl-ImageID イベントが出力される Microsoft の ETW からの情報：実行可能ファイルおよび動的ライブラリの情報（名前、画像サイズ、完全パス）、PDB ファイルの情報（名前、識別子）、実行可能ファイルの VERSIONINFO リソースデータ（名前、説明、作成者、場所、アプリケーションのバージョンと識別子、ファイルのバージョンと識別子）。

- FileIo / DiskIo / Image / Windows Kernel Disk イベントが出力される Microsoft の ETW からの情報：ファイルおよびディスク操作に関する情報（種別、容量、開始時刻、完了時刻、継続時間、完了ステータス、PID、TID、ドライバーの関数呼び出しアドレス、I/O 要求パケット（IRP）、Windows ファイルオブジェクト属性）、ファイルおよびディスク操作に関連するファイルに関する情報（名前、バージョン、サイズ、完全パス、属性、オフセット、イメージのチェックサム、オープンおよびアクセスのオプション）。

- PageFault イベントが出力される Microsoft の ETW からの情報：メモリページのアクセスエラーに関する情報（アドレス、時間、容量、PID、TID、Windows ファイルオブジェクトの属性、メモリ割り当てパラメータ）。

- Thread イベントが出力される Microsoft の ETW からの情報：スレッドの作成または完了に関する情報、開始されたスレッドに関する情報（PID、TID、スタックのサイズ、CPU リソースの優先順位と割り当て、I/O リソース、スレッド間のメモリページ、スタックアドレス、init 関数のアドレス、スレッド環境ブロック（TEB：Thread Environment Block）のアドレス、Windows サービスタグ）。

- Microsoft Windows Kernel Memory イベントが出力される Microsoft の ETW からの情報：メモリ管理操作に関する情報（完了ステータス、時刻、数量、PID）、メモリ割り当て構造（種別、容量、セッション識別子、PID）。

- パフォーマンスの問題が発生した場合のソフトウェア操作に関する情報：ソフトウェアのインストール識別子、パフォーマンス低下の種別と値、ソフトウェア内のイベントの順序に関する情報（時間、タイムゾーン、種別、完了状況、ソフトウェアコンポーネント識別子、ソフトウェアの操作シナリオの識別子、TID、PID、関数呼び出しアドレス）、チェックするネットワーク接続に関する情報（URL、接続方向、ネットワークパッケージのサイズ）、PDB ファイルに関する情報（名前、識別子、実行可能ファイルのイメージサイズ）、チェックするファイルに関する情報（名前、完全パス、チェックサム）、ソフトウェアパフォーマンス監視パラメータ。

- 最新の OS の再起動の失敗に関する情報：OS をインストールしてから再起動に失敗した回数、システムダンプに関する情報（エラーのコードおよびパラメータ、OS の動作エラーの原因となったモジュールの名前、バージョンおよびチェックサム（CRC32）、モジュールのオフセットとしてのエラーのアドレス、システムダンプのチェックサム（MD5、SHA2-256、SHA1））。

- ファイルの署名に使用されるデジタル署名の信頼性を検証するための情報：証明書のフィンガープリント、チェックサムのアルゴリズム、証明書の公開鍵およびシリアル番号、証明書の発行者名、証明書の検証結果および証明書のデータベース識別子。

- 本ソフトウェアのセルフディフェンス機能への攻撃を実行したプロセスに関する情報：プロセスファイルの名前およびサイズ、チェックサム（MD5、SHA2-256、SHA1）、プロセルファイルへの完全パスおよびファイルパスのテンプレートコード、作成またはビルド時のタイムスタンプ、実行ファイルのフラグ、プロセスファイルの属性、プロセスファイルの署名に使用された証明書に関する情報、プロセスを実行したアカウントのコード、プロセスにアクセスするために実行した操作の識別子、操作の実行時に使用したリソースの種別（プロセス、ファイル、レジストリオブジェクト、FindWindow 検索関数）、操作の実行時に使用したリソースの名前、操作の成功を示すフラグ、プロセスのファイルのステータスおよび KSN に準拠した署名。

- 本ソフトウェアに関する情報：詳細バージョン、種別、ソフトウェアの言語および動作状況、インストールされた本ソフトウェア機能のバージョンおよびその動作状況、インストールされた本ソフトウェアのアップデートに関する情報、TARGET フィルターの値、権利者のサービスに接続するために使用されたプロトコルのバージョン。

- コンピューターにインストールされたハードウェアに関する情報：種別、名前、機種、ファームウェアのバージョン、搭載または接続されたデバイスのパラメータ、本ソフトウェアをインストールしたコンピューターの一意な識別子。

- オペレーティングシステムのバージョンおよびインストールされているアップデートに関する情報：ビットサイズ、エディションおよび OS 実行方法のパラメータ、OS カーネルファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、OS の起動日時。

- 実行ファイルおよび非実行ファイルの全体および一部。

- コンピューターの RAM の一部。

- OS 起動時に採用されるセクター。

- ネットワーク通信のデータパケット。

- 疑わしい、および悪意のあるオブジェクトを含む Web ページまたはメール。

- WMI リポジトリ上のクラスおよびそれらのインスタンスの記述。
- アプリケーション活動に関するレポート：
  - 送信されるファイルの名前、サイズおよびバージョン、説明およびチェックサム（MD5、SHA2-256、SHA1）、ファイル形式の識別子、ファイルの製造元の名前、ファイルが属するアプリケーションの名前、コンピューター上の完全パス、ファイルのパステンプレートコード、ファイルの作成日時および更新日時。
  - 証明書の有効期間の開始日時と終了日時（ファイルにデジタル署名がある場合）、署名適用の日時、証明書の発行者名、証明書の所有者に関する情報、証明書のフィンガープリント、公開鍵およびそれぞれの生成アルゴリズム、証明書のシリアル番号。
  - 実行中のプロセスを開始したアカウント名。
  - プロセスが実行されている端末名のチェックサム（MD5、SHA2-256、SHA1）。
  - プロセスウィンドウのタイトル。
  - 定義データベースの識別子、カスペルスキーの分類による検知された脅威の名前。
  - 使用中のライセンスに関するデータ、識別子、種別および有効期限。
  - 情報提供時点の端末のローカル時間。
  - プロセスがアクセスしたファイルの名前とパス。
  - プロセスがアクセスしたレジストリキーの名前および値。
  - プロセスがアクセスした URL および IP アドレス。
  - 実行ファイルのダウンロード元 URL および IP アドレス。

Detection and Response ソリューション使用中のデータ提供

Kaspersky Endpoint Security がインストールされたコンピューターでは、Kaspersky Endpoint Detection and Response、Kaspersky Sandbox、Kaspersky Anti Targeted Attack Platform への自動送信用に準備されたデータを保存しています。ファイルは、暗号化されていない平文でコンピューターに保存されます。

Kaspersky Endpoint Security が使用されるソリューションにより、データの内容は異なります。

Kaspersky Endpoint Detection and Response

コンピューターのローカルに保存されるすべてのデータは、Kaspersky Endpoint Security のアンインストール時にコンピューターから削除されます。

IOC スキャン タスクの実行結果として受け取ったデータ（標準タスク）

Kaspersky Endpoint Security は、*IOC スキャン タスク*の実行結果に関するデータを Kaspersky Security Center に自動で送信します。

*IOC スキャン タスク*の実行結果内のデータには、次の情報が含まれることがあります。

- ARP テーブルからの IP アドレス
- ARP テーブルからの物理アドレス
- DNS レコード種別および名前
- 保護対象コンピューターの IP アドレス
- 保護対象コンピューターの物理アドレス（MAC アドレス）
- イベントログエントリの識別子
- ログ内のデータソース名
- ログの名前
- イベントの日時
- ファイルの MD5 および SHA256 ハッシュ
- ファイルの詳細名（パスを含む）
- ファイルサイズ
- スキャン中に接続が確立されたリモート IP アドレスおよびポート
- ローカルアダプタの IP アドレス
- ローカルアダプタで開いていたポート
- 数値のプロトコル（IANA 規格に準拠したもの）
- プロセス名
- プロセス引数
- プロセスファイルのパス
- プロセスの Windows 識別子（PID）
- 親プロセスの Windows 識別子（PID）
- プロセスを開始したユーザーアカウント
- プロセスが開始された日時

- サービス名
- サービスの説明
- DLL サービス（svchost）のパスおよび名前
- サービス実行ファイルのパスおよび名前
- サービスの Windows 識別子（PID）
- サービス種別（例：カーネルドライバーまたはアダプタ）
- サービスステータス
- サービス開始モード
- ユーザーアカウント名。
- ボリュームの名前
- ボリュームの文字
- ボリューム種別
- Windows のレジストリ値
- レジストリのハイブ値
- レジストリキーのパス（ハイブ名、値の名前なし）
- レジストリ設定
- システム（環境）
- コンピューターにインストールされたオペレーティングシステムの名前およびバージョン
- 保護対象コンピューターのネットワーク名
- 保護対象コンピューターが属するドメインまたはグループ
- ブラウザー名
- ブラウザーのバージョン
- Web リソースに最後にアクセスした時間
- HTTP リクエストからの URL
- HTTP リクエストに使用されたアカウントの名前
- HTTP リクエストを作成したプロセスのファイル名
- HTTP リクエストを作成したプロセスのファイルの完全パス
- HTTP リクエストを作成したプロセスの Windows 識別子（PID）

- HTTP 参照元（HTTP リクエストのソース URL）
- HTTP で要求されたリソースの URI
- HTTP ユーザーエージェント（HTTP リクエストを作成したアプリケーション）に関する情報
- HTTP リクエストの実行時間
- HTTP リクエストを作成したプロセスの一意な識別子

脅威の活動連鎖の作成用データ

既定では、脅威の活動連鎖の作成用データは 7 日間保存されます。データ Kaspersky Security Center に自動的に送信されます。

脅威の活動連鎖の作成用データには次のデータが含まれることがあります：

- インシデントの日時
- 検知名
- スキャンモード
- 検知に関連する最終操作のステータス
- 検知処理が失敗した理由
- 検知されたオブジェクトの種別
- 検知されたオブジェクト名
- オブジェクトの処理後の脅威のステータス
- オブジェクトに対する操作の実行が失敗した理由
- 悪意のある操作をロールバックするために実行された操作
- 処理されたオブジェクトに関する情報：
  - プロセスの一意な識別子
  - 親プロセスの一意な識別子
  - プロセスファイルの一意な識別子
  - Windows プロセスの識別子（PID）
  - プロセスのコマンドライン
  - プロセスを開始したユーザーアカウント
  - プロセスが実行されているログオンセッションのコード

- プロセスが実行されているセッションの種別
- 処理中のプロセスの整合性レベル
- プロセスを開始したユーザーアカウントが権限のあるローカルおよびドメイングループに属しているかどうか
- 処理されたオブジェクトの識別子
- 処理されたオブジェクトの詳細名
- 保護対象端末の識別子
- オブジェクトの詳細名（ローカルファイル名またはダウンロードファイルの Web アドレス）
- 処理されたオブジェクトの MD5 または SHA256 ハッシュ
- 処理されたオブジェクトの種別
- 処理されたオブジェクトの作成日
- 処理されたオブジェクトの最終更新日
- 処理されたオブジェクトのサイズ
- 処理されたオブジェクトの属性
- 処理されたオブジェクトに署名した組織
- 処理されたオブジェクトのデジタル署名検証の結果
- 処理されたオブジェクトのセキュリティ識別子（SID）
- 処理されたオブジェクトのタイムゾーン識別子
- 処理されたオブジェクトがダウンロードされた Web アドレス（ディスク上のファイルのみ）
- ファイルをダウンロードしたアプリケーション名
- ファイルをダウンロードしたアプリケーションの MD5 および SHA256 ハッシュ
- ファイルを最後に変更したアプリケーション名
- ファイルを最後に変更したアプリケーションの MD5 および SHA256 ハッシュ
- 処理されたオブジェクトの開始数
- 処理されたオブジェクトが初めて開始された日時
- ファイルの一意な識別子
- ファイルの詳細名（ローカルファイル名またはダウンロードファイルの Web アドレス）
- 処理された Windows レジストリの変数のパス

- 処理された Windows レジストリの変数の名前
- 処理された Windows レジストリの変数の値
- 処理された Windows レジストリの変数の種別
- 自動実行ポイントにおける処理されたレジストリキーのメンバーシップを示すインジケーター
- 処理された Web リクエストの Web アドレス
- 処理された Web リクエストのリンク元
- 処理された Web リクエストのユーザーエージェント
- 処理された Web リクエストの種別（[GET] または [POST]）
- 処理された Web リクエストのローカル IP ポート
- 処理された Web リクエストのリモート IP ポート
- 処理された Web リクエストの接続方向（インバウンドまたはアウトバウンド）
- 悪意のあるコードが埋め込まれたプロセスの識別子

Kaspersky Sandbox

コンピューターのローカルに保存されるすべてのデータは、Kaspersky Endpoint Security のアンインストール時にコンピューターから削除されます。

サービスデータ

Kaspersky Endpoint Security は、自動応答中に処理される次のデータを保存します。

- 処理されたファイルと Kaspersky Endpoint Security の組み込みエージェントの設定中にユーザーにより入力されたデータ：
  - 隔離されたファイル
  - Kaspersky Sandbox との連携に使用された証明書の公的鍵
- Kaspersky Endpoint Security の組み込みエージェントのキャッシュ：
  - スキャン結果がキャッシュに書き込まれた時間
  - スキャンタスクの MD5 ハッシュ
  - スキャンタスクの識別子
  - オブジェクトのスキャン結果

- オブジェクトスキャン要求のキュー：
  - キュー内のオブジェクトの識別子
  - キュー内にオブジェクトが配置された時間
  - キュー内のオブジェクトの処理ステータス
  - オブジェクトのスキャンタスクが作成されたオペレーティングシステム内のユーザーセッションの識別子
  - タスクを作成するためにアカウントが使用されたオペレーティングシステムのユーザーのシステム識別子（SID）
  - オブジェクトのスキャンタスクの MD5 ハッシュ
- Kaspersky Sandbox からのスキャン結果を待っている Kaspersky Endpoint Security の組み込みエージェントのタスクに関する情報：
  - オブジェクトのスキャンタスクを受け取った時間
  - オブジェクトの処理ステータス
  - オブジェクトのスキャンタスクが作成されたオペレーティングシステム内のユーザーセッションの識別子
  - オブジェクトのスキャンタスクの識別子
  - オブジェクトのスキャンタスクの MD5 ハッシュ
  - タスクを作成するためにアカウントが使用されたオペレーティングシステムのユーザーのシステム識別子（SID）
  - 自動的に作成された IOC の XML スキーマ
  - スキャンされたオブジェクトの MD5 または SHA256 ハッシュ
  - 処理エラー
  - タスクが作成されたオブジェクトの名前
  - オブジェクトのスキャン結果

Kaspersky Sandbox へのリクエストのデータ

Kaspersky Endpoint Security の組み込みエージェントの要求から Kaspersky Sandbox への次のデータは、コンピューターのローカルに保存されます。

- スキャンタスクの MD5 ハッシュ
- スキャンタスクの識別子
- スキャンされたオブジェクトと関連するすべてのファイル

IOC スキャン タスクの実行結果として受け取ったデータ（スタンドアロンタスク）

Kaspersky Endpoint Security は、*IOC スキャン タスク*の実行結果に関するデータを Kaspersky Security Center に自動で送信します。

*IOC スキャン タスク*の実行結果内のデータには、次の情報が含まれることがあります。

- ARP テーブルからの IP アドレス
- ARP テーブルからの物理アドレス
- DNS レコード種別および名前
- 保護対象コンピューターの IP アドレス
- 保護対象コンピューターの物理アドレス（MAC アドレス）
- イベントログエントリの識別子
- ログ内のデータソース名
- ログの名前
- イベントの日時
- ファイルの MD5 および SHA256 ハッシュ
- ファイルの詳細名（パスを含む）
- ファイルサイズ
- スキャン中に接続が確立されたリモート IP アドレスおよびポート
- ローカルアダプタの IP アドレス
- ローカルアダプタで開いていたポート
- 数値のプロトコル（IANA 規格に準拠したもの）
- プロセス名
- プロセス引数
- プロセスファイルのパス
- プロセスの Windows 識別子（PID）
- 親プロセスの Windows 識別子（PID）
- プロセスを開始したユーザーアカウント
- プロセスが開始された日時

- サービス名
- サービスの説明
- DLL サービス（svchost）のパスおよび名前
- サービス実行ファイルのパスおよび名前
- サービスの Windows 識別子（PID）
- サービス種別（例：カーネルドライバーまたはアダプタ）
- サービスステータス
- サービス開始モード
- ユーザーアカウント名。
- ボリュームの名前
- ボリュームの文字
- ボリューム種別
- Windows のレジストリ値
- レジストリのハイブ値
- レジストリキーのパス（ハイブ名、値の名前なし）
- レジストリ設定
- システム（環境）
- コンピューターにインストールされたオペレーティングシステムの名前およびバージョン
- 保護対象コンピューターのネットワーク名
- 保護対象コンピューターが属するドメインまたはグループ
- ブラウザー名
- ブラウザーのバージョン
- Web リソースに最後にアクセスした時間
- HTTP リクエストからの URL
- HTTP リクエストに使用されたアカウントの名前
- HTTP リクエストを作成したプロセスのファイル名
- HTTP リクエストを作成したプロセスのファイルの完全パス
- HTTP リクエストを作成したプロセスの Windows 識別子（PID）

- HTTP 参照元（HTTP リクエストのソース URL）
- HTTP で要求されたリソースの URI
- HTTP ユーザーエージェント（HTTP リクエストを作成したアプリケーション）に関する情報
- HTTP リクエストの実行時間
- HTTP リクエストを作成したプロセスの一意な識別子

Kaspersky Anti Targeted Attack Platform (EDR)

コンピューターのローカルに保存されるすべてのデータは、Kaspersky Endpoint Security のアンインストール時にコンピューターから削除されます。

サービスデータ

Kaspersky Endpoint Security の組み込みエージェントは次のデータをローカルに保存します。

- 処理されたファイルと Kaspersky Endpoint Security の組み込みエージェントの設定中にユーザーにより入力されたデータ：
  - 隔離されたファイル
  - Kaspersky Endpoint Security の組み込みエージェントの設定：
    - Central Node との連携に使用された証明書の公的鍵
    - ライセンスデータ
- Central Node との連携に必要なデータ：
  - テレメトリイベントのパケットキュー
  - Central Node から受け取った IOC ファイルの識別子のキャッシュ
  - *Get file* タスクでサーバーに渡されるオブジェクト
  - *Get forensic* タスクの結果レポート

KATA (EDR) へのリクエスト内のデータ

Kaspersky Anti Targeted Attack Platform と連携するとき、次のデータがコンピューターのローカルに保存されます。

Kaspersky Endpoint Security の組み込みエージェントから Central Node コンポーネントへの要求データ：

- 同期リクエスト：
  - 一意な ID
  - サーバー Web アドレスの基本部分
  - コンピューター名
  - コンピューター IP アドレス
  - コンピューター MAC アドレス
  - コンピューターの時刻
  - Kaspersky Endpoint Security のセルフディフェンスのステータス
  - コンピューターにインストールされたオペレーティングシステムの名前およびバージョン
  - Kaspersky Endpoint Security のバージョン
  - 本製品の設定およびタスク設定のバージョン
  - タスクのステータス：タスクの識別子、実行ステータス、エラーコード
- サーバーからのファイル取得リクエスト：
  - ファイルの一意な識別子
  - Kaspersky Endpoint Security の一意な識別子
  - 証明書の一意な識別子
  - Central Node コンポーネントがインストールされたサーバーの Web アドレスの基本部分
  - ホスト IP アドレス
- タスク実行結果のレポート：
  - ホスト IP アドレス
  - IOC スキャンまたは YARA スキャン中に検知されたオブジェクトに関する情報
  - タスク完了時に実行された追加操作のフラグ
  - タスクの実行エラーとリターンコード
  - タスクの完了ステータス
  - タスクの完了時刻
  - タスクの実行に使用された設定のバージョン

- サーバーに送信されたオブジェクト、隔離されたオブジェクト、隔離から復元されたオブジェクトに関する情報：オブジェクトのパス、MD5 および SHA256 ハッシュ、隔離されたオブジェクトの識別子
- サーバーからの要求により、コンピューターで起動または停止したプロセスに関する情報：PID および UniquePID、エラーコード、オブジェクトの MD5 および SHA256 ハッシュ
- サーバーからの要求により、コンピューターで起動または停止したサービスに関する情報：サービス名、起動種別、エラーコード、サービスのファイルイメージの MD5 および SHA256 ハッシュ
- YARA スキャン用に作成されたメモリダンプのオブジェクトに関する情報（パス、ダンプファイルの識別子）
- サーバーにより要求されたファイル
- テレメトリパケット
- 実行中のプロセスのデータ：
  - 完全パスおよび拡張子を含む実行ファイル名
  - プロセスの自動実行パラメータ
  - プロセス識別子
  - ログインセッションの識別子
  - ログインセッション名
  - プロセスが開始された日時
  - オブジェクトの MD5 および SHA256 ハッシュ
- ファイルのデータ：
  - ファイルパス
  - ファイル名
  - ファイルサイズ
  - ファイルの属性
  - ファイルが作成された日時
  - ファイルの最終更新日時
  - ファイルの説明
  - 会社名
  - オブジェクトの MD5 および SHA256 ハッシュ
  - レジストリキー（自動実行ポイント）

- オブジェクトに関する情報を取得した際に発生したエラーのデータ：
  - エラーが発生した際に処理されていたオブジェクトの詳細名
  - エラーコード
- テレメトリデータ：
  - ホスト IP アドレス
  - 更新操作が確定される前のレジストリのデータ種別
  - 変更操作が確定される前のレジストリキー内のデータ
  - 処理されたスクリプト本文またはその一部
  - 処理されたオブジェクトの種別
  - コマンドインタープリターへのコマンドの渡し方

Central Node コンポーネントの要求から Kaspersky Endpoint Security の組み込みエージェントへのデータ：

- タスク設定：
  - タスク種別
  - タスクのスケジュール設定
  - タスクを実行するアカウントの名前およびパスワード
  - 設定のバージョン
  - 隔離されたオブジェクトの識別子
  - オブジェクトのパス
  - オブジェクトの MD5 および SHA256 ハッシュ
  - 引数で処理を開始するコマンドライン
  - タスク完了時に実行された追加操作のフラグ
  - サーバーから取得する IOC ファイル識別子
  - IOC ファイル
  - サービス名
  - サービス開始種別
  - *Get forensic* タスクの結果を受け取るフォルダー
  - *Get forensic* タスクのオブジェクト名および拡張子のマスク

- ネットワーク分離の設定：
  - 設定種別
  - 設定のバージョン
  - ネットワーク分離の除外リストと除外リストの設定のリスト：通信方向、IP アドレス、ポート、プロトコル、実行ファイルの完全パス
  - 追加操作のフラグ
  - 自動分離を無効化した時刻
- 実行防止の設定：
  - 設定種別
  - 設定のバージョン
  - 実行防止ルールおよびルール設定のリスト：オブジェクトのパス、オブジェクト種別、オブジェクトの MD5 および SHA256 ハッシュ
  - 追加操作のフラグ
- イベントフィルタリング設定：
  - モジュール名
  - オブジェクトの完全パス
  - オブジェクトの MD5 および SHA256 ハッシュ
  - Windows イベントログ内の項目の識別子
  - デジタル証明書の設定
  - 通信方向、IP アドレス、ポート、プロトコル、実行ファイルの完全パス
  - ユーザー名
  - ユーザーのログイン種別
  - フィルタが適用されたテレメトリイベントの種別

YARA スキャン結果

Kaspersky Endpoint Security は脅威の活動連鎖を作成するため、YARA スキャンタスクの実行結果に関するデータを Kaspersky Anti Targeted Attack Platform に自動で送信します。

Kaspersky Anti Targeted Attack Platform にタスクの実行結果を送信するため、データは一時的にローカルのキューに保存されます。データは送信後に一時保管領域から削除されます。

YARA スキャン結果には次のデータが含まれます：

- ファイルの MD5 および SHA256 ハッシュ
- ファイルの詳細名
- ファイルパス
- ファイルサイズ
- プロセス名
- プロセス引数
- プロセスファイルのパス
- プロセスの Windows 識別子（PID）
- 親プロセスの Windows 識別子（PID）
- プロセスを開始したユーザーアカウント
- プロセスが開始された日時

欧州連合の規則（GDPR）の順守

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

- Kaspersky Security Network を使用する
- アクティベーションコードで本製品をアクティベートする
- 製品機能と定義データベースをアップデートする
- 製品インターフェイス内のリンクを使用する

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

Kaspersky Endpoint Security を使用する前に、使用許諾契約書およびKaspersky Security Network に関する声明の転送されるデータの説明をよく読み、ご確認ください。説明されている方法で Kaspersky Endpoint Security から転送される特定のデータが、お客様の地域の法律または基準により個人データと分類される場合は、これらのデータは合法的に処理され、このようなデータの転送および収拾についてはお客様の同意のもと行われるものであることをお客様自身が保証する必要があります。

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

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

Kaspersky Security Network の使用

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

アクティベーションコードで本製品をアクティベートする

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

製品機能と定義データベースをアップデートする

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

製品インターフェイス内のリンクを使用する

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

ダンプ書き込み

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

使用開始時に行う設定

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

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

Kaspersky Security Center の管理コンソール

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

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

Kaspersky Security Center を使用した本製品の管理について詳しくは、Kaspersky Security Center ヘルプを参照してください。

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

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

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

Web コンソールと Cloud コンソールでは次の操作を実行できます：

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

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

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

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

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

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

Kaspersky Endpoint Detection and Response Optimum ソリューションの一部として Kaspersky Endpoint Security を使用している場合は、Kaspersky Endpoint Detection and Response 管理プラグインをインストールする必要があります。アラートの詳細を表示するには、管理プラグインが必要です。*アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。したがって、脅威の対応タスクを作成するには、Kaspersky Endpoint Security 管理プラグインが必要であり、アラートの詳細を表示するには、EDR 管理プラグインが必要です。

Web プラグインのインストール

Web プラグインをインストールするには、次の操作を実行します：

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

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

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

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

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

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

Kaspersky Endpoint Security 12.11 for Windows 以降では、Web プラグインのインストール手順が変更されました。配布パッケージには、*Kaspersky Endpoint Security for Windows 12.12.0* および *Unified Protection and Management Plug-in* の 2 つの Web プラグインが含まれるようになりました。これは、 カスペルスキー製品を管理するための単一の統合された Web プラグインへの移行によるものです。統合された Web プラグインを使用すると、単一のポリシーを作成して複数のカスペルスキー製品（Kaspersky Endpoint Security for Windows、macOS、Linux など）を管理できます。統合された Web プラグインへの移行には、複数のリリースが必要になる場合があります。移行が完了すると、配布パッケージには*Unified Protection and Management Plug-in*のみが含まれるようになります。

管理プラグインのアップデート

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

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

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

Web プラグインをアップデートするには、次の操作を実行します：

- Web プラグインのリストを使用して Web プラグインをアップデート（オンラインモードの場合）

  Web プラグインをアップデートするには、Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージを選択します（[**コンソールの設定**] → [**Web プラグイン**]）。Web コンソールは、Kaspersky サーバーで利用可能なアップデートを確認し、関連するアップデートをダウンロードします。

- ファイルから Web プラグインをアップデート

  Web プラグインをアップデートするには、Web コンソールのインターフェイスで、Kaspersky Endpoint Security の Web プラグインの配布パッケージの ZIP アーカイブファイルを選択する必要があります（[**コンソールの設定**] → [**Web プラグイン**]）。Web プラグインの配布パッケージは、たとえば Kaspersky Web サイトからダウンロードできます。Kaspersky Endpoint Security の Web プラグインは、より新しいバージョンの Web プラグインにのみアップデートできます。Web プラグインをバージョンの古い Web プラグインにアップデートすることはできません。

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

異なるバージョンの管理プラグインを使用する場合の留意点

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

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

管理コンソールに Kaspersky Endpoint Security の管理プラグインがインストールされていて、より新しいバージョンの管理プラグインをインストールする際には次の事項に留意してください：

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

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

本製品の新機能について詳しくは、リリースノートまたはヘルプ内のページを参照してください。

- 新しいバージョンの管理プラグインで既存の設定項目に新しく設定できるパラメータが追加された場合は、この設定項目でこれまでに指定されていた設定のロックの状態（ / ）は変更されません。

外部サービスと相互作用する暗号化プロトコルを使用する場合の留意点

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

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

TLS の使用は次の機能を提供することで本製品を保護します：

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

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

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

製品のインターフェイス



メインウィンドウ

監視	• **レポート**：本製品の動作中、個別の機能およびタスク中に発生したイベントを表示します。 • **バックアップ**：本製品が削除した感染ファイルのコピーのリストを表示します。 • **脅威検知技術**：脅威の検知技術およびこの技術により検知された脅威の数に関する情報を表示します。 • **Kaspersky Security Network**：Kaspersky Endpoint Security と Kaspersky Security Network との接続ステータスとグローバル KSN 統計です。*KSN（Kaspersky Security Network）*はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対する Kaspersky Endpoint Security の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。 • **アプリケーション動作モニター**：インストールされたアプリケーションの動作に関する情報を表示します。アプリケーション動作モニターは、アプリケーションと関連するファイル、レジストリ、オペレーティングシステムのイベントを追跡します。 • **ネットワークモニター**：リアルタイムでコンピューターのネットワークの動作に関する情報を表示します。 • **暗号化モニター**：リアルタイムでディスクの暗号化または復号化プロセスを確認します。暗号化モニターは、Kaspersky Disk Encryption または BitLocker Drive Encryption がインストールされている場合のみ利用可能です。
セキュリティ	インストールされた機能の動作ステータスです。機能の設定やレポートを表示することもできます。
アップデート	Kaspersky Endpoint Security のアップデートタスクを管理します。定義データベースと製品機能のアップデートおよび最新のアップデートのロールバックができます。管理者はセクションをユーザーに対して非表示にしたり、タスク管理を制限したりできます。
タスク	Kaspersky Endpoint Security のスキャンタスクを管理します。マルウェアのスキャンおよびアプリケーション整合性チェックを実行できます。管理者はユーザーに対してタスクを非表示にしたり、タスクの管理を制限したりできます。
ライセンス	製品のライセンスライセンスの購入、本製品のアクティベート、または定額制サービスの更新ができます。現在のライセンスに関する情報を表示することもできます。
⚙	本製品の設定：管理者はKaspersky Security Center の設定の変更を禁止することができます。

	本製品に関する情報：Kaspersky Endpoint Security の現在のバージョン、定義データベースの公開日、ライセンスおよびその他の情報です。製品の購入、インストール、製品の使用方法などについて役立つ情報、推奨事項、よくある質問に対する回答を提供するカスペルスキーの情報源を表示することも可能です。
	利用可能なアップデートや暗号化されたファイルやデバイスへのアクセスの要求に関する情報を含むメッセージです。

タスクバーの通知領域の製品アイコン

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

タスクバーの通知領域の製品アイコンが非表示になっている場合、管理者は、ポリシーで製品のインターフェイスの表示をオフにしています。

このアイコンは、次の目的で表示されます：

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

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

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

製品アイコンのコンテキストメニューには、次の項目があります：

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

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

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

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

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

- **設定**：本製品の設定ウィンドウが表示されます。

- **サポート**：カスペルスキーのテクニカルサポートへの問い合わせに必要な情報を確認できるウィンドウが表示されます。

- **製品情報**：この項目を指定すると、製品の詳細を確認できる情報ウィンドウが表示されます。

- **終了**：この項目を指定すると、Kaspersky Endpoint Security が終了します。コンテキストメニューでこの項目をクリックすると、コンピューターの RAM が解放されます。



製品アイコンのコンテキストメニュー

簡略化したアプリケーションインターフェイス

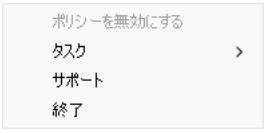
Kaspersky Endpoint Security がインストールされたクライアントコンピューターに対し、簡略化した製品インターフェイスを表示するよう設定された Kaspersky Security Center ポリシーが適用されている場合、そのクライアントコンピューターでは製品のメインウィンドウが使用できません。Kaspersky Endpoint Security のアイコン（以下の図を参照）を右クリックすると、次の項目を含むコンテキストメニューが表示されます：

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

- **タスク**：ドロップダウンリストの内容は次のとおりです：

  - **アプリケーション整合性チェック**
  - **以前の定義データベースのバージョンにロールバック**
  - **完全スキャン**
  - **オブジェクトスキャン**
  - **簡易スキャン**
  - **アップデート**

- **サポート**：カスペルスキーのテクニカルサポートへの問い合わせに必要な情報を確認できるウィンドウが表示されます。
- **終了**：この項目を指定すると、Kaspersky Endpoint Security が終了します。コンテキストメニューでこの項目をクリックすると、コンピューターの RAM が解放されます。



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

製品インターフェイスの表示の設定

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

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

管理コンソール（MMC）で製品インターフェイスの表示モードを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**インターフェイス**］の順に選択します。
4. ［**ユーザーインターフェイス**］ブロックで、次のいずれかを実行します：
   - 以下のインターフェイス要素をクライアントコンピューターに表示するには、［**ユーザーインターフェイスを表示する**］をオンにします。
     - ［**スタート**］メニュー内の製品名を含むフォルダー
     - Microsoft Windows タスクバーの通知領域にある Kaspersky Endpoint Security のアイコン
     - ポップアップ通知

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

- すべての Kaspersky Endpoint Security のインターフェイスをクライアントコンピューターで非表示にするには、［**ユーザーインターフェイスを表示する**］をオフにします。

5. Kaspersky Endpoint Security がインストールされたクライアントコンピューターで簡略化した製品インターフェイスを表示する場合は、［**ユーザーインターフェイス**］ブロックで［**簡略化したインターフェイスを表示する**］をオンにします。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**ユーザーへの可視性**］ブロックで、表示される製品のインターフェイスを設定します。

   - **製品アイコンを表示する**：クライアントコンピューターの通知領域にアプリケーションアイコンが表示されます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。
   - **ユーザーにアプリケーションインターフェイスを表示しない**：クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウにアクセスできなくなり、通知領域のアイコンだけが使用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の一定範囲に限定された操作を実行できます。製品アイコンの上の通知も表示されます。
6. 変更内容を保存します。

本製品の使用準備

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

- ポリシーを作成して設定する。

  ポリシーを使用して、同じ Kaspersky Endpoint Security 設定を管理グループ内のすべてのクライアントコンピューターに適用できます。Kaspersky Security Center のクイックスタートウィザードでは、Kaspersky Endpoint Security のポリシーが自動的に作成されます。
- ［*定義データベースと製品機能のアップデート*］タスクと［*マルウェアのスキャン*］タスクを作成する。

  ［*定義データベースと製品機能のアップデート*］タスクは、コンピューターのセキュリティを最新の状態に保つために必要です。このタスクを実行すると、Kaspersky Endpoint Security の定義データベースと製品機能がアップデートされます。*定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

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

管理コンソール（MMC）でマルウェアのスキャン タスクを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**マルウェアのスキャン**］の順に選択します。

ステップ 2：スキャン範囲

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

ステップ 3：Kaspersky Endpoint Security の処理

脅威の検知時の処理を選択します：

- **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。
- **駆除する。駆除できない場合は通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
- **通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。

- **すぐに特別な駆除を実行する**：チェックボックスがオンの場合、Kaspersky Endpoint Security は特別な駆除を使用してスキャン中にアクティブな脅威を処理します。

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

- **コンピューターを使用していないときにのみ実行する**：コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。

ステップ 4：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。

- *未割り当てデバイス*など、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。

- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

ステップ 5：タスクを実行するアカウントの選択

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

ステップ 6：タスク開始スケジュールの設定

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

ステップ 7：タスク名の定義

タスクの名前を入力します。たとえば、「*毎日の完全スキャン*」など。

ステップ 8：タスク作成の完了

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

Web コンソールでマルウェアのスキャンタスクを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**マルウェアのスキャン**］を選択します。
   c. ［**タスク名**］に「*週次のスキャン*」などの短く分かりやすい名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。
6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. タスクのスケジュールを設定するには、タスクのプロパティを開きます。
   週に 1 回以上の頻度でタスクが実行されるようにスケジュール設定することを推奨します。
8. タスクの横にあるチェックボックスをオンにします。
9. ［**開始**］をクリックします。
   タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。

設定が完了すると、指定したスケジュールに従ってユーザーのコンピューターでマルウェアのスキャンタスクが実行されるようになります。

- Kaspersky Endpoint Security のパフォーマンスを最適化する。

ポリシーの管理

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

各ポリシーの設定には（「南京錠」）属性があります。この属性の状態によって、設定が管理グループ内の管理対象デバイスに渡されるかどうかが決まります：

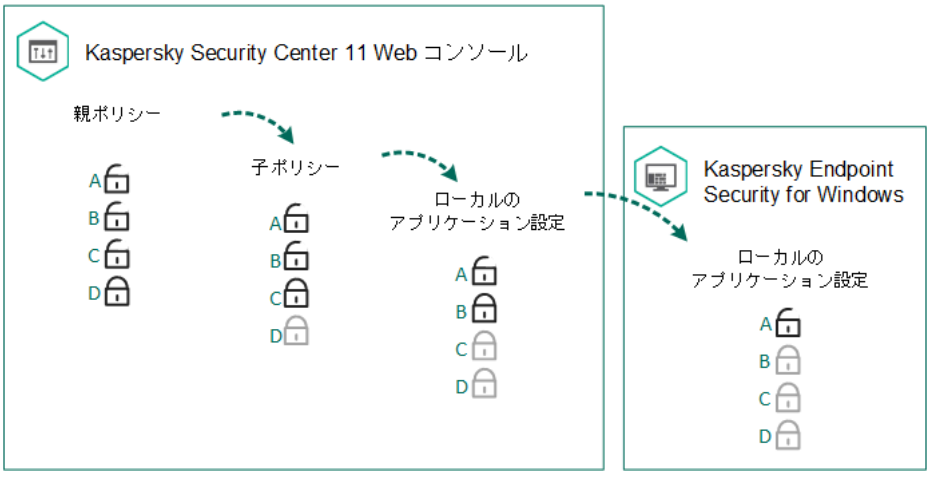
- 「南京錠」が開いている場合（）、この設定の値は管理対象デバイスには渡されません。設定は、本製品のローカルインターフェイスで変更できます。このような設定は、*ロック解除済み*と呼ばれます。
- 「南京錠」が閉じている場合（）、この設定の値は、管理対象デバイスに渡され、適用されます。このような設定は、*ロック済み*と呼ばれます。ブロックされた設定は、本製品のローカルインターフェイスでは変更できません。

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

設定の継承

管理者グループのようなポリシーは、階層構造になっています。*子ポリシー*は、階層レベルで下位のポリシーで、下位の管理グループまたはセカンダリ管理サーバーに割り当てられているポリシーです。

既定では、子ポリシーは親ポリシーの設定を継承します。親ポリシーの設定に（閉じた「南京錠」）属性があり、子ポリシーとローカル環境用の製品設定がある場合、親ポリシーに従ってその設定の値が上書きされて、設定がロックされます。必要に応じて、親ポリシーからの設定の継承を無効にすることができます。モバイルユーザーポリシーは、管理グループの階層でその他のポリシーに影響を及ぼしません。



設定の継承

ポリシー設定にアクセスする権限（読み取り、書き込み、実行）は、Kaspersky Security Center 管理サーバーへのアクセス権を持つ各ユーザーに対して指定され、さらに Kaspersky Endpoint Security の各機能の範囲に対して個別に指定されます。ポリシー設定へのアクセス権限を設定するには、Kaspersky Security Center 管理サーバーのプロパティウィンドウの［**セキュリティ**］セクションに移動します（既定では、このセクションはコンソールインターフェイスに表示されません）。

ポリシーの作成

ポリシーを作成する際に、選択されたモードに関連する設定がウィザードから提案されます。たとえば、Light Agent モードの場合は、Protection Server (SVM) を追加する必要があります。SQL サーバーを保護するために本製品を使用する場合は、サーバーの動作が妨げられないように、設定済みの信頼するオブジェクトを追加する必要があります。モードを選択すると、関連するポリシー設定がウィザードで提案されます。その後、ポリシーのプロパティでこれらの設定を編集できます。

管理コンソール（MMC）でポリシーを作成する方法

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

ステップ 1：グループポリシーを作成するにアプリケーションの選択

Kaspersky Endpoint Security for Windows (12.12) のアプリケーションを選択します。

ステップ 2：グループポリシー名の入力

グループポリシーの名前を入力します（「*オフィスのポリシー*」など）。

新規ポリシーウィザードを使用して、既存のポリシーに基づいて新しいポリシーを作成することもできます。これを行うには、グループポリシー名を指定する際に、［**旧バージョンのアプリケーションのポリシー設定を使用する**］チェックボックスをオンにします。このウィザードでは、Kaspersky Security for Windows Server（KSWS）や Kaspersky Security for Virtualization Light Agent for Windows などの別のソリューションのポリシーに基づいて、Kaspersky Endpoint Security（KES）ポリシーを作成することもできます。

ステップ 3：Kaspersky Security Network への参加

Kaspersky Security Network（KSN）に関する声明の内容を確認し、同意するかどうかを選択します。

ステップ 4：コンピューターでのアプリケーション使用モードの選択

Kaspersky Endpoint Security の使用目的に応じて、Kaspersky Endpoint Security はをさまざまなモードで導入できます。

- 標準モード

  このモードを選択した場合は、ウィザードの実行中に基本的なポリシー設定を指定できます。設定ファイルから基本的なポリシー設定をインポートすることもできます。

- Endpoint Detection and Response Agent

  このモードを選択した場合は、既定の設定のみでポリシーを作成できます。EDR Agent を設定するには、ウィザードが完了した後でポリシーのプロパティに移動する必要があります。

- 仮想環境を保護する Light Agent

  このモードを選択した場合は、次の手順で、Protection Server（SVM）への接続を設定する必要があります。本製品を Light Agent モードで動作させるには、これらの設定が必要です。

Kaspersky Endpoint Security は、すべての製品モードと OS の種別に対して共通のポリシーを提供します。つまり、ポリシーはすべての設定をカバーすることになります。ただし、一部の機能を使用できないモードで Kaspersky Endpoint Security が導入されているため、本製品で一部のポリシー設定が無視される場合があります。たとえば、Endpoint Detection and Response Agent モードで本製品を使用する場合、Kaspersky Detection and Response ソリューションとの連携と KUMA との連携に関連する設定しか使用できません。

さまざまなモードやオペレーティングシステムの種類に応じて異なるポリシーを使用することを推奨します。

ステップ 5：信頼ゾーンの設定

信頼ゾーンを設定します。設定済みの信頼するオブジェクトとアプリケーションを追加できます。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Light Agent モードの Kaspersky Endpoint Security を迅速に設定することもできます。

ステップ 6：ポリシーステータスの選択

- **アクティブ**：次の同期の実行後、このポリシーがクライアントコンピューター上でアクティブなポリシーとして使用されます。

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

- **非アクティブ**：バックアップ用のポリシーです。必要に応じて、非アクティブなポリシーのステータスをアクティブに変更できます。

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

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

ウィザードを終了します。

Web コンソールと Cloud コンソールでポリシーを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. ［**追加**］をクリックします。

   ポリシーウィザードが起動します。

3. Kaspersky Endpoint Security for Windows を選択し、［**次へ**］をクリックします。

4. Kaspersky Security Network（KSN）に関する声明の内容を確認し、同意するかどうかを選択して［**次へ**］をクリックします。

5. 製品のモードを選択します：

   - ワークステーションとサーバーを保護する標準モード

   - 先進の脅威や標的型攻撃から保護する Endpoint Detection and Response Agent

     このモードを選択した場合は、コンピューターと Kaspersky Detection and Response ソリューションを連携させるポリシーを作成できます。このウィザードでは、Kaspersky Managed Detection and Response との連携を設定してから、Kaspersky Anti Targeted Attack Platform（EDR）との連携を設定するよう要求されます。

   - 仮想環境を保護する Light Agent

     このモードを選択した場合は、次の手順で、Protection Server（SVM）への接続を設定する必要があります。本製品を Light Agent モードで動作させるには、これらの設定が必要です。

   Kaspersky Endpoint Security は、すべての製品モードと OS の種別に対して共通のポリシーを提供します。つまり、ポリシーはすべての設定をカバーすることになります。ただし、一部の機能を使用できないモードで Kaspersky Endpoint Security が導入されているため、本製品で一部のポリシー設定が無視される場合があります。たとえば、Endpoint Detection and Response Agent モードで本製品を使用する場合、Kaspersky Detection and Response ソリューションとの連携と KUMA との連携に関連する設定しか使用できません。

さまざまなモードやオペレーティングシステムの種類に応じて異なるポリシーを使用することを推奨します。

6. 信頼ゾーンを設定します。設定済みの信頼するオブジェクトとアプリケーションを追加できます。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Light Agent モードの Kaspersky Endpoint Security を迅速に設定することもできます。

7. ［**全般**］タブで次の操作を実行できます：

   - ポリシー名の変更
   - ポリシーのステータスの選択：
     - **アクティブ**：次の同期の実行後、このポリシーがクライアントコンピューター上でアクティブなポリシーとして使用されます。

       アクティブなポリシーの設定は、同期中にクライアントコンピューターに保存されます。1台のコンピューターに複数のポリシーを同時に適用することはできません。各管理グループでアクティブにできるポリシーは1つの製品につき1つのみです。
     - **非アクティブ**：バックアップ用のポリシーです。必要に応じて、非アクティブなポリシーのステータスをアクティブに変更できます。

       非アクティブポリシーは個数の制限なく作成できます。非アクティブポリシーは、ネットワーク内のコンピューターの製品設定に影響を及ぼしません。非アクティブポリシーは、ウイルス攻撃などの非常時に設定を切り替える準備を行う目的で使用されます。たとえば、フラッシュドライブを使用した攻撃が発生した場合、フラッシュドライブへのアクセスをブロックするポリシーをアクティブにできます。この場合、それまでアクティブだったポリシーは自動的に非アクティブになります。
     - **モバイルユーザー**：このポリシーは、コンピューターが組織ネットワーク外に出た場合に有効になります。
   - 設定の継承設定：
     - **親ポリシーから設定を継承する**：このスイッチをオンにすると、上位のポリシーからポリシーの設定値が継承されます。親ポリシーで🔒が指定されている設定は子ポリシーで変更できません。
     - **設定を子ポリシーへ強制的に継承させる**：このオプションがオンの場合、ポリシー設定の値が子ポリシーに反映されます。子ポリシーのプロパティで、［**親ポリシーから設定を継承する**］は自動的にオンになり、オフにすることはできません。設定のステータスが🔓以外の設定は親ポリシーから子ポリシーに設定が継承されます。親ポリシーで🔒ステータスが設定された子ポリシーは編集できません。

8. ［**アプリケーション設定**］タブで、Kaspersky Endpoint Security のポリシー設定を編集できます。

9. ウィザードを終了します。

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

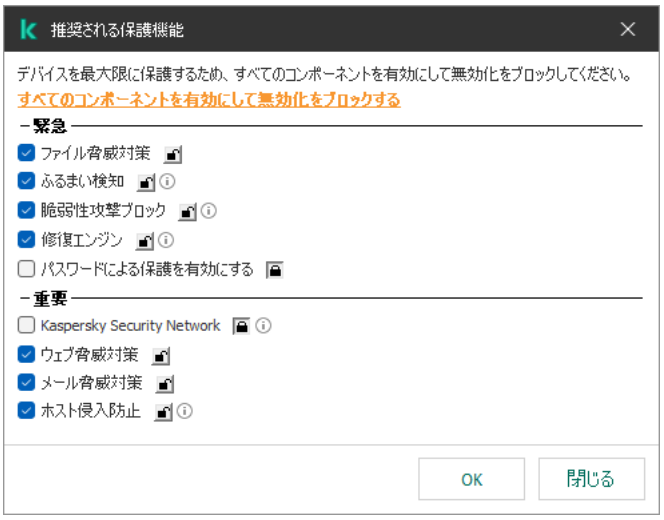
セキュリティレベルインジケーター

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

- **保護レベル：高**：以下のカテゴリのすべての保護機能が有効になっている場合、インジケーターがこの値で緑色になります。
  - **緊急**：このカテゴリには以下のコンポーネントが含まれます：
    - ファイル脅威対策
    - ふるまい検知
    - 脆弱性攻撃ブロック
    - 修復エンジン
    - 外部からの管理に対するアプリケーションサービスの保護
  - **重要**：このカテゴリには以下のコンポーネントが含まれます：
    - Kaspersky Security Network
    - ウェブ脅威対策
    - メール脅威対策
    - ホスト侵入防止
    - パスワードによる保護
- **保護レベル：中**：「重要」コンポーネントのいずれかが無効になっている場合、インジケーターがこの値で黄色になります。
- **保護レベル：低**：以下のいずれかの場合、インジケーターがこの値で赤になります：
  - 「緊急」コンポーネントのいずれかが無効になっている場合
  - 2 つ以上の「重要」コンポーネントが無効になっている場合

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

本製品をアップグレードすると、保護レベルのインジケーターで、アップグレード前よりも低い保護レベルが示される場合があります。これは、本製品の新しいバージョンで、コンピューターのセキュリティにとって重要な新しいコンポーネントまたは機能が導入されたことにより発生します。本製品をアップグレードした後は、保護レベルを高く維持するために新しい設定を管理する必要があります。



ポリシーのセキュリティレベルインジケーター

タスクの管理

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

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

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

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

- **マルウェアのスキャン**：タスク設定で指定したコンピューターの領域でウイルスやその他の脅威をスキャンします。Kaspersky Endpoint Security による保護が適切に機能するには、［マルウェアのスキャン］タスクが必要となります。このタスクはクイックスタートウィザードで作成されます。週に1回以上の頻度でタスクが実行されるようにスケジュール設定することを推奨します。
- **ライセンスの追加**：このタスクの実行時に、製品をアクティベートするライセンス（予備のライセンスを含む）が追加されます。タスクを実行する前に、タスクの実行対象となるコンピューターの台数がライセンスで利用が許可されるコンピューターの台数を超過しないことを確認してください。
- **コンポーネントの変更**：タスクの設定で指定されたコンポーネントのリストに従って、コンポーネントをインストールまたは削除します。ファイル脅威対策は削除できません。Kaspersky Endpoint Security のコンポーネントの最適な組み合わせを使用することで、コンピューターのリソース消費量を抑制できます。
- **インベントリ**：コンピューターに保管されているすべてのアプリケーションの実行ファイルに関する情報が取得されます。［インベントリ］タスクは、アプリケーションコントロール機能によって実行されます。アプリケーションコントロール機能がインストールされていない場合、このタスクはエラーにより失敗します。

- **定義データベースと製品機能のアップデート**：定義データベースおよび製品機能をアップデートします。Kaspersky Endpoint Security による保護が適切に機能するには、［*定義データベースと製品機能のアップデート*］タスクが必要となります。このタスクはクイックスタートウィザードで作成されます。1日に1回以上の頻度でタスクが実行されるようにスケジュール設定することを推奨します。

- **データの消去**：Kaspersky Endpoint Security は、指定した設定に応じて、即座にまたは Kaspersky Security Center への接続が長期間行われなかったときにユーザーのコンピューターのファイルとフォルダーを削除します。

- **アップデートのロールバック**：前回アップデートした定義データベースと製品機能を元に戻します。このタスクは、新しい定義データベースに、安全なアプリケーションのブロックにつながる可能性のある不正確なデータが含まれてしまっていた場合などに必要です。

- **アプリケーション整合性チェック**：Kaspersky Endpoint Security が、アプリケーションファイルを分析し、ファイルに破損や変更がないかと、アプリケーションファイルのデジタル署名を検証します。

- **認証エージェントアカウントの管理**：Kaspersky Endpoint Security は、認証エージェントのアカウントを設定します。暗号化されたドライブを操作するには、認証エージェントが必要です。オペレーティングシステムを読み込む前に、ユーザーはエージェントで認証を完了する必要があります。

本製品がカスペルスキーの Endpoint Detection and Response ソリューションの一部として機能している場合、検出・応答の処理として追加のタスクを実行できます（responses）。たとえば、*プロセスの終了*タスクを使用してリモートからプロセスを終了することができます。

タスクは、コンピューター上で Kaspersky Endpoint Security が起動され動作中の場合にのみ実行されます。

タスクの作成

管理コンソール（MMC）でタスクを作成する方法

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

Web コンソールと Cloud コンソールでタスクを作成する方法

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

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］ドロップダウンリストで、クライアントコンピューター上で実行するタスクを選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。

5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。

6. ウィザードを終了します。

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

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

タスクのアクセスの管理

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

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

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

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**ローカルタスク**］→［**タスク管理**］の順に選択します。

4. タスク管理モードを設定します（下記の表を参照）。

5. 変更内容を保存します。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**許可される操作**］で、タスク管理モードを設定します（下記の表を参照）。
6. 変更内容を保存します。

タスク管理の設定

パラメータ	説明
ローカルタスクへのアクセス	このチェックボックスをオンにすると、ローカルタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。その他のポリシー制限がない場合、ユーザーはタスクの設定と実行ができます。ただし、ユーザーはタスク実行スケジュールを設定することはできません。ユーザーはタスクを手動でのみ実行できます。 チェックボックスをオフにすると、ローカルタスクの使用を停止します。このモードでは、スケジュールにのっとったローカルタスクの実行は行われません。Kaspersky Endpoint Security のローカルインターフェイスでタスクの開始や設定ができなくなります。また、コマンドラインの使用時にもタスクの開始や設定ができなくなります。 ファイルまたはフォルダーのスキャンについては、スキャンするファイルまたはフォルダーのコンテキストメニューから［**スキャン**］を選択すれば開始できます。オブジェクトスキャンタスクの既定の設定値で、スキャンタスクが開始します。
グループタスクを表示する	このチェックボックスをオンにすると、グループタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。ユーザーは製品インターフェイスでタスクのリストを表示できます。 このチェックボックスをオフにすると、空白のタスクリストを表示します。
グループタスクを管理する	このチェックボックスをオンにすると、Kaspersky Security Center コンソール内で指定されたグループタスクを開始および停止できます。ユーザーは製品インターフェイスまたは簡略化した製品インターフェイスでタスクを開始および停止できます。 このチェックボックスをオフにすると、Kaspersky Security Center コンソールがスケジュールされたタスクを自動的に開始するか、管理者が Kaspersky Security Center で手動でタスクを開始します。

個別のローカル環境用の製品設定

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

管理コンソール（MMC）で個別のローカル環境用の製品設定を設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**デバイス**］タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。

6. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Endpoint Security for Windows (12.12)**］を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。

7. ［**全般設定**］セクションで、Kaspersky Endpoint Security の設定値およびレポートや保管領域の設定値を指定します。

   アプリケーションのプロパティウィンドウの残りのセクションは、Kaspersky Security Center の標準と同じです。これらのセクションの説明については、Kaspersky Security Center のオンラインヘルプを参照してください。

   > 特定の設定に対する変更をブロックするポリシーがアプリケーションに適用される場合、それらの設定は、［**全般設定**］セクションでのアプリケーション設定時には編集できません。

8. 変更内容を保存します。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ローカル環境用の製品設定を行うコンピューターを選択します。

   コンピューターのプロパティが表示されます。

3. ［**アプリケーション**］タブを選択します。

4. **Kaspersky Endpoint Security for Windows** をクリックします。

   ローカルアプリケーション設定が表示されます。

5. ［**アプリケーション設定**］タブを選択します。

6. ローカルアプリケーション設定を編集します。

7. 変更内容を保存します。

ローカルアプリケーション設定の項目は暗号化の設定を除いてポリシー設定と同一です。

Kaspersky Endpoint Security の起動と終了

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

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

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

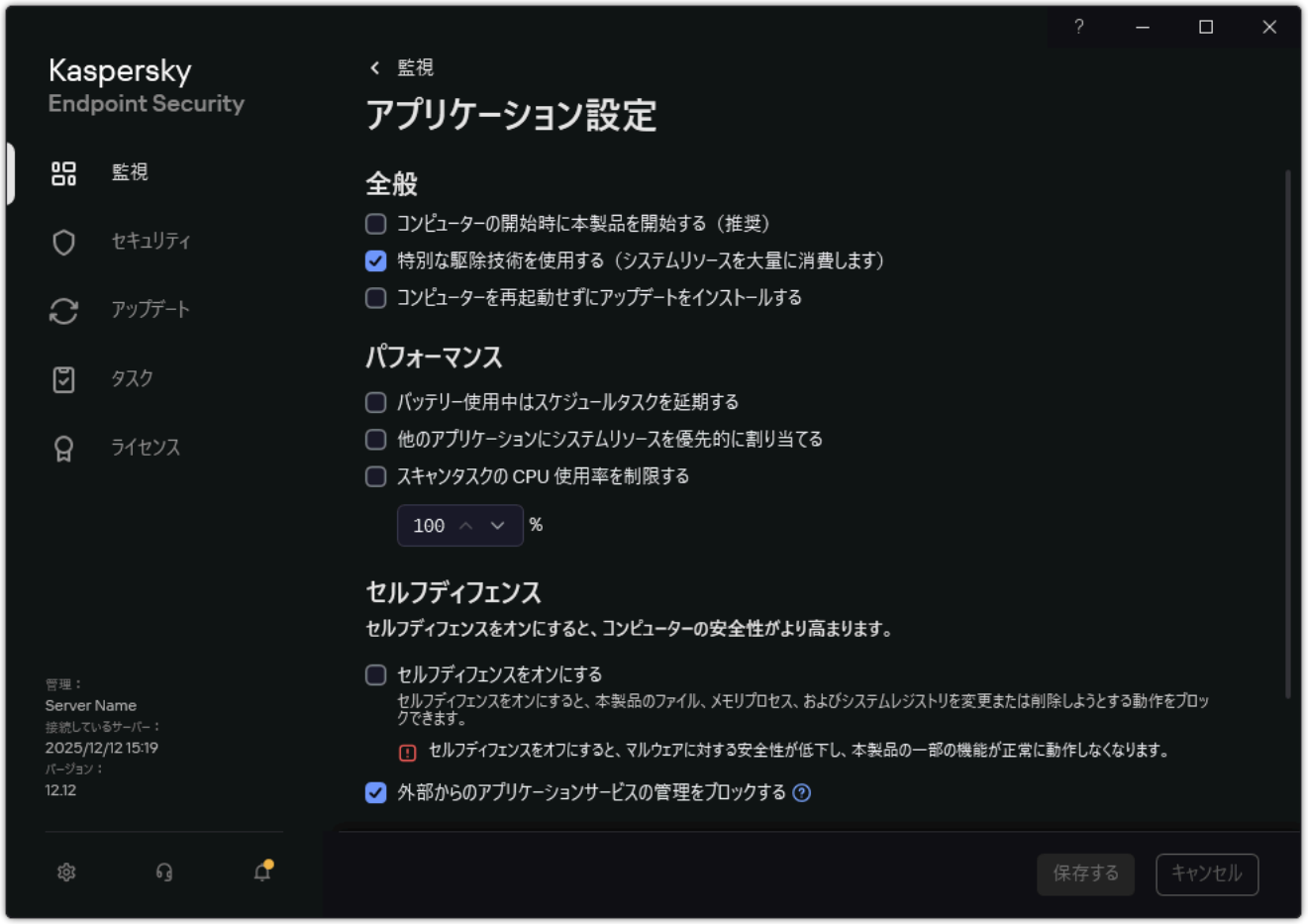
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. 製品の自動起動を設定するには、［**コンピューターの開始時に本製品を開始する（推奨）**］をオンにします。
5. 変更内容を保存します。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. 製品の自動起動を設定するには、［**コンピューターの開始時に Kaspersky Endpoint Security を開始する（推奨）**］をオンにします。
6. 変更内容を保存します。

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

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. 製品の自動起動を設定するには、［**コンピューターの開始時に本製品を開始する（推奨）**］をオンにします。
4. 変更内容を保存します。

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

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

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

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**デバイス**］タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。

5. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。

6. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Endpoint Security for Windows (12.12)**］を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。

7. 次のいずれかの手順を実行します：

   - 本製品を起動するには、カスペルスキー製品リストの右側にある ボタンをクリックします。
   - 本製品を停止するには、カスペルスキー製品リストの右側にある ボタンをクリックします。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. 本製品を起動または停止するコンピューターを選択します。
   コンピューターのプロパティウィンドウが開きます。

3. ［**アプリケーション**］タブを選択します。

4. **Kaspersky Endpoint Security for Windows** のチェックボックスを選択します。

5. ［**開始**］または［**停止**］をクリックします。

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

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。

2. klpsm.exe の実行ファイルがあるフォルダーに移動します。

3. コマンドラインから製品を起動するには、「`klpsm.exe start_avp_service`」と入力します。

4. コマンドラインから製品を停止するには、「`klpsm.exe stop_avp_service`」と入力します。

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



コマンドラインからの製品の開始または停止

プロテクションとコントロールの一時停止と再開

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

製品のステータスは、タスクバーの通知領域の製品アイコンによって示されます。

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

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

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

プロテクションとコントロールを一時停止するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューから［**保護機能の一時停止**］を選択します（下の図を参照）。
   コンテキストメニューのこの項目は、パスワードによる保護が有効な場合に選択できます。
3. 次のいずれかのオプションを選択します：
   - **指定時間経過後に再開**：プロテクションとコントロールは、下部のドロップダウンリストで指定した時間が経過すると再開されます。
   - **本製品の再起動後に再開**：プロテクションとコントロールは、製品を終了して再開したとき、またはオペレーティングシステムを再起動したときに再開されます。このオプションを使用するには、自動起動を有効にする必要があります。
   - **一時停止**：プロテクションとコントロールは、再び有効にしたときに再開されます。
4. ［**保護機能の一時停止**］をクリックします。

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



製品アイコンのコンテキストメニュー

プロテクションとコントロールを再開するには：

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

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

設定ファイルの作成と使用

Kaspersky Endpoint Security の設定を含む設定ファイルを使用すると、次の作業を実行できます：

- 定義済みの設定を使用してコマンドラインから Kaspersky Endpoint Security のローカルインストールを実行する。
- 定義済みの設定を使用して Kaspersky Security Center から Kaspersky Endpoint Security のリモートインストールを実行する。
- Kaspersky Endpoint Security の設定を別のコンピューターに移行する（以下の手順を参照してください）。

設定ファイルのエクスポート

設定ファイルを作成するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**設定の管理**］を選択します。
3. ［**エクスポート**］をクリックします。
4. 表示されたウィンドウで、設定ファイルを保存するパスを指定し、ファイル名を入力します。

   設定ファイルを Kaspersky Endpoint Security のローカルインストールまたはリモートインストールに使用するには、ファイル名を install.cfg にします。

5. 必要に応じて、製品設定をファイルにエクスポートするためのパスワードを入力します。

   設定情報ファイルを保存するには、パスワード保護を有効にする必要があります。ユーザーには「**設定のエクスポート**」操作を実行する権限が付与されている必要があります。

6. ファイルを保存します。

その結果、本製品は設定情報ファイルを作成します。設定情報ファイルにはユーザーアカウントの詳細が含まれている場合があるため、Kaspersky Endpoint Security はファイルを暗号化します。設定情報ファイルを編集することはできません。設定情報ファイルを変更しようとすると、ファイルが破損してしまいます。

設定ファイルのインポート

設定情報ファイルには、本製品に追加されたユーザーアカウントの詳細が含まれる場合があります。ファイルが作成されたのと同じコンピューターにファイルをインポートする場合、Kaspersky Endpoint Security はユーザーアカウントのパスワードをインポートします。別のコンピューターにファイルをインポートする場合は、パスワードを手動で入力する必要があります。

Kaspersky Endpoint Security の設定を設定ファイルから読み込むには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**設定の管理**］を選択します。
3. ［**インポート**］をクリックします。
4. 表示されたウィンドウで、設定ファイルのパスを入力します。
5. ファイルを開きます。

Kaspersky Endpoint Security のすべての設定値が、選択された設定ファイルに従って設定されます。



製品設定の管理

既定の設定の復元

カスペルスキーが推奨する製品設定はいつでも復元することができます。この設定が復元されると、すべての保護機能のセキュリティレベルが［**推奨**］に設定されます。

既定の設定を復元するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**設定の管理**］を選択します。

3. ［**復元**］をクリックします。

4. 変更内容を保存します。



製品設定の管理

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

Kaspersky Endpoint Security のパフォーマンスは、電力の消費量やコンピューターリソースの使用率だけでなく、コンピューターに損害を与える可能性があるオブジェクトのうち、どの種別のオブジェクトを検知対象に含めるかにも影響されます。

検知可能なオブジェクトの選択

Kaspersky Endpoint Security では、コンピューターで実行する保護機能の内容を詳細に調整し、動作中に検知するオブジェクトの種別を選択できます。Kaspersky Endpoint Security は必ずオペレーティングシステムのウイルス、ワーム、トロイの木馬をスキャンします。これらのオブジェクト種別のスキャンを無効にすることはできません。このようなマルウェアはコンピューターに重大な損害を与える可能性があります。コンピューターのセキュリティをさらに強化する場合は、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアの監視を有効にして、検知できるオブジェクト種別の範囲を拡大できます。

省エネモードの使用

アプリケーションの電力使用量は、ノートパソコンにとって重要な考慮事項です。Kaspersky Endpoint Security のスケジュールタスクは、通常、大量のリソースを消費します。コンピューターがバッテリー電源で稼働しているときには、省エネモードを使用することで、電力消費量を抑えることができます。

省エネモードでは、次のスケジュールされているタスクが自動的に延期されます：

- アップデートタスク
- 完全スキャンタスク
- 簡易スキャンタスク
- オブジェクトスキャンタスク
- 整合性チェックタスク

省エネモードが有効になっているかどうかとは関係なく、ノートパソコンの電源がバッテリー電源に切り替わると、Kaspersky Endpoint Security は暗号化タスクを一時停止します。ノートパソコンがバッテリー電源から主電源に切り替わると、暗号化タスクが再開されます。

他のアプリケーションに対するコンピューターリソースの優先割り当て

コンピューターをスキャンする際にコンピューターのリソースが消費されるため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。CPU およびハードディスクサブシステムの負荷が増大しているときに複数のアプリケーションが同時に動作することで発生する問題を解決するために、Kaspersky Endpoint Security は、他のアプリケーションにシステムリソースを優先的に割り当てることができます。

特別な駆除技術の使用

最近の悪意のあるアプリケーションは、オペレーティングシステムの最も深いレベルに侵入できるため、除去は、ほとんど不可能です。Kaspersky Endpoint Security はオペレーティングシステムで悪意のある活動を検知した後、特別な駆除技術を使用した広範囲な駆除処理を実行します。この*特別な駆除技術*の目的は、RAM 内部でそのプロセスを既に開始している悪意のあるプログラムをオペレーティングシステムから除去して Kaspersky Endpoint Security が他の方法でそれらのアプリケーションを除去しないようにすることです。その結果、脅威が駆除されます。特別な駆除を実行している間は、新しいプロセスの起動やオペレーティングシステムレジストリの修正を行わないように指示されます。特別な駆除には大量のオペレーティングシステムリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。

クライアントコンピューター用 Microsoft Windows が実行されているコンピューターで、特別な駆除処理が完了した後、Kaspersky Endpoint Security は、ユーザーにコンピューターを再起動する許可を求めます。システムの再起動後、Kaspersky Endpoint Security はマルウェアファイルを削除し、コンピューターで「簡易版」の完全スキャンを開始します。

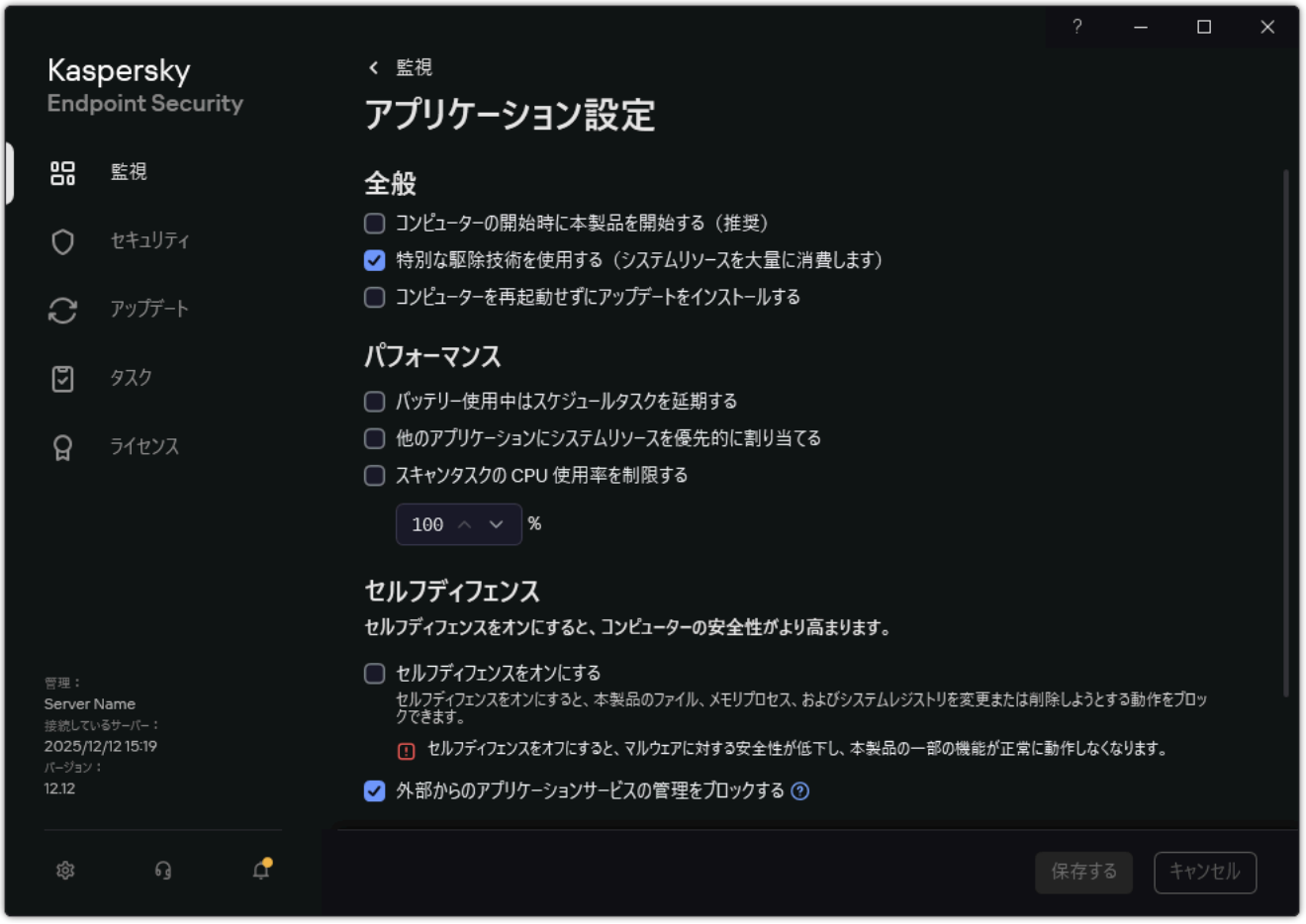
Kaspersky Endpoint Security の特性のため、サーバー用の Microsoft Windows が実行されているコンピューターではユーザーに再起動を実行してよいか確認メッセージを表示してから再起動することはできません。サーバーの予定外の再起動が問題を引き起こし、サーバーのデータが一時的に使用できなくなったり、保存されていないデータが失われたりする原因となることがあります。サーバーの再起動は、スケジュールに厳密に従ってください。この理由で、サーバーでは特別な駆除技術が既定で無効になっています。

サーバーでアクティブな感染が検知された場合、特別な駆除が必要であるという情報とともにイベントが Kaspersky Security Center へ送信されます。サーバーのアクティブな感染を駆除するには、サーバーの特別な駆除技術を有効化し、サーバーユーザーの都合のよい時間に、マルウェアのスキャングループタスクを開始します。

省エネモードの有効化または無効化

省エネモードを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**パフォーマンス**］ブロックで、［**バッテリー使用中はスケジュールタスクを延期する**］を使用して省エネモードを有効または無効にします。

   省エネモードが有効のときは、コンピューターがバッテリーの電力で動作している場合、以下のタスクがスケジュールされていても実行されません。

   - *定義データベースと製品機能のアップデート*
   - *完全スキャン*

- *簡易スキャン*
- *オブジェクトスキャン*
- *アプリケーション整合性チェック*
- *IOC スキャン*

4. 変更内容を保存します。

他のアプリケーションへのリソースの供与の有効化または無効化

Kaspersky Endpoint Security がコンピューターをスキャンする際にコンピューターのリソースを消費するため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。これにより、他のアプリケーションの動作が遅くなることがあります。パフォーマンスを最適化するために、Kaspersky Endpoint Security には、*他のアプリケーションにリソースを振り分けるモード*が用意されています。このモードでは、CPU の負荷が高い場合に、オペレーティングシステムが Kaspersky Endpoint Security のスキャンタスクスレッドの優先度を下げることができます。これにより、オペレーティングシステムのリソースを他のアプリケーションに再分配することが可能になり、スキャンタスクの CPU 時間が減ります。その結果、Kaspersky Endpoint Security のスキャンに時間がかかるようになります。既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。

管理コンソール（MMC）で他のアプリケーションへのシステムリソースの優先的な割り当てを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. ［**パフォーマンス**］ブロックで、［**他のアプリケーションにシステムリソースを優先的に割り当てる**］を使用して他のアプリケーションへのリソースの供与を有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで他のアプリケーションへのシステムリソースの優先的な割り当てを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**パフォーマンス**］に移動します。

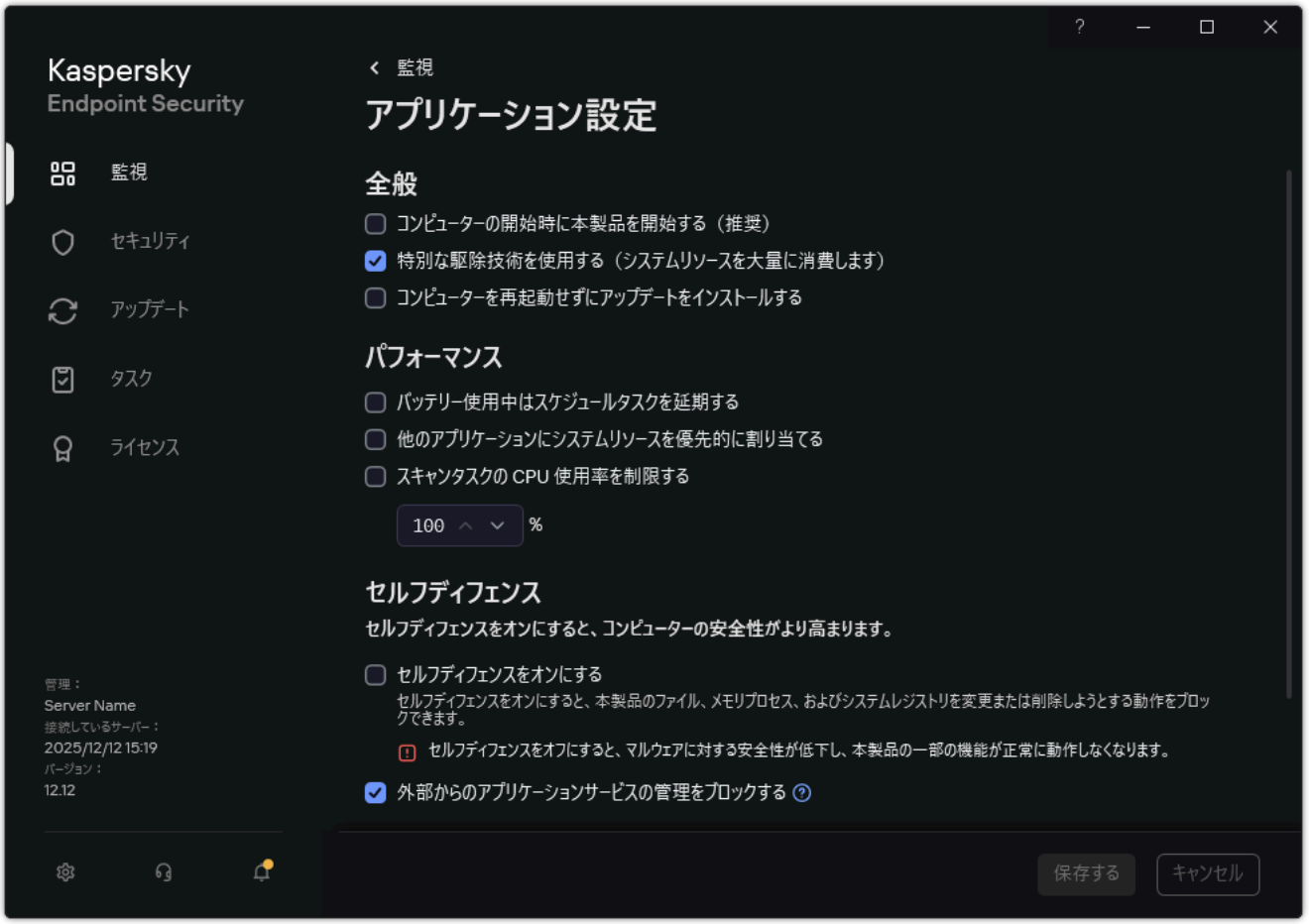
5. ［**他のアプリケーションにシステムリソースを優先的に割り当てる**］ブロックで、［**他のアプリケーションにシステムリソースを優先的に割り当てる**］を］を使用して他のアプリケーションへのリソースの供与を有効または無効にします。

6. 変更内容を保存します。

製品インターフェイスで他のアプリケーションへのシステムリソースの優先的な割り当てを有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**パフォーマンス**］ブロックで、［**他のアプリケーションにシステムリソースを優先的に割り当てる**］を使用して他のアプリケーションへのリソースの供与を有効または無効にします。

4. 変更内容を保存します。

Kaspersky Endpoint Security のパフォーマンス最適化のためのベストプラクティス

Kaspersky Endpoint Security for Windows の導入時、次の推奨事項を使用することでコンピューターの保護およびパフォーマンスを最適化できます。コンピューターのパフォーマンスの問題の対処方法については、テクニカルサポートのナレッジベースを参照してください。

全般

次の推奨事項に従って、本製品の全般設定を指定します。

1. Kaspersky Endpoint Security を最新のバージョンにアップグレードする。

   新しいバージョンの製品には、問題の修正、安定性の向上、パフォーマンスの最適化などが含まれています。

2. 既定の設定で保護機能を有効化する。

   既定の設定が最適と考えられます。これらの設定はカスペルスキーの専門家が推奨しています。既定の設定により、推奨される保護レベルおよび最適なリソースを使用できます。必要に応じて、既定の設定を復元できます。

3. アプリケーションのパフォーマンス最適化機能を有効にする。

   本製品には省エネモードおよび他のアプリケーションにシステムリソースを優先的に割り当てるといった、パフォーマンスの最適化機能があります。これらのオプションが有効になっていることを確認してください。

ワークステーションでのマルウェアのスキャン

ワークステーションでのマルウェアのスキャンを実行するには、バックグラウンドスキャンを有効にしておくことを推奨します。*バックグラウンドスキャンモード*では、Kaspersky Endpoint Security はユーザー向けの通知を表示せずにスキャンを実行します。バックグラウンドスキャンは、その他のスキャン種別（完全スキャンなど）よりも、リソース消費量が少なくなります。このモードでは、Kaspersky Endpoint Security はスタートアップオブジェクト、ブートセクター、システムメモリ、システムパーティションをスキャンします。バックグラウンドスキャンの設定は最適だと考えられます。これらの設定はカスペルスキーの専門家が推奨しています。コンピューターでマルウェアのスキャンを実行するには、バックグラウンドスキャンモードを使用するだけで、別のスキャンタスクの使用は必要ありません。

バックグラウンドスキャンが目的に沿わない場合は、次の推奨事項に従って *マルウェアのスキャン*を設定してください：

1. コンピュータのスキャン中の CPU リソース消費量に制限を設定する。

   *マルウェアのスキャンタスク*の実行中、CPU 使用率を制限することができます。これを行うには、アプリケーション設定で、コンピューターのスキャン中に利用できるすべてのコアにかかる最大 CPU 負荷率を指定します。これにより、コンピューターのスキャンにかかる時間が長くなる可能性があります。

2. 最適なコンピューターのスキャンスケジュールを設定する。

   コンピューターの負荷が最も少ないタイミングでタスクを実行するよう設定することができます。例えば、タスクを夜間または週末に実行するよう設定できます。

   ユーザーが営業時間外にコンピューターの電源をオフにする場合、Wake-on-LAN 機能を有効にすることができます。Wake-on-LAN 機能とは、ローカルネットワークを介して特殊な信号を送信することで遠隔からコンピューターの電源をオンにします。この機能を使用するには、BIOS 設定で Wake-on-LAN 機能を有効にする必要があります。または、タスクが完了してからコンピューターの電源をオフにするように設定することも可能です。

   適切なスキャンスケジュールを設定できない場合は、コンピューターの負荷が低い時間にのみタスクを実行するようにしてください。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。

3. スキャン範囲を定義する。

   スキャン対象として次のオブジェクトを選択します（スキャン範囲の最小セット）：

   - カーネルメモリ
   - 実行中のプロセスおよびスタートアップオブジェクト
   - ディスクブートセクター
   - %systemroot%（サブフォルダーは含まない）
   - %systemroot%\System（サブフォルダーは含まない）
   - %systemroot%\System32（サブフォルダーは含まない）
   - %systemroot%\System32\drivers（サブフォルダーは含まない）
   - %systemroot%\SysWOW64（サブフォルダーは含まない）
   - %systemroot%\SysWOW64\drivers（サブフォルダーは含まない）

4. iSwift と iChecker をオンにする。

   - iSwift テクノロジー：

     特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

   - iChecker テクノロジー：

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

   > iSwift および iChecker テクノロジーは管理コンソール（MMC）と Kaspersky Endpoint Security のインターフェイスでのみオンにできます。Kaspersky Security Center Web コンソールではオンにすることができません。

5. パスワードで保護されているアーカイブのスキャンを無効にする。

   パスワードで保護されているアーカイブのスキャンが有効になっていると、アーカイブのスキャン前にパスワードを求める画面が表示されます。タスクは業務時間外に実行することが推奨されるので、ユーザーはパスワードを入力することができません。パスワードで保護されているアーカイブは手動でスキャンすることができます。

6. 複数のスキャンタスクの同時起動を無効にする。

   現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。

サーバー上でのマルウェアのスキャン

次の推奨事項に従ってマルウェアのスキャンを設定してください。

1. コンピュータのスキャン中の CPU リソース消費量に制限を設定する。

   マルウェアのスキャンタスクの実行中、CPU 使用率を制限することができます。これを行うには、アプリケーション設定で、コンピューターのスキャン中に利用できるすべてのコアにかかる最大 CPU 負荷率を指定します。これにより、コンピューターのスキャンにかかる時間が長くなる可能性があります。

2. 最適なコンピューターのスキャンスケジュールを設定する。

   コンピューターの負荷が最も少ないタイミングでタスクを実行するよう設定することができます。例えば、タスクを夜間または週末に実行するよう設定できます。

3. iSwift と iChecker をオンにする。

   - iSwift テクノロジー：

     特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

   - iChecker テクノロジー：

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

   > iSwift および iChecker テクノロジーは管理コンソール（MMC）と Kaspersky Endpoint Security のインターフェイスでのみオンにできます。Kaspersky Security Center Web コンソールではオンにすることができません。

4. パスワードで保護されているアーカイブのスキャンを無効にする。

   パスワードで保護されているアーカイブのスキャンが有効になっていると、アーカイブのスキャン前にパスワードを求める画面が表示されます。タスクは業務時間外に実行することが推奨されるので、ユーザーはパスワードを入力することができません。パスワードで保護されているアーカイブは手動でスキャンすることができます。

5. 複数のスキャンタスクの同時起動を無効にする。

   現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。

Kaspersky Security Network

コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

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

次の推奨事項に従って Kaspersky Security Network を設定してください。

1. 拡張 KSN モードを無効にする

   *拡張 KSN モード*は、カスペルスキーに詳細なデータを送信するモードです。

2. Kaspersky Private Security Network の設定。

   Kaspersky Private Security Network (KPSN) は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。

3. クラウドモードを有効にする。

   *クラウドモード*で動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用しての本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。

マルウェアのスキャン

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

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

完全スキャン

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

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

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

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

簡易スキャン

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

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

オブジェクトスキャン

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

- システムメモリ
- オペレーティングシステムの起動時に読み込まれるオブジェクト
- システムバックアップ
- ハードディスク、リムーバブルドライブ、およびネットワークドライブ
- 選択した任意のファイル

バックグラウンドスキャン

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

アプリケーション整合性チェック

製品機能に破損や変更がないかチェックします。

コンピューターのスキャン

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

Kaspersky Endpoint Security には次の定義済みの標準タスクがあります：［*完全スキャン*］、［*簡易スキャン*］、［*オブジェクトスキャン*］。組織に Kaspersky Security Center 管理システムが配備されている場合、*マルウェアのスキャン*タスクを作成してスキャンを設定することができます。

管理コンソール（MMC）でスキャンタスクを実行する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。

3. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
   必要に応じて、マルウェアのスキャンタスクを作成します。

4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。

5. スキャンタスクを設定します（下の表を参照）。
   必要に応じて、スキャンタスクのスケジュールを設定します。

6. 変更内容を保存します。

7. スキャンタスクを実行します。

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

Web コンソールと Cloud コンソールでスキャンタスクを実行する方法

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

2. スキャンタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. スキャンタスクを設定します（下の表を参照）。
   必要に応じて、スキャンタスクのスケジュールを設定します。

5. 変更内容を保存します。

6. スキャンタスクを実行します。

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

製品インターフェイスでスキャンタスクを実行する方法

1. メインウィンドウで、［**タスク**］をクリックします。

2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。

3. スキャンタスクを設定します（下の表を参照）。
   必要に応じて、スキャンタスクのスケジュールを設定します。

4. 変更内容を保存します。

5. スキャンタスクを実行します。

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

コンピューターのスキャン中の Kaspersky Endpoint Security のパフォーマンスを最適化するために、*完全スキャンタスクの詳細設定を管理したり、CPU リソースの使用を制限したりできます*。

Kaspersky Security Center では、*完全スキャン*タスクの代わりにバックグラウンドスキャンタスクを使用して、本製品のパフォーマンスを最適化することもできます。これは、コンピューターのセキュリティレベルには影響しません。バックグラウンドスキャンを設定することはできません。

Kaspersky Endpoint Security はコンピューターをスキャンして、脅威が検知された場合は製品設定で指定されている処理を実行します。通常、本製品は感染したファイルを駆除しようとします。この結果、感染したファイルは次のステータスを受け取ります。

- **延期**：感染したファイルは駆除できませんでした。本製品はコンピューターの再起動後に感染したファイルを削除します。
- **イベントを記録しました**：感染したファイルは駆除できませんでした。本製品は、検知済みの感染ファイルに関する情報をアクティブな脅威のリストに追加します。
- **書き込みがサポートされていません**または**書き込みエラー**：感染したファイルは駆除できませんでした。本製品に書き込み権がありません。
- **処理済み**：本製品は以前感染したファイルを検知しました。本製品はコンピューターの再起動後に感染したファイルを駆除または削除します。

スキャンの設定

パラメータ	説明
セキュリティレベル	Kaspersky Endpoint Security はスキャンを実行するために異なる設定のグループを使用します。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます： • **高**：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**高**］の詳細レベルのヒューリスティック分析を使用します。 • **推奨**：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**中**］の詳細レベルのヒューリスティック分析を使用します。 • **低**：Kaspersky Endpoint Security は、指定されたファイル形式のみをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**低**］の詳細レベルのヒューリスティック分析を使用します。 セキュリティレベルは、事前に設定されているものから選択することも、手動で設定することもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

パラメータ	説明
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 **駆除する。駆除できない場合は通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。 **通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。 感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。 Windows ストアアプリの一部であるファイルで感染が検知された場合、そのファイルが削除されます。
すぐに特別な駆除を実行する *（Kaspersky Security Center コンソール内でのみ利用可能）*	コンピューターに適用されているポリシーのプロパティで特別な駆除が有効になっている場合のみ、コンピューター上のスキャンタスク中に特別な駆除が実行されます。 チェックボックスがオンの場合、Kaspersky Endpoint Security はスキャンタスクの実行中にアクティブな感染を検知すると、すぐに駆除します。アクティブな感染の駆除後、Kaspersky Endpoint Security はユーザーに通知せずにコンピューターを再起動します。 チェックボックスがオフの場合、Kaspersky Endpoint Security はスキャンタスクの実行中にアクティブな感染を検知してもすぐには駆除しません。Kaspersky Endpoint Security はローカルの製品レポートおよび Kaspersky Security Center でアクティブな感染イベントを作成します。アクティブな感染は、特別な駆除機能がオンになっているときにスキャンタスクが再度実行されたときに駆除することができます。このように、システム管理者は特別な駆除を実行し、コンピューターを自動的に再起動するために適切なタイミングを選択することができます。
スキャン範囲	スキャンタスクの実行時に、Kaspersky Endpoint Security によってスキャンされるオブジェクトのリスト。スキャン範囲に指定できるオブジェクトは次のとおりです：カーネルメモリ、実行中の処理、ブートセクター、システムのバックアップ保管領域、ハードディスク、リムーバブルドライブまたはネットワークドライブ、フォルダーまたはファイル。 Kaspersky Endpoint Security for Windows 12.12 では、メールは本製品のスキャン範囲から除外されます。送受信メールのスキャンはメール脅威対策機能によって実行されます。以前のバージョンの管理プラグインを使用している場合、ポリシーにメールが含まれていても、スキャン範囲からメールが除外されます。
スキャンスケジュール	**手動**：都合の良いときに手動でスキャンを開始できる実行方法です。 **スケジュールで指定**：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。
本製品の起動からタスク開始までの時間	本製品の開始後、遅れてスキャンタスクを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。
スキップしたタスクを実行する	このチェックボックスをオンにすると、スキップされたタスクは実行可能になると同時に開始されます。タスクの開始時間にコンピューターの電源がオフになっていた場合などに、タスクがスキップされることがあります。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。 このチェックボックスをオフにすると、スキップされたタスクは開始されません。代わりに、現在のスケジュールに従って、次のタスクが実行されます。
コンピューターを使用していないときにのみ実行する	コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。

パラメータ	説明
スキャンの実行方法を選択	既定では、スキャンタスクはオペレーティングシステムに登録されたユーザー名で実行されます。保護範囲には、ネットワークドライブやその他特定のアクセス権限を必要とするオブジェクトが含まれることがあります。製品設定で必要な権限を持っているユーザーを指定して、このユーザーアカウントでスキャンタスクを実行できます。
ファイル種別	Kaspersky Endpoint Security では、拡張子のないファイルは実行ファイルとみなされます。スキャン対象としたファイルの種類にかかわらず、必ず実行ファイルをスキャンします。 **すべてのファイル**：この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。 **ファイル形式でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。 **拡張子でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイル形式はファイルの拡張子に基づいて識別されます。 既定では、ファイルはその形式でスキャンされます。悪意のあるファイルには、「`.123`」など、感染ファイルの可能性がある拡張子のリストにはない拡張子が指定されていることがあるため、拡張子を指定するスキャンはあまり安全であるとは言えません。
新規作成または変更されたファイルのみスキャン	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
ファイルの最大スキャン時間	タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。
同時に複数のスキャンタスクを実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 しかし、次のスキャンタスクのうちいずれかが実行されている場合は、Kaspersky Endpoint Security はすぐにスキャンタスクを実行します： • 接続時のリムーバブルドライブのスキャン • コンテキストメニューからのスキャン • 侵害インジケーター（IOC）の検知時に開始される簡易スキャン このチェックボックスがオフの場合、同時に複数のスキャンタスクを実行できます。複数のスキャンタスクを実行すると、より多くのコンピューターリソースが消費されます。
アーカイブをスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配信パッケージをスキャン	サードパーティ製品の配布パッケージをスキャンします。
Microsoft Office形式のファイルをスキャン	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。

パラメータ	説明
メール形式のファイルをスキャン	メール形式とメールデータベースをスキャンします。MS Outlook と Windows Mail が使用する PST および OST ファイルや、EML ファイルもスキャンされます。 Kaspersky Endpoint Security は 64 ビットの MS Outlook メールクライアントはサポートしません。つまり、64 ビットの MS Outlook がコンピューターにインストールされていて、スキャン範囲にメールが含まれている場合でも、Kaspersky Endpoint Security は 64 ビットの MS Outlook のファイル（PST および OST ファイル）をスキャンしません。 このチェックボックスをオンにすると、メール形式のファイルはコンポーネント（ヘッダー、本文、添付ファイル）に分割され、それぞれで脅威がスキャンされます。 チェックボックスをオフにすると、Kaspersky Endpoint Security はメール形式のファイルを 1 つのファイルとしてスキャンします。 PST または OST ファイルで悪意のあるオブジェクトが検知されると、Kaspersky Endpoint Security は選択された処理（ファイルの駆除や削除など）に従ってそのオブジェクトを無害化します。 他のメールクライアント（Mozilla Thunderbird など）のファイルで悪意のあるファイルが検知されると、Kaspersky Endpoint Security は感染したメッセージのマークのみを行います。感染した添付ファイルを含むメッセージを手動で削除する必要があります。
パスワードで保護されているアーカイブをスキャン	このチェックボックスをオンにすると、パスワードで保護されたアーカイブをスキャンします。アーカイブのファイルをスキャンする前に、パスワードの入力が求められます。 このチェックボックスをオフにすると、パスワードで保護されたアーカイブのスキャンをスキップします。
大きな複合ファイルをスキャンしない	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。
機械学習とシグネチャ分析	機械学習とシグネチャ分析では、既知の脅威の説明と脅威を無効化する方法が登録された Kaspersky Endpoint Security の定義データベースを使用します。この方法を使用する保護では、許容できる最低限のセキュリティレベルが提供されます。 カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。
ヒューリスティック分析	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
iSwift *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iChecker には制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。

コンピューターに接続されたリムーバブルドライブのスキャン

Kaspersky Endpoint Security は、リムーバブルドライブ上にあるファイルでも、実行またはコピーしたすべてのファイルをスキャンします（ファイル脅威対策機能）。ウイルスやその他のマルウェアの拡散を防ぐため、リムーバブルドライブがコンピューターに接続された際に自動でスキャンされるよう設定することができます。Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。機械学習やヒューリスティック分析（高レベル）、署名分析を備えたスキャンを実行することでコンピューターの安全を保ちます。Kaspersky Endpoint Security はスキャンの最適化技術の iSwift および iChecker も使用します。これらは常に有効になっており、無効にすることはできません。

管理コンソール（MMC）でリムーバブルドライブのスキャンの実行を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**ローカルタスク**］→［**リムーバブルドライブスキャン**］の順に選択します。
4. ［**リムーバブルドライブ接続時の処理**］で、［**最大の保護**］または［**推奨**］を選択します。
5. リムーバブルドライブのスキャンの詳細なオプションを設定します（下の表を参照）。
6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでリムーバブルドライブのスキャンの実行を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**リムーバブルドライブスキャン**］に移動します。
5. ［**リムーバブルドライブスキャンは有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. ［**スキャン種別**］ブロックで［**詳細スキャン**］または［**簡易スキャン**］をオンにします。
7. リムーバブルドライブのスキャンの詳細なオプションを設定します（下の表を参照）。
8. 変更内容を保存します。

製品インターフェイスでリムーバブルドライブのスキャンの実行を設定する方法

1. メインウィンドウで、［**タスク**］をクリックします。
2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。

3. ［**リムーバブルドライブスキャン**］を使用してコンピューターへの接続時のリムーバブルドライブのスキャンを有効または無効にします。

4. リムーバブルドライブのスキャンの詳細なオプションを設定します（下の表を参照）。

5. 変更内容を保存します。

Kaspersky Endpoint Security は指定した最大サイズより大きくないリムーバブルドライブに対してリムーバブルドライブのスキャンを実行します。*リムーバブルドライブスキャン*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

リムーバブルドライブのスキャンタスクの設定

パラメータ	説明
スキャン種別	**詳細スキャン**：このオプションを選択した場合、リムーバブルドライブが接続されると、Kaspersky Endpoint Security は複合オブジェクト、アーカイブ、配布パッケージ内でネストしたファイルや Office 形式のファイルを含むリムーバブルドライブ上のすべてのファイルをスキャンします。Kaspersky Endpoint Security はメール形式やパスワード保護されたアーカイブのファイルはスキャンしません **簡易スキャン**：このオプションを選択した場合、リムーバブルドライブが接続されると、感染に対して最も脆弱な特定のファイル形式のファイルのみをスキャンします。複合オブジェクトは解凍しません。
最大ドライブサイズ（MB）	このチェックボックスをオンにすると、Kaspersky Endpoint Security は、指定された最大ドライブサイズ以下のサイズのリムーバブルドライブに対して、選択した処理を実行します。リムーバブルドライブのサイズが設定値を超える場合、Kaspersky Endpoint Security はスキャンをスキップします。 チェックボックスをオフにすると、Kaspersky Endpoint Security は、すべてのサイズのリムーバブルドライブに対して、選択した処理を実行します。
スキャン進捗バーを非表示にする	このチェックボックスをオンにすると、リムーバブルドライブのスキャンの進捗が別のウィンドウおよび［**タスク**］セクションに表示されます。 このチェックボックスをオフにすると、リムーバブルドライブのスキャンはバックグラウンドで実行されます。
ユーザーによるスキャン停止を禁止する	このチェックボックスをオンにすると、Kaspersky Endpoint Security のローカルインターフェイス内のリムーバブルドライブのスキャンタスクで、［**タスク**］セクションの［**停止**］ボタンおよびリムーバブルドライブのスキャンウィンドウの［**停止**］ボタンが使用できなくなります。

バックグラウンドスキャン

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

コンピューターのリソース消費量を抑えるために、完全スキャンタスクではなく、バックグラウンドスキャンタスクを使用することを推奨します。これは、コンピューターのセキュリティレベルには影響しません。これらのタスクは同じスキャン範囲を対象にします。コンピューターの負荷を最適化するため、完全スキャンとバックグラウンドスキャンは同時に実行されることはありません。完全スキャンタスクを既に実行済みの場合、バックグラウンドスキャンタスクは完全スキャンタスクが完了してから 7 日間は開始されません。

次のケースでは、バックグラウンドスキャンが開始されます。

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

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

- コンピューターが再びアクティブな状態になった。

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

- コンピューターがバッテリーモードに切り替わった（ノートパソコンなど）

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

管理コンソール（MMC）でバックグラウンドスキャンを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**ローカルタスク**］→［**バックグラウンドスキャン**］の順に選択します。
4. ［**バックグラウンドスキャンを有効にする**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。
5. ［**バックグラウンドスキャン**］で、［**バックグラウンドスキャンは有効です**］トグルスイッチを使用してバックグラウンドスキャンを有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでバックグラウンドスキャンを有効にする方法

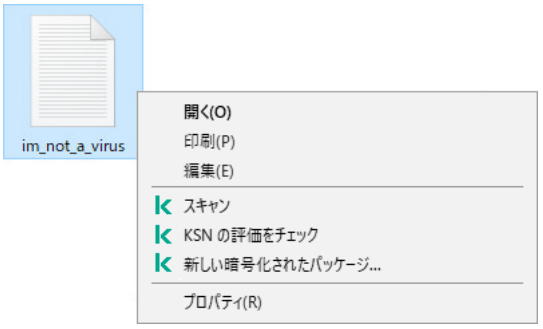
1. メインウィンドウで、［**タスク**］をクリックします。
2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。
3. ［**バックグラウンドスキャン**］を使用して機能を有効または無効にします。
4. 変更内容を保存します。

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

コンテキストメニューからのスキャン

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

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



コンテキストメニューからのスキャン

管理コンソール（MMC）でコンテキストメニューからのスキャンを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**ローカルタスク**］→［**コンテキストメニューからのスキャン**］の順に選択します。
4. コンテキストメニューからのスキャンを設定します（下の表を参照）。
5. 変更内容を保存します。

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

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

製品インターフェイスでコンテキストメニューからのスキャンを設定する方法

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

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

コンテキストメニューからのスキャンタスクの設定

パラメータ	説明
セキュリティレベル	Kaspersky Endpoint Security はスキャンを実行するために異なる設定のグループを使用します。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます： • **高**：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**高**］の詳細レベルのヒューリスティック分析を使用します。 • **推奨**：Kaspersky Endpoint Security は、すべての種類のファイルをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**中**］の詳細レベルのヒューリスティック分析を使用します。 • **低**：Kaspersky Endpoint Security は、指定されたファイル形式のみをスキャンします。複合ファイルをスキャンする場合、本製品はアーカイブ、配布パッケージ、Office 形式のファイルをスキャンしますが、パスワードで保護されているアーカイブはスキャンしません。このセキュリティレベルが設定されると、本製品は、［**低**］の詳細レベルのヒューリスティック分析を使用します。
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 **駆除する。駆除できない場合は通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。 **通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
ファイル種別	Kaspersky Endpoint Security では、拡張子のないファイルは実行ファイルとみなされます。スキャン対象としたファイルの種類にかかわらず、必ず実行ファイルをスキャンします。 **すべてのファイル**：この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。 **ファイル形式でファイルをスキャン**：この設定を有効にすると、[感染する可能性のあるファイルのみ](#)がスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。 **拡張子でファイルをスキャン**：この設定を有効にすると、[感染する可能性のあるファイルのみ](#)がスキャンされます。ファイル形式はファイルの拡張子に基づいて識別されます。 既定では、ファイルはその形式でスキャンされます。悪意のあるファイルには、「`.123`」など、感染ファイルの可能性がある拡張子のリストにはない拡張子が指定されていることがあるため、拡張子を指定するスキャンはあまり安全であるとは言えません。
新規作成または変更されたファイルのみスキャン	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
ファイルの最大スキャン時間	タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。
アーカイブをスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配信パッケージをスキャン	このチェックボックスでは、配布パッケージのスキャンを有効または無効にします。

パラメータ	説明
Microsoft Office 形式のファイルをスキャン	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1MB より小さいサイズの Office 形式のファイルをスキャンします。
メール形式のファイルをスキャン	メール形式とメールデータベースをスキャンします。MS Outlook と Windows Mail が使用する PST および OST ファイルや、EML ファイルもスキャンされます。 Kaspersky Endpoint Security は 64 ビットの MS Outlook メールクライアントはサポートしません。つまり、64 ビットの MS Outlook がコンピューターにインストールされていて、スキャン範囲にメールが含まれている場合でも、Kaspersky Endpoint Security は 64 ビットの MS Outlook のファイル（PST および OST ファイル）をスキャンしません。 このチェックボックスをオンにすると、メール形式のファイルはコンポーネント（ヘッダー、本文、添付ファイル）に分割され、それぞれで脅威がスキャンされます。 チェックボックスをオフにすると、Kaspersky Endpoint Security はメール形式のファイルを 1 つのファイルとしてスキャンします。 PST または OST ファイルで悪意のあるオブジェクトが検知されると、Kaspersky Endpoint Security は選択された処理（ファイルの駆除や削除など）に従ってそのオブジェクトを無害化します。 他のメールクライアント（Mozilla Thunderbird など）のファイルで悪意のあるファイルが検知されると、Kaspersky Endpoint Security は感染したメッセージのマークのみを行います。感染した添付ファイルを含むメッセージを手動で削除する必要があります。
パスワードで保護されているアーカイブをスキャン	このチェックボックスをオンにすると、パスワードで保護されたアーカイブをスキャンします。アーカイブのファイルをスキャンする前に、パスワードの入力が求められます。 このチェックボックスをオフにすると、パスワードで保護されたアーカイブのスキャンをスキップします。
大きな複合ファイルをスキャンしない	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。
機械学習とシグネチャ分析	機械学習とシグネチャ分析では、既知の脅威の説明と脅威を無効化する方法が登録された Kaspersky Endpoint Security の定義データベースを使用します。この方法を使用する保護では、許容できる最低限のセキュリティレベルが提供されます。 カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。
ヒューリスティック分析	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
iSwift	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iChecker には制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。

アプリケーション整合性チェック

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

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

アプリケーションの整合性が侵害されている状況として、次のケースがあります：

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

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

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**アプリケーション整合性チェック**］の順に選択します。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：タスク開始スケジュールの設定

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

ステップ 4：タスク名の定義

*コンピューターの感染後の整合性チェック*など、タスクの名前を入力します。

ステップ 5：タスク作成の完了

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

Web コンソールを使用してアプリケーションの整合性チェックを実行する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**アプリケーション整合性チェック**］を選択します。

c. ［**タスク名**］に「*コンピューターへの感染を検知後のアプリケーションの整合性のチェック*」などの短く分かりやすい名前を付けます。

d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。

5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。

6. ウィザードを終了します。

   タスクのリストに新しいタスクが表示されます。

7. タスクの横にあるチェックボックスをオンにします。

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

製品インターフェイスで整合性チェックを実行する方法

1. メインウィンドウで、［**タスク**］をクリックします。

2. タスクのリストが表示されます。*アプリケーション整合性チェック*タスクを選択してボタン［**実行**］をクリックします。

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

整合性チェックタスク

パラメータ	説明
スキャンスケジュール	**手動で開始**：都合の良いときに手動でスキャンを開始できる実行方法です。 **スケジュールで指定**：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。
スキップしたタスクを実行する	このチェックボックスをオンにすると、スキップされたタスクは実行可能になると同時に開始されます。タスクの開始時間にコンピューターの電源がオフになっていた場合などに、タスクがスキップされることがあります。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。 このチェックボックスをオフにすると、スキップされたタスクは開始されません。代わりに、現在のスケジュールに従って、次のタスクが実行されます。
コンピューターを使用していないときにのみ実行する	コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。

スキャン範囲の編集

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

スキャン範囲を編集するには、*オブジェクトスキャンタスク*の使用を推奨します。カスペルスキーのエキスパートは、*完全スキャン*および*簡易スキャン*タスクのスキャン範囲を変更しないことを推奨します。

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

- **システムメモリ**
- **スタートアップオブジェクト**
  システムの起動時に実行されるプロセスやアプリケーション実行ファイルによって使用されているメモリ。
- **ディスクブートセクター**
  ハードディスクおよびリムーバブルディスクのブートセクター。
- **システムバックアップ**
  System Volume Information フォルダーの内容。
- **すべての外部デバイス**
- **すべてのハードディスクドライブ**
- **すべてのネットワークドライブ**

Kaspersky Endpoint Security for Windows 12.12 では、メールは本製品のスキャン範囲から除外されます。送受信メールのスキャンはメール脅威対策機能によって実行されます。.以前のバージョンの管理プラグインを使用している場合、ポリシーにメールが含まれていても、スキャン範囲からメールが除外されます。

ネットワークドライブまたは共有フォルダーをスキャンするために、別のスキャンタスクを作成することを推奨します。［マルウェアのスキャン］タスクの設定で、このドライブへの書き込み権を持つユーザーを指定します。これは検知した脅威を緩和するために必要です。ネットワークドライブを持つサーバーに独自のセキュリティツールがある場合は、そのドライブに対してスキャンタスクを実行しないでください。それにより、オブジェクトを 2 回チェックすることを避け、サーバーのパフォーマンスを向上させることができます。

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

管理コンソール（MMC）でスキャン範囲を編集する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
   必要に応じて、マルウェアのスキャンタスクを作成します。
4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。
5. ［**スキャン範囲**］セクションで、［**設定**］をクリックします。
6. 表示されたウィンドウで、スキャン範囲に含めるまたは除外するオブジェクトを選択します。

7. スキャン範囲に新しいオブジェクトを追加するには：

   a. ［**追加**］をクリックします。

   b. ［**パス**］フィールドにフォルダーまたはファイルのパスを入力します。

      マスクを使用する

      - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

      - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

      ファイルまたはフォルダーのパスにマスクを使用できます。たとえば、コンピューター上のすべてのユーザーアカウントを対象として［ダウンロード］フォルダーをスキャンする場合は、「`C:\Users\*\Downloads\`」と入力します。

      コンピューターのファイルリソースのリスト内の［**この PC**］のオブジェクトには、［**すべてのハードディスク**］、［**すべてのネットワークドライブ**］、［**すべてのリムーバブルドライブ**］のオブジェクトが含まれます。

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

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

Web コンソールと Cloud コンソールでスキャン範囲を編集する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. スキャンタスクをクリックします。

   タスクのプロパティウィンドウが表示されます。必要に応じて、*マルウェアのスキャン*タスクを作成します。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**スキャン範囲**］で、スキャン範囲に含めるまたは除外するオブジェクトを選択します。

5. スキャン範囲に新しいオブジェクトを追加するには：

   a. ［**追加**］をクリックします。

   b. フォルダーまたはファイルのパスを入力します。

マスクを使用する

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C:ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

ファイルまたはフォルダーのパスにマスクを使用できます。たとえば、コンピューター上のすべてのユーザーアカウントを対象として［ダウンロード］フォルダーをスキャンする場合は、「`C:\Users\*\Downloads\`」と入力します。

スキャン範囲のオブジェクトのリストからオブジェクトを削除しなくてもオブジェクトをスキャンから除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。

6. 変更内容を保存します。

製品インターフェイスでスキャン範囲を編集する方法

1. メインウィンドウで、［**タスク**］をクリックします。

2. タスクのリストが表示されます。*オブジェクトスキャンタスク*を選択してボタン［**選択**］をクリックします。

   その他のタスクのスキャン範囲も編集することができます。カスペルスキーのエキスパートは、*完全スキャン*および*簡易スキャンタスク*のスキャン範囲を変更しないことを推奨します。

3. 表示されたウィンドウで、スキャン範囲に含めるオブジェクトを選択します。

4. 変更内容を保存します。

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

スケジュールされたスキャンの実行

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

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

- データベースのアップデート後：

  Kaspersky Endpoint Security はアップデートシグネチャがあるデータベースでコンピューターのスキャンを実行します。

- 本製品の起動後：

  製品の開始から指定した時間が経過した際、Kaspersky Endpoint Security はスキャンを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。

- Wake-on-LAN 機能：

  コンピューターの電源がオフの場合でも、Kaspersky Endpoint Security はスケジュールに従ってコンピューターのスキャンを実行します。そのため、本製品はオペレーティングシステムの Wake-on-LAN 機能を使用します。Wake-on-LAN 機能とは、ローカルネットワークを介して特殊な信号を送信することで遠隔からコンピューターの電源をオンにします。この機能を使用するには、BIOS 設定で Wake-on-LAN 機能を有効にする必要があります。

  Wake-on-LAN を使用したスキャンの実行を設定できるのは、 Kaspersky Security Center の *マルウェアのスキャン*のみです。製品インターフェイスではコンピューターのスキャンの Wake-on-LAN を有効にすることはできません。

- コンピューターを使用していないとき：

  Kaspersky Endpoint Security は、スクリーンセーバーが起動しているまたは画面がロックされているときにスケジュールに従ってコンピューターのスキャンを実行します。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はスキャンを一時停止します。そのため、本製品がコンピューターの完全スキャンを実行するのに数日かかることがあります。

管理コンソール（MMC）でスキャンのスケジュールを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。

   必要に応じて、*マルウェアのスキャン*タスクを作成します。
4. コンピューターのプロパティウィンドウで、［**スケジュール**］セクションを選択します。
5. スキャンタスクのスケジュールを設定します。
6. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。
7. 変更内容を保存します。

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

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。
2. スキャンタスクをクリックします。

   タスクのプロパティウィンドウが表示されます。

3. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

4. スキャンタスクのスケジュールを設定します。

5. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。

6. 変更内容を保存します。

製品インターフェイスでスキャンのスケジュールを設定する方法

コンピューターにポリシーが適用されていない場合にのみスキャンスケジュールを設定することができます。ポリシーが適用されているコンピューターは、Kaspersky Security Center で *マルウェアのスキャン* のスケジュールを設定してください。

1. メインウィンドウで、［**タスク**］をクリックします。

2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。

   完全スキャン、簡易スキャンまたは整合性チェックの実行スケジュールを設定できます。カスタムスキャンは手動でのみ実行できます。

3. ［**スキャンスケジュール**］をクリックします。

4. 表示されたウィンドウで、スキャンタスクの実行のスケジュールを設定します。

5. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。

6. 変更内容を保存します。

スキャンスケジュールの設定

パラメータ	説明
スキャンスケジュール	**手動で開始**：都合の良いときに手動でスキャンを開始できる実行方法です。 **スケジュールで指定**：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。
本製品の起動からタスク開始までの時間	本製品の開始後、遅れてスキャンタスクを実行します。オペレーティングシステムの開始時には多くのプロセスが実行されています。そのため、Kaspersky Endpoint Security の開始直後にスキャンを実行するより、遅れてスキャンを実行するほうが効率的です。
スキップしたタスクを実行する	このチェックボックスをオンにすると、スキップされたタスクは実行可能になると同時に開始されます。タスクの開始時間にコンピューターの電源がオフになっていた場合などに、タスクがスキップされることがあります。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。 このチェックボックスをオフにすると、スキップされたタスクは開始されません。代わりに、現在のスケジュールに従って、次のタスクが実行されます。
コンピューターを使用していないときにのみ実行する	コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。
タスクの開始を自動的かつランダムに遅延させる *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスがオンの場合、タスクはスケジュールに厳密に従わず、特定の間隔でランダムに、つまりタスクの開始時刻は分散して実行されます。ランダムに開始することで、タスクがスケジュール通りに実行されることにより、多数のコンピューターから同時に管理サーバーにアクセスが集中することを避けられます。 ランダムに開始されるタスクの開始時刻の範囲は、タスクが作成された際、そのタスクが割り当てられたコンピューターの数に基づいて自動的に計算されます。それ以降、タスクは算出された開始時刻に実行されます。しかし、タスクの設定が変更されたり手動で実行された場合は、計算される開始時刻は変更されます。 チェックボックスがオフの場合、タスクはスケジュールされた時刻に実行されます。

パラメータ	説明
タスクの開始を次の時間範囲内でランダムに遅延させる（分）	このチェックボックスをオンにすると、タスクは特定の時間枠内のランダムな時間にコンピューター上で実行されます。ランダムに開始することで、タスクがスケジュール通りに実行されることにより、多数のコンピューターから同時に管理サーバーにアクセスが集中することを避けられます。 チェックボックスがオフの場合、タスクはスケジュールされた時刻に実行されます。
次の時間を超える場合はタスクを停止する（分） *（Kaspersky Security Center コンソール内でのみ利用可能）*	タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。 タスクの実行時間を短縮するため、スキャン範囲を設定したり、スキャンを最適化したりすることができます。
Wake on LAN の機能を使用してタスク開始前にデバイスを起動する（分） *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスがオンの場合、コンピューターのオペレーティングシステムの起動が完了するまで指定した時間をおいてからタスクが実行されます。既定の時間は 5 分です。 電源がオフのコンピューターも含めてすべてのコンピューターでタスクを実行する場合はこのチェックボックスをオンにしてください。
タスク完了後にデバイスをシャットダウンする *（Kaspersky Security Center コンソール内でのみ利用可能）*	たとえば、この機能を有効にして、金曜日の勤務時間後にコンピューターをスキャンできます。タスクが終了すると、本製品によって週末の間コンピューターの電源がオフになります。

異なるユーザーとしてスキャンの実行

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

異なるユーザーを指定して実行できるのは次のスキャンです：

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

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

管理コンソール（MMC）で異なるユーザーとしてスキャンを実行する方法

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

6. スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。

7. 変更内容を保存します。

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

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

2. スキャンタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。

3. ［**設定**］タブを選択します。

4. ［**アカウント**］ブロックの［**設定**］をクリックします。

5. スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。

6. 変更内容を保存します。

製品インターフェイスで異なるユーザーとしてスキャンを実行する方法

1. メインウィンドウで、［**タスク**］をクリックします。

2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。

3. タスクのプロパティで、［**詳細設定**］→［**スキャンの実行方法を選択**］を選択します。

4. 表示されるウィンドウで、スキャンタスクの実行に使用するユーザーアカウントの認証情報を入力します。

5. 変更内容を保存します。

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

スキャンの最適化

コンピューターのスキャン中に CPU 使用率を制限する

マルウェアのスキャンタスクの実行中、CPU 使用率を制限することができます。これにより、コンピューターのスキャンにかかる時間が長くなる可能性があります。

管理コンソール（MMC）でコンピューターをスキャンするときに CPU 使用率を制限する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。

4. ［**パフォーマンス**］の下で、［**スキャンタスクの CPU 使用率を制限する**］をオンにして、CPU リソース消費量の平均値をパーセントで入力します。

5. 変更内容を保存します。

Web コンソールと Cloud コンソールでコンピューターをスキャンするときに CPU 使用率を制限する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**パフォーマンス**］に移動します。

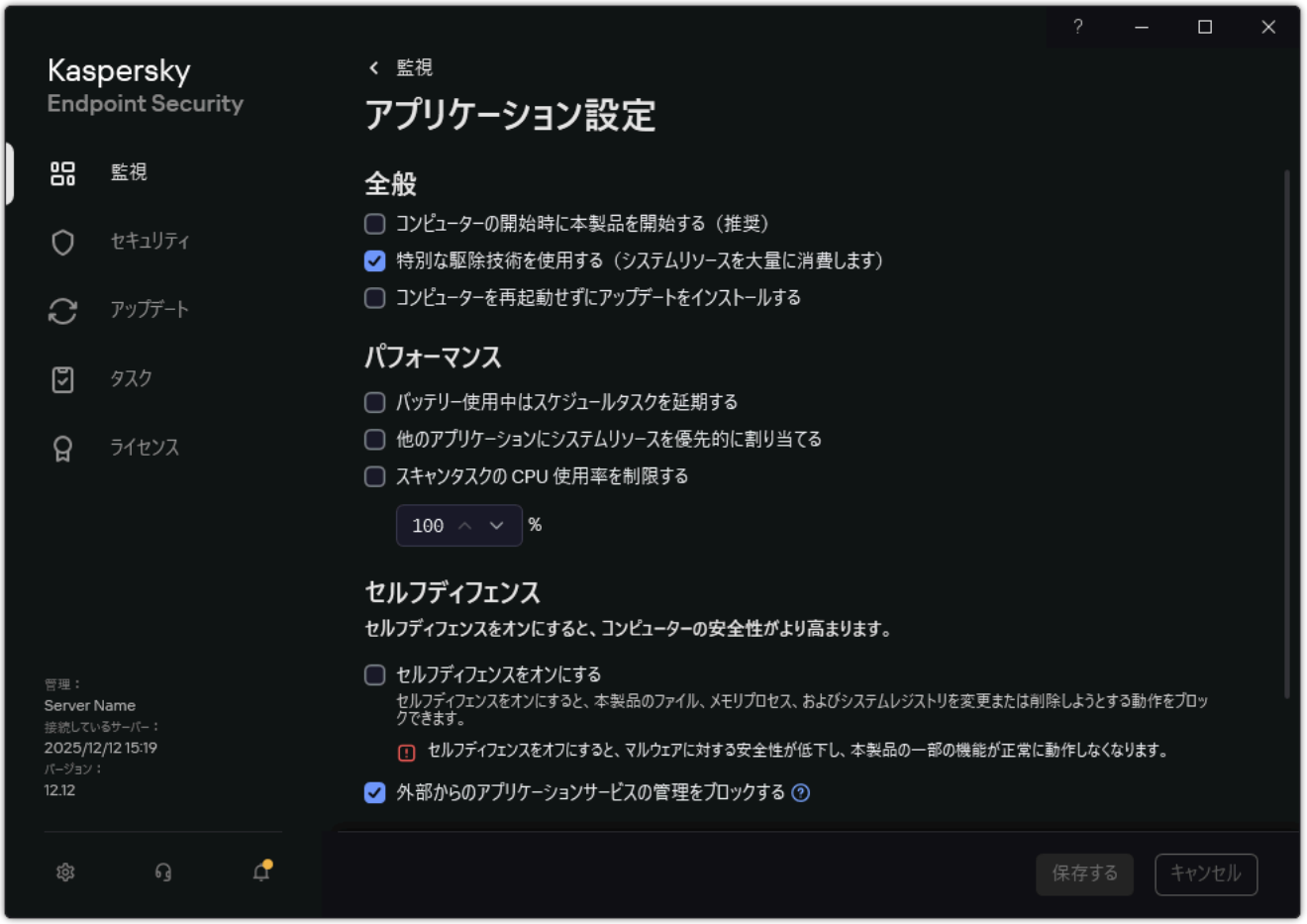
5. ［**スキャンタスクの CPU 使用率を制限する**］の下で、スイッチを［**スキャンタスクの CPU 使用率を制限する**］に設定して、CPU リソース消費量の平均値をパーセントで入力します。

6. 変更内容を保存します。

製品のインターフェイスでコンピューターをスキャンするときに CPU 使用率を制限する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**パフォーマンス**］の下で、［**スキャンタスクの CPU 使用率を制限する**］をオンにして、CPU リソース消費量の平均値をパーセントで入力します。

4. 変更内容を保存します。

マルウェアのスキャンのタスクの詳細設定を指定します。

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

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

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

管理コンソール（MMC）でスキャンを最適化する方法

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーで、［**タスク**］を選択します。

3. スキャンタスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
   必要に応じて、マルウェアのスキャンタスクを作成します。

4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。

5. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。
   タスクの設定ウィンドウが表示されます。

6. ［**最適化**］ブロックで、スキャンを設定します：

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

     新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。

- **ファイルの最大スキャン時間：<N>秒**：タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

- **同時に複数のスキャンタスクを実行しない**：スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。

7. ［**詳細**］をクリックします。

   複合ファイルのスキャンの設定ウィンドウが表示されます。

8. ［**サイズ制限**］ブロックで、［**大きな複合ファイルをスキャンしない**］をオンにします。タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

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

9. ［**OK**］をクリックします。

10. ［**詳細**］タブに移動します。

11. ［**スキャン技術**］ブロックで、スキャンで使用する方法の名前の横にあるチェックボックスをオンにします。

    - **iSwift**：特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

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

12. 変更内容を保存します。

Web コンソールと Cloud コンソールでスキャンを最適化する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. スキャンタスクをクリックします。

   タスクのプロパティウィンドウが表示されます。必要に応じて、マルウェアのスキャンタスクを作成します。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**脅威の検知時の処理**］ブロックで、［**新規作成または変更されたファイルのみスキャン**］をオンにします。新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。

   新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。

5. ［**スキャンの最適化**］ブロックで、［**大きな複合ファイルをスキャンしない**］をオンにします。タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

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

6. ［**同時に複数のスキャンタスクを実行しない**］チェックボックスをオンにします。スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。

7. ［**詳細設定**］ブロックで、［**ファイルの最大スキャン時間（秒）**］をオンにします。タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

8. 変更内容を保存します。

製品インターフェイスでスキャンを最適化する方法

1. メインウィンドウで、［**タスク**］をクリックします。
2. タスクのリストで、スキャンタスクを選択してボタン（⚙）をクリックします。
3. ［**詳細設定**］をクリックします。
4. ［**最適化**］ブロックで、スキャンを設定します：

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

     新しいファイルのスキャンを種別で設定することもできます。たとえば、すべての配布パッケージをスキャンしたり、新しいアーカイブやオフィス形式のファイルのみスキャンすることもできます。

- **ファイルの最大スキャン時間：<N>秒**：タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

- **複数のスキャンタスクを同時に実行しないでください**：スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。

5. ［**サイズ制限**］ブロックで、［**大きな複合ファイルをスキャンしない**］をオンにします。タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

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

6. ［**スキャン技術**］ブロックで、スキャンで使用する方法の名前の横にあるチェックボックスをオンにします。

   - **iSwift**：特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。

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

7. 変更内容を保存します。

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

定義データベースとソフトウェアモジュールのアップデート

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

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

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

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

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

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

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

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

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

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

定義データベースが長期間アップデートされていない場合、アップデートパッケージのサイズが大きくなり、インターネットトラフィックが最大で数十 MB まで増加することがあります。

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

アップデート結果、およびアップデートタスクの実行中に発生するイベントに関する情報が Kaspersky Endpoint Security のレポートに記録されます。

本製品が Light Agent モードで動作している場合、定義データベースとモジュールのアップデート時に特別な考慮事項が適用されます。

データベースと製品機能のアップデートシナリオ

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

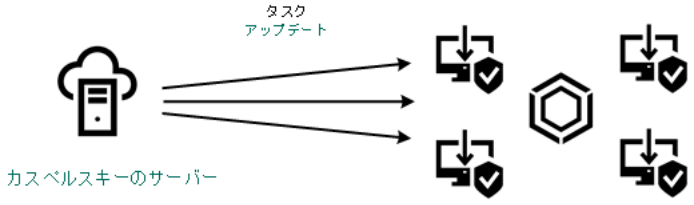
ユーザーのコンピューター上で次のオブジェクトがアップデートされます。

- 定義データベース：定義データベースには、マルウェアを識別するシグネチャのデータベース、ネットワーク攻撃の説明、悪意のある Web サイトおよびフィッシングサイトの URL のデータベースと、バナーのデータベース、スパムのデータベースなどのデータが含まれています。
- 製品機能：製品機能のアップデートは、製品に含まれる脆弱性の解決とコンピューターの保護技術の強化のために実施されます。モジュールのアップデートにより、製品機能の動作が変更されたり、新機能が追加される場合があります。

Kaspersky Endpoint Security では、定義データベースと製品機能のアップデート方法として、次の方法をサポートしています：

- カスペルスキーのサーバーからアップデートを実行

  カスペルスキーのアップデートサーバーは世界中のさまざまな国に設置されています。これにより、アップデート処理を高い信頼度で実行できます。あるサーバーからアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を次のサーバーに切り替えます。



カスペルスキーのサーバーからアップデートを実行

- 一元的なアップデート

  一元的なアップデートを使用すると、ネットワーク外部とのインターネットトラフィック量を減らすことができ、なおかつアップデートの監視が容易になります。

  一元的なアップデートでは次の手順を実行します。

  1. 組織ネットワーク内のリポジトリにアップデートパッケージをダウンロードします。

     アップデートパッケージは、管理サーバーの「*管理サーバーのリポジトリへのアップデートのダウンロード*」タスクを使用してリポジトリにダウンロードされます。

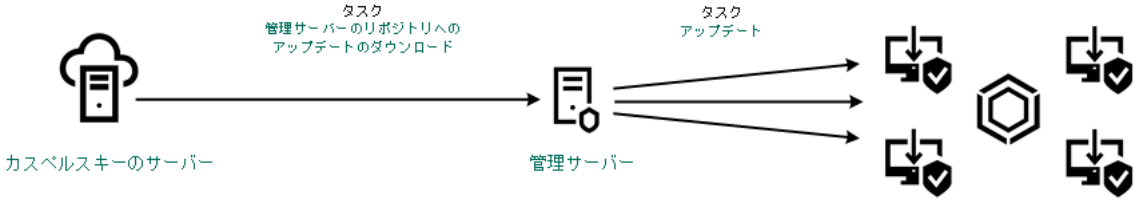
  2. アップデートパッケージを共有フォルダーにダウンロードします（必要ない場合は省略可能な手順）。

次の方法を使用して共有フォルダーにアップデートパッケージをダウンロードできます。

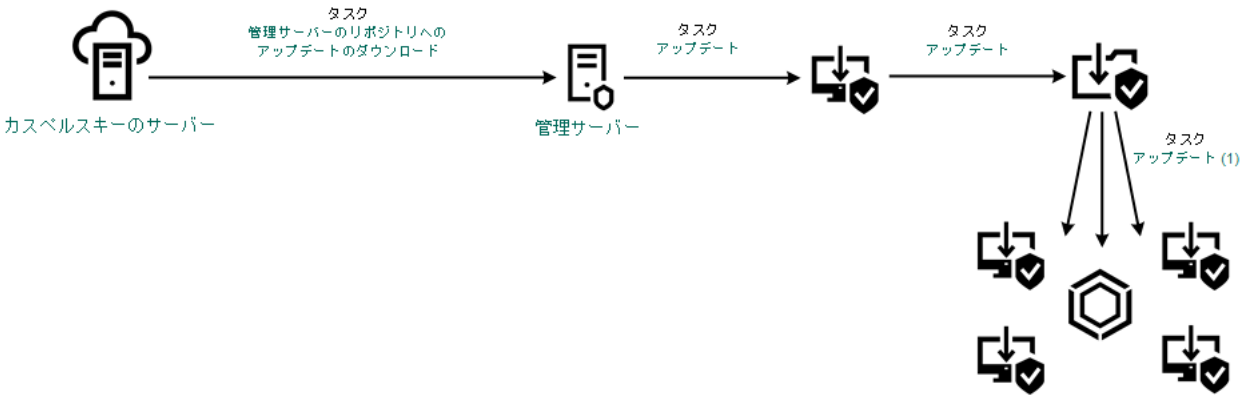
- Kaspersky Endpoint Security の［*定義データベースと製品機能のアップデート*］タスクを使用する。このタスクは、企業のローカルネットワーク内のコンピューター1台を対象とします。
- Kaspersky Update Utility を使用する。Kaspersky Update Utility の使用について詳しくは、カスペルスキーのナレッジベースを参照してください。

3. クライアントコンピューターにアップデートパッケージを配布します。

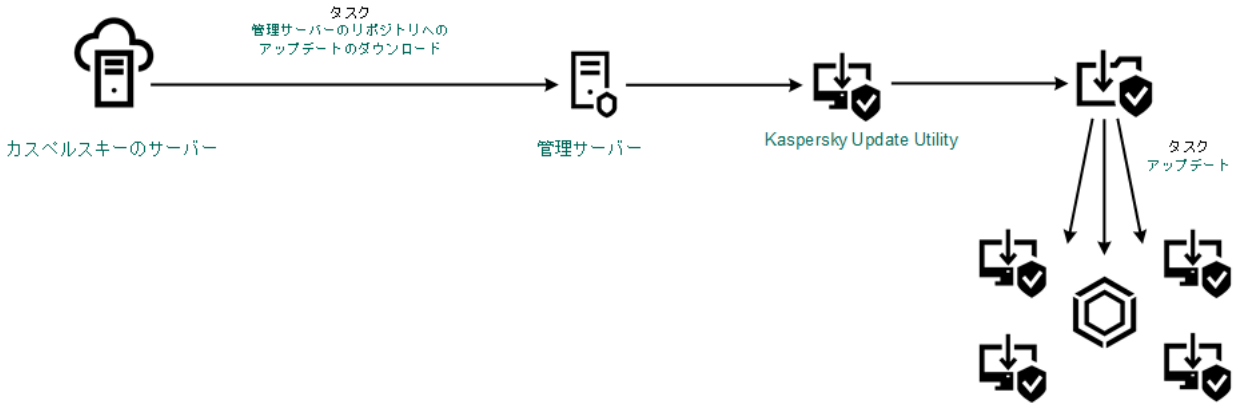
   アップデートパッケージは、Kaspersky Endpoint Security の［*定義データベースと製品機能のアップデート*］タスクを使用して配布されます。管理グループごとに、個数の制限なくアップデートタスクを作成できます。



サーバーリポジトリからアップデート



共有フォルダーからアップデート



Kaspersky Update Utility を使用してのアップデート

Kaspersky Security Center の場合、アップデート元の既定のリストには Kaspersky Security Center 管理サーバーとカスペルスキーのアップデートサーバーが含まれています。Kaspersky Security Center Cloud コンソールの場合、アップデート元の既定のリストにはディストリビューションポイントとカスペルスキーのアップデートサーバーが含まれています。ディストリビューションポイントについて詳しくは、Kaspersky Security Center Cloud コンソールのヘルプを参照してください。リストに他のアップデート元を追加できます。アップデート元には、HTTP/FTP サーバーと共有フォルダーを指定できます。あるアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を次のアップデート元に切り替えます。

アップデートは通常のネットワークプロトコルを使用してカスペルスキーのアップデートサーバーまたはその他の FTP サーバーか HTTP サーバーからダウンロードされます。アップデート元へのアクセスにプロキシサーバーへの接続が必要になった場合、Kaspersky Endpoint Security のポリシー設定でプロキシサーバー設定を指定します。

サーバーリポジトリからアップデート

インターネットトラフィックの増加を抑えるために、ローカルエリアネットワーク上のコンピューターがサーバーリポジトリからアップデートを受け取るように定義データベースと製品機能のアップデートを設定できます。これを行うには、Kaspersky Security Center がカスペルスキーのアップデートサーバーからリポジトリ（FTP サーバー、HTTP サーバー、ネットワークフォルダー、ローカルフォルダーのいずれか）にアップデートパッケージをダウンロードする必要があります。ローカルエリアネットワーク上のコンピューターは、アップデートパッケージを該当するサーバーリポジトリから取得できるようになります。

サーバーリポジトリから定義データベースと製品機能のアップデートを取得するように設定するには、次の手順を実行します：

1. 管理サーバーのリポジトリにアップデートをダウンロードするタスクを設定します（［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスク）。

   ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは、管理サーバークイックスタートウィザードで自動的に作成されます。また、このタスクは1つしか作成できません。既定では、Kaspersky Security Center はアップデートパッケージをフォルダー `\\<server name>\KLSHARE\Updates` にコピーします。管理サーバーのリポジトリにアップデートをダウンロードする方法について詳しくは、Kaspersky Security Center ヘルプを参照してください。

2. 指定したサーバーリポジトリからローカルエリアネットワーク上のコンピューターに定義データベースと製品機能のアップデートを実行するための設定（［*定義データベースと製品機能のアップデート*］タスク）を行います。

   管理コンソール（MMC）で指定したサーバー保管領域からの Kaspersky Endpoint Security のアップデートを設定する方法

   1. Kaspersky Security Center の管理コンソールを開きます。

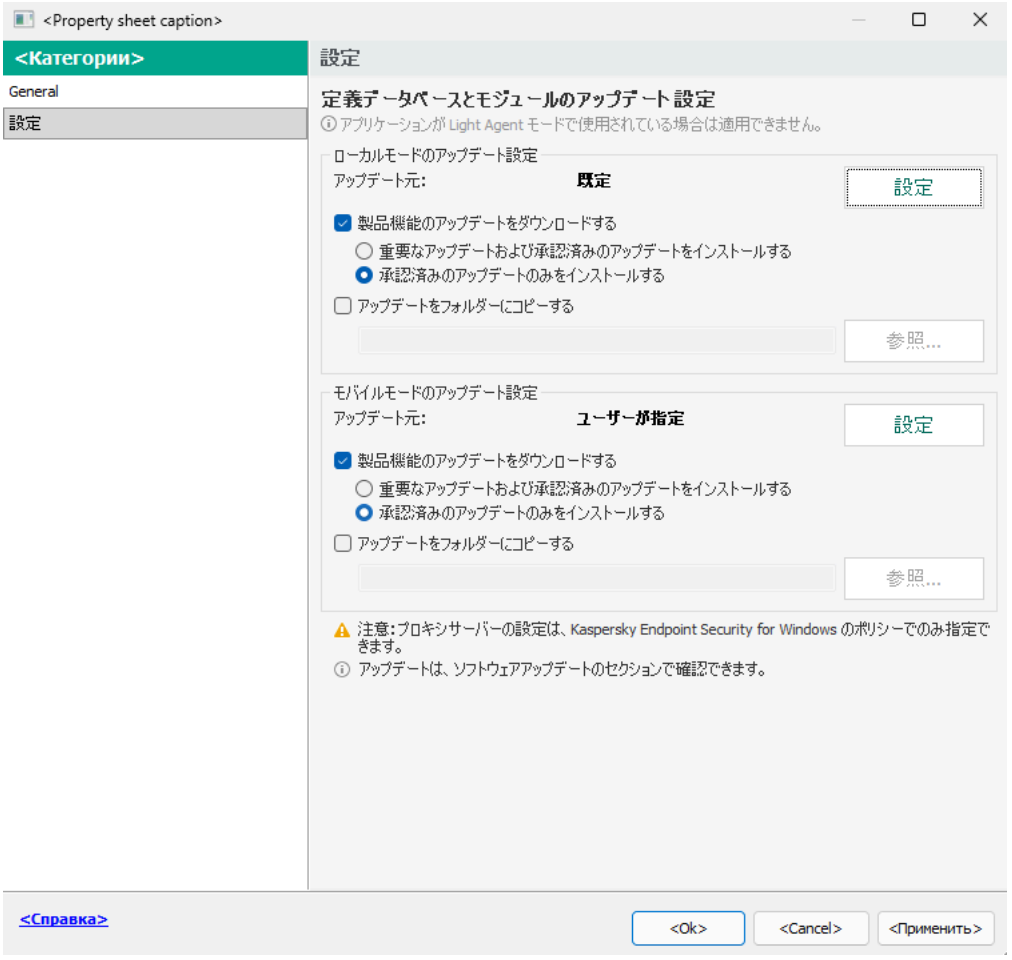
      コンソールツリーで、［**タスク**］を選択します。

   2. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。

      タスクのプロパティウィンドウが表示されます。

      *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

4. ［**ローカルモードのアップデート設定**］ブロックの［**設定**］をクリックします。

5. アップデート元の一覧で、アップデート元として［**Kaspersky Security Center**］が有効になっていることを確認してください。また、［**Kaspersky Security Center**］の優先度が一番高い状態になっている必要があります。

6. 必要に応じて、アップデート元を追加します。

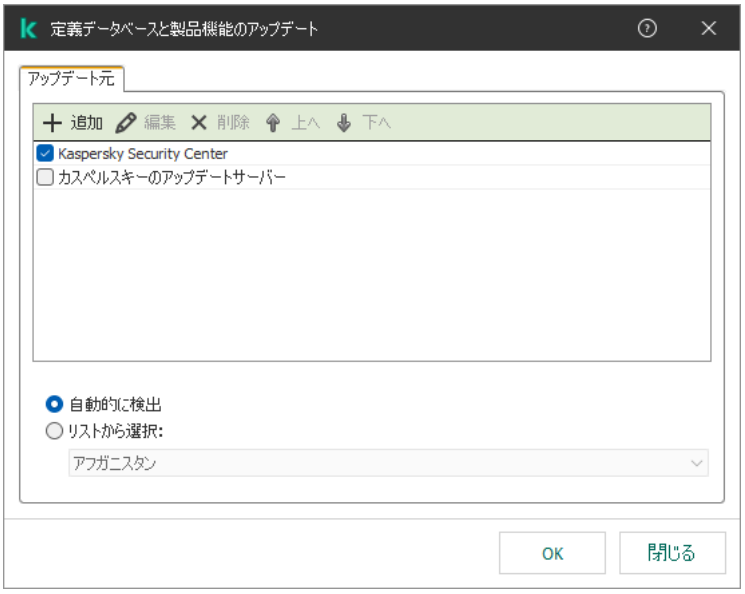
   a. アップデート元のリストで、［**追加**］をクリックします。

   b. ［**アップデート元**］で、Kaspersky Security Center がカスペルスキーのアップデートサーバーから取得したアップデートパッケージをコピーする保存先となっている FTP サーバー、HTTP サーバー、ネットワークフォルダー、またはローカルフォルダーのアドレスを指定します。

   > アップデート元のアドレスは、アップデートのダウンロード先となるサーバー保管領域を指定するときに［**アップデート保存先フォルダー**］に入力したアドレス（*管理サーバーのリポジトリへのアップデートのダウンロード*タスク）と一致する必要があります。

   c. ［**OK**］をクリックします。

アップデート元のリストから削除しなくても、アップデート元を除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。



アップデート元

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

8. タスクのプロパティウィンドウで、［**スケジュール**］セクションを選択し、タスクの実行モードを設定します。

9. 既定では、Kaspersky Endpoint Security はタスクを手動モードで実行します。

10. 変更内容を保存します。

Web コンソールで、指定したサーバー保管領域からの Kaspersky Endpoint Security のアップデートを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. Kaspersky Endpoint Security の **アップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   アップデートタスクは管理サーバークイックスタートウィザードによって自動で作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。

4. アップデート元の一覧で、アップデート元として［**Kaspersky Security Center**］が有効になっていることを確認してください。また、［**Kaspersky Security Center**］の優先度が一番高い状態になっている必要があります。

5. 必要に応じて、アップデート元を追加します。

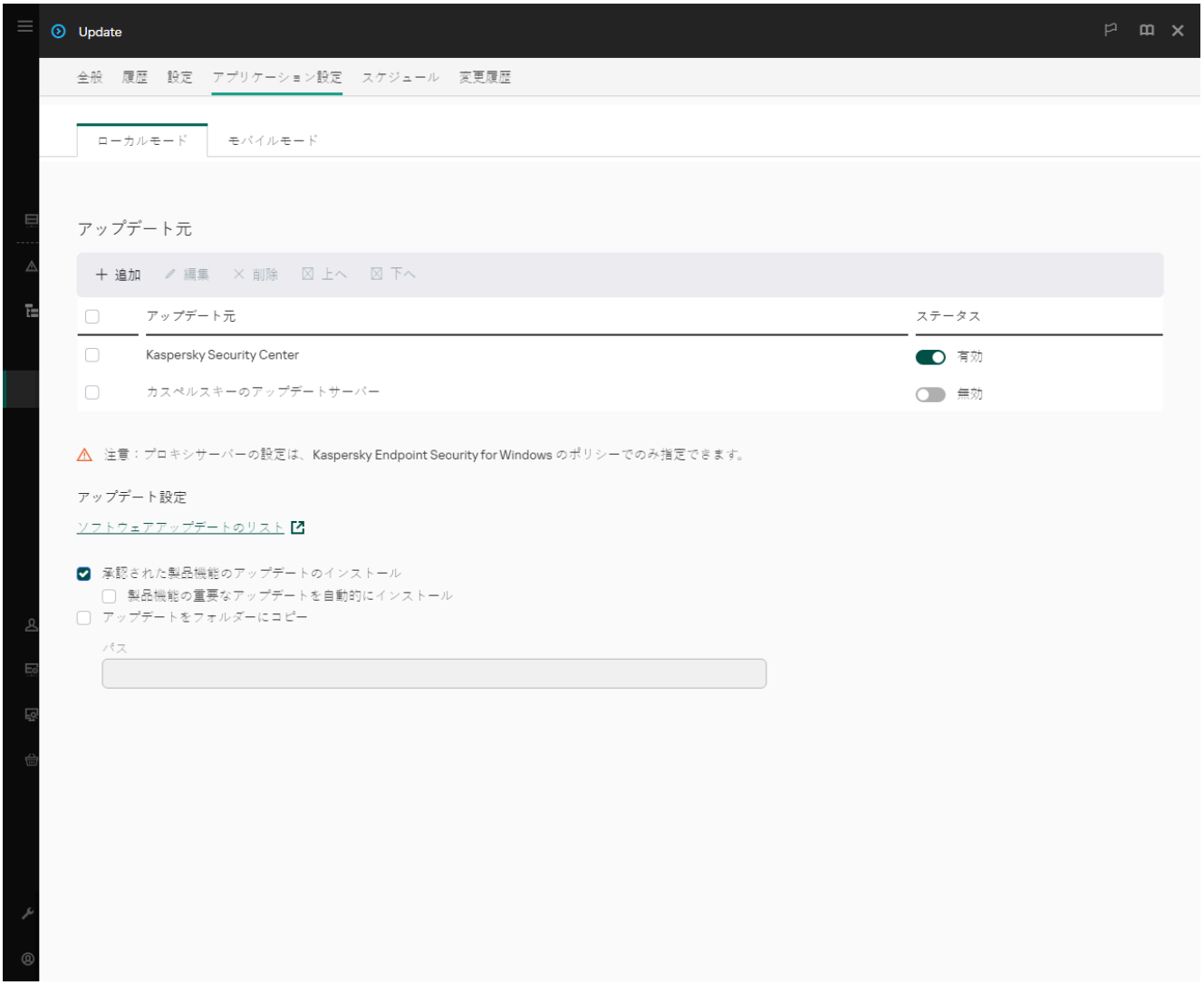
   a. アップデート元のリストで、［**追加**］をクリックします。

   b. ［**アップデート元**］で、Kaspersky Security Center がカスペルスキーのアップデートサーバーから取得したアップデートパッケージをコピーする保存先となっている FTP サーバー、HTTP サーバー、ネットワークフォルダー、またはローカルフォルダーのアドレスを指定します。

      アップデート元のアドレスは、アップデートのダウンロード先となるサーバー保管領域を指定するときに［**アップデート保存先フォルダー**］に入力したアドレス（*管理サーバーのリポジトリへのアップデートのダウンロードタスク*）と一致する必要があります。

   c. ［**保存**］をクリックします。

アップデート元のリストから削除しなくても、アップデート元を除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。



アップデート元

6. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

7. タスクのプロパティウィンドウで、［**スケジュール**］セクションを選択し、タスクの実行モードを設定します。

8. 既定では、Kaspersky Endpoint Security はタスクを手動モードで実行します。

9. 変更内容を保存します。

製品インターフェイスで、指定したサーバー保管領域からの Kaspersky Endpoint Security のアップデートを設定する方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. タスクのプロパティウィンドウで、［**アップデート元の選択**］をクリックします。

4. アップデート元の一覧で、アップデート元として［**Kaspersky Security Center**］が有効になっていることを確認してください。また、［**Kaspersky Security Center**］の優先度が一番高い状態になっている必要があります。

5. 必要に応じて、アップデート元を追加します。

a. アップデート元のリストで、［**追加**］をクリックします。



アップデート元

a. Kaspersky Security Center がカスペルスキーのアップデートサーバーから取得したアップデートパッケージをコピーする保存先となっている FTP サーバー、HTTP サーバー、ネットワークフォルダー、またはローカルフォルダーのアドレスを指定します。

> アップデート元のアドレスは、アップデートのダウンロード先となるサーバー保管領域を指定するときに［**アップデート保存先フォルダー**］に入力したアドレス（*管理サーバーのリポジトリへのアップデートのダウンロードタスク*）と一致する必要があります。

b. ［**選択する**］をクリックします。

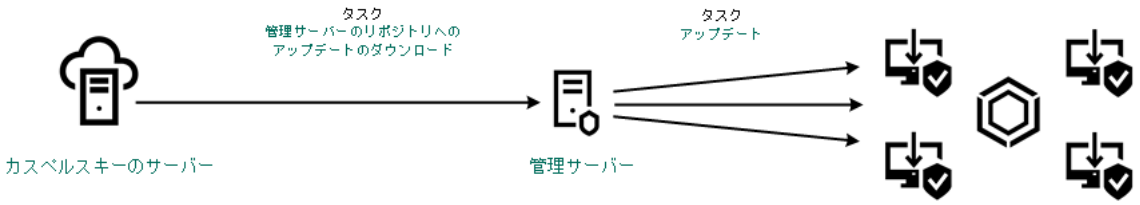
アップデート元のリストから削除しなくても、アップデート元を除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。

6. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

コンピューターが Kaspersky Security Center で管理されている場合は、*定義データベースと製品機能のアップデート*タスクの実行モードを設定することはできません。タスクは手動でのみ実行できます。

7. 変更内容を保存します。



サーバーリポジトリからアップデート

共有フォルダーからアップデート

インターネットトラフィックの増加を抑えるために、ローカルエリアネットワーク上のコンピューターが共有フォルダーからアップデートを受け取るように定義データベースと製品機能のアップデートを設定できます。これを行うには、ローカルエリアネットワーク上のいずれかのコンピューターが Kaspersky Security Center の管理サーバーまたはカスペルスキーのアップデートサーバーからアップデートパッケージを取得し、取得したアップデートパッケージを共有フォルダーにコピーする必要があります。ローカルエリアネットワーク上のその他のコンピューターは、アップデートパッケージを共有フォルダーから取得できるようになります。

共有フォルダーにアップデートパッケージをコピーする Kaspersky Endpoint Security アプリケーションのバージョンおよび言語は、共有フォルダーからデータベースをアップデートするアプリケーションのバージョンと言語と一致している必要があります。アプリケーションのバージョンが一致しない場合、データベースのアップデートはエラーで終了する可能性があります。

共有フォルダーから定義データベースと製品機能のアップデートを取得するように設定するには、次の手順を実行します：

1. サーバーリポジトリからの定義データベースと製品機能のアップデートを設定します。

2. ローカルエリアネットワーク上のいずれかのコンピューターで、アップデートパッケージの共有フォルダーへのコピーを有効にします。

   管理コンソール（MMC）でアップデートパッケージの共有フォルダーへのコピーを有効にする方法

   1. Kaspersky Security Center の管理コンソールを開きます。

   2. コンソールツリーで、［**タスク**］を選択します。

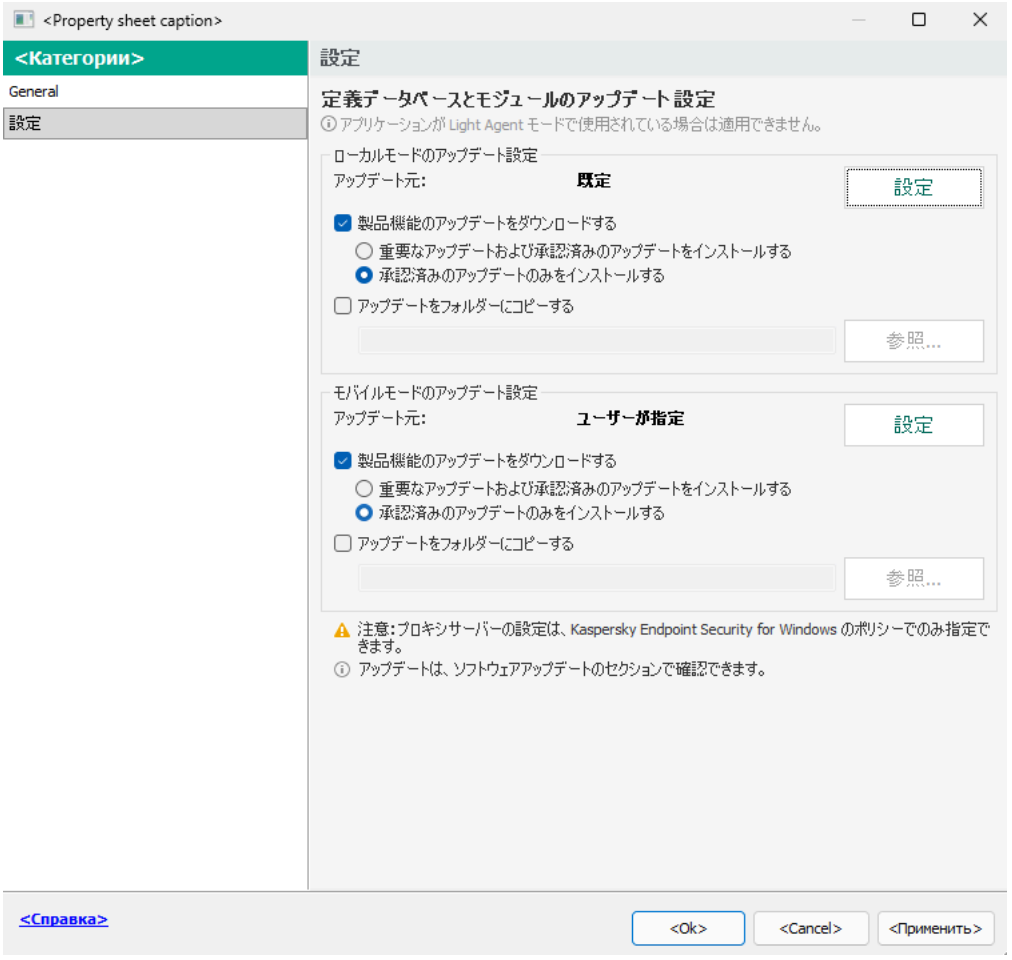
      この［*定義データベースと製品機能のアップデート*］タスクは、その他のコンピューターのアップデート元として動作するコンピューターに割り当てる必要があります。

   3. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。

      タスクのプロパティウィンドウが表示されます。

      *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

5. ［**ローカルモードのアップデート設定**］ブロックの［**設定**］をクリックします。

6. アップデート元を設定します。

   アップデート元は、カスペルスキーのアップデートサーバー、 Kaspersky Security Center の管理サーバー、その他の FTP サーバーまたは HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。

7. ［**アップデートをフォルダーにコピーする**］チェックボックスをオンにします。

8. ［**フォルダーパス**］フィールドに、共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

   フィールドが空白の場合、Kaspersky Endpoint Security はアップデートパッケージをフォルダー `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` にコピーします。

9. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでアップデートパッケージの共有フォルダーへのコピーを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

この［アップデート］タスクは、その他のコンピューターのアップデート元として動作するコンピューターに割り当てる必要があります。

2. Kaspersky Endpoint Security の **アップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   アップデートタスクは管理サーバークイックスタートウィザードによって自動で作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。

4. アップデート元を設定します。

   アップデート元は、カスペルスキーのアップデートサーバー、 Kaspersky Security Center の管理サーバー、その他の FTP サーバーまたは HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。

5. ［**アップデートをフォルダーにコピー**］チェックボックスをオンにします。

6. ［**パス**］フィールドに、共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

   フィールドが空白の場合、Kaspersky Endpoint Security はアップデートパッケージをフォルダー `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` にコピーします。

7. 変更内容を保存します。

製品インターフェイスでアップデートパッケージの共有フォルダーへのコピーを有効にする方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アップデートの配信**］ブロックで、［**アップデートをフォルダーにコピー**］をオンにします。

4. 共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

5. 変更内容を保存します。

3. 指定した共有フォルダーからローカルエリアネットワーク上の残りのコンピューターに定義データベースと製品機能のアップデートを実行するための設定を行います。

管理コンソール（MMC）で共有フォルダーからのアップデートを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. ［**追加**］をクリックします。
   タスクウィザードが起動します。

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］から［**定義データベースと製品機能のアップデート**］を選択します。

4. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。

5. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**定義データベースと製品機能のアップデート**］の順に選択します。

ステップ 2：アップデート元の選択

新しいアップデート元として共有フォルダーを追加します。ソースアドレスは、アップデートパッケージのコピー先となる共有フォルダーを指定する時に［**フォルダーパス**］フィールドに入力したアドレスと一致する必要があります。必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

この*定義データベースと製品機能のアップデート*タスクは、アップデート元として動作するコンピューター以外の、ローカルエリアネットワーク内のコンピューターに割り当てる必要があります。

ステップ 4：タスクを実行するアカウントの選択

*定義データベースと製品機能のアップデート*を実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。

ステップ 5：タスク開始スケジュールの設定

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

ステップ 6：タスク名の定義

*共有フォルダーからのアップデート*などのタスクの名前を入力します。

ステップ 7：タスク作成の完了

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

Web コンソールおよび Cloud コンソールで共有フォルダーからのアップデートを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**アップデート**］を選択します。
   c. ［**タスク名**］に「*共有フォルダーからのアップデート*」などの簡潔な名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

   > このアップデートタスクは、アップデート元として動作するコンピューター以外の、ローカルエリアネットワーク内のコンピューターに割り当てる必要があります。

4. タスク範囲の指定方法に応じて、対象デバイスを選択し、次の手順に進みます。

5. ウィザードを終了します。
   タスクのテーブルに新しいタスクが表示されます。

6. 新しく作成した［アップデート］タスクをクリックします。
   タスクのプロパティウィンドウが表示されます。

7. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。

8. ［**アップデート元**］ブロックの［**追加**］をクリックします。

9. 表示されたウィンドウで、共有フォルダーへのパスを入力します。

   > ソースアドレスは、アップデートパッケージのコピー先となる共有フォルダーを指定するときに［**パス**］に入力したアドレス（先述した手順のを参照）と一致する必要があります。

10. ［**OK**］をクリックします。

11. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

12. 変更内容を保存します。

製品のインターフェイスで共有フォルダーからのアップデートを設定する方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者により[ポリシー内でローカルタスクの使用が禁止](#)されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アップデート元の選択**］をクリックします。

4. 表示されたウィンドウで、［**追加**］をクリックします。

5. 表示されたウィンドウで、共有フォルダーへのパスを入力します。

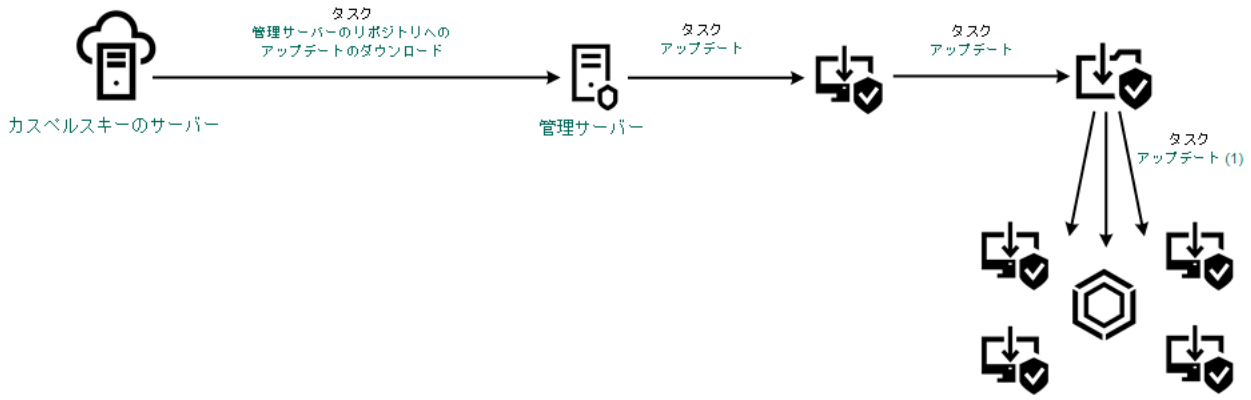
   ソースアドレスは、アップデートパッケージのコピー先となる共有フォルダーを指定するときに入力したアドレス（先述した手順を参照）と一致する必要があります。

6. ［**選択する**］をクリックします。

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

8. 変更内容を保存します。



共有フォルダーからアップデート

Kaspersky Update Utility を使用してのアップデート

インターネットトラフィックの増加を抑えるために、 Kaspersky Update Utility を使用して共有フォルダーにアップデートを配置し、ローカルエリアネットワーク上のコンピューターが共有フォルダーからアップデートを受け取るように、定義データベースと製品機能のアップデートを設定できます。これを行うには、ローカルエリアネットワーク上のいずれかのコンピューターが Kaspersky Security Center の管理サーバーまたはカスペルスキーのアップデートサーバーからアップデートパッケージを取得し、取得したアップデートパッケージを Kaspersky Update Utility を使用して共有フォルダーにコピーする必要があります。ローカルエリアネットワーク上のその他のコンピューターは、アップデートパッケージを共有フォルダーから取得できるようになります。

共有フォルダーにアップデートパッケージをコピーする Kaspersky Endpoint Security アプリケーションのバージョンおよび言語は、共有フォルダーからデータベースをアップデートするアプリケーションのバージョンと言語と一致している必要があります。アプリケーションのバージョンが一致しない場合、データベースのアップデートはエラーで終了する可能性があります。

共有フォルダーから定義データベースと製品機能のアップデートを取得するように設定するには、次の手順を実行します：

1. サーバーリポジトリからの定義データベースと製品機能のアップデートを設定します。

2. ローカルエリアネットワーク内のいずれか1台のコンピューターに Kaspersky Update Utility をインストールします。

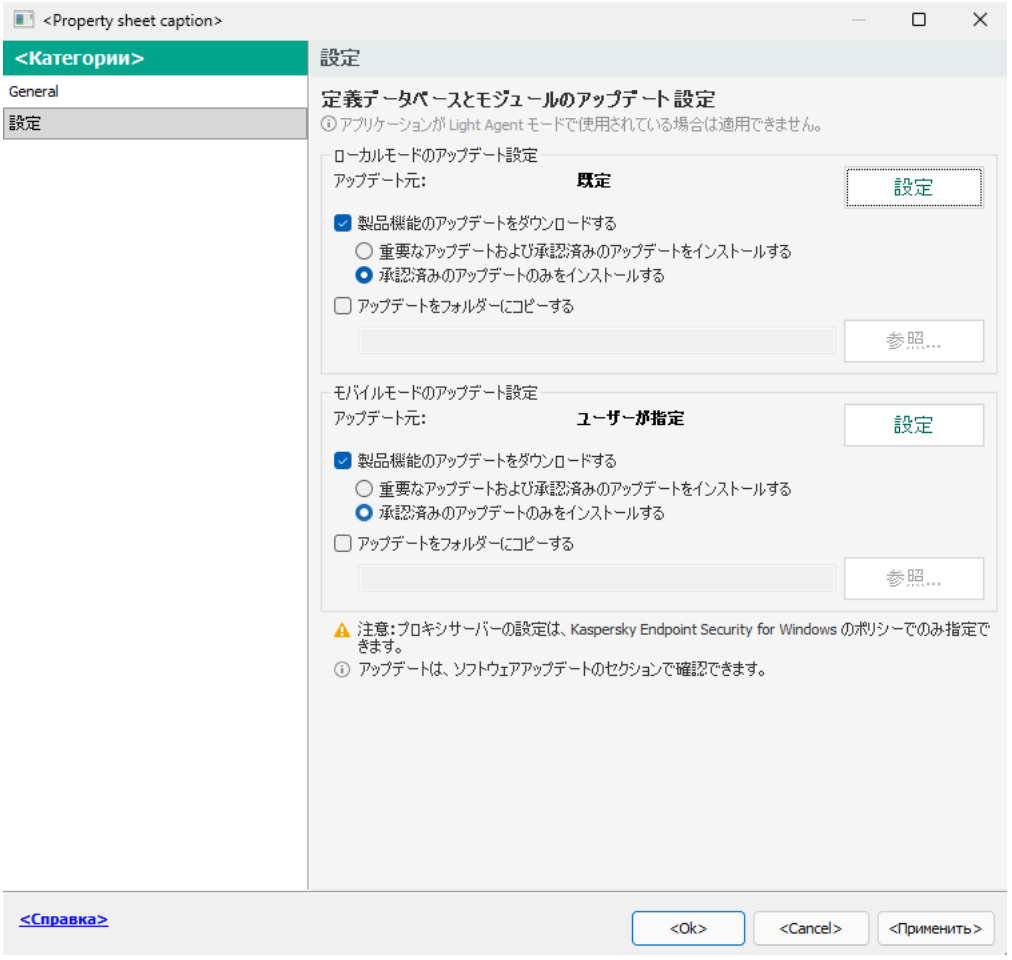
3. アップデートパッケージの共有フォルダーへのコピーを、Kaspersky Update Utility の設定で指定します。

   Kaspersky Update Utility の配布パッケージは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。Kaspersky Update Utility のインストールが完了したら、アップデート元（たとえば、管理サーバーのリポジトリなど）と、アップデートパッケージのコピー先となる共有フォルダーをそれぞれ選択します。Kaspersky Update Utility の使用について詳しくは、カスペルスキーのナレッジベースを参照してください。

4. 指定した共有フォルダーからローカルエリアネットワーク上の残りのコンピューターに定義データベースと製品機能のアップデートを実行するための設定を行います。

管理コンソール（MMC）で共有フォルダーからのアップデートを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
   *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。
4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

5. ［**ローカルモードのアップデート設定**］ブロックの［**設定**］をクリックします。
6. アップデート元のリストで、［**追加**］をクリックします。
7. 表示されたウィンドウで、共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

   ソースアドレスは、Kaspersky Update Utility の設定で指定したアドレスと一致する必要があります。

8. ［**OK**］をクリックします。

9. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

10. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで共有フォルダーからのアップデートを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. Kaspersky Endpoint Security の **アップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   アップデートタスクは管理サーバークイックスタートウィザードによって自動で作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。

4. アップデート元のリストで、［**追加**］をクリックします。

5. 表示されたウィンドウで、共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

   ソースアドレスは、Kaspersky Update Utility の設定で指定したアドレスと一致する必要があります。

6. ［**OK**］をクリックします。

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

8. 変更内容を保存します。

製品のインターフェイスで共有フォルダーからのアップデートを設定する方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者により[ポリシー内でローカルタスクの使用が禁止](#)されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. タスクのプロパティウィンドウで、［**アップデート元の選択**］をクリックします。

4. アップデート元のリストで、［**追加**］をクリックします。



アップデート元

5. 共有フォルダーへの UNC パスを入力します（例：`\\<server name>\KLSHARE\Updates`）。

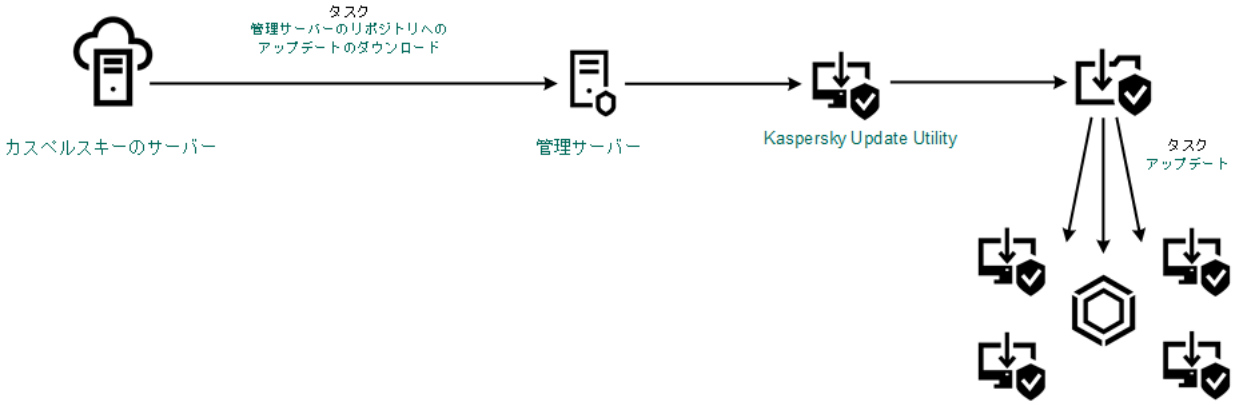
ソースアドレスは、Kaspersky Update Utility の設定で指定したアドレスと一致する必要があります。

6. ［**選択する**］をクリックします。

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

8. 変更内容を保存します。



Kaspersky Update Utility を使用してのアップデート

モバイルモードでのアップデート

*モバイルモード*とは、コンピューターを組織ネットワーク外で使用しているとき（*オフラインのコンピューター*）の Kaspersky Endpoint Security の操作モードです。オフラインのコンピューターとモバイルユーザーについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

組織ネットワーク外のオフラインコンピューターは、管理サーバーに接続して定義データベースと製品機能のアップデートを行うことができません。既定では、カスペルスキーのアップデートサーバーのみが、モバイルモードでデータベースと製品機能をアップデートするためのアップデート元として使用されます。インターネット接続でプロキシサーバーを使用するかどうかはモバイルユーザーポリシーで指定されます。モバイルユーザーポリシーは別途作成する必要があります。Kaspersky Endpoint Security がモバイルモードに切り替わると、アップデートタスクが 2 時間ごとに起動されます。

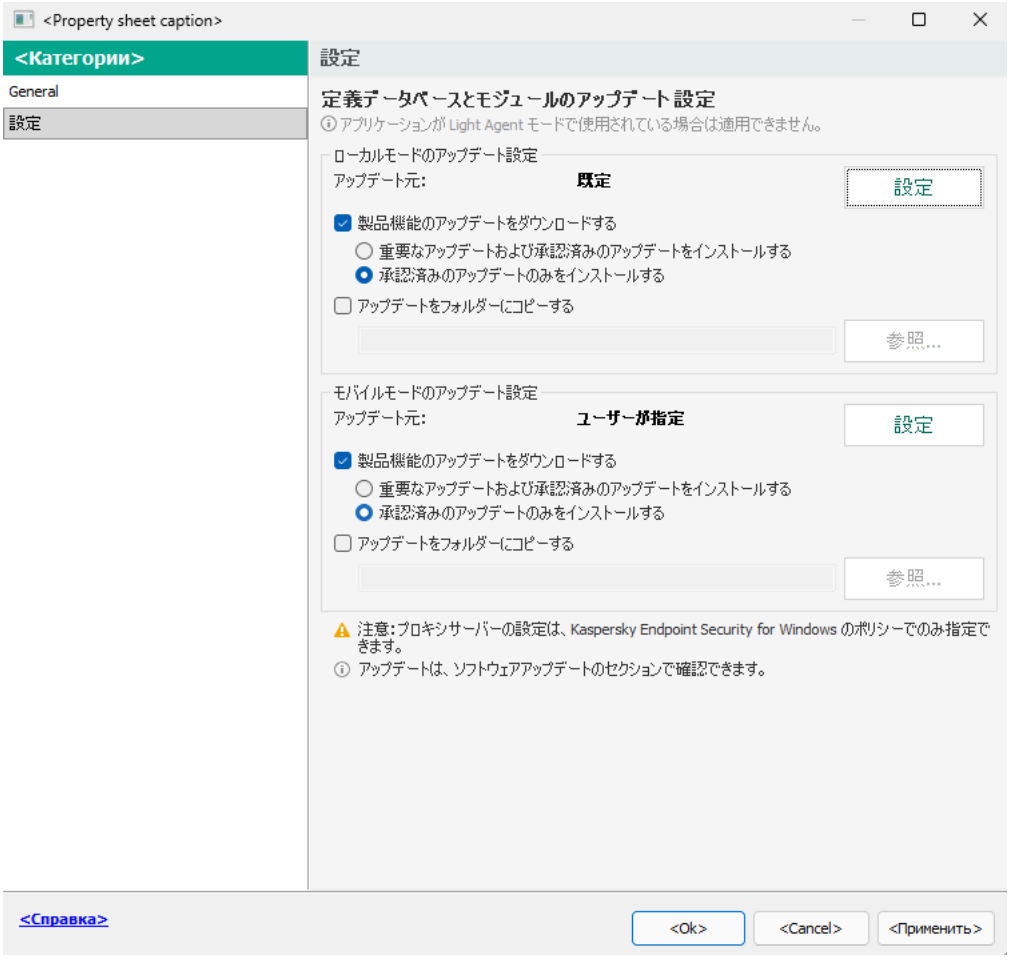
管理コンソール（MMC）でモバイルモードのアップデート設定をする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

5. ［**モバイルモードのアップデート設定**］ブロックの［**設定**］をクリックします。

6. アップデート元を設定します。アップデート元は、カスペルスキーのアップデートサーバー、その他の FTP サーバーおよび HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでモバイルモードのアップデート設定をする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. Kaspersky Endpoint Security の **アップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   アップデートタスクは管理サーバークイックスタートウィザードによって自動で作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**モバイルモード**］タブを選択します。

4. アップデート元を設定します。アップデート元は、カスペルスキーのアップデートサーバー、その他の FTP サーバーおよび HTTP サーバー、ローカルフォルダー、ネットワークフォルダーを指定できます。

5. 変更内容を保存します。

指定した設定に応じて、クライアントコンピューターがモバイルモードに切り替わったときも定義データベースと製品機能がアップデートされます。

アップデートタスクの開始と停止

Kaspersky Endpoint Security アップデートタスクは、選択したアップデートタスクの実行方法にかかわらず、いつでも開始または停止することができます。

アップデートタスクを開始または停止するには、次の手順を実行します：

1. メインウィンドウで、［**アップデート**］をクリックします。
2. ［**定義データベースと製品機能のアップデート**］タイルで、アップデートを開始する場合は［**アップデートする**］をクリックします。

   Kaspersky Endpoint Security は製品機能および定義データベースのアップデートを開始します。タスクの進捗、ダウンロードされたファイルおよびアップデート元が表示されます。［**アップデートの停止**］ボタンを押すことでいつでもタスクを停止することができます。

簡略化した製品インターフェイスが表示されている場合にアップデートタスクを開始または停止するには：

1. タスクバーの通知領域にある製品アイコンを右クリックして、コンテキストメニューを表示します。
2. コンテキストメニューの［**タスク**］で、以下のいずれかを実行します：
   - 実行されていないアップデートタスクを選択して開始する
   - 実行中のアップデートタスクを選択して停止する
   - 一時停止中のアップデートタスクを選択して再開する

別のユーザーアカウントの権限でのアップデートタスクの開始

既定では、Kaspersky Endpoint Security のアップデートタスクは、オペレーティングシステムへのログインに使用したアカウントを持つユーザーの代わりに開始されます。ただし、Kaspersky Endpoint Security は、必要な権利がないことが原因でユーザーがアクセスできないアップデート元（アップデートパッケージを含む共有フォルダーからアップデートを実行する場合など）やプロキシサーバーの認証が設定されていないアップデート元からアップデートされる場合があります。製品設定でアップデートの権限を持つユーザーを指定して、そのユーザーアカウントで Kaspersky Endpoint Security のアップデートタスクを開始できます。

別のユーザーアカウントでアップデートタスクを開始するには：

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者により[ポリシー内でローカルタスクの使用が禁止](#)されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**ユーザー権限で定義データベースをアップデート**］をクリックします。

4. 表示されるウィンドウで、［**他のユーザー**］を選択します。

5. アップデート元にアクセスするために必要な権限をもつユーザーのアカウント認証情報を入力します。

6. 変更内容を保存します。

アップデートタスクの実行方法の選択

何らかの理由（コンピューターの電源が入っていないなど）でアップデートタスクを実行できない場合、スキップされたタスクが実行可能になると同時に自動的に開始されるように設定することができます。

アップデートタスクの実行方法に［**スケジュールで指定**］を選択した場合、および Kaspersky Endpoint Security の開始時間とアップデートタスクの開始スケジュールが一致する場合は、製品が開始されるまでアップデートタスクの実行を延期することができます。アップデートタスクは、Kaspersky Endpoint Security の開始後、指定した期間が経過した後にのみ実行できます。

アップデートタスクの実行方法を選択するには：

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**実行方法**］をクリックします。

4. 表示されたウィンドウで、アップデートタスクの実行モードを選択します。

- Kaspersky Endpoint Security で、アップデートパッケージがアップデート元から使用できるかどうかに応じてアップデートタスクを実行するには、［**自動**］を選択します。Kaspersky Endpoint Security によるアップデートパッケージの確認の頻度は、ウイルスの発生中には高くなり、そうでないときには低くなります。

- アップデートタスクを手動で開始するには、［**手動で開始**］を選択します。

- アップデートタスクの実行スケジュールを設定するには、別のオプションを選択します。アップデートタスクを開始する詳細について設定します：

  - ［**本製品の起動からタスク開始までの時間**］に、Kaspersky Endpoint Security 開始後、アップデートタスクを開始するまでの期間を指定します。

  - 実行されなかったタスクを機会のあり次第実行するには、［**コンピューターがオフの場合、スケジュールされたスキャンを翌日に実行する**］をオンにします。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。

5. 変更内容を保存します。

アップデート元の追加

「*アップデート元*」は、Kaspersky Endpoint Security の定義データベースと機能のアップデートを含むリソースです。

アップデート元には、Kaspersky Security Center サーバーやカスペルスキーのアップデートサーバー、ネットワークフォルダーまたはローカルフォルダーが含まれます。

アップデート元の既定のリストには Kaspersky Security Center とカスペルスキーのアップデートサーバーが含まれています。リストに他のアップデート元を追加できます。アップデート元には、HTTP/FTP サーバーと共有フォルダーを指定できます。

Kaspersky Endpoint Security は、カスペルスキーのアップデートサーバーである場合を除き、HTTPS サーバーからのアップデートをサポートしません。

複数のリソースがアップデート元として選択されている場合は、リスト上位のリソースから次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。

既定では、Kaspersky Endpoint Security は Kaspersky Security Center サーバーを最初のアップデート元として使用します。これにより、アップデート時のトラフィックを節約することができます。ポリシーがコンピューターに適用されていない場合、製品が Kaspersky Security Center サーバーにアクセスできない可能性があるため、ローカルタスクの *定義データベースと製品機能のアップデート* 設定でカスペルスキーサーバーが最初のアップデート元として選択されます。

本製品が Light Agent モードで実行されている場合、SVM 上のフォルダーがアップデート元として選択されます。

管理コンソール（MMC）でアップデート元を追加する方法

1. Kaspersky Security Center の管理コンソールを開きます。

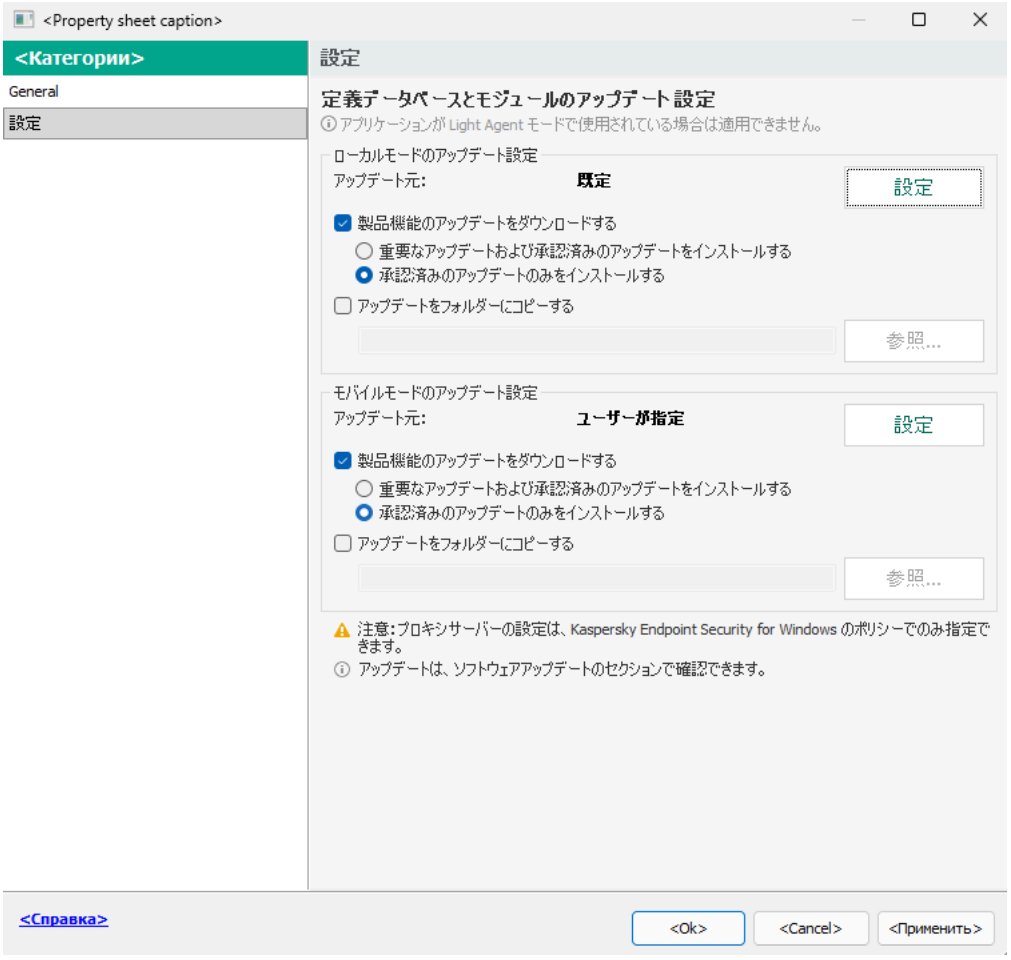
   コンソールツリーで、［**タスク**］を選択します。

2. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

4. ［**ローカルモードのアップデート設定**］ブロックの［**設定**］をクリックします。



アップデート元

5. アップデート元のリストで、［**追加**］をクリックします。

6. ［**アップデート元**］フィールドで、アップデートパッケージが含まれる FTP/HTTP サーバーのアドレス、ネットワークフォルダーまたはローカルフォルダーを指定します。

   アップデート元について次のパス形式が使用されます：

   - FTP サーバーまたは HTTP サーバーの場合は、その Web アドレスまたは IP アドレスを入力します。

     例：`http://dnl-01.geo.kaspersky.com/` または `93.191.13.103`。

     FTP サーバーの場合は、認証設定をアドレスに含めるかたちで次の形式で指定できます：`ftp://<username>:<password>@<node>:<port>`

   - ネットワークフォルダーの場合は、UNC パスを入力します。

     例：「`\\Server\Share\Update distribution`」。

   - ローカルフォルダーの場合は、フォルダーへの完全パスを入力します。

     例：「`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`」。

   アップデート元のリストから削除しなくても、アップデート元を除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

7. ［OK］をクリックします。

8. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1 番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

9. 必要に応じて、モバイルモードのアップデート元を追加します。*モバイルモード*とは、コンピューターを組織ネットワーク外で使用しているとき（*オフラインのコンピューター*）の Kaspersky Endpoint Security の操作モードです。

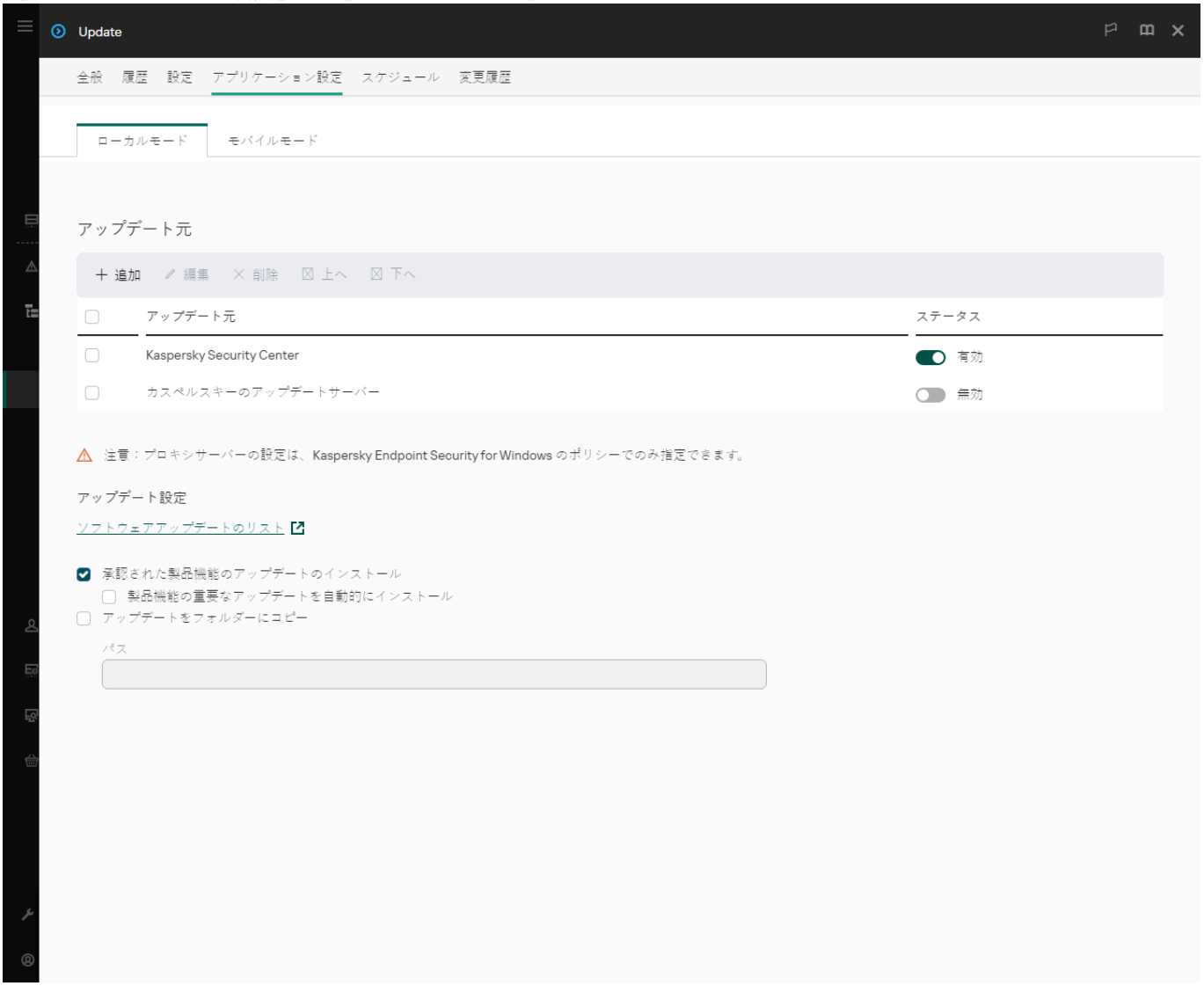
10. 変更内容を保存します。

Web コンソールと Cloud コンソールでアップデート元を追加する方法

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

2. Kaspersky Endpoint Security の **アップデート**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
   アップデートタスクは管理サーバークイックスタートウィザードによって自動で作成されます。アップデートタスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。



アップデート元

4. アップデート元のリストで、［**追加**］をクリックします。

5. 表示されるウィンドウで、アップデートパッケージが含まれる FTP/HTTP サーバーのアドレス、ネットワークフォルダーまたはローカルフォルダーを指定します。
   アップデート元について次のパス形式が使用されます：

   - FTP サーバーまたは HTTP サーバーの場合は、その Web アドレスまたは IP アドレスを入力します。
     例：`http://dnl-01.geo.kaspersky.com/` または `93.191.13.103`。

FTP サーバーの場合は、認証設定をアドレスに含めるかたちで次の形式で指定できます：`ftp://<username>:<password>@<node>:<port>`

- ネットワークフォルダーの場合は、UNC パスを入力します。

  例：「`\\Server\Share\Update distribution`」。

- ローカルフォルダーの場合は、フォルダーへの完全パスを入力します。

  例：「`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`」。

アップデート元のリストから削除しなくても、アップデート元を除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。

6. ［**OK**］をクリックします。

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

   1番上で指定したアップデート元からアップデートを実行できない場合、Kaspersky Endpoint Security はアップデート元を自動的に次のアップデート元に切り替えます。

8. 必要に応じて、モバイルモードのアップデート元を追加します。*モバイルモード*とは、コンピューターを組織ネットワーク外で使用しているとき（*オフラインのコンピューター*）の Kaspersky Endpoint Security の操作モードです。

9. 変更内容を保存します。

製品インターフェイスでアップデート元を追加する方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アップデート元の選択**］をクリックします。

4. 表示されたウィンドウで、［**追加する**］をクリックします。



アップデート元

5. 表示されるウィンドウで、アップデートパッケージが含まれる FTP/HTTP サーバーのアドレス、ネットワークフォルダーまたはローカルフォルダーを指定します。

   アップデート元について次のパス形式が使用されます：

   - FTP サーバーまたは HTTP サーバーの場合は、その Web アドレスまたは IP アドレスを入力します。

     例：`http://dnl-01.geo.kaspersky.com/` または `93.191.13.103`。

     FTP サーバーの場合は、認証設定をアドレスに含めるかたちで次の形式で指定できます：`ftp://<username>:<password>@<node>:<port>`

   - ネットワークフォルダーの場合は、UNC パスを入力します。

     例：「`\\Server\Share\Update distribution`」。

   - ローカルフォルダーの場合は、フォルダーへの完全パスを入力します。

     例：「`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`」。

6. ［**選択する**］をクリックします。

7. 必要に応じて、［**上へ**］と［**下へ**］でアップデート元の優先順位を編集します。

8. 変更内容を保存します。

製品機能のアップデート

製品機能のアップデートには、エラーの修正、パフォーマンスの向上、新機能の追加が含まれます。新しい製品機能のアップデートが利用可能になると、これらのアップデートのインストールを確認する必要があります。製品のインターフェイスまたは Kaspersky Security Center のどちらからでも製品機能のアップデートのインストールの確認ができます。アップデートが利用可能な場合は、Kaspersky Endpoint Security のメインウィンドウに通知（）が表示されます。製品機能のアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。

製品のアップデートのインストール後、コンピューターの再起動が必要になることがあります。

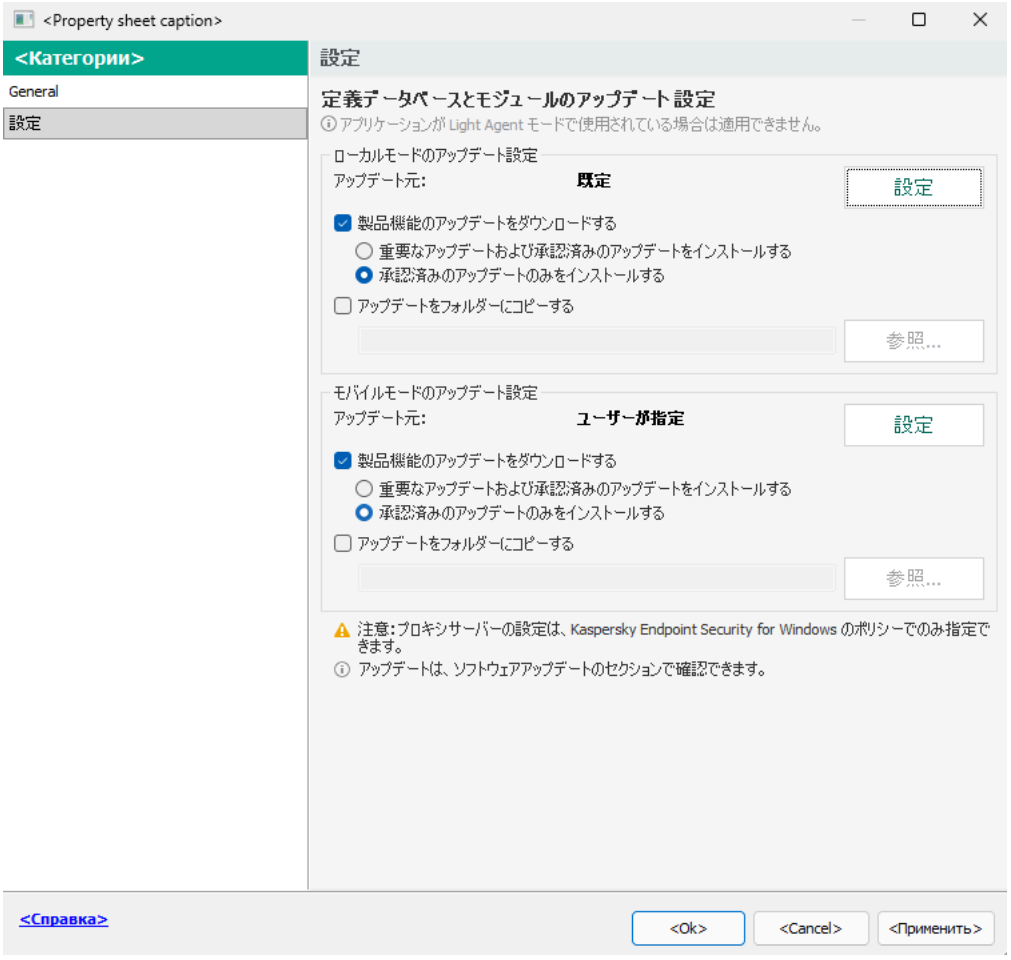
管理コンソール（MMC）で製品機能のアップデートを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。



［定義データベースと製品機能のアップデート］タスクの設定

5. ［**ローカルモードのアップデート設定**］ブロックで、［**製品機能のアップデートをダウンロードする**］をオンにします。

   製品機能のアップデートをダウンロードしないようにしたい場合は、［**製品機能のアップデートをダウンロードする**］をオフにして、ユーザーによるローカルタスクの使用を禁止します。

6. インストールする製品機能のアップデートを選択します。

   - **重要なアップデートおよび承認済みのアップデートをインストールする**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。

   - **承認済みのアップデートのみをインストールする**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。

7. 必要に応じて、モバイルモードの製品機能のアップデートを設定してください。*モバイルモード*とは、コンピューターを組織ネットワーク外で使用しているとき（*オフラインのコンピューター*）の Kaspersky Endpoint Security の操作モードです。

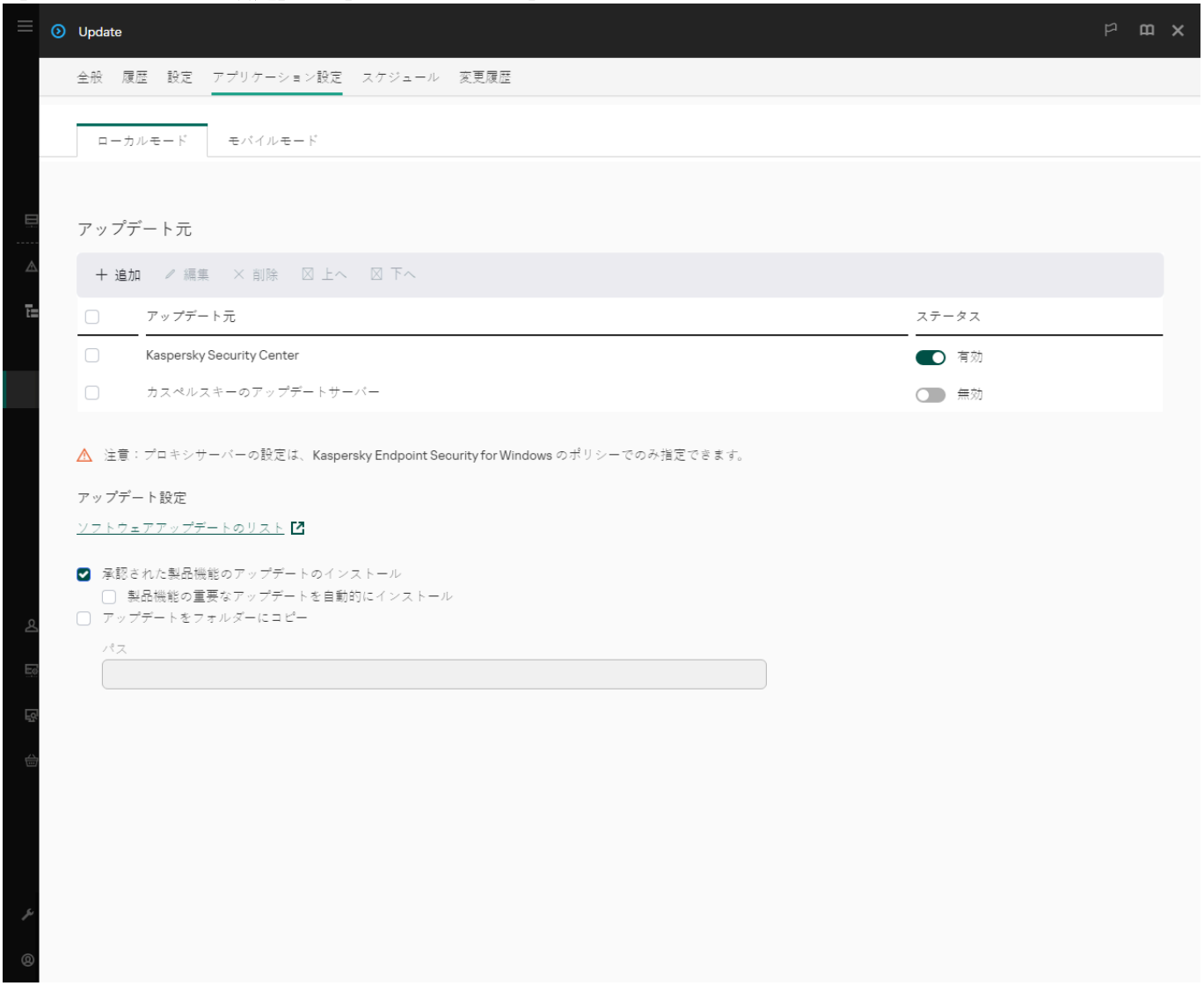
8. 変更内容を保存します。

Web コンソールと Cloud コンソールで製品機能のアップデートを設定する方法

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

2. Kaspersky Endpoint Security の **定義データベースと製品機能のアップデート**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
   *定義データベースと製品機能のアップデート*タスクは管理サーバークイックスタートウィザードによって自動で作成されます。*定義データベースと製品機能のアップデート*タスクを作成するには、ウィザードの実行中に、Kaspersky Endpoint Security for Windows 管理プラグインをインストールします。

3. ［**アプリケーション設定**］→［**ローカルモード**］タブを選択します。



［アップデート］タスクの設定

4. ［**アップデート設定**］で、インストールする製品機能のアップデートを選択します。

   - **承認された製品機能のアップデートのインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。

   - **製品機能の重要なアップデートを自動的にインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。

   製品機能のアップデートをダウンロードしないようにしたい場合は、［**承認された製品機能のアップデートのインストール**］および［**製品機能の重要なアップデートを自動的にインストール**］をオフにして、ユーザーによるローカルタスクの使用を禁止します。

5. 必要に応じて、モバイルモードの製品機能のアップデートを設定してください。*モバイルモード*とは、コンピューターを組織ネットワーク外で使用しているとき（*オフラインのコンピューター*）の Kaspersky Endpoint Security の操作モードです。

6. 変更内容を保存します。

製品インターフェイスで製品機能のアップデートを設定する方法

製品のインターフェイスでグループタスク［*定義データベースと製品機能のアップデート*］を設定することはできません。ユーザーは、ローカルアップデートタスク［*定義データベースと製品機能のアップデート*］のみ使用できます。*定義データベースと製品機能のアップデート*タスクが表示されない場合は、管理者によりポリシー内でローカルタスクの使用が禁止されていることを意味します。

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. タスクのリストが表示されます。*定義データベースと製品機能のアップデート*タスクを選択してボタン（⚙）をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**製品機能のダウンロードおよびアップデートのインストール**］ブロックで、［**製品機能のアップデートをダウンロード**］をオンにします。

4. インストールする製品機能のアップデートを選択します。

   - **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。

   - **承認済みのアップデートのみをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。

5. 変更内容を保存します。

プロキシサーバーを使用してのアップデート

定義データベースおよび製品機能のアップデートのアップデート元からのダウンロード用に、必要に応じてプロキシサーバー設定を指定できます。アップデート元が複数ある場合、すべてのアップデート元にプロキシサーバー設定が適用されます。一部のアップデート元ではプロキシサーバーを使用する必要がない場合、ポリシーのプロパティでプロキシサーバーの使用を無効化できます。Kaspersky Endpoint Security は、プロキシサーバーを使用して、Kaspersky Security Network およびアクティベーションサーバーにアクセスします。

アップデート元へのプロキシサーバー経由の接続を設定するには：

1. Web コンソールのメインウィンドウで、⚙ をクリックします。
   管理サーバーのプロパティウィンドウが表示されます。

2. ［**インターネットアクセスの設定**］に移動します。

3. ［**プロキシサーバーを使用する**］チェックボックスをオンにします。

4. プロキシサーバーのアドレスと認証設定（ユーザー名とパスワード）を入力してプロキシサーバーの接続設定を指定します。

5. 変更内容を保存します。

特定の管理グループでプロキシサーバーの使用を無効にするには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

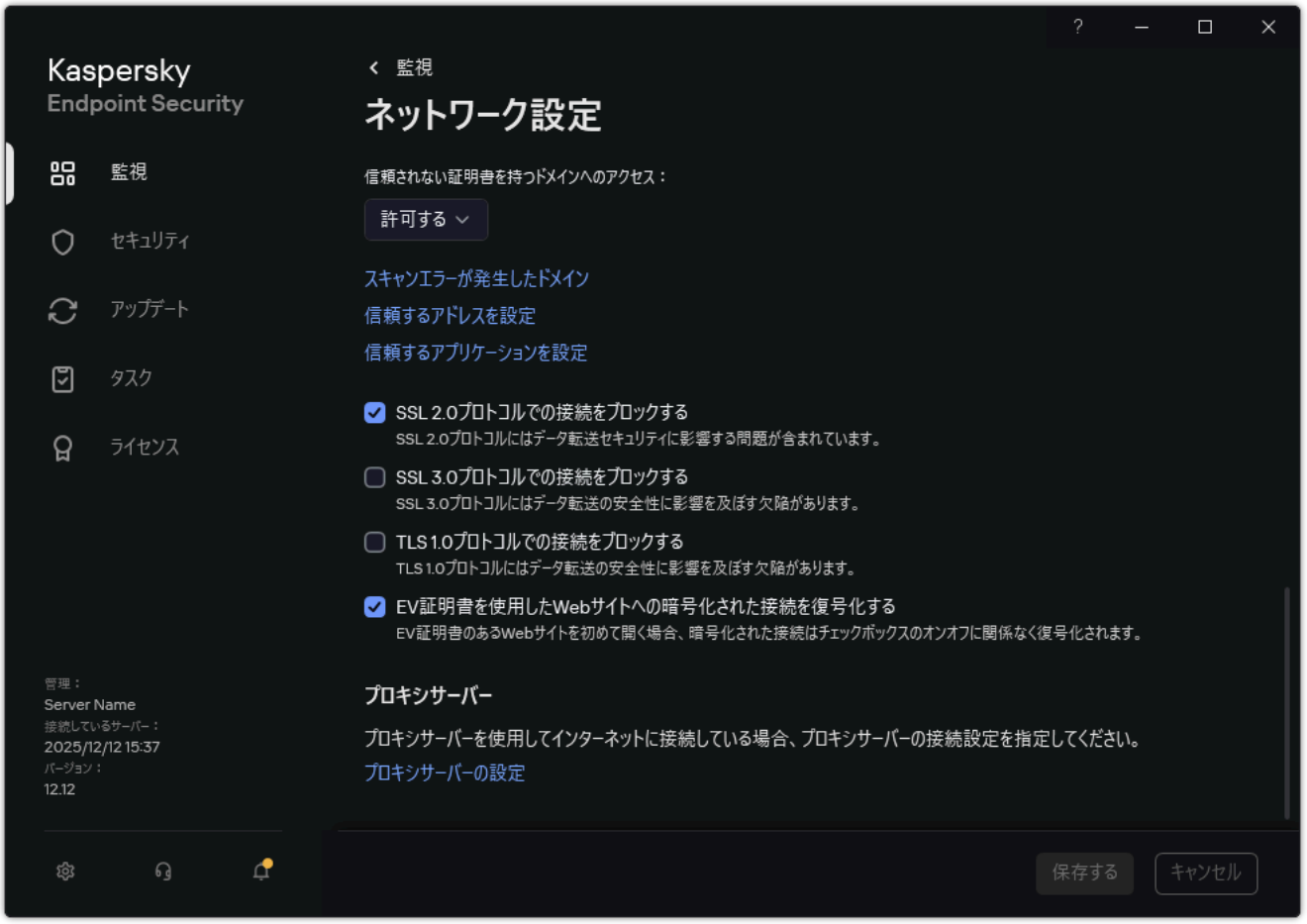
4. ［**全般設定**］→［**ネットワーク設定**］に移動します。

5. ［**プロキシサーバー**］ブロックの［**設定**］をクリックします。

6. 表示されたウィンドウで、［**ローカルアドレスにはプロキシサーバーを使用しない**］をオンにします。
7. 変更内容を保存します。

製品インターフェイスでプロキシサーバーを設定するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。



製品のネットワーク設定

3. ［**プロキシサーバー**］セクションで、［**プロキシサーバーの設定**］をクリックします。



プロキシサーバーの接続設定

4. 表示されたウィンドウで、プロキシサーバーのアドレスを特定する方法を選択します：

   - **OSのプロキシサーバー設定を使用する**

     既定ではこのオプションが選択されます。Kaspersky Endpoint Security はオペレーティングシステムの設定で定義されているプロキシサーバーを使用します

   - **プロキシサーバーを設定する**

     このオプションを選択した場合は、プロキシサーバーへの接続の設定（プロキシサーバーのアドレスおよびポート）を指定する必要があります。

5. プロキシサーバー上での本製品の認証方法を選択します。既定では、本製品は現在のユーザーのドメインの NTLM 認証を使用します。

6. 共有フォルダーから定義データベースと製品機能をアップデートする時にプロキシサーバーの使用を無効にする場合は、［**ローカルアドレスにはプロキシサーバーを使用しない**］をオンにします。

7. 変更内容を保存します。

Kaspersky Endpoint Security は製品機能および定義データベースのアップデートのダウンロードにプロキシサーバーを使用します。Kaspersky Endpoint Security は、プロキシサーバーを使用して、KSN サーバーおよびカスペルスキーのアクティベーションサーバーにアクセスします。プロキシサーバーで認証情報が必要で、ユーザーアカウントの認証情報が提供されていないか正しくなかった場合、Kaspersky Endpoint Security はユーザー名とパスワードを入力するよう促します。

前回のアップデートのロールバック

定義データベースと製品機能が初めてアップデートされてから、定義データベースと製品機能を以前のバージョンにロールバックする機能が有効になります。

ユーザーがアップデートプロセスを開始するごとに、Kaspersky Endpoint Security によって現在の定義データベースと製品機能のバックアップコピーが作成されます。これにより、必要に応じて、定義データベースと製品機能を前のバージョンにロールバックすることができます。前回のアップデートへのロールバックは、新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。

Light Agent モードの Kaspersky Endpoint Security は、*アップデートのロールバック*タスクをサポートしません。

管理コンソール（MMC）で前回のアップデートにロールバックする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

   タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

1. ［**Kaspersky Endpoint Security for Windows (12.12)**］→［**アップデートのロールバック**］の順に選択します。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：タスク開始スケジュールの設定

タスクのスケジュールを設定します（たとえば、［手動］など）。

ステップ 4：タスク名の定義

タスクの名前を入力します。

ステップ 7：タスク作成の完了

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

Web コンソールで前回のアップデートにロールバックする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**アップデートのロールバック**］を選択します。
   c. ［**タスク名**］に「*アップデートのロールバック*」などの短く分かりやすい名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。
6. ウィザードを終了します。
7. タスクのリストに新しいタスクが表示されます。
8. タスクの横にあるチェックボックスをオンにします。
9. ［**開始**］をクリックします。

製品インターフェイスで前回のアップデートにロールバックする方法

1. メインウィンドウで、［**アップデート**］をクリックします。



ローカルのアップデートタスク

2. ［**以前のバージョンの定義データベースへのロールバック**］タイルで、［**ロールバックする**］をクリックします。

Kaspersky Endpoint Security は定義データベースをアップデート前の状態に戻します。ロールバックの進捗、ダウンロードされたファイルおよびアップデート元が表示されます。［**アップデートを停止する**］ボタンを押すことでいつでもタスクを停止することができます。

特別な駆除の技術

Kaspersky Endpoint Security は、特別な駆除を使用してアクティブな脅威を処理します。特別な駆除はワークステーションとサーバーに対して異なる動作をします。［マルウェアのスキャン］タスクの設定および製品設定で特別な駆除を設定できます。

Kaspersky Endpoint Security がマルウェアの実行を停止できない場合、特別な駆除技術を使用することができます。ポリシーが適用されているコンピューターの場合、特別な駆除に大量のコンピューターリソースが必要になるため、既定では特別な駆除は無効になっています。 ポリシーが適用されていないコンピューターの場合、既定では特別な駆除は有効になっています。

特別な駆除はワークステーションとサーバーに対して異なる動作をします。サーバーでこの技術を使用する場合は、*マルウェアのスキャン*タスクのプロパティで［すぐに特別な駆除を実行する］を有効にする必要があります。ワークステーションでこの技術を使う場合、事前準備は必要ありません。

管理コンソール（MMC）で特別な駆除を有効または無効にする方法

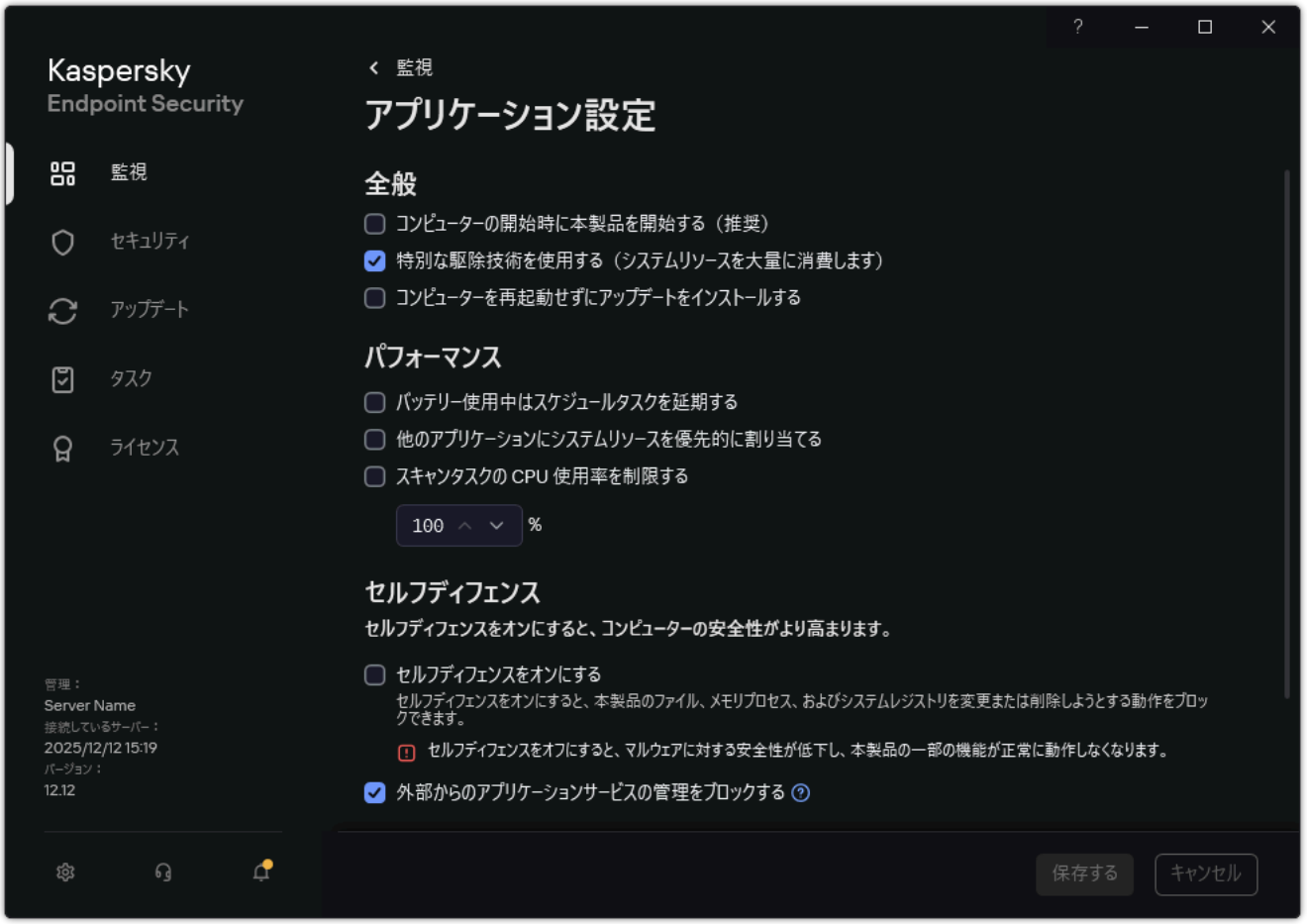
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. ［**全般**］ブロックで、［**特別な駆除を有効にする**］をオンまたはオフにして、特別な駆除技術を有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで特別な駆除を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**検知の設定**］の順に選択します。
5. ［**特別な駆除**］ブロックで、［**特別な駆除は有効です**］トグルスイッチをオンまたはオフにして、特別な駆除技術を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスで特別な駆除を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**全般**］ブロックで、［**特別な駆除技術を使用する（システムリソースを大量に消費します）**］をオンまたはオフにして、特別な駆除技術を有効または無効にします。
4. 変更内容を保存します。

特別な駆除が実行されている間、ユーザーはオペレーティングシステムの多くの機能を使用できなくなります。駆除が完了すると、コンピューターは再起動されます。

ワークステーションにおけるアクティブな脅威の駆除

ワークステーションでアクティブな脅威を処理するには、製品設定で特別な駆除技術を有効にしてください。次に、マルウェアのスキャンタスクのプロパティで設定します。タスクのプロパティには［**すぐに特別な駆除を実行する**］チェックボックスがあります。オンにすると、Kaspersky Endpoint Security はユーザーに通知せずに駆除を実行します。駆除が完了すると、コンピューターは再起動されます。オフの場合、Kaspersky Endpoint Security はアクティブな脅威に関する通知を表示します（下の図を参照してください）。ファイルを処理せずにこの通知を閉じることはできません。

コンピューターに適用されているポリシーのプロパティで特別な駆除が有効になっている場合のみ、コンピューター上のスキャンタスク中に特別な駆除が実行されます。



アクティブな脅威についての通知

サーバーにおけるアクティブな脅威の駆除

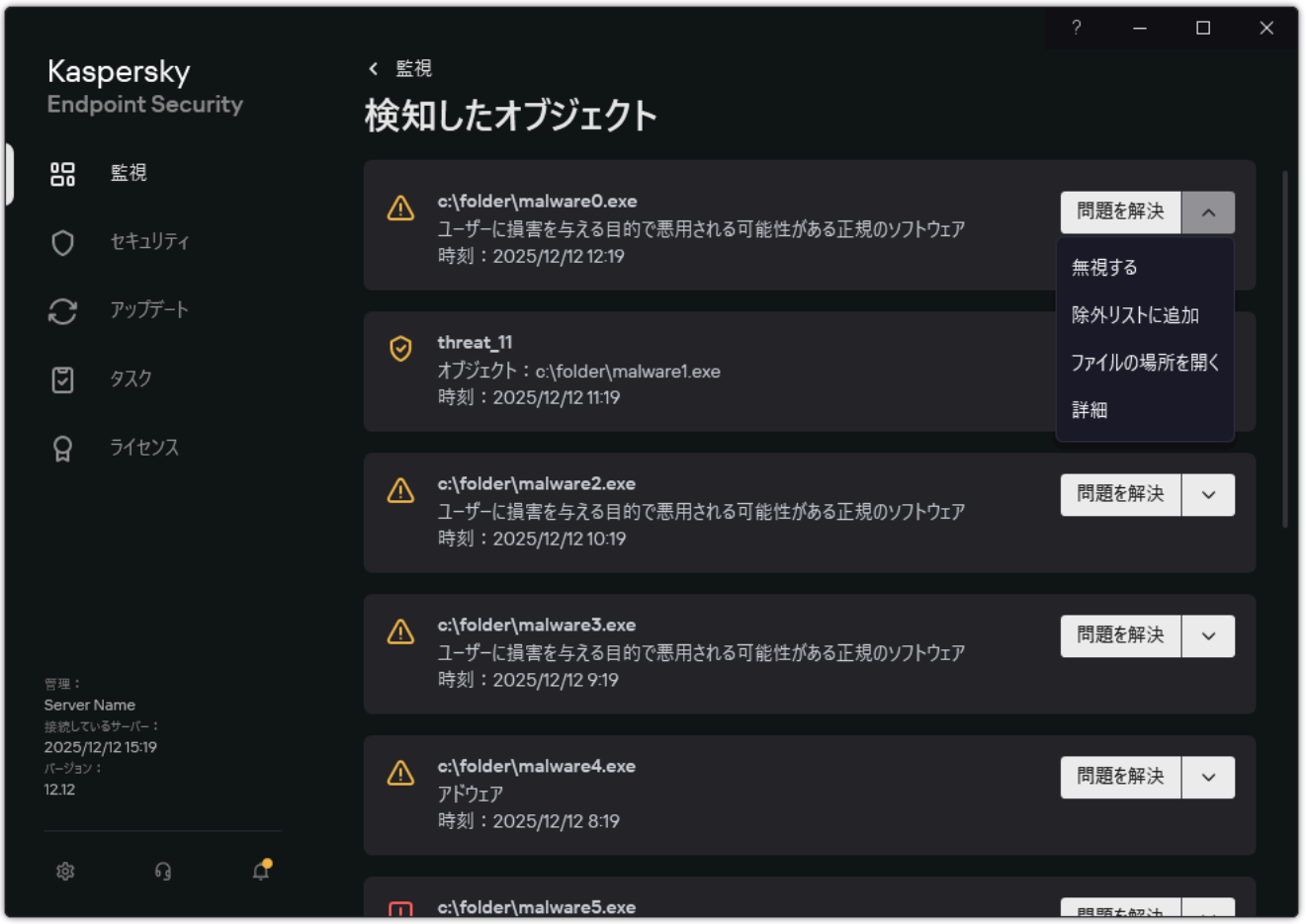
サーバーでアクティブな脅威を処理するには、次の操作を行います：

- 製品設定で特別な駆除技術を有効にします。
- マルウェアのスキャンタスクのプロパティで［すぐに特別な駆除を実行する］を有効にします。

サーバー向けの Windows を実行しているコンピューターに Kaspersky Endpoint Security がインストールされている場合、Kaspersky Endpoint Security は通知を表示しません。そのため、アクティブな脅威を駆除する操作を選択することはできません。脅威を駆除するには、製品設定で特別な駆除を有効にして、マルウェアのスキャンタスクの設定ですぐに特別な駆除を実行するよう設定する必要があります。その後 マルウェアのスキャンタスクを開始します。

処理されていない脅威の排除

Kaspersky Endpoint Security は、何らかの理由で処理されていないファイルに関する情報を記録します。この情報は、アクティブな脅威のリストにイベントの形式で記録されます（下の図を参照）。



アクティブな脅威のリスト

Kaspersky Endpoint Security がコンピューターのウイルスやその他のマルウェアのスキャンの一環としてファイルを駆除したり脅威を取り除いた場合、感染したファイルは「*処理済み*」と認識されます。

ウイルスなどの脅威の検知のためのコンピュータースキャンの際に、Kaspersky Endpoint Security が指定された製品設定に基づいて感染したファイルにいずれかの処理を試み、何らかの理由で失敗した場合、そのファイルがアクティブな脅威のリストに移動されます。

このようなケースは、次のような場合に発生します：

- スキャンされたファイルを使用できない場合。たとえば、スキャンされたファイルが、書き込み権限のないネットワークドライブやリムーバブルドライブに配置されているような場合です。
- マルウェアのスキャンタスクの設定で、脅威の検知時の処理が［**通知**］に設定されている場合。次に、感染したファイルに関する通知が画面に表示されたときにユーザーが［**無視する**］を選択した場合。

処理されていない脅威がある場合は、Kaspersky Endpoint Security はアイコンを（）に変更します。メインウィンドウで、脅威に関する通知が表示されます（下の図を参照）。Kaspersky Security Center コンソールでは、コンピューターの状態は緊急（）に変更されます。

管理コンソール（MMC）で脅威を処理する方法

1. 管理コンソールで、［**管理サーバー**］→［**詳細**］→［**リポジトリ**］→［**アクティブな脅威**］の順に移動します。

   アクティブな脅威のリストが表示されます。

2. 処理するオブジェクトを選択します。

3. 脅威をどのように処理するか選択します：

   - **駆除**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **削除**：このオプションをオンにすると、本製品は、アクティブな脅威のリポジトリの検知された感染したファイルを削除します。この場合、本製品は、検知されたファイルをコンピューターのメモリに保存します。コンピューターから脅威を排除するには、［**駆除**］をオンにします。

Web コンソールと Cloud コンソールで脅威を処理する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］→［**アクティブな脅威**］をクリックします。

   アクティブな脅威のリストが表示されます。

2. 処理するオブジェクトを選択します。

3. 脅威をどのように処理するか選択します：

   - **駆除**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **削除**：このオプションをオンにすると、本製品は、アクティブな脅威のリポジトリの検知された感染したファイルを削除します。この場合、本製品は、検知されたファイルをコンピューターのメモリに保存します。コンピューターから脅威を排除するには、［**駆除**］をオンにします。

製品インターフェイスで脅威を処理する方法

1. 製品のメインウィンドウの［**監視**］で、［**危険にさらされています**］をクリックします。

   アクティブな脅威のリストが表示されます。

2. 処理するオブジェクトを選択します。

3. 脅威をどのように処理するか選択します：

   - **問題を解決**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **除外リストに追加する**：この処理が選択されていると、Kaspersky Endpoint Security はファイルをスキャンの除外リストに追加するよう求めます。除外の設定は自動で設定されます。除外の追加ができない場合は、管理者がポリシーの設定で除外の追加を無効にしている可能性があります。

   - **無視する**：このオプションを選択すると、Kaspersky Endpoint Security はアクティブな脅威のリストからこの項目を削除します。ほかにアクティブな脅威がない場合は、コンピューターのステータスは *OK* に変わります。オブジェクトが次に検知された場合は、Kaspersky Endpoint Security はアクティブな脅威のリストに新しい項目を追加します。

- **ファイルの場所を開く**：このオプションを選択すると、Kaspersky Endpoint Security はファイルマネージャーでオブジェクトのあるフォルダーを開きます。オブジェクトを手動で削除する、または保護範囲に含まれないフォルダーに移動することができます。

- **詳細**：このオプションを選択すると、Kaspersky Endpoint Security はカスペルスキーの脆弱性と脅威のデータベースの Web サイトを開きます。

Kaspersky Security Center コンソールでアクティブな脅威を処理するには、未処理のファイルに関する情報の管理サーバーへの転送を有効にする必要があります。既定ではデータ転送は有効になっています。

管理コンソール（MMC）で未処理のファイルのデータ転送を有効にする方法

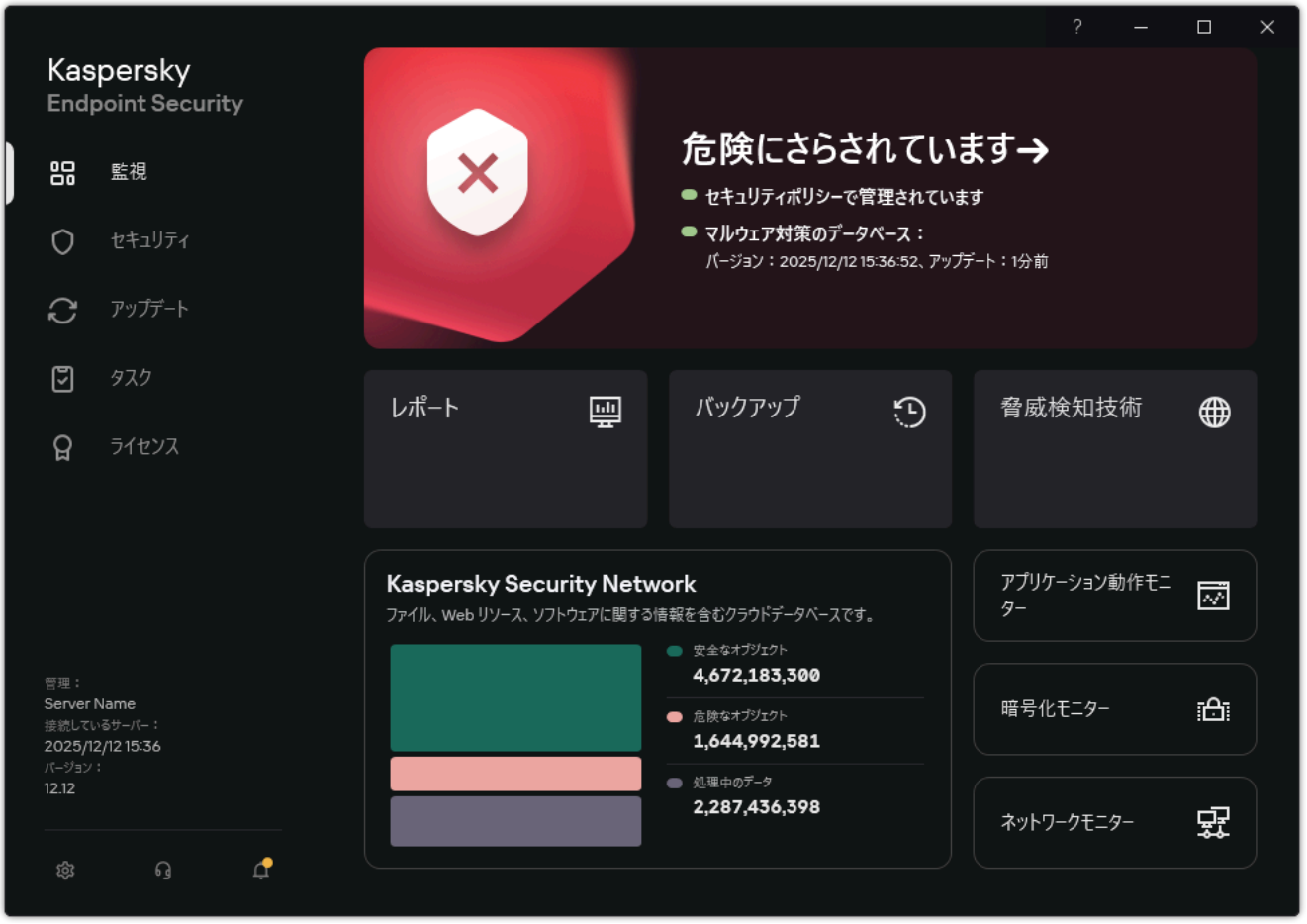
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**レポートと保管領域**］の順に選択します。
4. ［**管理サーバーへのデータ転送**］ブロックの［**設定**］をクリックします。
5. ［**未処理ファイル**］チェックボックスをオンにします。
6. 変更内容を保存します。

Web コンソールで未処理のファイルのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**KSC 連携**］に移動します。

5. ［**管理サーバーへのデータ転送**］ブロックで、［**未処理のファイルの情報**］をオンにします。

6. 変更内容を保存します。



脅威が検知された際のメインウィンドウ

コンピューターの保護

ファイル脅威対策

ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターの RAM に常駐し、開いたファイル、保存したファイル、実行されたファイルのすべてをリアルタイムでスキャンします。このコンポーネントは、接続されているドライブを含むすべてのコンピューターのドライブ上のファイルをスキャンします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

コンポーネントは、ユーザーまたはアプリケーションがアクセスしたファイルをスキャンします。悪意のあるファイルが検知された場合、Kaspersky Endpoint Security はファイル操作をブロックします。その後、ファイル脅威対策の設定に応じて、悪意のあるファイルを駆除または削除します。

コンテンツが OneDrive クラウドストレージ上にあるファイルにアクセスしようとすると、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードしてスキャンします。

ファイル脅威対策の有効化と無効化

既定では、ファイル脅威対策は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。ファイル脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます：**高**、**推奨**、**低**。カスペルスキーのエキスパートが推奨する設定グループは、［**推奨**］セキュリティレベルです（下の表を参照）。セキュリティレベルは、事前に設定されているものから選択することも、手動で設定することもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

ファイル脅威対策は別の製品機能から受け取ったデータを使用します。これらの機能は有効にしなくても Kaspersky Managed Detection and Response を使用できます。追加のデータを提供する機能は次の通りです：

- Kaspersky Security Network
- ホスト侵入防止
- ふるまい検知

管理コンソール（MMC）でファイル脅威対策を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］の順に選択します。
4. ［**ファイル脅威対策**］を使用して機能を有効または無効にします。

5. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。

   - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：

     - **高**：このファイルセキュリティレベルを選択すると、ファイル脅威対策は開いたファイル、保存したファイル、実行されたファイルのすべてに対して最も厳しいコントロールを適用します。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているすべてのファイルの種類をスキャンします。また、アーカイブ、インストールパッケージ、OLE 埋め込みオブジェクトもスキャンします。

     - **推奨**：このセキュリティレベルはカスペルスキーが推奨するセキュリティレベルです。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の形式のファイル、OLE 埋め込みオブジェクトをスキャンします。アーカイブまたはインストールパッケージはスキャンしません。

     - **低**：このファイルセキュリティレベル設定では、スキャンの速度が最大になります。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されている、指定した拡張子のファイルのみをスキャンします。複合ファイルはスキャンしません。

   - カスタムのセキュリティレベルを設定する場合は、［**設定**］をクリックして、機能の設定を定義します。

     ［**既定**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

6. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、Kaspersky Endpoint Security はファイルをブロックします（読み取り / 書き込み）。

   - **ブロックする**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。

   - **通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。

   感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでファイル脅威対策を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。

5. ［**ファイル脅威対策は有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. 保護範囲に新しいオブジェクトを追加するには：

   a. ［**詳細設定**］で、［**保護範囲**］を選択します。

   b. ［**追加**］をクリックします。

   c. 表示されたウィンドウで、保護範囲に含めるオブジェクトを選択します。

   マスクを使用する

   - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

   - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

   ファイルまたはフォルダーのパスにマスクを使用できます。たとえば、コンピューター上のすべてのユーザーアカウントを対象として［ダウンロード］フォルダーをスキャンする場合は、「`C:\Users\*\Downloads\`」と入力します。

   保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトを保護範囲から除外することができます。そうするには、オブジェクトの隣にあるトグルスイッチをオフの位置に移動します。

   d. 変更内容を保存します。

7. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、Kaspersky Endpoint Security はファイルをブロックします（読み取り / 書き込み）。

   - **ブロックする**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。

   感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。

8. 必要に応じて、ファイル脅威対策の詳細設定を編集します。

9. 変更内容を保存します。

製品インターフェイスでファイル脅威対策を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。

3. ［**ファイル脅威対策**］トグルスイッチを使用して機能を有効または無効にします。

4. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。

   - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：

     - **高**：このファイルセキュリティレベルを選択すると、ファイル脅威対策は開いたファイル、保存したファイル、実行されたファイルのすべてに対して最も厳しいコントロールを適用します。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているすべてのファイルの種類をスキャンします。また、アーカイブ、インストールパッケージ、OLE 埋め込みオブジェクトもスキャンします。

     - **推奨**：このセキュリティレベルはカスペルスキーが推奨するセキュリティレベルです。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の形式のファイル、OLE 埋め込みオブジェクトをスキャンします。アーカイブまたはインストールパッケージはスキャンしません。

     - **低**：このファイルセキュリティレベル設定では、スキャンの速度が最大になります。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されている、指定した拡張子のファイルのみをスキャンします。複合ファイルはスキャンしません。

   - カスタムのセキュリティレベルを設定する場合は、［**詳細設定**］をクリックして、機能の設定を定義します。

     ［**推奨のセキュリティレベルに戻す**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

5. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

   - **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、Kaspersky Endpoint Security はファイルをブロックします（読み取り / 書き込み）。

   - **ブロック**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。

   - **通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。

感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。

6. 変更内容を保存します。

カスペルスキーが推奨するファイル脅威対策の設定値（推奨されるセキュリティレベル）

パラメータ	値	説明
ファイル種別	**ファイル形式でファイルをスキャン**	この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。
ヒューリスティック分析	**低**	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
新規作成または変更されたファイルのみスキャン	**オン**	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
iSwift を使用する	**オン**	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker を使用する	**オン**	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iChecker には制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。
Microsoft Office 形式のファイルをスキャン	**オン**	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
メール形式のファイルをスキャン	**オン**	メール形式のファイルをスキャンします。本製品は MSG および EML ファイルをスキャンします。メール形式のファイルには OLE オブジェクトおよび MHT ファイルが含まれます。チェックボックスのオンオフにかかわらず、Kaspersky Endpoint Security は 1 MB より小さいサイズのメール形式のファイルをスキャンします。
スキャンモード	**スマートモードでスキャン**	オブジェクトに対する処理の分析に基づいて、オブジェクトをスキャンします。たとえば、Microsoft Office ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**	このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。

ファイル脅威対策の自動的な一時停止

指定した時間、または指定したアプリケーションの使用中に、ファイル脅威対策が自動的に一時停止するよう設定できます。

ファイル脅威対策が他のアプリケーションと競合した場合、ファイル脅威対策が最も優先されます。機能の実行中に競合が発生した場合は、カスペルスキーのテクニカルサポートにお問い合わせください。サポート担当者が、ファイル脅威対策と他のアプリケーションが同時に作動できるように設定するお手伝いをします。

ファイル脅威対策の自動一時停止を設定するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**ファイル脅威対策の一時停止**］セクションで、［**ファイル脅威対策の一時停止**］をクリックします。
5. 表示されたウィンドウで、ファイル脅威対策の一時停止の設定を指定します：
   a. ファイル脅威対策が自動で一時停止するスケジュールを設定します。
   b. ファイル脅威対策が動作を一時停止するアプリケーションのリストを作成します。
6. 変更内容を保存します。

感染したファイルに対してファイル脅威対策が行う処理の変更

既定では、ファイル脅威対策は、検知した感染したファイルすべての駆除を自動的に試みます。駆除に失敗した場合は、ファイルを削除します。

感染したファイルに対してファイル脅威対策が行う処理を変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**脅威の検知時の処理**］ブロックで、関連するオプションを選択します。
   - **駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。
   - **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、Kaspersky Endpoint Security はファイルをブロックします（読み取り / 書き込み）。
   - **ブロック**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。

   感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。
4. 変更内容を保存します。

ファイル脅威対策の保護範囲の設定

保護範囲とは、このコンポーネントが有効な場合にスキャンされるオブジェクトを意味します。各コンポーネントの保護範囲には、それぞれ異なる特性があります。ファイル脅威対策の保護範囲のプロパティは、スキャン対象ファイルの場所と種別です。既定では、ファイル脅威対策のスキャン対象は、ハードディスク、リムーバブルドライブ、およびネットワークドライブから実行された感染する可能性があるファイルのみです。

スキャンするファイル種別を選択するときには、次の点に留意してください：

1. 特定の形式（TXT 形式など）の場合、その形式のファイルに悪意のあるコードが侵入し、その後有効化されるというケースはあまり発生しません。一方で、実行コードを含んでいる形式のファイル（exe、dll など）があります。実行コードは、この目的を意図していないファイル形式（DOC 形式など）にも含まれている場合があります。このようなファイルについては、悪意のあるコードの侵入と有効化のリスクが高くなります。

2. 侵入者はウイルスやその他の悪意のあるアプリケーションの拡張子を txt に変え、実行ファイルの形式でコンピューターに送信する可能性があります。拡張子でのファイルのスキャンを選択すると、このようなファイルのスキャンはスキップされます。ファイル形式でのスキャンが選択されている場合、Kaspersky Endpoint Security は拡張子に関係なくファイルのヘッダーを分析します。この分析により、ファイルが実行ファイル形式（例：EXE）であることが判明した場合、スキャンが実行されます。

保護範囲を作成するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**ファイル種別**］ブロックで、ファイル脅威対策がスキャンするファイルの種別を指定します。
   - **すべてのファイル**：この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。
   - **ファイル形式でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。
   - **拡張子でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイル形式はファイルの拡張子に基づいて識別されます。
5. ［**保護範囲の編集**］リンクをクリックします。
6. 表示されたウィンドウで、保護範囲に含めるまたは除外するオブジェクトを選択します。

既定で保護範囲に含まれているオブジェクトの削除または編集はできません。

7. 保護範囲に新しいオブジェクトを追加するには：

   a. ［**追加**］をクリックします。

      フォルダーのツリーが開きます。

   b. ［**パス**］フィールドにフォルダーまたはファイルのパスを入力します。

      マスクを使用する

      - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

      - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

      ファイルまたはフォルダーのパスにマスクを使用できます。たとえば、コンピューター上のすべてのユーザーアカウントを対象として［ダウンロード］フォルダーをスキャンする場合は、「`C:\Users\*\Downloads\`」と入力します。

      コンピューターのファイルリソースのリスト内の［**この PC**］のオブジェクトには、［**すべてのハードディスク**］、［**すべてのネットワークドライブ**］、［**すべてのリムーバブルドライブ**］のオブジェクトが含まれます。

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

8. 変更内容を保存します。

スキャン方法の使用

Kaspersky Endpoint Security は、機械学習とシグネチャ分析と呼ばれるスキャン技術を使用します。Kaspersky Endpoint Security のシグネチャ分析では、検知されたオブジェクトと定義データベース内のレコードが照合されます。カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。

保護の有効性を高めるには、ヒューリスティック分析を使用します。悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。

ファイル脅威対策でのヒューリスティック分析の使用を設定するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. 脅威に対してヒューリスティック分析を使用する場合は、［**スキャン方法**］ブロックの［**ヒューリスティック分析**］を選択します。次に、スライダーを使用して、ヒューリスティック分析レベル（**低**、**中**、**高**のいずれか）を設定します。
5. 変更内容を保存します。

ファイル脅威対策で使用するスキャン技術の設定

ファイル脅威対策で使用するスキャン技術を設定するには：

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

スキャンの最適化

ファイル脅威対策が行うファイルのスキャンを最適化し、スキャン時間を短縮したり、Kaspersky Endpoint Security の処理速度を向上させたりすることができます。スキャンを最適化するには、新しいファイルと前回のスキャン以降に変更されたファイルのみをスキャンします。このモードは、簡易ファイルと複合ファイルの両方に適用されます。

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

ファイルスキャンを最適化するには、次の手順を実行します：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**最適化**］ブロックで、［**新規作成または変更されたファイルのみスキャン**］をオンにします。
5. 変更内容を保存します。

複合ファイルのスキャン

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

感染している複合ファイルの処理方法（駆除または削除）は、ファイルの種別により異なります。

ファイル脅威保護では ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 形式の複合ファイルが駆除されます。それ以外の形式のファイルはすべて削除されます（メールデータベースを除く）。

複合ファイルのスキャンを設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、アーカイブ、配布パッケージ、メールまたは Office 形式のファイルのいずれかを指定します。
5. 新しいファイルおよび更新されたファイルのみのスキャンが無効になっている場合は、複合ファイルの種別ごとにスキャンの設定（特定の種別のファイルをすべてスキャンまたは新しいファイルのみスキャン）を指定してください。

   新しいファイルまたは更新されたファイルのみのスキャンが有効になっている場合は、Kaspersky Endpoint Security はすべての種別の複合ファイルで新しいまたは更新されたもののみをスキャンします。
6. 複合ファイルのスキャンを詳細に設定します。
   - **大きな複合ファイルをスキャンしない**

このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。

このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。

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

- **複合ファイルをバックグラウンドで展開する**

  このチェックボックスをオンにすると、指定された値よりも大きいサイズの複合ファイルには、これらのファイルをスキャンする前にアクセスできます。この場合、複合ファイルの解凍とスキャンはバックグラウンドで実行されます。

  指定された値より小さいサイズの複合ファイルには、これらのファイルを解凍してスキャンした後にのみアクセスできます。

  このチェックボックスをオフにすると、すべてのサイズのファイルを解凍してスキャンした後にのみ複合ファイルにアクセスできます。

7. 変更内容を保存します。

スキャン方法の変更

［スキャンモード］では、ファイル脅威対策によるファイルスキャンを実行する条件が設定されています。既定では、ファイルはスマートモードでスキャンされます。このモードでは、ファイルがスキャンされるかどうかの判断は、ユーザー、ユーザーに代わるアプリケーション（ログインに使用されたアカウントまたは異なるユーザーアカウントで実行）、またはオペレーティングシステムによるファイルの操作が分析された後に決定されます。たとえば、Microsoft Office Word ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。

ファイルスキャン方法を変更するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**スキャンモード**］ブロックで目的のモードを選択します。

   - **スマートモードでスキャン**：オブジェクトに対する処理の分析に基づいて、オブジェクトをスキャンします。たとえば、Microsoft Office ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。

   - **ファイルのアクセス時と更新時にスキャン**：オブジェクトを開こうとするときまたは修正しようとするときにオブジェクトをスキャンします。

- **ファイルのアクセス時にスキャン**：オブジェクトを開こうとする際にのみオブジェクトをスキャンします。
- **ファイルの実行時にスキャン**：オブジェクトを実行しようとする際にのみオブジェクトをスキャンします。

5. 変更内容を保存します。

コンテナスキャン

コンテナーは、アプリケーションがオペレーティングシステムと直接やり取りすることなく実行できる分離された環境です。コンテナーを使用すると、次のようなリスクが伴います：

- ハッカーがコンテナー化の脆弱性を悪用して、コンテナー内のアプリケーションを侵害する可能性があります。
- ハッカーがコンテナー環境の安全でない設定を悪用して、コンピューター上のデータに不正にアクセスしたり、システムの整合性を侵害したりする可能性があります。
- コンテナーへの攻撃が成功すると、ハッカーがコンピューター上のデータにアクセスできるようになる可能性があります。
- ハッカーがネットワークの脆弱性を悪用してネットワークトラフィックを傍受する可能性があります。

Kaspersky Endpoint Security は、ディスク上のファイルだけでなくコンテナー内のファイルもスキャンします。つまり、Kaspersky Endpoint Security は、コンテナー内の悪意のあるアクティビティを検知するための外部ツールです。これにより、コンテナーのパフォーマンスを維持し、コンテナー内の他のアプリケーションとの競合を防ぐことができます。コンテナー内への Kaspersky Endpoint Security のインストールはサポートされていません。

Kaspersky Endpoint Security は、コンテナーのセキュリティの確保に加え、アプリケーションコントロールを使用したコンテナー内のアプリケーションの管理を可能にします。アプリケーションコントロールは、コンピューターにインストールされたアプリケーションと同じ方法でコンテナー用に設定されます。システム変更監視でもコンテナーがサポートされます。

コンテナーの要件

- コンテナーは Docker コンテナーである必要があります。その他のコンテナー化ツールはサポートされていません。
- コンテナーはプロセス分離モードで実行する必要があります。Hyper-V 分離モードはサポートされていません。
- コンテナーは、Windows Server 2016、2019、2022 サーバーのいずれかに配置する必要があります（Docker Host）。
- コンテナーには Windows イメージ（Docker Image）が含まれる必要があります。Windows 10 および 11 はサポートされていません。Linux イメージはサポートされていません。

脅威の検知時の処理

コンテナー内で脅威が検知された場合、ファイル脅威対策に対して選択された処理が適用されます。コンテナーのスキャンには追加の設定があります（以下の手順を参照）。脅威が検知されると、悪意のある動作がブロックされて、選択した処理が実行されます（オブジェクト駆除の試行など）。Kaspersky Endpoint Security は、検知されたオブジェクトを駆除できない場合に、コンテナーを停止できます。既定では、コンテナー停止機能は無効になっています。

管理コンソール（MMC）でコンテナスキャンを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］の順に選択します。
4. ［**設定**］をクリックします。
5. 表示されたウィンドウで、**詳細**タブを選択します。
6. ［**Windows コンテナー内で実行されたファイル操作のスキャン**］ブロックで、コンテナスキャンを設定します：
   - **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する十分な読み取りおよび書き込み権限がない可能性があります。その場合、検知したオブジェクトを駆除したり削除したりすることはできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナーを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。
   - **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナーをリアルタイムで継続的にスキャンします。
7. 変更内容を保存します。

Web コンソールと Cloud コンソールでコンテナスキャンを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。
5. ［**詳細設定**］で、［**パフォーマンス**］を選択します。

6. ［**スキャンの最適化**］ブロックで、コンテナスキャンを設定します：

   - **駆除できなかった場合はコンテナを停止**：本製品に、検知したオブジェクトに対する十分な読み取りおよび書き込み権限がない可能性があります。その場合、検知したオブジェクトを駆除したり削除したりすることはできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナーを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。

   - **Windows コンテナ内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナーをリアルタイムで継続的にスキャンします。

7. 変更内容を保存します。

製品インターフェイスでコンテナスキャンを設定する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイル脅威対策**］を選択します。

3. ［**Windows コンテナー内で実行されたファイル操作のスキャン**］ブロックで、コンテナスキャンを設定します：

   - **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する十分な読み取りおよび書き込み権限がない可能性があります。その場合、検知したオブジェクトを駆除したり削除したりすることはできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナーを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。

   - **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナーをリアルタイムで継続的にスキャンします。

4. 変更内容を保存します。

ホスト侵入防止

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。

コンポーネントは、*アプリケーション権限*を使用してアプリケーションの動作を制御します。アプリケーション権限には、次のアクセスパラメータが含まれます：

- オペレーティングシステムリソースへのアクセス（自動起動オプション、レジストリキーなど）
- 個人データ（ファイルやアプリケーションなど）へのアクセス

アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

アプリケーションの最初の起動時に、ホスト侵入防止は次の処理を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティを確認する

   ホスト侵入防止がより効果的に機能するように、Kaspersky Security Network に参加することを推奨します。

3. *信頼済み*、*弱い制限付き*、*強い制限付き*、*ブロック*のうちいずれかの信頼グループにアプリケーションを配置します。

   信頼グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

   Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

   KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は ホスト侵入防止の設定に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じてアプリケーション動作をブロックします。たとえば、*強い制限付き*の信頼グループのアプリケーションは、オペレーティングシステムモジュールへのアクセスを拒否されます。

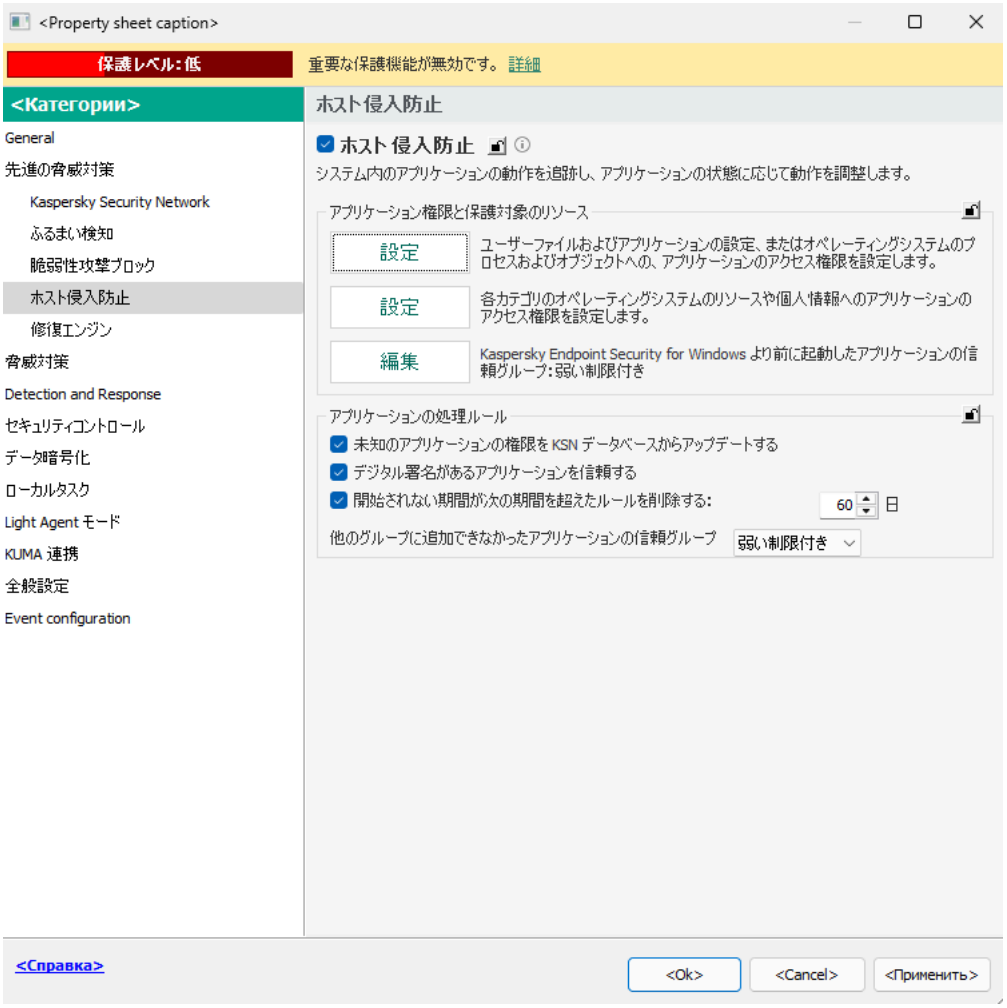
次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のアプリケーション権限をそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

ホスト侵入防止の有効化と無効化

既定では、ホスト侵入防止は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。

管理コンソール（MMC）でホスト侵入防止を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**ホスト侵入防止**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでホスト侵入防止を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。
5. ［**ホスト侵入防止は有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでホスト侵入防止を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**ホスト侵入防止**］トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

ホスト侵入防止機能が有効になっている場合、Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。Kaspersky Endpoint Security は信頼グループに基づいてアプリケーションの操作をブロックします。

アプリケーションの信頼グループの管理

アプリケーションを初めて起動するたびに、ホスト侵入防止がアプリケーションのセキュリティをチェックし、信頼グループの1つに割り当てます。

アプリケーションスキャンでは、Kaspersky Endpoint Security はまず既知のアプリケーションの定義データベースを検索して一致するエントリを探し、同時に Kaspersky Security Network データベースに要求を送信します（インターネット接続が利用できる場合）。定義データベースと Kaspersky Security Network データベースの検索結果に基づいて、アプリケーションがいずれかの信頼グループに配置されます。次回以降、アプリケーションが起動するたびに、Kaspersky Endpoint Security は KSN にアプリケーションの評価を問い合わせ、KSN データベースでのアプリケーションの評価が変更された場合には、アプリケーションを別の信頼グループに移動します。

Kaspersky Endpoint Security がすべての不明なアプリケーションを自動的に配置する信頼グループを指定することもできます。Kaspersky Endpoint Security を起動する前に実行されていたアプリケーションは、ホスト侵入防止設定で設定された信頼グループに自動的に配置されます。

> Kaspersky Endpoint Security より前に起動したアプリケーションについては、ネットワーク動作のみ管理されます。管理は、ファイアウォールで指定されたネットワークルールに従って実行されます。

アプリケーションの信頼グループを変更する

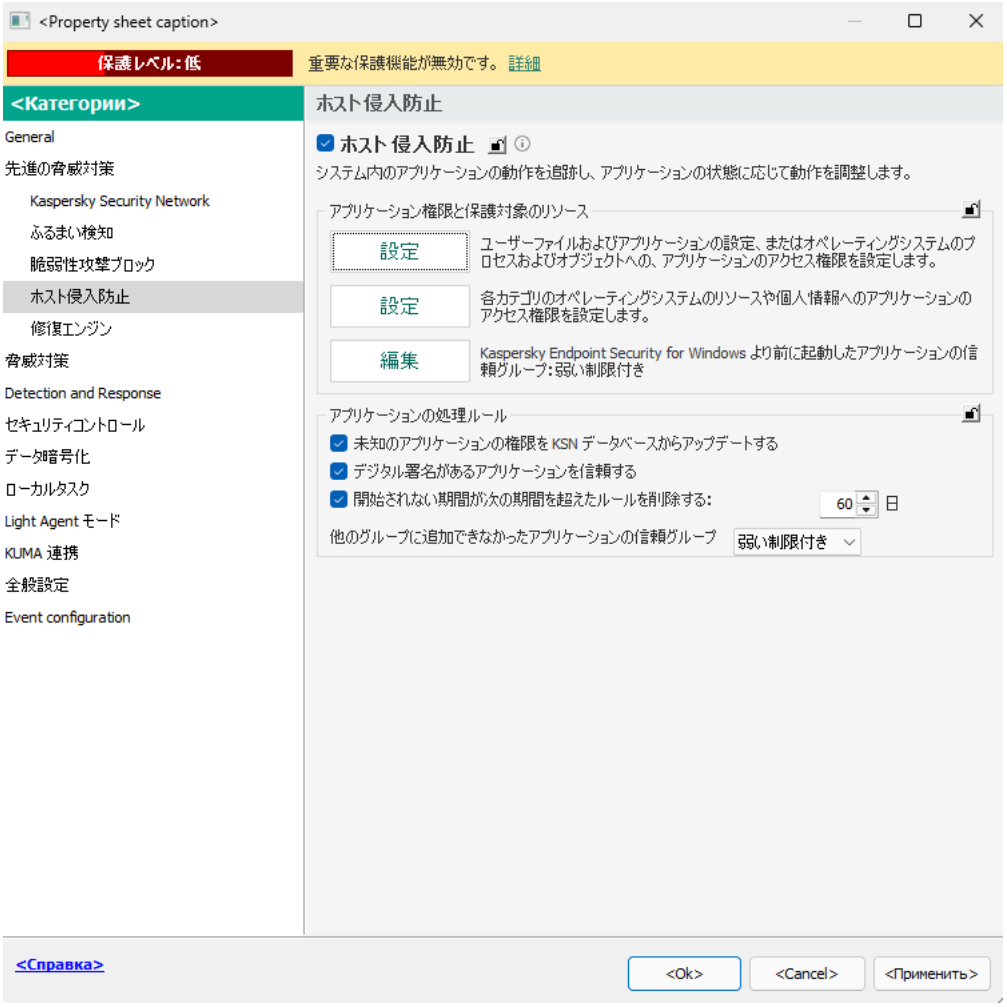
アプリケーションを初めて起動するたびに、ホスト侵入防止がアプリケーションのセキュリティをチェックし、信頼グループの1つに割り当てます。

> アプリケーションを自動的に割り当てられた信頼グループから別の信頼グループに移動することは推奨されません。代わりに、必要に応じて、個別のアプリケーションの権限を編集できます。

管理コンソール（MMC）でアプリケーションの信頼グループを変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーション権限と保護対象のリソース**］ブロックの［**設定**］をクリックします。

   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

5. ［**アプリケーション権限**］タブを選択します。

6. ［**追加**］をクリックします。

7. 表示されたウィンドウで、信頼グループを変更するアプリケーションを検索する条件を入力します。

   アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

8. ［**更新**］をクリックします。

   Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。

9. 必要なアプリケーションを選択します。

10. ［**選択したアプリケーションを次の信頼グループに追加**］で、アプリケーションの信頼グループを選択します。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで製品の信頼グループを変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。
5. ［**アプリケーション権限と保護対象のリソース**］セクションで、［**アプリケーション権限と保護対象のリソース**］をクリックします。
   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
6. ［**アプリケーション権限**］タブを選択します。
   ウィンドウの左側に信頼グループのリスト、右側にそのプロパティが表示されます。
7. ［**追加**］をクリックします。
   ウィザードがアプリケーションを信頼グループに追加します。
8. アプリケーションに対して適切な信頼グループを選択します。
9. **アプリケーション**の種別を選択します。次の手順に進みます。
   複数のアプリケーションの信頼グループを変更する場合は、［**グループ**］を選択してアプリケーショングループの名前を定義します。
10. アプリケーションのリストで、変更するアプリケーショングループを選択します。
    フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
11. ウィザードを終了します。
    アプリケーションが信頼グループに追加されます。
12. 変更内容を保存します。

製品のインターフェイスでアプリケーションの信頼グループを変更する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**アプリケーションの管理**］をクリックします。
   インストール済みのアプリケーションのリストが開きます。
4. 必要なアプリケーションを選択します。
5. アプリケーションのコンテキストメニューから［**制限**］→**<信頼グループ>** をクリックします。
6. 変更内容を保存します。

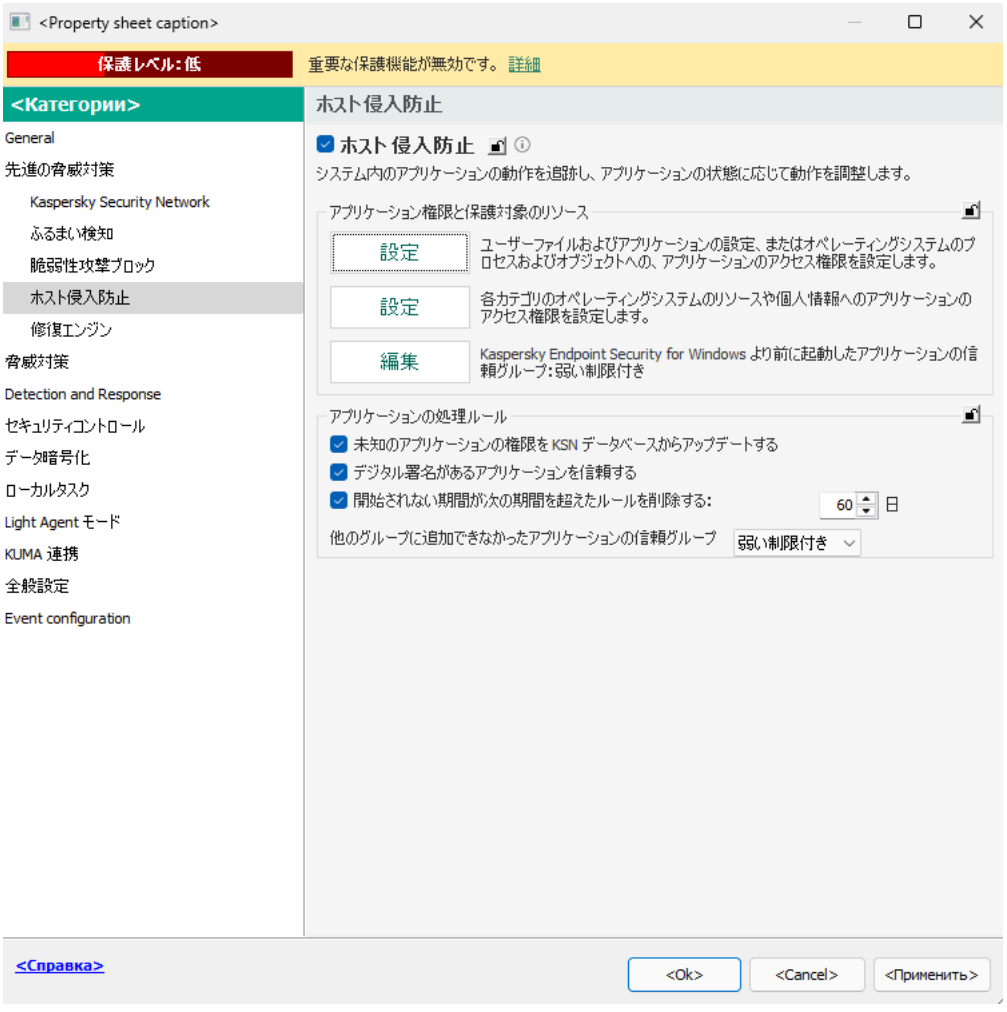
アプリケーションは別の信頼グループに追加されます。Kaspersky Endpoint Security は信頼グループに基づいてアプリケーションの操作をブロックします。（カスタム）ステータスがアプリケーションに割り当てられます。Kaspersky Security Network でアプリケーションの評価が変更された場合、ホスト侵入防止機能はアプリケーションの信頼グループを変更しません。

信頼グループの権限の設定

既定では、信頼グループごとに最適なアプリケーション権限が作成されます。信頼グループに含まれるアプリケーショングループの権限の設定は、信頼グループの権限の設定を継承します。

管理コンソール（MMC）で信頼グループの権限を変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーション権限と保護対象のリソース**］ブロックの［**設定**］をクリックします。
   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
5. ［**アプリケーション権限**］タブを選択します。
6. 必要な信頼グループを選択します。

7. 信頼グループのコンテキストメニューから［**グループの権限**］を選択します。
   信頼グループのプロパティが開きます。

8. 次のいずれかの手順を実行します：

   - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］タブを選択します。

   - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］タブを選択します。

   > アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

9. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可**（）または**ブロック**()。

10. コンピューターのリソース使用を監視する場合は、［**イベントを記録**］（/）を選択します。
    Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールと Cloud コンソールで信頼グループの権限を変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。

5. ［**アプリケーション権限と保護対象のリソース**］セクションで、［**アプリケーション権限と保護対象のリソース**］をクリックします。
   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

6. ［**アプリケーション権限**］タブを選択します。
   ウィンドウの左側に信頼グループのリスト、右側にそのプロパティが表示されます。

7. ウィンドウの左側で、対応する信頼グループを選択します。

8. ウィンドウの右側で、ドロップダウンリストから次のいずれかを実行します：

   - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］を選択します。

   - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］を選択します。

アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

9. 関連するリソースに関しては、対応する操作の列で必要な次のオプションを選択します：**継承**、**許可する**（）**ブロックする**()。

10. コンピューターのリソース使用を監視する場合は、［**イベントの記録**］（/）を選択します。

    Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

11. 変更内容を保存します。

製品インターフェイスで信頼グループの権限を変更する方法

1. メインウィンドウで、をクリックします。

2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。

3. ［**アプリケーションの管理**］をクリックします。

   インストール済みのアプリケーションのリストが開きます。

4. 必要な信頼グループを選択します。

5. 信頼グループのコンテキストメニューから［**詳細とルール**］を選択します。

   信頼グループのプロパティが開きます。

6. 次のいずれかの手順を実行します：

   - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］タブを選択します。
   - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］タブを選択します。

アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

7. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可する**（）または**ブロック**()。

8. コンピューターのリソース使用を監視する場合は、［**イベントを記録**］（）を選択します。

   Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

9. 変更内容を保存します。

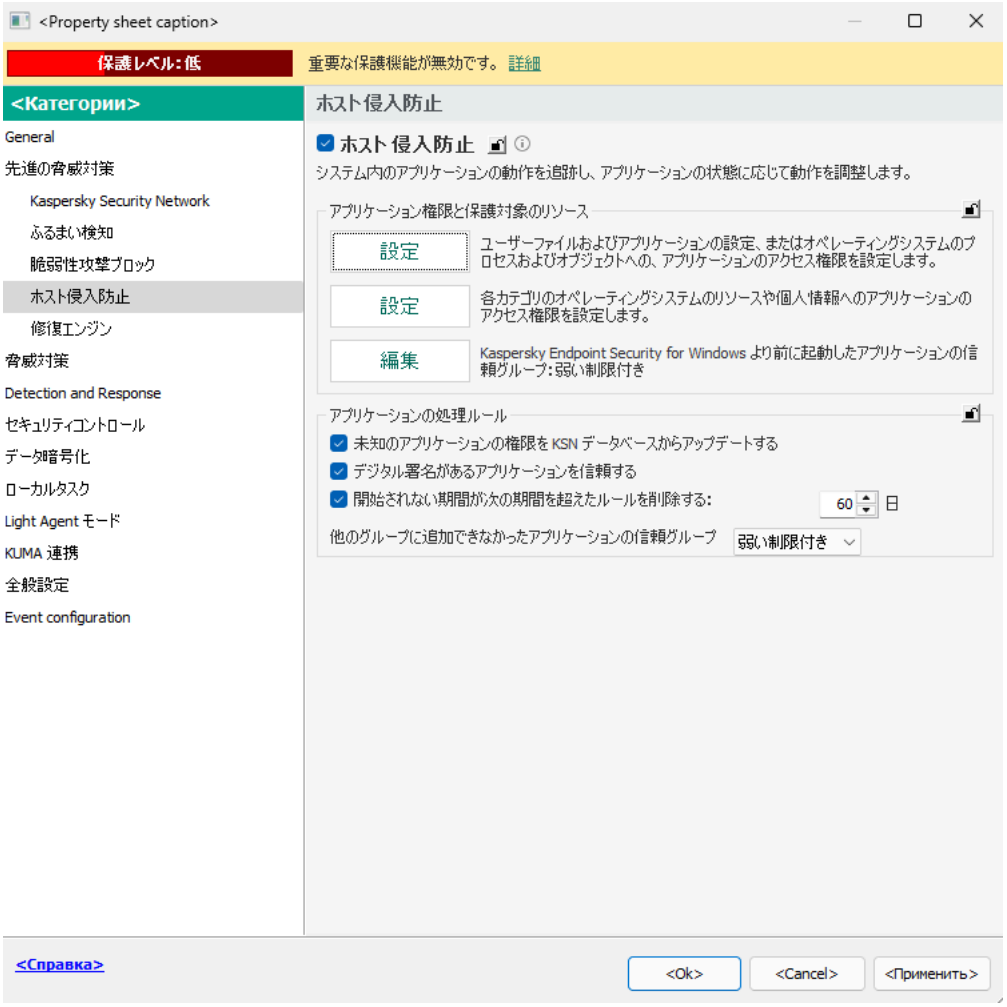
信頼グループの権限が変更されます。Kaspersky Endpoint Security は信頼グループに基づいてアプリケーションの操作をブロックします。の状態（*カスタム*）が信頼グループに割り当てられます。

Kaspersky Endpoint Security の前に起動したアプリケーションの信頼グループを選択する

Kaspersky Endpoint Security より前に起動したアプリケーションについては、ネットワーク動作のみ管理されます。管理は、ファイアウォールで指定されたネットワークルールに従って実行されます。アプリケーションのネットワーク活動を監視するときに適用するネットワークルールを指定するには、信頼グループを選択します。

管理コンソール（MMC）で Kaspersky Endpoint Security の前に起動したアプリケーションの信頼グループを選択する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーション権限と保護対象のリソース**］ブロックの［**編集**］をクリックします。
5. ［**Kaspersky Endpoint Security より前に起動したアプリケーションの許可グループ**］には、適切な信頼グループを選択します。
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソール で Kaspersky Endpoint Security の前に起動したアプリケーションの信頼グループを選択する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。
5. ［**Kaspersky Endpoint Security より前に起動したアプリケーションの許可グループ**］には、適切な信頼グループを選択します。
6. 変更内容を保存します。

製品インターフェイスで Kaspersky Endpoint Security の前に起動したアプリケーションの信頼グループを選択する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**Kaspersky Endpoint Securityより前に開始したアプリケーションの信頼グループ**］ブロックで、適切な信頼グループを選択します。
4. 変更内容を保存します。

Kaspersky Endpoint Security より前に起動したアプリケーションはその他の信頼グループに追加されます。Kaspersky Endpoint Security は信頼グループに基づいてアプリケーションの操作をブロックします。

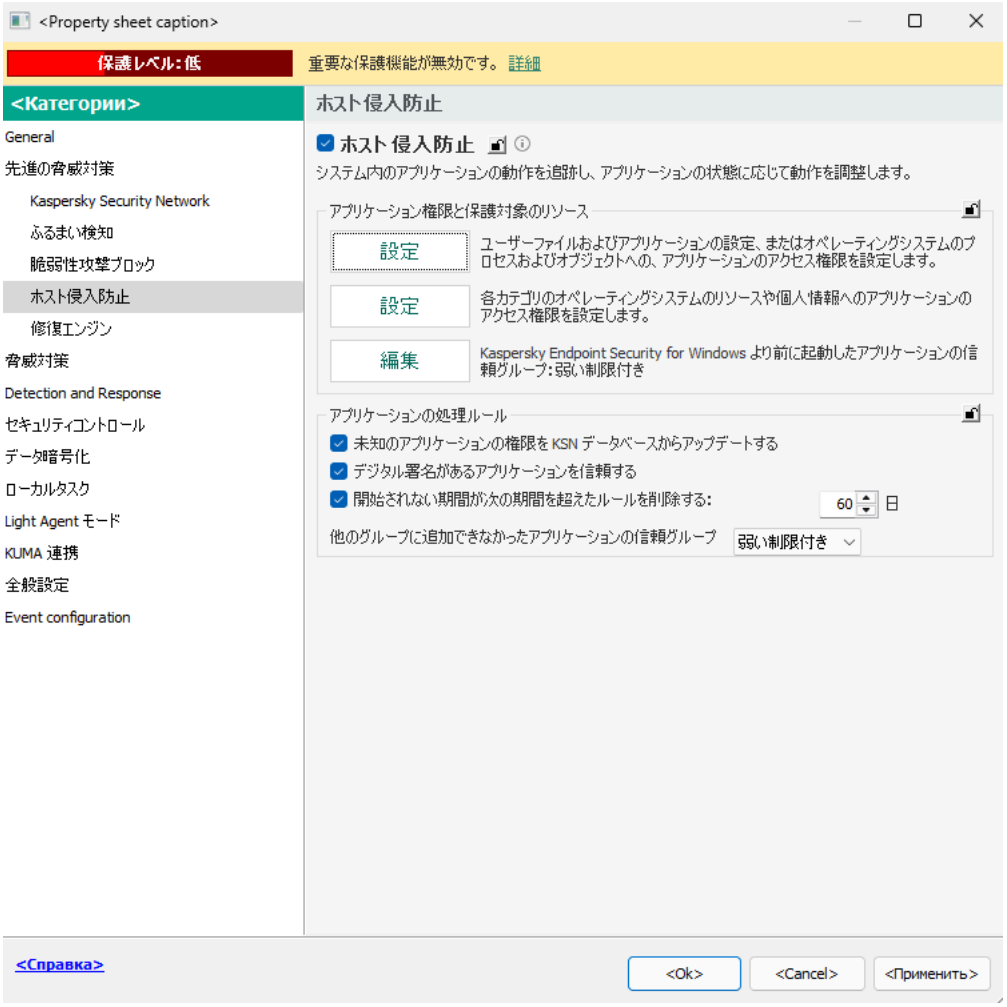
不明なアプリケーションに信頼グループを選択する

アプリケーションの初回起動時に、ホスト侵入防止機能はアプリケーションの信頼グループを決定します。インターネット接続がないか、Kaspersky Security Network にこのアプリケーションに関する情報がない場合、Kaspersky Endpoint Security は既定でこのアプリケーションを「*弱い制限付き*」グループに配置します。KSN でこの不明だったアプリケーションに関する情報が検知されると、Kaspersky Endpoint Security はこのアプリケーションの権限を更新します。その後、アプリケーションの権限を手動で編集できます。

管理コンソール（MMC）で不明なアプリケーションに信頼グループを選択する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーションの処理ルール**］ブロックで、［**他のグループに追加できなかったアプリケーションの信頼グループ**］ドロップダウンリストから必要な信頼グループを選択します。

   Kaspersky Security Network への参加が有効な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の信頼グループに振り分けられることがあります。

5. ［**未知のアプリケーションの権限を KSN データベースからアップデートする**］を使用して、不明なアプリケーションの権限の自動更新を設定します。

6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで不明なアプリケーションに信頼グループを選択する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。

5. ［**アプリケーションの処理ルール**］ブロックで、［**他のグループに追加できなかったアプリケーションの信頼グループ**］ドロップダウンリストから必要な信頼グループを選択します。

   Kaspersky Security Network への参加が有効な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の信頼グループに振り分けられることがあります。

6. ［**未知のアプリケーションの権限を KSN データベースからアップデートする**］を使用して、不明なアプリケーションの権限の自動更新を設定します。

7. 変更内容を保存します。

製品インターフェイスで不明なアプリケーションに信頼グループを選択する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。

3. ［**アプリケーションの処理ルール**］ブロックで、適切な信頼グループを選択します。

   Kaspersky Security Network への参加が有効な場合、アプリケーションが起動するたびに、Kaspersky Endpoint Security が KSN にアプリケーションの評価を問い合わせます。KSN からの応答に基づいて、アプリケーションがホスト侵入防止での設定とは別の信頼グループに振り分けられることがあります。

4. ［**不明だったアプリケーションのルールを KSN から更新する**］を使用して、不明なアプリケーションの権限の自動更新を設定します。

5. 変更内容を保存します。

デジタル署名されたアプリケーションに信頼グループを選択する

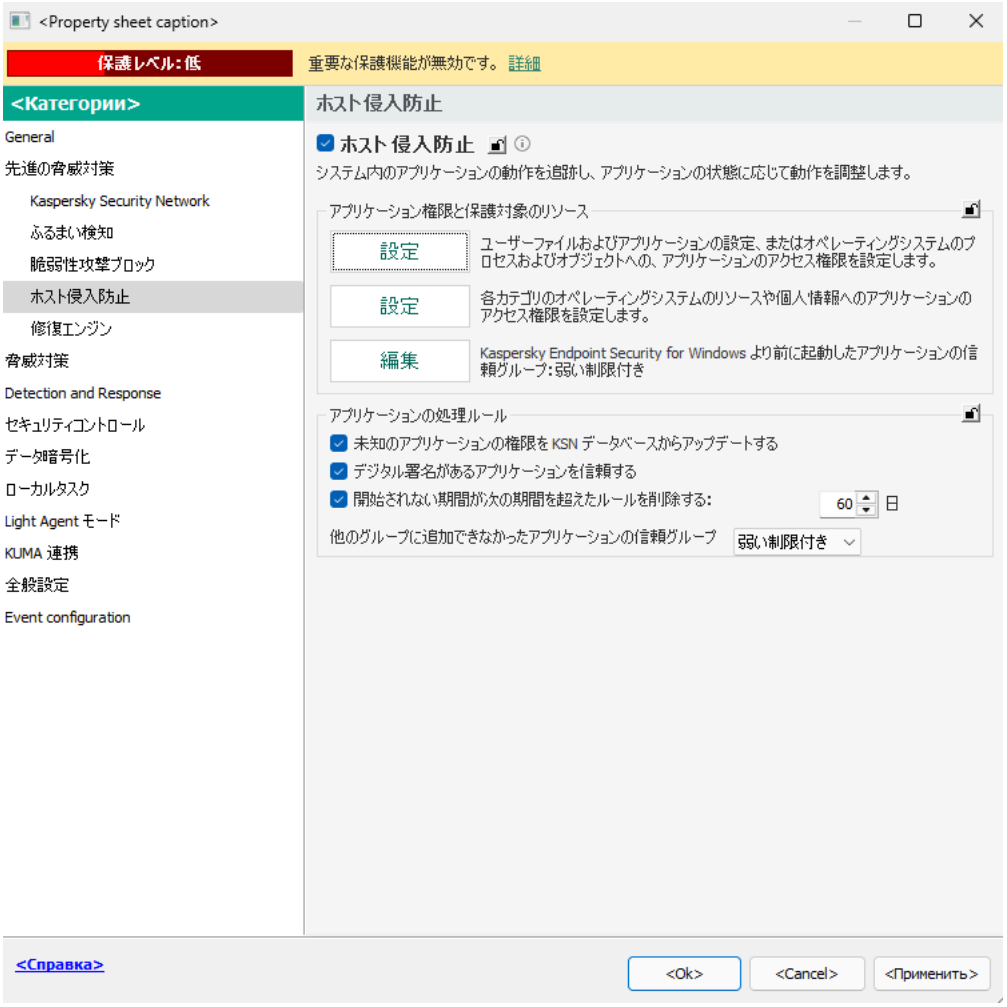
Kaspersky Endpoint Security は、Microsoft の証明書およびカスペルスキーの証明書で署名されたアプリケーションを常に「*信頼済み*」グループに配置します。

管理コンソール（MMC）でデジタル署名されたアプリケーションに信頼グループを選択する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーションの処理ルール**］ブロックで、［**デジタル署名があるアプリケーションを信頼する**］を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する［許可］信頼グループの自動割り当てを有効または無効にします。

   *信頼済みの製造元*とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加することも可能です。

   このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して信頼グループを決定します。

5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでデジタル署名されたアプリケーションに信頼グループを選択する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。

5. ［**アプリケーションの処理ルール**］ブロックで、［**デジタル署名があるアプリケーションを信頼する**］を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する［許可］信頼グループの自動割り当てを有効または無効にします。

   *信頼済みの製造元*とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加することも可能です。

   このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して信頼グループを決定します。

6. 変更内容を保存します。

製品インターフェイスでデジタル署名されたアプリケーションに信頼グループを選択する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**アプリケーションの処理ルール**］ブロックで、［**デジタル署名があるアプリケーションを信頼する**］を使用して信頼済みの製造元によりデジタル署名されたアプリケーションに対する［許可］信頼グループの自動割り当てを有効または無効にします。

   *信頼済みの製造元*とは、カスペルスキーによる信頼済みのグループに含まれるソフトウェアベンダーです。手動で信頼済みシステム証明書ストアに製造元のデジタル署名を追加することも可能です。

   このチェックボックスをオフにすると、ホスト侵入防止はデジタル署名付きのアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して信頼グループを決定します。

4. 変更内容を保存します。

アプリケーション権限の管理

既定では、アプリケーションの動作は、アプリケーションの権限によってコントロールされます。このルールは、Kaspersky Endpoint Security が初めて起動したときにアプリケーションを割り当てた信頼グループに定義されます。必要に応じて、信頼グループ全体、個別のアプリケーション、あるいは信頼グループ内に定義されているアプリケーショングループのアプリケーションの権限を編集できます。

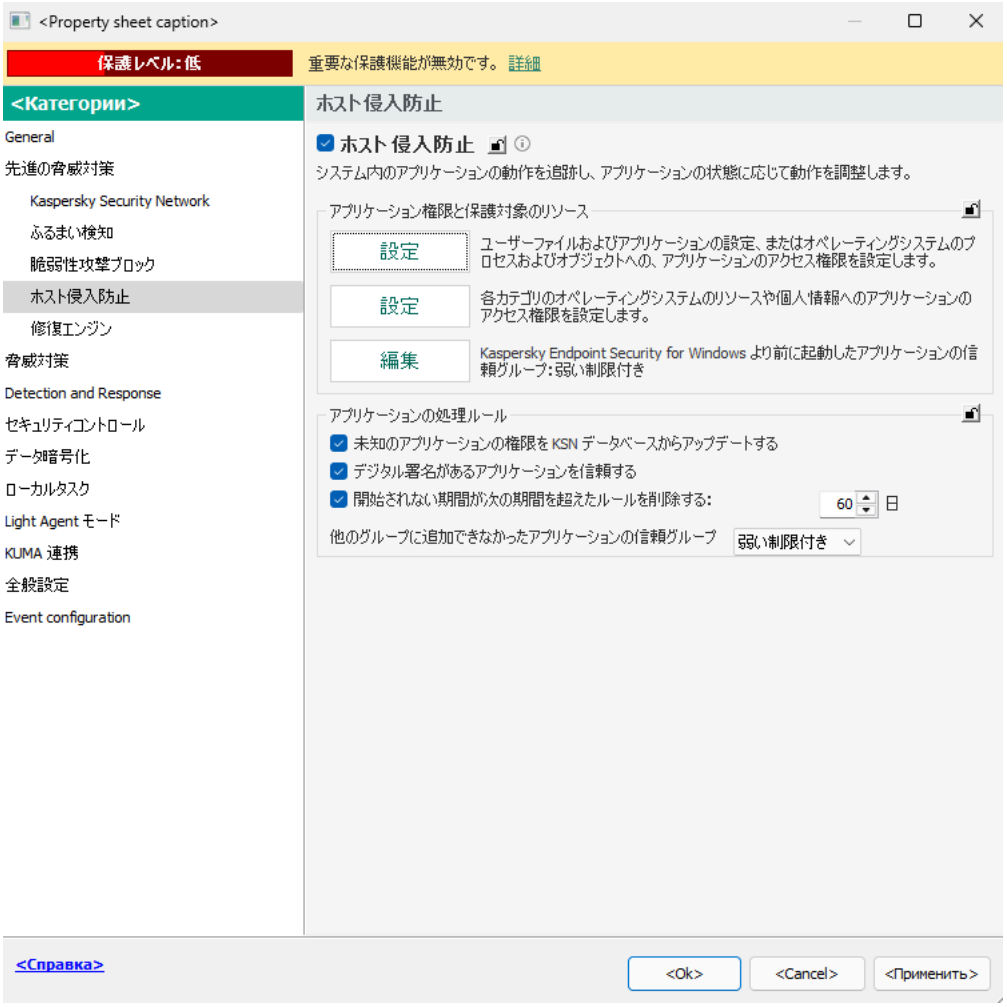
手動で定義されたアプリケーションの権限は、信頼グループに定義されたアプリケーションの権限より優先されます。言い換えると、手動で定義されたアプリケーションの権限が信頼グループに定義されたアプリケーションの権限と異なる場合、ホスト侵入防止はそのアプリケーションに対して手動で定義された権限に従って操作を制御します。

アプリケーションに対して作成したルールは、子アプリケーションに継承されます。例えば、cmd.exe のすべてのネットワーク操作をブロックした場合、cmd.exe により開始された notepad.exe ではすべてのネットワーク操作がブロックされます。アプリケーションが、アプリケーションの子アプリケーションでない別のアプリケーションから開始された場合、ルールは継承されません。

管理コンソール（MMC）でアプリケーションの権限を変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーション権限と保護対象のリソース**］ブロックの［**設定**］をクリックします。

   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

5. ［**アプリケーション権限**］タブを選択します。

6. ［**追加**］をクリックします。

7. 表示されたウィンドウで、アプリケーションの権限を変更するアプリケーションを検索する条件を入力します。

   アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

8. ［**更新**］をクリックします。

   Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。

9. 必要なアプリケーションを選択します。

10. ［**選択したアプリケーションを次の信頼グループに追加**］で、［**既定のグループ**］を選択し、［OK］をクリックします。

    アプリケーションが既定のグループに追加されます。

11. 対象のアプリケーションを選択して、アプリケーションのコンテキストメニューから［**アプリケーション権限**］を選択します。

    アプリケーションのプロパティが表示されます。

12. 次のいずれかの手順を実行します：

    - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］タブを選択します。
    - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］タブを選択します。

    アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

13. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可**（）または**ブロック**()。

14. コンピューターのリソース使用を監視する場合は、［**イベントを記録**］（/）を選択します。

    Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

15. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールと Cloud コンソールでアプリケーションの権限を変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

    ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。

5. ［**アプリケーション権限と保護対象のリソース**］セクションで、［**アプリケーション権限と保護対象のリソース**］をクリックします。

    アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

6. ［**アプリケーション権限**］タブを選択します。

    ウィンドウの左側に信頼グループのリスト、右側にそのプロパティが表示されます。

7. ［**追加**］をクリックします。

    ウィザードがアプリケーションを信頼グループに追加します。

8. アプリケーションに対して適切な信頼グループを選択します。

9. **アプリケーション**の種別を選択します。次の手順に進みます。

    複数のアプリケーションの信頼グループを変更する場合は、［**グループ**］を選択してアプリケーショングループの名前を定義します。

10. アプリケーションのリストで、変更するアプリケーションの権限を選択します。

    フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

11. ウィザードを終了します。

    アプリケーションが信頼グループに追加されます。

12. ウィンドウの左側で、アプリケーションを選択します。

13. ウィンドウの右側で、ドロップダウンリストから次のいずれかを実行します：

    - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］を選択します。
    - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］を選択します。

    アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

14. 関連するリソースに関しては、対応する操作の列で必要な次のオプションを選択します：**継承**、**許可する**（  ）**ブロックする**()。

15. コンピューターのリソース使用を監視する場合は、［**イベントの記録**］（  /  ）を選択します。

    Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

16. 変更内容を保存します。

製品インターフェイスでアプリケーションの権限を変更する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**アプリケーションの管理**］をクリックします。

    インストール済みのアプリケーションのリストが開きます。

4. 必要なアプリケーションを選択します。
5. アプリケーションのコンテキストメニューから［**詳細とルール**］を選択します。

    アプリケーションのプロパティが表示されます。

6. 次のいずれかの手順を実行します：

    - オペレーティングシステムのレジストリの操作、ユーザーファイル、および製品設定への信頼グループの権限を編集するには、［**ファイルとシステムレジストリ**］タブを選択します。
    - オペレーティングシステムのプロセスおよびオブジェクトへのアクセスに関する信頼グループの権限を編集する場合は、［**権限**］タブを選択します。

7. 関連するリソースに関しては、対応する操作の列で右クリックしてコンテキストメニューを開き、必要な次のオプションを選択します：**継承**、**許可する**（）または**ブロック**()。

8. コンピューターのリソース使用を監視する場合は、［**イベントを記録**］（）を選択します。

   Kaspersky Endpoint Security は操作に関する情報をホスト侵入防止機能に記録します。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

9. ［**除外リスト**］タブを選択して、アプリケーションの詳細を設定します（下記の表を参照）。

10. 変更内容を保存します。

アプリケーションの詳細設定

パラメータ	説明
ファイルを開く前にスキャンしない	アプリケーションが開いたファイルはすべて Kaspersky Endpoint Security のスキャンの対象外になります。例えば、信頼するアプリケーションを使用してファイルのバックアップをしていた場合など、この機能により Kaspersky Endpoint Security のリソースの消費量を減少させることができます。
アプリケーションの動作を監視しない	Kaspersky Endpoint Security はアプリケーションのファイルとオペレーティングシステム内のネットワークアクティビティを監視しません。Kaspersky Endpoint Security の別の機能で、アプリケーション処理の監視を設定できます： • **保護および管理コンポーネントを監視しない**：アプリケーションの動作は、ふるまい検知、脆弱性攻撃ブロック、ホスト侵入防止、修復エンジンおよびファイアウォールにより監視されています。 • **Managed Detection and Response および Endpoint Detection and Response を監視しない**：アプリケーションの動作は、組み込みの MDR エージェントおよび組み込みの EDR (KATA) エージェントによって監視されます。 • **Endpoint Detection and Response 用のコンソールでの対話的入力を読み取らない**：Kaspersky Endpoint Security はコンソール上のアプリケーションの管理に関するテレメトリデータを送信しません。テレメトリデータは Kaspersky Anti Targeted Attack Platform (EDR) で使用されます。
親プロセス（アプリケーション）の制限を継承しない	親プロセスで設定された制限は子プロセスには適用されません。親プロセスは、アプリケーション権限（ホスト侵入防止）およびアプリケーションネットワークルール（ファイアウォール）が設定されたアプリケーションによって開始されます。
子アプリケーションの動作を監視しない	Kaspersky Endpoint Security はファイルまたはこのアプリケーションによって開始されたアプリケーションのネットワークの動作を監視しません。例外は再帰的に適用できます。そのため、子アプリケーションのチェーン全体の動作は監視されません。
Kaspersky Endpoint Security のインターフェイスの操作を許可する	Kaspersky Endpoint Security のセルフディフェンスは、リモートコンピューターからのアプリケーションサービスを管理しようとする試みをすべてブロックします。このチェックボックスをオンにすると、リモートアクセスアプリケーションで Kaspersky Endpoint Security インターフェイスを経由して Kaspersky Endpoint Security 設定を管理できます。
暗号化されたネットワークトラフィックをスキャンしない / すべてのトラフィックをスキャンしない	アプリケーションにより開始されたネットワークトラフィックは Kaspersky Endpoint Security のスキャンから除外されます。すべてのトラフィックまたは暗号化されたトラフィックをスキャンから除外することも可能です。個別の IP アドレスおよびポート番号をスキャンから除外することも可能です。

オペレーティングシステムのリソースと個人データの保護

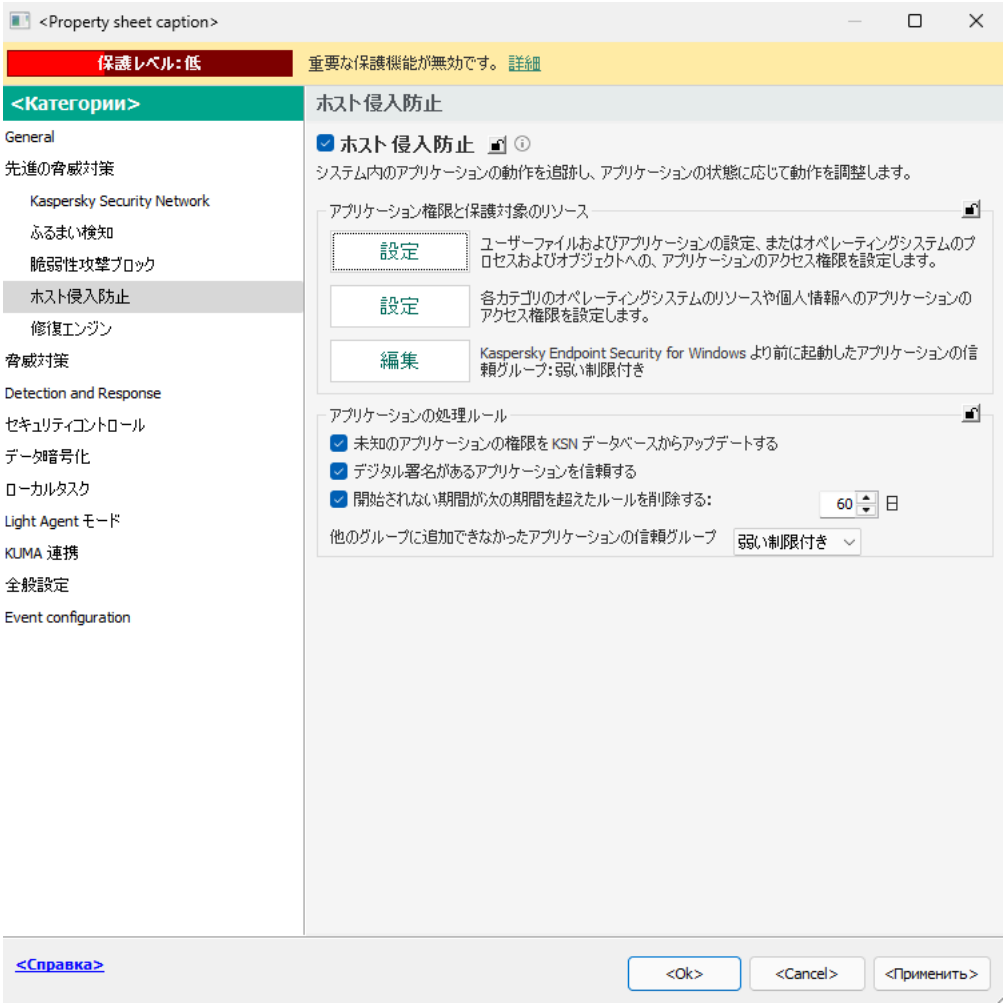
ホスト侵入防止は、さまざまなカテゴリのオペレーティングシステムリソースおよび個人情報の処理を可能にするアプリケーションの権限を管理します。カスペルスキーのエキスパートは、保護対象のリソースの事前設定カテゴリを確立しています。たとえば、［*オペレーティングシステム*］カテゴリには、アプリケーションの自動実行に関連付けられたすべてのレジストリキーを一覧にする［*スタートアップ設定*］サブカテゴリがあります。これらのカテゴリ内の保護対象のリソースまたは保護対象のリソースの事前設定カテゴリを編集したり、削除したりすることはできません。

管理コンソール（MMC）で保護対象のリソースを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーション権限と保護対象のリソース**］ブロックの［**設定**］をクリックします。

   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

5. ［**保護対象のリソース**］タブを選択します。

   ウィンドウの左側に保護対象のリソースのリストと、対応する信頼グループに基づいたこれらのリソースにアクセスするための権限が表示されます。

6. 新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。

   サブカテゴリを追加する場合は、［**追加**］→［**カテゴリ**］の順に選択します。

7. ［**追加**］を選択します。ドロップダウンリストで、追加したいリソースの種別を選択します：［**ファイルまたはフォルダー**］、または［**レジストリキー**］。

8. 表示されたウィンドウで、ファイル、フォルダーまたはレジストリキーを選択します。

   追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security が各信頼グループのアクセス権を表示します。新しいリソースの横にあるチェックボックスを使用して、リソースに対するアプリケーションの操作のコントロールを無効にすることも可能です。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールと Cloud コンソールで保護対象のリソースを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。
5. ［**アプリケーション権限と保護対象のリソース**］セクションで、［**アプリケーション権限と保護対象のリソース**］をクリックします。
   アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。
6. ［**保護対象のリソース**］タブを選択します。
   ウィンドウの左側に保護対象のリソースのリストと、対応する信頼グループに基づいたこれらのリソースにアクセスするための権限が表示されます。
7. ［**追加**］をクリックします。
   新規リソースウィザードが表示されます。
8. ［**グループ名**］ブロックで、新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。
   サブカテゴリを追加する場合は、［**保護対象のリソースのカテゴリ**］を選択します。
9. 追加したいリソースの種別を選択します：［**ファイルまたはフォルダー**］、または［**レジストリキー**］。
10. ファイル、フォルダー、またはレジストリキーを選択します。
11. ウィザードを終了します。
    追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security が各信頼グループのアクセス権を表示します。［**ステータス**］列のチェックボックスを使用して、アプリケーションのリソースに対する操作のコントロールを無効にできます。
12. 変更内容を保存します。

製品インターフェイスで保護対象のリソースを追加する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**リソースの管理**］をクリックします。
   保護対象のリソースのリストが表示されます。
4. 新しい保護対象のリソースを追加する保護対象のリソースのカテゴリを選択します。
   サブカテゴリを追加する場合は、［**追加**］→［**カテゴリ**］の順に選択します。
5. ［**追加**］を選択します。ドロップダウンリストで、追加したいリソースの種別を選択します：［**ファイルまたはフォルダー**］、または［**レジストリキー**］。

6. 表示されたウィンドウで、ファイル、フォルダーまたはレジストリキーを選択します。

   追加されたリソースにアクセスするために必要なアプリケーションの権限を表示できます。ウィンドウ左ペインで追加されたリソースを選択すると、Kaspersky Endpoint Security がアプリケーションのリストおよび各アプリケーションのアクセス権を表示します。［**コントロールを有効にする**］列の［**ステータス**］（）を使用して、リソースに対するアプリケーションの操作のコントロールを無効にすることができます。

7. 変更内容を保存します。

Kaspersky Endpoint Security は追加されたオペレーティングシステムのリソースや個人データへのアクセスを管理します。Kaspersky Endpoint Security はアプリケーションに割り当てられた信頼グループに基づいてアプリケーションのリソースへのアクセスをコントロールします。アプリケーションの信頼グループは手動で変更できます。

未使用のアプリケーションに関する情報の削除

Kaspersky Endpoint Security は、アプリケーションの権限を使用して、アプリケーションの活動を制御します。アプリケーションの権限は、信頼グループによって決定されます。Kaspersky Endpoint Security はアプリケーションの初回起動時にアプリケーションを信頼グループに追加します。アプリケーションの信頼グループは手動で変更できます。個々のアプリケーションの権限を手動で構成することもできます。Kaspersky Endpoint Security は、アプリケーションに関する次の情報を保存します：アプリケーションの信頼グループ、およびアプリケーション権限。

Kaspersky Endpoint Security は、未使用のアプリケーションに関する情報を自動的に削除して、コンピューターのリソースを節約します。Kaspersky Endpoint Security は、次のルールに従ってアプリケーションの情報を削除します：

- アプリケーションの信頼グループと権限が自動的に決定された場合は、Kaspersky Endpoint Security は 30 日後にこのアプリケーションに関する情報を削除します。アプリケーション情報の保管期間を変更したり、自動削除をオフにしたりすることはできません。

- アプリケーションを手動で信頼グループに入れるか、アクセス権を設定した場合、Kaspersky Endpoint Security は 60 日（既定の保存期間）後にこのアプリケーションに関する情報を削除します。アプリケーションの情報の保存期間を変更するか、自動削除をオフにすることができます（以下の手順を参照）。

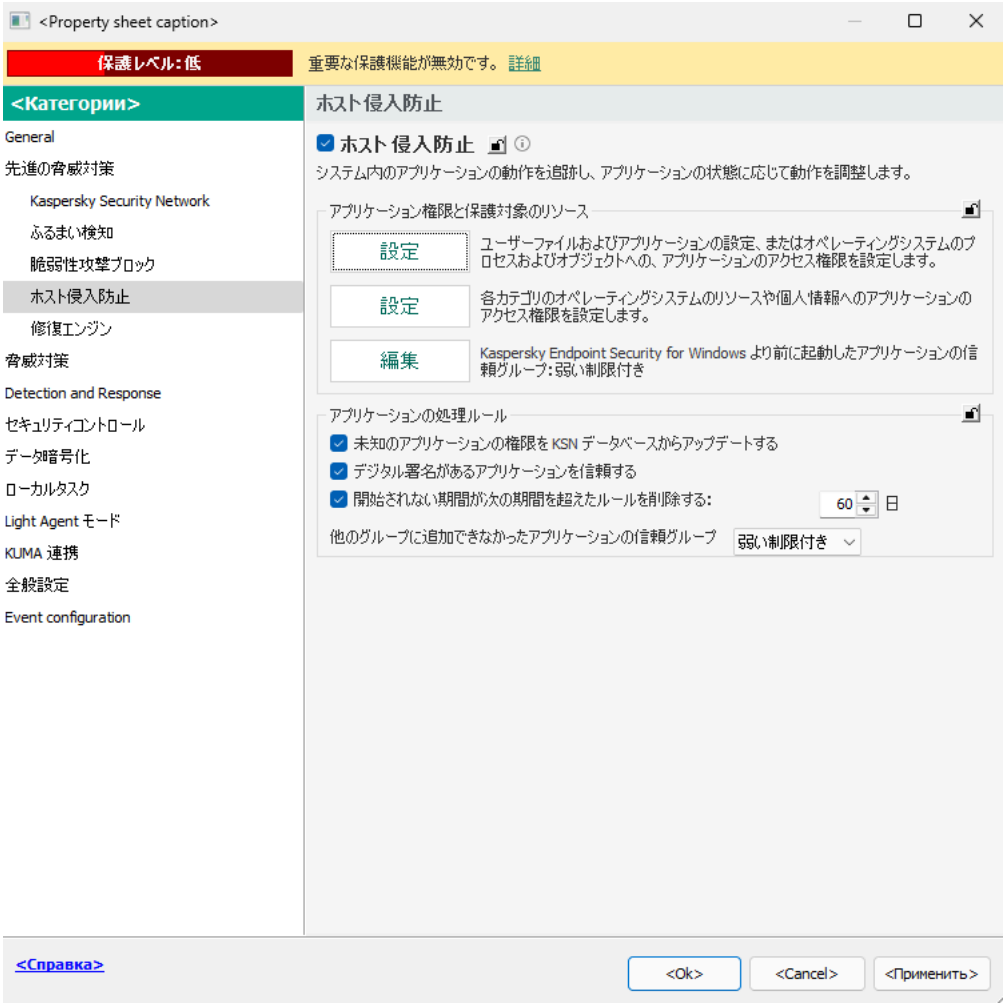
情報が削除されたアプリケーションを起動すると、Kaspersky Endpoint Security はそのアプリケーションを初めて起動したかのように分析します。

管理コンソール（MMC）で未使用のアプリケーションに関する情報の自動削除を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］の順に選択します。



侵入防止の設定

4. ［**アプリケーションの処理ルール**］ブロックで、次のいずれかを実行します：

- 自動削除を設定する場合は、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する**］をオンにして、日数を入力します。

  手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30 日後に Kaspersky Endpoint Security によって削除されます。

- 接続が一定期間なかったときにデータを削除する場合、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する**］をオンにします。

  手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。

5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで未使用のアプリケーションに関する情報の自動削除を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ホスト侵入防止**］に移動します。
5. ［**アプリケーションの処理ルール**］ブロックで、次のいずれかを実行します：

   - 自動削除を設定する場合は、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する（日単位、1〜90 まで）**］をオンにして、日数を入力します。

     手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30 日後に Kaspersky Endpoint Security によって削除されます。

   - 接続が一定期間なかったときにデータを削除する場合、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する（日単位、1〜90 まで）**］をオンにします。

     手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。
6. 変更内容を保存します。

製品インターフェイスで未使用のアプリケーションに関する情報の自動削除を設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ホスト侵入防止**］を選択します。
3. ［**アプリケーションの処理ルール**］ブロックで、次のいずれかを実行します：

   - 自動削除を設定する場合は、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する**］をオンにして、日数を入力します。

     手動で信頼グループに配置したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、定義された日数が経過すると Kaspersky Endpoint Security によって削除されます。信頼グループとアプリケーションの権限が自動的に決定されたアプリケーションに関する情報も、30 日後に Kaspersky Endpoint Security によって削除されます。

   - 接続が一定期間なかったときにデータを削除する場合、［**起動しない期間が次の期間を超えたアプリケーションのルールを削除する**］をオンにします。

     手動で信頼グループに追加したアプリケーション、または手動で設定したアクセス権を持つアプリケーションに関する情報は、Kaspersky Endpoint Security によって無期限に保存され、保存期間の制限はありません。Kaspersky Endpoint Security は、信頼グループとアプリケーション権限が 30 日後に自動的に決定されたアプリケーションに関する情報のみを削除します。
4. 変更内容を保存します。

ホスト侵入防止の監視

ホスト侵入防止機能の操作に関するレポートを受け取ることができます。レポートには、アプリケーションにより実行されたコンピューターリソースの操作に関する情報が記載されます（許可または禁止）。各リソースを使用したアプリケーションに関する情報もレポートに含まれます。

ホスト侵入防止の操作を監視するには、レポートの書き込みを有効にする必要があります。例えば、ホスト侵入防止機能の設定で個別のアプリケーションのレポートの転送を有効にすることができます。

ホスト侵入防止の監視を設定する際には、Kaspersky Security Center へのイベント転送時のネットワーク負荷を考慮に入れてください。レポートは Kaspersky Endpoint Security のローカルログ内にのみレポートを保存することも可能です。

音声、映像へのアクセスの保護

犯罪者はマイクや Web カメラなどの音声や映像を記録する端末にアクセスするために特別なプログラムを使用することがあります。Kaspersky Endpoint Security はアプリケーションがいつ音声または映像ストリームを受け取るかを制御し、認証されないデータの傍受からデータを保護します。

既定では、 Kaspersky Endpoint Security は、［*信頼済み*］グループのアプリケーションからの音声または映像ストリームの受信のみを許可します。［*弱い制限付き*］、［*強い制限付き*］および［*ブロック*］グループのアプリケーションは端末からの音声ストリームと映像ストリームを受信できません。手動でアプリケーションの音声または映像ストリームの受信を許可することができます。

音声ストリームの保護の特性

音声ストリームの保護には、次の特性があります：

- ホスト侵入防止が有効になっている場合にのみ、この機能が動作します。
- ホスト侵入防止が開始するより前にアプリケーションが音声ストリームの受信を始めた場合、そのアプリケーションの音声ストリームの受信は許可され、通知は表示されません。
- アプリケーションが音声ストリームの受信を始めたあと、そのアプリケーションを［*ブロック*］または［*強い制限付き*］グループに移動した場合、そのアプリケーションの音声ストリームの受信は許可され、通知は表示されません。
- 音声録音デバイスへのアプリケーションのアクセス設定を変更したのち（たとえば、アプリケーションの音声ストリーム受信をブロックしたのち）、そのアプリケーションの音声ストリームの受信を停止するには、アプリケーションを再起動する必要があります。
- 音声録音デバイスからの音声ストリームのアクセスの管理は、アプリケーションの Web カメラアクセス設定に依存しません。

- Kaspersky Endpoint Security は、内蔵マイクおよび外付けマイクへのアクセスのみを保護します。その他の音声ストリーミングデバイスはサポートされません。
- デジタル一眼レフカメラ、ポータブルビデオカメラ、アクションカメラなどのデバイスからの音声ストリームの保護は保証されません。
- Kaspersky Endpoint Security をインストールしたのち、音声および映像を記録または再生するアプリケーションを最初に起動すると、音声および映像の再生または記録が中断することがあります。これは、音声録音デバイスへのアプリケーションのアクセスを管理する機能を有効にするために必要です。Kaspersky Endpoint Security が最初に起動するときに、音声ハードウェアを管理するシステムサービスが再起動します。

アプリケーションの Web カメラへのアクセスの保護機能の特性

Web カメラへのアクセスの保護機能には、次の考慮事項と制限があります：

- 本製品は、Web カメラのデータの処理で得られた映像および静止画を管理します。
- 本製品は、Web カメラから受信した映像ストリームの一部である音声ストリームを管理します。
- 本製品は、USB または IEEE1394 で接続され、Windows のデバイスマネージャーで［イメージング デバイス］として表示される Web カメラのみを管理します。
- Kaspersky Endpoint Security は、以下の Web カメラをサポートします：
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  このリストにない Web カメラのサポートは保証されません。

有害 USB 攻撃ブロック

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

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

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します（下の図を参照）。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID/PID、接続されたポートの番号）が認証キーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターの USB ポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、新しいコードが生成されます。数値コードの入力試行回数は指定できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合（下の図を参照）、本製品はキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックは、既定ではインストールされません。有害 USB 攻撃ブロックが必要な場合は、製品のインストール前にインストールパッケージのプロパティにコンポーネントを追加するか、製品のインストール後に利用可能なコンポーネントを変更できます。



キーボード承認

有害 USB 攻撃ブロックの有効化と無効化

有害 USB 攻撃ブロックのインストール前にオペレーティングシステムによってキーボードとして識別され、コンピューターに接続された USB デバイスは、コンポーネントのインストール後は、認証済みとみなされます。

管理コンソール（MMC）で有害 USB 攻撃ブロックを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］の順に選択します。
4. ［**有害 USB 攻撃ブロック**］を使用して機能を有効または無効にします。
5. ［**USB デバイスの接続時の認証**］ブロックで、認証コードの入力に関するセキュリティ設定を調整します：
   - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は 1～10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。
   - **最大試行回数を超えた場合のタイムアウト（分）**：認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。有効な値は 1～180（分）です。
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで有害 USB 攻撃ブロックを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。
5. ［**有害 USB 攻撃ブロックは有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. ［**USB デバイスの認証**］ブロックで、認証コードの入力に関するセキュリティ設定を調整します：

   - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は 1～10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。

   - **最大試行回数に達した場合のタイムアウト（分）**：認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。有効な値は 1～180（分）です。

7. 変更内容を保存します。

製品インターフェイスで有害 USB 攻撃ブロックを有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］を選択します。



有害 USB 攻撃ブロックの設定

3. ［**有害 USB 攻撃ブロック**］トグルスイッチを使用して機能を有効または無効にします。

4. ［**USB デバイスの接続時の認証**］ブロックで、認証コードの入力に関するセキュリティ設定を調整します：

   - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は 1 ～ 10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。

   - **最大試行回数を超えた場合のタイムアウト**：認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。有効な値は 1 ～ 180（分）です。

5. 変更内容を保存します。

有害 USB 攻撃ブロックが有効になると、Kaspersky Endpoint Security はオペレーティングシステムによってキーボードとして認識された接続済みの USB デバイスの認証を要求します。認証されていないキーボードは、認証されるまでユーザーは使用できません。

USB デバイスの認証時のセキュリティキーボードの使用

セキュリティキーボードは、任意の文字の入力をサポートしない USB デバイス（バーコードスキャナーなど）の認証時にのみ使用してください。未知の USB デバイスの認証時に、セキュリティキーボードを使用しないでください。

管理コンソール（MMC）でセキュリティキーボードを使用した認証を許可またはブロックする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］の順に選択します。

4. ［**USB デバイスの認証時にセキュリティキーボードの使用を禁止する**］を使用して認証時のセキュリティキーボードの使用をブロックまたは許可します。

5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでセキュリティキーボードを使用した認証を許可またはブロックする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

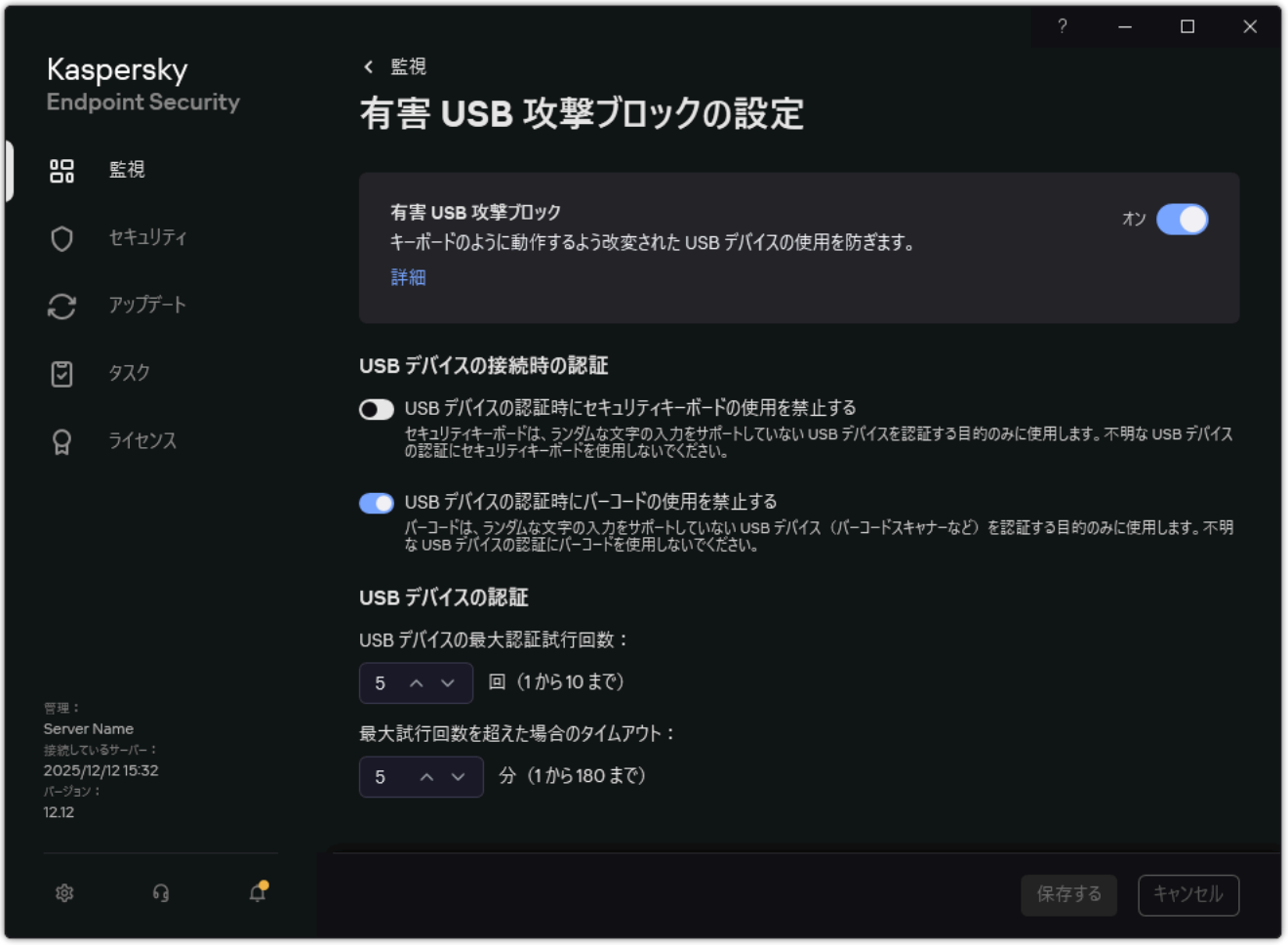
4. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。

5. ［**USB デバイスの認証時にセキュリティキーボードの使用を禁止する**］トグルスイッチを使用して認証時のセキュリティキーボードの使用をブロックまたは許可します。

6. 変更内容を保存します。

製品インターフェイスでセキュリティキーボードを使用した認証を許可またはブロックする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］を選択します。



有害 USB 攻撃ブロックの設定

3. ［**USB デバイスの認証時にセキュリティキーボードの使用を禁止する**］トグルスイッチを使用して認証時のセキュリティキーボードの使用をブロックまたは許可します。

4. 変更内容を保存します。



USB デバイスの認証

バーコードスキャナー認証

バーコードスキャナーをコンピューターに接続すると、有害 USB 攻撃ブロックが、このデバイスを入力デバイスとして識別し、認証を実行するように要求します。バーコードスキャナーを認証するには、画面に表示されるバーコードをスキャンする必要があります。本製品は、ほとんどのバーコードスキャナーおよび QR コードスキャナーでサポートされている Code39 形式のバーコードを生成します。

Kaspersky Endpoint Security は、もう 1 つのバーコードスキャナーの認証方法もサポートしています。タッチスクリーンデバイスを使用している場合は、セキュリティキーボードを使用してコードを入力できます。そのためには、セキュリティキーボードを許可する必要があります。この方法は、たとえばレジに組み込まれた固定式のバーコードスキャナーの場合に便利です。その他のバーコードスキャナーの認証方法は禁止されています。

既定では、本製品は USB デバイスの認証にバーコードを使用しません。

管理コンソール（MMC）でバーコードによる USB デバイスの認証を有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］の順に選択します。

5. ［**USB デバイスの認証時にバーコードの使用を禁止する**］を使用して認証時のバーコードの使用をブロックまたは許可します。

6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでバーコードによる USB デバイスの認証を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。

5. ［**USB デバイスの認証時にバーコードの使用を禁止する**］スイッチを使用して認証時のバーコードの使用をブロックまたは許可します。

6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスでバーコードによる USB デバイスの認証を有効にする方法

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**有害 USB 攻撃ブロック**］を選択します。



有害 USB 攻撃ブロックの設定

3. ［**USB デバイスの認証時にバーコードの使用を禁止する**］スイッチを使用して認証時のバーコードの使用をブロックまたは許可します。

4. 変更内容を保存します。

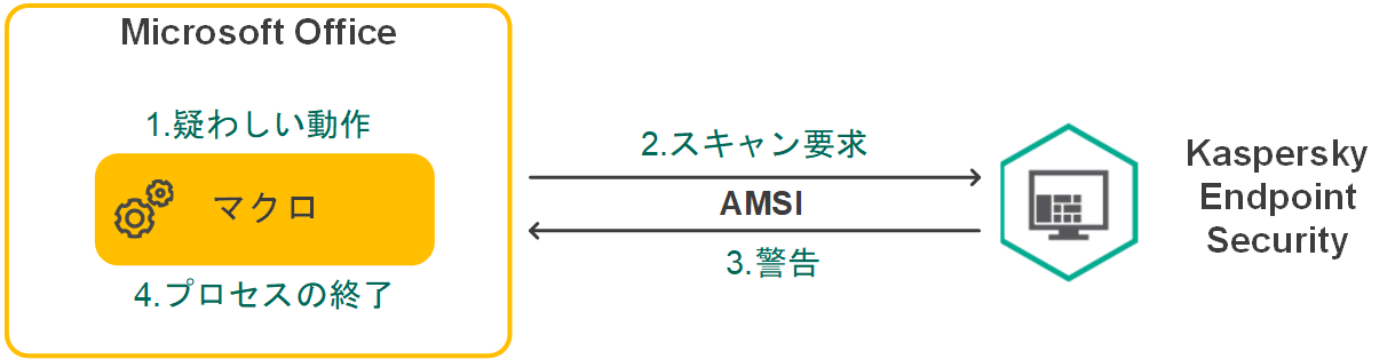


バーコードスキャナー認証

AMSI 保護

AMSI 保護コンポーネントは、Microsoft の Antimalware Scan Interface をサポートする目的で設計されています。*AMSI（Antimalware Scan Interface）*により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト（たとえば、PowerShell スクリプトなど）のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。対象となるサードパーティ製品としては、たとえば Microsoft Office 製品があります。AMSI について詳しくは、Microsoft 社の資料を参照してください。

AMSI 保護機能では、脅威の検知とサードパーティ製品への検知された脅威に関する通知のみを実行できます。脅威に関する通知を受信したサードパーティ製品側では、脅威による悪意のあるふるまいを許可しません（たとえば、プロセスを終了します）。



AMSI の動作例

また、一定間隔の間に特定のサードパーティ製品から上限を超えてスキャン要求を受信した場合などにも、AMSI 保護機能でそのサードパーティ製品からのスキャン要求を拒否する場合があります。Kaspersky Endpoint Security は、拒否したサードパーティ製品のスキャン要求に関する情報を管理サーバーに送信します。AMSI 保護機能は、継続的な AMSI 保護機能との連携が有効になっているサードパーティ製品からのリクエストはブロックしません。

AMSI 保護機能は、ワークステーションおよびサーバー用の次のオペレーティングシステムで使用できます：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise マルチセッション
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2019 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition （Server Core モードを含む）
- Windows Server 2025 Standard / Datacenter

AMSI 保護の有効化と無効化

既定では、AMSI 保護は有効になっており、カスペルスキーが推奨するモードで動作します（下の表を参照）。

管理コンソール（MMC）で AMSI 保護を有効または無効にする方法

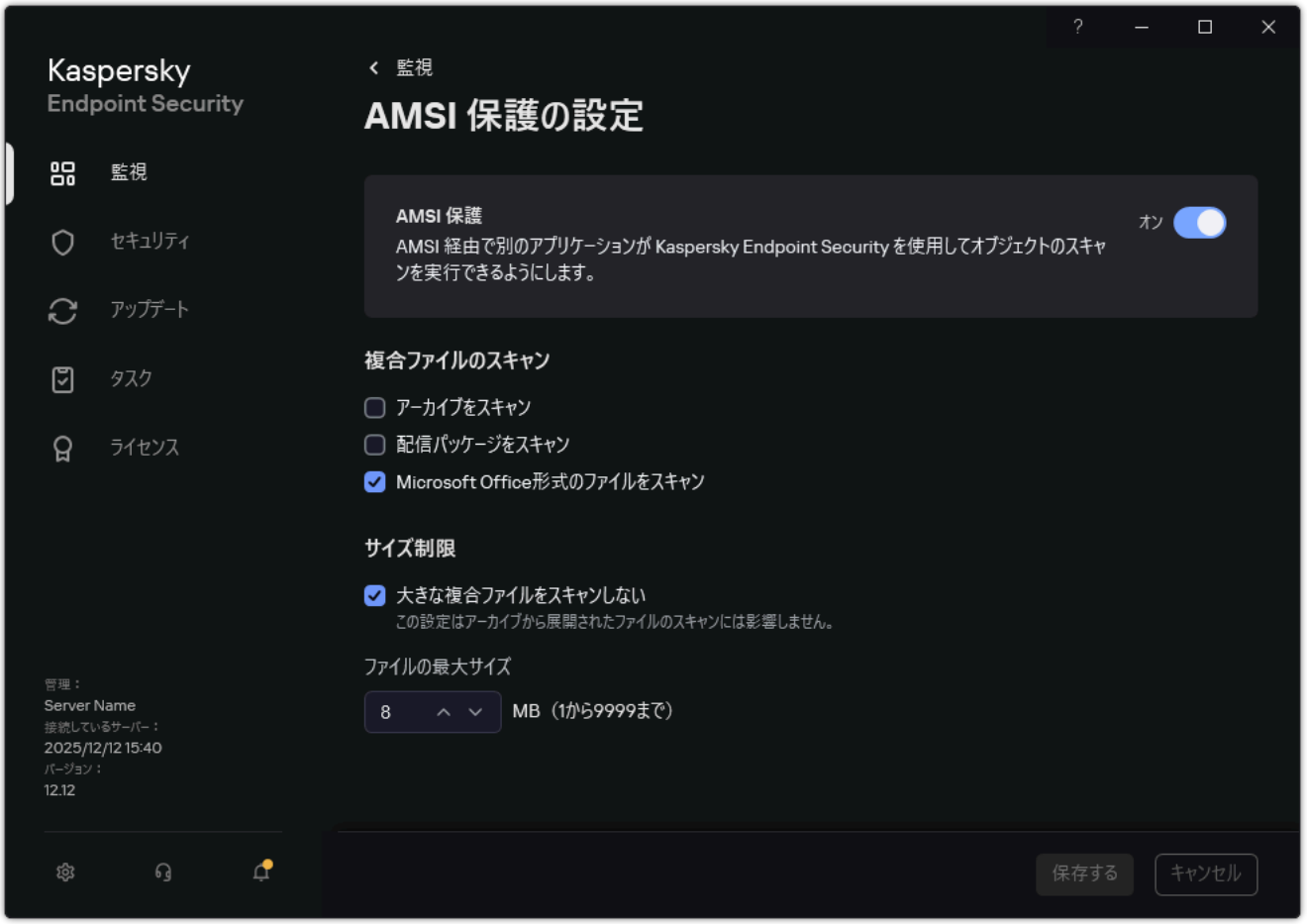
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**AMSI スキャナー**］の順に選択します。
4. ［**AMSI スキャナー**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで AMSI 保護を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**AMSI 保護**］に移動します。
5. ［**AMSI 保護は有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで AMSI 保護を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**AMSI 保護**］を選択します。



AMSI 保護の設定

3. ［**AMSI 保護**］トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

カスペルスキーのエキスパートが推奨する AMSI 保護の設定

パラメータ	値	説明
アーカイブをスキャン	**オフ**	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配信パッケージをスキャン	**オフ**	サードパーティ製品の配布パッケージをスキャンします。
Microsoft Office形式のファイルをスキャン	**オン**	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
大きな複合ファイルをスキャンしない	**ファイルの最大サイズ：8 MB**	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。

AMSI 保護によるファイルスキャンの最適化

ファイルスキャンを最適化することができます。最適化することで、スキャン時間を短縮したり、Kaspersky Endpoint Security の処理速度を向上させたりすることができます。スキャンが必要な複合ファイル（アーカイブ、配布パッケージ、またはオフィス形式のファイル）を選択できます。スキャンする複合ファイルのサイズを制限することもできます。指定された値を超えるサイズのファイルは解凍されません。

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

管理コンソール（MMC）で AMSI 保護によるファイルスキャンの最適化を行う方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**AMSI スキャナー**］の順に選択します。
4. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。
5. ［**サイズ制限**］ブロックで、次のいずれかを実行します：
   - AMSI 保護を使用して大きな複合ファイルを解凍しない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
   - AMSI 保護を使用して大きな複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

   > アーカイブから展開されるサイズの大きいファイルは、［**大きな複合ファイルをスキャンしない**］がオンにされているかどうかに関係なくスキャンされます。
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで AMSI 保護によるファイルスキャンの最適化を行う方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**AMSI 保護**］に移動します。
5. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。

6. ［**スキャンの最適化**］ブロックで、次のいずれかを実行します：

   - AMSI 保護を使用して大きな複合ファイルを解凍しない場合は、［**サイズを制限する**］をオンにし、任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
   - AMSI 保護を使用して大きな複合ファイルを解凍する場合は、［**サイズを制限する**］をオフにします。

   アーカイブから展開されるサイズの大きいファイルは、［**サイズを制限する**］がオンにされているかどうかに関係なくスキャンされます。

7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで AMSI 保護によるファイルスキャンの最適化を行う方法

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**AMSI 保護**］を選択します。



AMSI 保護の設定

3. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。
4. ［**サイズ制限**］ブロックで、次のいずれかを実行します：

   - AMSI 保護を使用して大きな複合ファイルを解凍しない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
   - AMSI 保護を使用して大きな複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

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

5. 変更内容を保存します。

ウェブ脅威対策

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

Kaspersky Endpoint Security では、HTTP、HTTPS、FTP のトラフィック、URL、IP アドレスがスキャンされます。

ウェブ脅威対策を使用するには、本製品の初期設定を完了する必要があります。

- HTTPS トラフィックを監視するには、 暗号化された接続のスキャンを有効にします（既定では有効になっています）。
- Kaspersky Endpoint Security が監視する必要があるポートを選択します（既定では、本製品はすべてのポートを監視します）。
- Kaspersky Endpoint Security がトラフィックを監視するアプリケーションを選択します。ほとんどのブラウザーは、カスペルスキーが推奨するアプリケーションのリストに含まれています。ブラウザーがリストにない場合は、手動で追加してください。
- Web トラフィックに Web ページとの連携スクリプトを埋め込むことを推奨します（既定では、スクリプトの挿入は無効になっています）。このスクリプトにより、ウェブ脅威対策のイベントをアプリケーションイベントログ、OS イベントログ、レポートに登録できるようになります。

ユーザーが、悪意のある Web サイトやフィッシングサイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックし、警告を表示します（下の図を参照）。



Web サイトへのアクセスが拒否されたことを示すメッセージ

ウェブ脅威対策の有効化と無効化

既定では、ウェブ脅威対策は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。ウェブ脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます：**高**、**推奨**、**低**。カスペルスキーのエキスパートが推奨する設定グループは、［**推奨**］セキュリティレベルです（下の表を参照）。HTTP および GTP プロトコルを介して受け取りまたは転送された Web トラフィックに対して、Web トラフィックのセキュリティレベルを事前インストールされたセキュリティレベルから選択することも、カスタマイズすることもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

セキュリティレベルを選択もしくは設定できるのは、管理コンソール（MMC）または本製品のローカルインターフェイスのみです。Web コンソールまたは Cloud コンソールではセキュリティレベルの選択や設定はできません。

管理コンソール（MMC）でウェブ脅威対策を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。
4. ［**ウェブ脅威対策**］を使用して機能を有効または無効にします。
5. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。
   - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：
     - **高**：HTTP や FTP 経由でコンピューターが受信する Web トラフィックをウェブ脅威対策が最大限にスキャンするときのセキュリティレベル。ウェブ脅威対策は、あらゆる定義データベースを使用してすべての Web トラフィックオブジェクトを詳細にスキャンし、最も徹底的なヒューリスティック分析を実行します。
     - **推奨**：本製品のパフォーマンスと Web トラフィックのセキュリティの間で最適なバランスが取れたセキュリティレベル。ウェブ脅威対策は中スキャンレベルでヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、この Web トラフィックセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。
     - **低**：この Web トラフィックセキュリティレベルの設定により、Web トラフィックのスキャンの速度が最大になります。ウェブ脅威対策は低スキャンレベルでヒューリスティック分析を実行します。
   - カスタムのセキュリティレベルを設定する場合は、［**設定**］をクリックして、機能の設定を定義します。

     ［**既定**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

6. ［**脅威の検知時の処理**］ブロックで、悪意のある Web トラフィックオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **ブロック**：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。

   - **通知する**：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでウェブ脅威対策を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ウェブ脅威対策**］に移動します。

5. ［**ウェブ脅威対策は有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. ［**脅威の検知時の処理**］ブロックで、悪意のある Web トラフィックオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **ブロックする**：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。

   - **許可する、通知する、または手動選択（OS により異なります）**：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。

7. 必要に応じて、信頼する Web アドレスのリストを作成します。

8. 変更内容を保存します。

ウェブ脅威対策を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］を選択します。

3. ［**ウェブ脅威対策**］トグルスイッチを使用して機能を有効または無効にします。

4. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。

- 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：

  - **高**：HTTP や FTP 経由でコンピューターが受信する Web トラフィックをウェブ脅威対策が最大限にスキャンするときのセキュリティレベル。ウェブ脅威対策は、あらゆる定義データベースを使用してすべての Web トラフィックオブジェクトを詳細にスキャンし、最も徹底的なヒューリスティック分析を実行します。

  - **推奨**：本製品のパフォーマンスと Web トラフィックのセキュリティの間で最適なバランスが取れたセキュリティレベル。ウェブ脅威対策は中スキャンレベルでヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、この Web トラフィックセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。

  - **低**：この Web トラフィックセキュリティレベルの設定により、Web トラフィックのスキャンの速度が最大になります。ウェブ脅威対策は低スキャンレベルでヒューリスティック分析を実行します。

- カスタムのセキュリティレベルを設定する場合は、［**詳細設定**］をクリックして、機能の設定を定義します。

  ［**推奨のセキュリティレベルに戻す**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

5. ［**脅威の検知時の処理**］ブロックで、悪意のある Web トラフィックオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

- **ブロックする**：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。

- **通知する**：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。

6. 変更内容を保存します。

カスペルスキーが推奨するウェブ脅威対策の設定値（推奨されるセキュリティレベル）

パラメータ	値	説明
悪意のあるWebサイトのデータベースでWebアドレスをチェックする	**オン**	Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
フィッシングサイトのデータベースでWebアドレスをチェックする	**オン**	フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
ヒューリスティック分析を使用する（ウェブ脅威対策）	**中**	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。

パラメータ	値	説明
ヒューリスティック分析を使用する（フィッシング対策）	**オン**	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。
脅威の検知時の処理	**ブロックする**	このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。

悪意のある Web アドレスの検知方法

ウェブ脅威対策は、定義データベース、Kaspersky Security Network クラウドサービス、ヒューリスティック分析を使用して悪意のある Web アドレスを検知します。

悪意のある Web アドレスの検知方法を選択できるのは、管理コンソール（MMC）または本製品のローカルインターフェイスのみです。Web コンソールまたは Cloud コンソールでは、Web アドレスの検知方法を選択することはできません。既定では、悪意のある Web アドレスのデータベースで Web アドレスをチェックします（スキャンレベル「中」）。

悪意のある Web アドレスのデータベースを使用したスキャン

Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。

悪意のある Web アドレスのデータベース内に登録があるかどうかを判断するためにすべてのリンクをスキャンします。本製品のセキュアな接続のスキャン設定はリンクのスキャン機能に影響しません。暗号化された接続のスキャンが無効になっている場合、Kaspersky Endpoint Security は、ネットワークトラフィックが暗号化された接続を経由して転送されていても悪意のある Web サイトのデータベースでリンクをチェックします。

管理コンソール（MMC）を使用して［悪意のある Web アドレスのデータベースで Web アドレスをチェックする］を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。
5. 表示されるウィンドウの［**スキャン方法**］ブロックで、［**悪意のある Web アドレスのデータベースで Web アドレスをチェックする**］をオンまたはオフにして、悪意のある Web アドレスのデータベースでの Web アドレスのチェックを有効または無効にします。
6. 変更内容を保存します。

ローカルインターフェイスを使用して［悪意のある Web アドレスのデータベースで Web アドレスをチェックする］を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**スキャン方法**］ブロックで、［**悪意のあるWebサイトのデータベースでWebアドレスをチェックする**］をオンまたはオフにして、悪意のある Web アドレスのデータベースでの Web アドレスのチェックを有効または無効にします。
5. 変更内容を保存します。

ヒューリスティック分析

Kaspersky Endpoint Security のヒューリスティック分析では、オペレーティングシステムにおけるアプリケーションの動作が分析されます。ヒューリスティック分析を使用することで、Kaspersky Endpoint Security の定義データベースに現在登録されていない脅威を検知できます。

ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。

管理コンソール（MMC）でヒューリスティック分析の使用を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。
5. ウイルスやその他のマルウェアを見つけるためにヒューリスティック分析を使用して Web トラフィックをスキャンする場合は、表示されたウィンドウで、［**スキャン方法**］ブロックの［**ヒューリスティック分析を使用する**］を選択します。
6. 次に、スライダーを使用して、ヒューリスティック分析レベル（**低**、**中**、**高**のいずれか）を設定します。

   ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
7. 変更内容を保存します。

製品インターフェイスでヒューリスティック分析の使用を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ウイルスやその他のマルウェアを見つけるためにヒューリスティック分析を使用して Web トラフィックをスキャンする場合は、［**スキャン方法**］ブロックで、［**ヒューリスティック分析を使用する**］を選択します。

   ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
5. 変更内容を保存します。

フィッシング対策

ウェブ脅威対策では、リンクがフィッシングサイトへのリンクでないか確認します。これは*フィッシング攻撃*の防止になります。フィッシング攻撃は偽装して行われることがあります。たとえば、メールが銀行から来たもので、その銀行のオフィシャル Web サイトへのリンクが含まれているように見せかけます。リンクをクリックすると、その銀行の偽装サイトに移動します。偽装サイトにアクセスしているにもかかわらず、ブラウザーにはその銀行の実際の Web アドレスが表示されているように見えることがあります。それ以降、偽装サイトでの処理がすべて追跡され、現金が盗まれることがあります。

フィッシングサイトへのリンクは、メールからだけでなく、メッセンジャーなどの他のソースから受け取ることもあります。このため、ウェブ脅威対策は、Web トラフィックのレベルでフィッシングサイトへのアクセスを試行し、その Web サイトへのアクセスをブロックします。フィッシングサイトの URL のリストは、Kaspersky Endpoint Security の配信キットに含まれています。

フィッシング対策を設定できるのは、管理コンソール（MMC）または本製品のローカルインターフェイスのみです。Web コンソールまたは Cloud コンソールではフィッシング対策の設定はできません。既定では、フィッシング対策ではヒューリスティック分析が有効になっています。

管理コンソール（MMC）でフィッシング対策を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。

5. 表示されるウィンドウの［**フィッシング対策の設定**］ブロックで、［**フィッシングサイトのデータベースでWeb アドレスをチェックする**］を使用してフィッシング対策をオンまたはオフにします。

   フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。

6. フィッシングリンクを含む Web ページを見つけるためにヒューリスティック分析を使用してスキャンする場合は、［**ヒューリスティック分析を使用する**］を選択します。

   Kaspersky Endpoint Security のヒューリスティック分析では、オペレーティングシステムにおけるアプリケーションの動作が分析されます。ヒューリスティック分析を使用することで、Kaspersky Endpoint Security の定義データベースに現在登録されていない脅威を検知できます。

   定義データベースおよびヒューリスティック分析に加えて、リンクをスキャンするには Kaspersky Security Network の評価データベースを使用します。

7. 変更内容を保存します。

製品インターフェイスでフィッシング対策を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ウェブ脅威対策機能でフィッシングサイトのデータベースを使用してリンクをチェックする場合は［**フィッシング対策**］ブロックで［**フィッシングサイトのデータベースでWebアドレスをチェックする**］を選択します。フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
5. フィッシングリンクを含む Web ページを見つけるためにヒューリスティック分析を使用してスキャンする場合は、［**ヒューリスティック分析を使用する**］を選択します。

   Kaspersky Endpoint Security のヒューリスティック分析では、オペレーティングシステムにおけるアプリケーションの動作が分析されます。ヒューリスティック分析を使用することで、Kaspersky Endpoint Security の定義データベースに現在登録されていない脅威を検知できます。

   定義データベースおよびヒューリスティック分析に加えて、リンクをスキャンするには Kaspersky Security Network の評価データベースを使用します。

6. 変更内容を保存します。

信頼する URL のリストの作成

悪意のある Web サイトやフィッシング Web サイトのほかにも Web サイトをブロックすることができます。例えば、ウェブ脅威対策は RFC 標準に適合しない HTTP トラフィックをブロックします。コンテンツが信頼できる Web サイトのリストを作成できます。ウェブ脅威対策は、信頼する URL からの情報にウイルスおよびその他の脅威が含まれるかどうかを分析しません。既知の Web サイトからのファイルのダウンロードが、ウェブ脅威対策によって妨げられる場合などに、このオプションを使用してください。

URL は特定の Web ページのアドレスまたは Web サイトのアドレスです。

信頼ゾーンは、管理コンソール（MMC）と Web コンソールで異なる方法でグループ化されます。同様に、信頼ゾーンのパラメータ変更を防止する方法も異なります（別の「南京錠」）。本製品の管理には、Web コンソールのみを使用することを推奨します。別のコンソールで信頼ゾーンを設定すると、管理プラグインによって「南京錠」が既定の状態にリセットされる場合があります。

管理コンソール（MMC）を使用して信頼する URL を追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、**信頼する Web アドレス**タブを選択します。
6. ［**信頼する Web アドレスの Web トラフィックをスキャンしない**］チェックボックスをオンにします。
   このオプションをオンにすると、ウェブ脅威対策は、信頼する Web サイトにアドレスが含まれている Web ページ / Web サイトのコンテンツをスキャンしません。信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。
7. 信頼するコンテンツを含む URL / Web サイトのリストを作成します。
   Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
   また、信頼する URL のリストを XML ファイルからインポートすることもできます。
8. 変更内容を保存します。

Web コンソールと Cloud コンソールで信頼する URL を追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**ウェブ脅威対策**］に移動します。

5. ［**信頼する Web アドレス**］をクリックします。

6. 信頼するコンテンツを含む URL / Web サイトのリストを作成します。

   Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。

   また、信頼する URL のリストを XML ファイルからインポートすることもできます。

7. 変更内容を保存します。

製品インターフェイスで信頼する URL を追加する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］を選択します。

3. ［**詳細設定**］をクリックします。

4. ［**信頼するWebサイトに登録したURLのトラフィックはスキャンしない**］をオンにします。

   このオプションをオンにすると、ウェブ脅威対策は、信頼する Web サイトにアドレスが含まれている Web ページ / Web サイトのコンテンツをスキャンしません。信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。

5. 信頼するコンテンツを含む URL / Web サイトのリストを作成します。

   Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。

   また、信頼する URL のリストを XML ファイルからインポートすることもできます。

6. 変更内容を保存します。

ウェブ脅威対策で、信頼する URL のトラフィックはスキャンされなくなります。ユーザーは信頼する Web サイトを常に開くことができ、その Web サイトからファイルをダウンロードすることができます。Web サイトにアクセスできない場合は、暗号化された接続のスキャン、ウェブコントロール、およびネットワークポートの監視コンポーネントの設定を確認してください。Kaspersky Endpoint Security が、信頼する Web サイトからダウンロードしたファイルを悪意のあるファイルとして検知する場合は、このファイルを除外リストに追加することができます。

また、暗号化された接続の全般的な除外リストを作成することもできます。この場合 Kaspersky Endpoint Security は、ウェブ脅威対策、メール脅威対策、ウェブコントロールが動作している間は信頼する URL の HTTPS トラフィックはスキャンしません。

信頼する URL のリストのエクスポート / インポート

信頼する URL のリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の Web アドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、信頼する URL のリストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で信頼する URL のリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**脅威対策**］→［**ウェブ脅威対策**］の順に選択します。

4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。

5. 表示されたウィンドウで、**信頼する Web アドレス**タブを選択します。

6. 信頼する URL のリストをエクスポートするには：

   a. 編集対象の信頼する URL を選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

      信頼する URL が何も選択されていない場合、すべての URL がエクスポートされます。

   b. ［**エクスポート**］リンクをクリックします。

   c. 表示されたウィンドウで、信頼する URL のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

      Kaspersky Endpoint Security は、信頼する URL のリスト全体を XML ファイルにエクスポートします。

7. 信頼する URL のリストをインポートするには：

   a. ［**インポート**］リンクをクリックします。

      表示されたウィンドウで、信頼するアドレスのリストをインポートする XML ファイルを選択します。

   b. ファイルを開きます。

      コンピューターに信頼するアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで信頼する URL のリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ウェブ脅威対策**］に移動します。

5. ［**ルールリスト**］ブロックで除外リストをエクスポートするには：

   a. 編集対象の信頼する URL を選択します。

   b. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーに信頼する Web アドレスのリストを JSON ファイルでエクスポートします。

6. ［**ルールリスト**］ブロックで除外リストをインポートするには：

   a. → ［**インポート**］を選択します。

      表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

b. ファイルを開きます。

コンピューターに信頼するアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

メール脅威対策

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

メール脅威対策は、受信メッセージと送信メッセージの両方をスキャンすることができます。製品は、以下のメールクライアントの POP3、SMTP、IMAP、NNTP をサポートしています。

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird、MyOffice Mail、R7-Office Organizer の各メールクライアントでトラフィックをスキャンするには、証明書ストアにカスペルスキーの証明書を追加し、独自の証明書ストアを選択する必要があります。

メール脅威対策は、他のプロトコルやメールクライアントをサポートしていません。

メール脅威対策は、メッセージに*プロトコルレベル*でアクセスできるとは限りません（たとえば、Microsoft Exchange ソリューションを使用する場合）。このため、メール脅威対策には、Microsoft Office Outlook 用の機能拡張が含まれています。この機能拡張により、*メールクライアントレベル*でメッセージをスキャンすることができます。メール脅威対策の機能拡張は Outlook 2010、2013、2016、2019 および 2021 の操作をサポートします。

メールクライアントがブラウザーで開いている場合、メール脅威対策はメッセージをスキャンしません。

添付ファイルに悪意のあるファイルが検知されると、Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed]* <*メッセージの元の件名*>」のように変更します。

メール脅威対策の有効化と無効化

既定では、メール脅威対策は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。メール脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます：**高**、**推奨**、**低**。カスペルスキーのエキスパートが推奨する設定グループは、［**推奨**］のメールセキュリティレベルです（下の表を参照）。事前インストールされたメールセキュリティレベルから選択するか、セキュリティレベルをカスタマイズすることもできます。セキュリティレベルの設定を変更した場合、いつでも推奨の設定に戻すことができます。

Mozilla Thunderbird メールクライアントを使用する場合、フィルターを使用してメールを［受信トレイ］フォルダーから移動すると、メール脅威対策は IMAP プロトコルで送信されるメールのウイルスなどの脅威をスキャンしません。

管理コンソール（MMC）でメール脅威対策を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**メール脅威対策**］の順に選択します。
4. ［**メール脅威対策**］を使用して機能を有効または無効にします。
5. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。
   - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：
     - **高**：このメールセキュリティレベルを選択すると、メール脅威対策は最も厳格にメールをスキャンします。メール脅威対策は送受信されたメールメッセージをスキャンし、徹底的なヒューリスティック分析を実行します。リスクの高い環境で作業している場合には［高］メールセキュリティレベルが推奨されます。このような環境の例としては、一元化されたメールアンチウイルスで守られていない家庭用ネットワークからのフリーメールサービスへの接続などがあります。
     - **推奨**：本製品のパフォーマンスとメールのセキュリティの間で最適なバランスが取れたメールセキュリティレベル。メール脅威対策は送受信メールをスキャンし、中レベルのヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、このメールセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。
     - **低**：このメールセキュリティレベルを選択すると、メール脅威対策は受信メールのみをスキャンし、簡易ヒューリスティック分析を実行します。メールに添付されている圧縮ファイルはスキャンしません。このメールセキュリティレベルでは、オペレーティングシステムのリソースの使用を最小限に抑えながら、メールのスキャン速度が最大化します。「低」メールセキュリティレベルは、十分に保護された環境で作業している場合に推奨されます。このような環境の例としては、一元化されたメールセキュリティが適用された企業 LAN などがあります。
   - カスタムのセキュリティレベルを設定する場合は、［**設定**］をクリックして、機能の設定を定義します。

     ［**既定**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

6. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

   - **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

   - **ブロック**：感染したオブジェクトが受信メッセージで検知された場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでメール脅威対策を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**メール脅威対策**］に移動します。

5. ［**メール脅威対策は有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

   - **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

   - **ブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

7. 必要に応じて、メール脅威対策の詳細設定を編集します。

8. 変更内容を保存します。

製品インターフェイスでメール脅威対策を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**メール脅威対策**］を選択します。

3. ［**メール脅威対策**］トグルスイッチを使用して機能を有効または無効にします。

4. この機能を有効にした場合は［**セキュリティレベル**］ブロックで次の操作を実行してください。

   - 事前に設定されているセキュリティレベルのいずれかを適用する場合は、スライダーを使って選択します：

     - **高**：このメールセキュリティレベルを選択すると、メール脅威対策は最も厳格にメールをスキャンします。メール脅威対策は送受信されたメールメッセージをスキャンし、徹底的なヒューリスティック分析を実行します。リスクの高い環境で作業している場合には［高］メールセキュリティレベルが推奨されます。このような環境の例としては、一元化されたメールアンチウイルスで守られていない家庭用ネットワークからのフリーメールサービスへの接続などがあります。

     - **推奨**：本製品のパフォーマンスとメールのセキュリティの間で最適なバランスが取れたメールセキュリティレベル。メール脅威対策は送受信メールをスキャンし、中レベルのヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、このメールセキュリティレベルを推奨しています。推奨されるセキュリティレベルの設定値は次の表を参照してください。

     - **低**：このメールセキュリティレベルを選択すると、メール脅威対策は受信メールのみをスキャンし、簡易ヒューリスティック分析を実行します。メールに添付されている圧縮ファイルはスキャンしません。このメールセキュリティレベルでは、オペレーティングシステムのリソースの使用を最小限に抑えながら、メールのスキャン速度が最大化します。「低」メールセキュリティレベルは、十分に保護された環境で作業している場合に推奨されます。このような環境の例としては、一元化されたメールセキュリティが適用された企業 LAN などがあります。

- カスタムのセキュリティレベルを設定する場合は、［**詳細設定**］をクリックして、機能の設定を定義します。

  ［**推奨のセキュリティレベルに戻す**］をクリックすると、事前設定されたセキュリティレベルの値を復元できます。

5. ［**脅威の検知時の処理**］ブロックで、悪意のあるオブジェクトに対して Kaspersky Endpoint Security が実行する処理を選択します。

   - **駆除する。駆除できない場合は削除する**：感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

   - **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

   - **ブロック**：感染したオブジェクトが受信メッセージで検知された場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。

6. 変更内容を保存します。

カスペルスキーが推奨するメール脅威対策の設定値（推奨されるセキュリティレベル）

パラメータ	値	説明
保護範囲	**送受信メッセージ**	*保護範囲* には、機能の実行中にチェックするオブジェクトが含まれます： 送受信メッセージまたは受信メッセージ。 お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。
Microsoft Outlookアドインに接続	**オン**	このチェックボックスをオンにすると、POP3、SMTP、NNTP、IMAP プロトコルで送信されるメールのスキャンは、Microsoft Outlook に組み込まれた拡張機能側で有効になります。 メールのスキャンに Microsoft Outlook 用機能拡張を使用している場合は、Cached Exchange Modeを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、マイクロソフトサポート技術情報を参照してください。
添付のアーカイブのスキャン	**オン**	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
添付のMicrosoft Office形式のファイルをスキャン	**オン**	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
添付ファイル	**選択した種別の添付ファイルの名前を変更する**	このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。

パラメータ	値	説明
ヒューリスティック分析	**中**	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**	感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

感染したメールに対する処理の変更

既定では、メール脅威対策は、検知した感染ファイルすべての駆除を自動的に試みます。駆除に失敗した場合は、感染したメールを削除します。

感染したメールに対する処理を変更するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**メール脅威対策**］を選択します。
3. ［**脅威の検知時の処理**］ブロックで、Kaspersky Endpoint Security が感染したメールを検知したときに実行する処理を選択します。
   - **駆除する。駆除できない場合は削除する**：感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。
   - **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。
   - **ブロック**：感染したオブジェクトが受信メッセージで検知された場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。
4. 変更内容を保存します。

メール脅威対策の保護範囲の設定

*保護範囲*とは、あるコンポーネントが有効な場合にスキャンされるオブジェクトを意味します。各コンポーネントの保護範囲には、それぞれ異なる特性があります。メール脅威対策の保護範囲には、本コンポーネントをメールクライアントに拡張する設定、および本機能でトラフィックをスキャンするメールメッセージの種類とメールプロトコルが含まれます。既定では、Kaspersky Endpoint Security は送受信メールと POP3、SMTP、NNTP、IMAP プロトコル経由のトラフィックをスキャンし、Microsoft Office Outlook メールクライアントに統合されます。

メール脅威対策の保護範囲を設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**メール脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**保護範囲**］ブロックで、スキャンするメッセージを選択します。
   - **送受信メッセージ**
   - **受信メッセージ**

   お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。

   受信メッセージのみのスキャンを選択した場合は、メールで拡散するメールワームがコンピューター上に存在する可能性があるため、すべての送信メールを一度スキャンしてください。これにより、感染したメッセージが監視されずにコンピューターから大量送信されるという問題を避けることができます。
5. ［**接続とプラグイン**］ブロックで、次を実行します：
   - POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメッセージがコンピューターで受信される前にスキャンする場合は、［**POP3、SMTP、NNTP、IMAP トラフィックをスキャンする**］をオンにします。

     POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメッセージがコンピューターで受信される前にスキャンしない場合は、［**POP3、SMTP、NNTP、IMAP トラフィックをスキャンする**］をオフにします。この場合、［**Microsoft Outlook アドインに接続**］がオンになっていれば、メッセージはコンピューターが受信した後 Microsoft Office Outlook に組み込まれたメール脅威対策機能拡張によってスキャンされます。

     ［**POP3、SMTP、NNTP、IMAP トラフィックをスキャンする**］がオフになっていると、Microsoft Office Outlook 以外のメールクライアントを使用している場合にメール脅威対策は POP3、SMTP、NNTP、IMAP プロトコル経由で送信されたメッセージをスキャンしません。

- Microsoft Office Outlook からメールアンチウイルスを設定できるようにし、POP3、SMTP、NNTP、IMAP、MAPI プロトコル経由で送信されたメールをコンピューターで受信した後 Microsoft Office Outlook に組み込まれた機能拡張でスキャンする場合は、［**Microsoft Outlookアドインに接続**］をオンにします。

  Microsoft Office Outlook からメールアンチウイルス設定へのアクセスをブロックし、POP3、SMTP、NNTP、IMAP、MAPI プロトコル経由で送信されたメールをコンピューターで受信した後 Microsoft Office Outlook に組み込まれたプラグインでスキャンしない場合は、［**Microsoft Outlookアドインに接続**］をオフにします。

  メール脅威対策の機能拡張は、Kaspersky Endpoint Security のインストール中に Microsoft Office Outlook メールクライアントに組み込まれます。

6. 変更内容を保存します。

メールに添付されている複合ファイルのスキャン

メッセージの添付ファイルのスキャンを有効化または無効化することができます。また、スキャン対象となる添付ファイルの最大サイズとスキャンの最長時間を制限することもできます。

メールに添付されている複合ファイルのスキャンを設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**メール脅威対策**］を選択します。
3. ［**詳細設定**］をクリックします。
4. ［**複合ファイル**］ブロックで、スキャンを設定します：
   - **添付のMicrosoft Office形式のファイルをスキャン**：Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
   - **添付のアーカイブのスキャン**：ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。

     スキャン中にメッセージ本文に圧縮ファイルのパスワードを検出した場合は、このパスワードを使用して圧縮ファイルの内容に対して悪意のあるアプリケーションのスキャンを実行します。この場合、パスワードは保存されません。圧縮ファイルはスキャン中に解凍されます。圧縮ファイルの解凍中にアプリケーションでエラーが発生した場合、次のパスに保存されたファイルを手動で削除できます：%systemroot%\temp。このファイルには接頭辞 PR が付いています。

- **次のサイズより大きいアーカイブをスキャンしない：<N>MB（1から9999まで）**：このチェックボックスをオンにすると、メール脅威対策が指定したサイズを超える、メールメッセージに添付されたアーカイブをスキャンしません。このチェックボックスをオフにすると、添付オブジェクトのサイズに関係なく、メール脅威対策がメール添付のアーカイブをスキャンします。

- **アーカイブのチェックを次の時間制限する：<N>秒（1から9999まで）**：このチェックボックスを選択すると、メールメッセージに添付されたアーカイブのスキャンに割り当てられる時間が指定の時間に制限されます。

5. 変更内容を保存します。

メール添付ファイルのフィルター

添付ファイルのフィルター機能は、送信されるメールには適用されません。

悪意のあるアプリケーションは、メールの添付ファイルという形式で配信されることがあります。メールの添付ファイル種別によるフィルタリングを設定し、特定の種類のファイルを自動的に名前変更したり削除したりできます。特定の種類の添付ファイルの名前を変更することにより、悪意のあるアプリケーションの自動実行を防ぐことができます。

添付ファイルのフィルター処理を設定するには：

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**メール脅威対策**］を選択します。

3. ［**詳細設定**］をクリックします。

4. ［**添付ファイル**］ブロックで、次のいずれかを実行します：

   - **フィルタリングをオフにする**：このオプションをオンにした場合、メール脅威対策は、メールに添付されているファイルをフィルター処理しません。

   - **選択した種別の添付ファイルの名前を変更する**：このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。

   - **選択した種別の添付ファイルを削除する**：このオプションをオンにした場合、メール脅威対策は特定の種類の添付ファイルをメールから削除します。

5. 前の手順で［**選択した種別の添付ファイルの名前を変更する**］または［**選択した種別の添付ファイルを削除する**］をオンにした場合、必要なファイル種別の横にあるチェックボックスをオンにします。

6. 変更内容を保存します。

添付ファイルのフィルターの拡張子のエクスポートおよびインポート

添付ファイルのフィルターの拡張子を XML ファイルにエクスポートすることができます。また、エクスポートまたはインポート機能を使用して、拡張子のバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で添付ファイルのフィルターの拡張子のリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**メール脅威対策**］に移動します。
5. ［**添付ファイルのフィルター**］ブロックで拡張子のリストをエクスポートするには：
   a. エクスポートする拡張子を選択します。
   b. ［**エクスポート**］リンクをクリックします。
   c. 表示されたウィンドウで、拡張子のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。
      Kaspersky Endpoint Security は、拡張子のリスト全体を XML ファイルにエクスポートします。
6. ［**添付ファイルのフィルター**］ブロックで拡張子のリストをインスポートするには：
   a. ［**インポート**］リンクをクリックします。
   b. 表示されたウィンドウで、拡張子のリストをインポートする XML ファイルを選択します。
   c. ファイルを開きます。
      コンピューターに拡張子のリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
7. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**メール脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。

5. 表示されたウィンドウで、**添付ファイルのフィルター**タブを選択します。

6. 拡張子のリストをエクスポートするには：

   a. エクスポートする拡張子を選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

   b. ［**エクスポート**］リンクをクリックします。

   c. 表示されたウィンドウで、拡張子のリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

   Kaspersky Endpoint Security は、拡張子のリスト全体を XML ファイルにエクスポートします。

7. 拡張子のリストをインスポートするには：

   a. ［**インポート**］リンクをクリックします。

   b. 表示されたウィンドウで、拡張子のリストをインポートする XML ファイルを選択します。

   c. ファイルを開きます。

   コンピューターに拡張子のリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

Microsoft Office Outlook におけるメールのスキャン

Kaspersky Endpoint Security のインストール中に、メール脅威対策の機能拡張が Microsoft Office Outlook（以降、「Outlook」）に組み込まれます。この機能拡張により、プロトコルレベルではなく、メールクライアントのレベルでメッセージをスキャンすることができます。この機能拡張では、メッセージに加えて、Microsoft Exchange のリポジトリから MAPI インターフェイスを通じて受信したオブジェクト（たとえば、カレンダー内のオブジェクト）をスキャンすることができます。このスキャンは、メールクライアントで行われます。

この機能拡張を使用して、Outlook 内からメール脅威対策コンポーネント設定を開いたり、メールメッセージについてウイルスなどの脅威をスキャンするタイミングを指定したりすることができます。

メール脅威対策の機能拡張は Outlook 2010、2013、2016、2019 および 2021 の操作をサポートします。

Outlook では、受信メッセージはまずメール脅威対策によってスキャンされ（Kaspersky Endpoint Security のインターフェイスで［POP3、SMTP、NNTP、IMAP トラフィックをスキャンする］がオンになっている場合）、次にメール脅威対策の Outlook 用機能拡張によってスキャンされます。メール脅威対策がメッセージ内で悪意のあるオブジェクトを検知すると、通知が表示されます。

Kaspersky Endpoint Security のインターフェイスで［Microsoft Outlook アドインに接続］がオンになっている場合、メール脅威対策の設定を Outlook で直接指定できます（以下の図を参照）。



Outlook でのメール脅威対策の設定

送信メッセージは、まずメール脅威対策の Outlook 用機能拡張によってスキャンされ、次にメール脅威対策によってスキャンされます。

メールのスキャンにメール脅威対策の Outlook 用機能拡張を使用している場合は、Exchange キャッシュモードを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、マイクロソフトサポート技術情報を参照してください。

メール脅威対策の Outlook 用機能拡張の操作モードを設定するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**メール脅威対策**］の順に選択します。
4. ［**セキュリティレベル**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、［**接続**］ブロックの［**設定**］をクリックします。
6. ［**メール保護**］ウィンドウで、次のいずれかの手順を実行します：
   - 受信メッセージがメールボックスに届いたときにメッセージをスキャンする場合は、［**メール受信時にスキャンする**］を選択します。
   - 受信したメッセージをユーザーが開いたときにメッセージをスキャンする場合は、［**メール閲覧時にスキャンする**］を選択します。
   - 送信時にメッセージをスキャンする場合は、［**メール送信時にスキャンする**］を選択します。
7. 変更内容を保存します。

Thunderbird、MyOffice、R7-Office におけるメールのスキャン

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。Mozilla Thunderbird、MyOffice Mail、および R7-Office Organizer メールクライアントの場合、本製品は、*プロトコルレベル*（POP3、SMTP、IMAP、NNTP）でのみメッセージへのアクセス権を取得します。

Mozilla Thunderbird、MyOffice Mail、R7-Office Organizer の各メールクライアントでトラフィックをスキャンするには、証明書ストアにカスペルスキーの証明書を追加し、独自の証明書ストアを選択する必要があります。

メールクライアントがブラウザーで開いている場合、メール脅威対策はメッセージをスキャンしません。

リアルタイムメール脅威対策

メール脅威対策は、受信メッセージと送信メッセージの両方をスキャンすることができます。既定では、メール脅威対策は、検知した感染ファイルすべての駆除を自動的に試みます。駆除に失敗した場合は、感染したメールを削除します。添付ファイルに悪意のあるファイルが検知されると、Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

Mozilla Thunderbird メールクライアントを使用する場合、フィルターを使用してメールを［受信トレイ］フォルダーから移動すると、メール脅威対策は IMAP プロトコルで送信されるメールのウイルスなどの脅威をスキャンしません。

メールデータベースのマルウェアのスキャン

マルウェアのスキャンタスクは、メール形式のファイルのスキャンを許可します。これらのメールクライアントのファイルで悪意のあるオブジェクトが検知されると、Kaspersky Endpoint Security は検知したオブジェクトに関する情報のアクティブな脅威のリストへの追加のみを行います。本製品は、タスク設定に関係なく、メールデータベース内の感染したファイルを駆除することも削除することもありません。

アクティブな脅威の排除

メール脅威対策はプロトコルレベルでコンピューターの感染を防ぎますが、Kaspersky Endpoint Security がインストールされる前にコンピューターが感染していた場合、メールデータベース内の脅威しか検知されない場合があります。メール脅威対策には、Microsoft Office Outlook に関して、メッセージを各部分（ヘッダー、本文、添付ファイル）に明確に分解できるコンポーネントは含まれていません。したがって、本製品は検知したオブジェクトを削除することも駆除することもできません。Kaspersky Endpoint Security は、検知したオブジェクトに関する情報をアクティブな脅威のリストに追加します。

アクティブな脅威を排除するには：

1. メールクライアントのインターフェイスで、検知したオブジェクトを含むメッセージを手動で探して削除します。

   本製品は、検知したオブジェクトに関する情報をアクティブな脅威のリストに表示されます。

   検知したオブジェクトカードの例：

	HEUR:Trojan.PDF.Phish.gen オブジェクト：`C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. データベースの圧縮操作を実行します。

   ユーザーインターフェイスでメッセージが削除されると、メールクライアントは削除マークの追加のみを行います。メールクライアントは、データベースの圧縮後にのみメッセージを実際に削除します。データベースの圧縮について詳しくは、メールクライアントのヘルプを参照してください（例：Mozilla Thunderbird）。

3. マルウェアのスキャンタスクを再度実行し、脅威が存在しなくなったことを確認します。

ネットワーク脅威対策

*ネットワーク脅威対策*コンポーネント（侵入検知システム、IDS とも呼ばれます）は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視します。本製品は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、定義データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、定義データベースと製品機能のアップデート時にアップデートされます。

ネットワーク脅威対策の有効化と無効化

既定では、ネットワーク脅威対策は有効になっており、最適モードで実行されています。Kaspersky Endpoint Security は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視し、攻撃をブロックします。

管理コンソール（MMC）でネットワーク脅威対策を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］の順に選択します。
4. ［**ネットワーク脅威対策**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでネットワーク脅威対策を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**ネットワーク脅威対策**］に移動します。
5. ［**ネットワーク脅威対策は有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでネットワーク脅威対策を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］を選択します。



ネットワーク脅威対策の設定

3. ［**ネットワーク脅威対策**］トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

攻撃元コンピューターのブロック

ネットワーク脅威対策が有効になっている場合、Kaspersky Endpoint Security は自動的にネットワーク攻撃をブロックします。さらに、本製品は攻撃元コンピューターをブロックし、一定の時間ネットワークパケットの送信を制限することができます。既定では、Kaspersky Endpoint Security はコンピューターを 1 時間ブロックします。

管理コンソール（MMC）で攻撃元コンピューターをブロックする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］の順に選択します。
4. ［**ネットワーク脅威対策の設定**］で、［**攻撃元の端末をブロックする時間**］をオンにします。

   このオプションを有効にすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は 1 分です。最大値は 999 分です。
5. ［**攻撃元の端末をブロックする時間**］の右側のフィールドで、別に攻撃元のコンピューターをブロックする時間を設定します。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールで攻撃元コンピューターをブロックする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**ネットワーク脅威対策**］に移動します。
5. ［**脅威の検知時の処理**］ブロックで、［**攻撃をブロックし、攻撃元の端末をブロックする時間（分）**］をオンにします。

   このオプションを有効にすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は 1 分です。最大値は 999 分です。
6. 攻撃元コンピューターのブロック期間を変更します。
7. 変更内容を保存します。

製品のユーザーインターフェイスで攻撃元コンピューターをブロックする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］を選択します。



ネットワーク脅威対策の設定

3. ［**攻撃元の端末をブロックする時間N分間**］をオンにします。

   このオプションを有効にすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は1分です。最大値は999分です。

4. ［**攻撃元の端末をブロックする時間**］の下のフィールドで、別に攻撃元のコンピューターをブロックする時間を設定します。
5. 変更内容を保存します。

Kaspersky Endpoint Security は、ユーザーのコンピューターへのネットワーク攻撃の開始を検知すると、攻撃しているコンピューターとのすべてのネットワーク接続をブロックします。Kaspersky Endpoint Security は［*ネットワーク攻撃が検知されました*］イベントを作成します。イベントには、攻撃元コンピューターの情報（IP アドレスと MAC アドレス）が含まれています。

攻撃元コンピューターの MAC アドレスは、本製品のユーザーインターフェイスまたは Kaspersky Security Center コンソールのバージョン 15.1 以降でのみ確認できます。



ネットワーク攻撃の検知についての通知

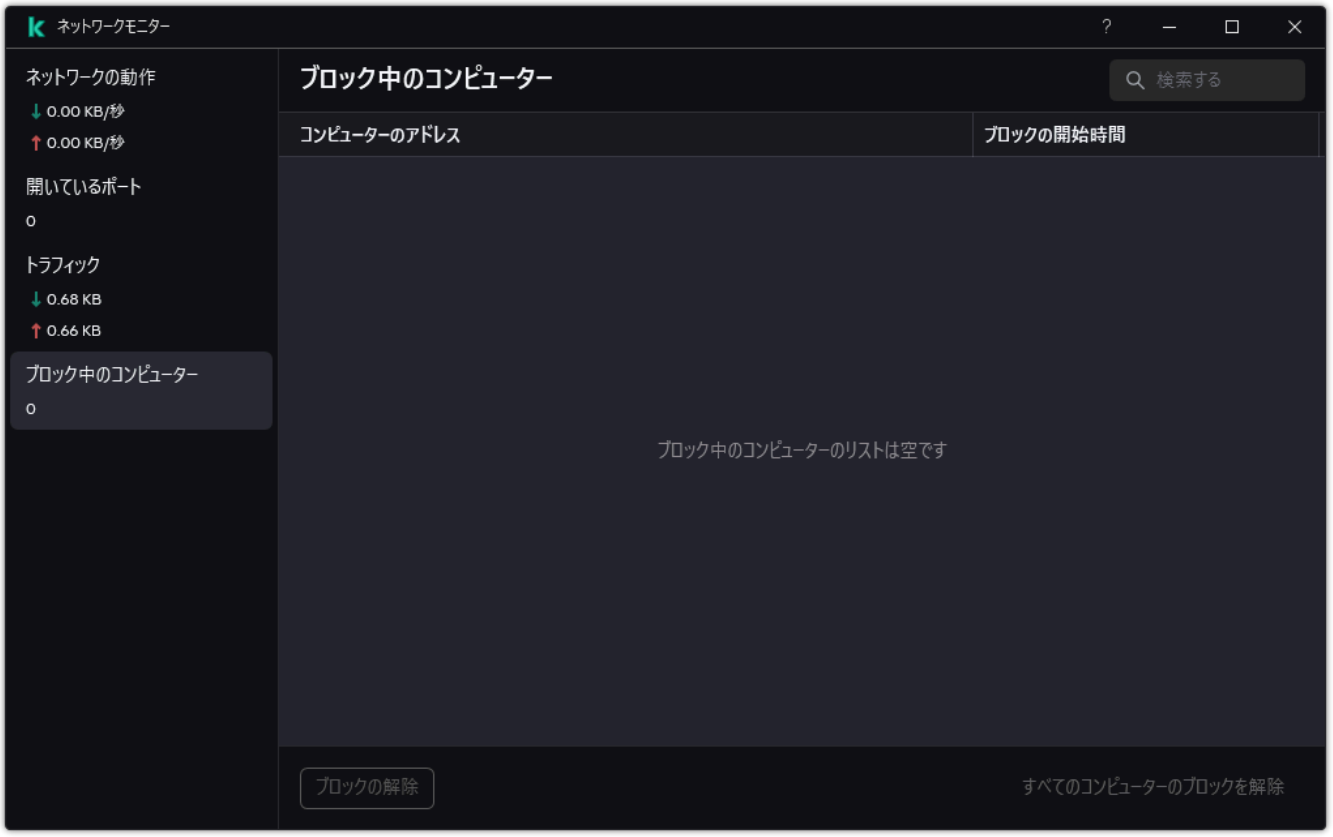
Kaspersky Endpoint Security は、指定された時間が経過すると、コンピューターのロックを解除します。Kaspersky Security Center コンソールでは、レポート内の［*ネットワーク攻撃が検知されました*］イベント以外にブロック中のコンピューターを監視するツールは提供されていません。製品のインターフェイスで、ブロック中のコンピューターのリストを表示することのみ可能です。この機能は*ネットワークモニター*ツールによって提供されます。ネットワークモニターツールを使用してコンピューターのブロックを解除することもできます。

コンピューターのブロックを解除するには：

1. 製品のメインウィンドウの［**監視**］で、［**ネットワークモニター**］をクリックします。
2. ［**ブロック中のコンピューター**］タブを選択します。
   ブロック中のコンピューターのリストが表示されます（下図を参照）。

Kaspersky Endpoint Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。

3. ブロック解除するコンピューターを選択して［**ブロックの解除**］をクリックします。



ブロック中のコンピューター

ブロックから除外するアドレスの設定

Kaspersky Endpoint Security はネットワーク攻撃を認識し、パケット数の大きな保護されていないネットワーク接続（監視カメラなど）をブロックすることができます。信頼するデバイスについては、除外リストにデバイスの IP アドレスを追加できます。コミュニケーションに使用されるプロトコルとポートを選択して、特定のネットワーク活動を許可することもできます。

プロトコルとポートを選択して除外する機能は Kaspersky Endpoint Security 12.2 で追加されました。本製品と管理プラグインがバージョン 12.2 以降にアップデートされていることをご確認ください。以前のバージョンの本製品と管理プラグインを使用している場合、Kaspersky Endpoint Security は IP アドレスでのみネットワーク活動を許可できます。

管理コンソール（MMC）でブロックから除外するアドレスを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］の順に選択します。
4. ［**ネットワーク脅威対策の設定**］ブロックの［**除外リスト**］をクリックします。
5. 表示されたウィンドウで、［**追加**］をクリックします。

6. ネットワーク攻撃防御の対象にしないコンピューターの IP アドレスを入力します。
   必要に応じて、データを転送するプロトコルとポートを選択します。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでブロックから除外するアドレスを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ネットワーク脅威対策**］に移動します。

5. ウィンドウの上部で、［**信頼する IP アドレス**］リンクをクリックします。

6. 表示されたウィンドウで、［**追加**］をクリックします。

7. ネットワーク攻撃防御の対象にしないコンピューターの IP アドレスを入力します。
   必要に応じて、データを転送するプロトコルとポートを選択します。

8. 変更内容を保存します。

製品のユーザーインターフェイスでブロックから除外するアドレスを設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］を選択します。



ネットワーク脅威対策の設定

3. ［**除外リストの管理**］リンクをクリックします。
4. 表示されたウィンドウで、［**追加**］をクリックします。
5. ネットワーク攻撃防御の対象にしないコンピューターの IP アドレスを入力します。
   必要に応じて、データを転送するプロトコルとポートを選択します。
6. 変更内容を保存します。

ブロックの除外対象のリストのエクスポート / インポート

除外リストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で除外リストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］の順に選択します。

4. ［**ネットワーク脅威対策の設定**］ブロックの［**除外リスト**］をクリックします。

5. ルールのリストをエクスポートするには：

   a. エクスポートする除外リストを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

   除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。

   b. → ［**エクスポート**］を選択します。

   c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

   Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。

6. 除外リストをインポートするには：

   a. → ［**インポート**］を選択します。

   b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

   c. ファイルを開きます。

   コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで除外リストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ネットワーク脅威対策**］に移動します。

5. ウィンドウの上部で、［**信頼する IP アドレス**］リンクをクリックします。

   除外リストが表示されます。

6. ルールのリストをエクスポートするには：

   a. エクスポートする除外リストを選択します。

   b. → ［**エクスポート**］を選択します。

   Kaspersky Endpoint Security は既定のダウンロードフォルダーに除外リストを JSON ファイルでエクスポートします。

7. 除外リストをインポートするには：

   a. → ［**インポート**］を選択します。

      表示されたウィンドウで、除外リストをインポートする JSON ファイルを選択します。

   b. ファイルを開きます。

      コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

種別ごとのネットワーク脅威対策の設定

Kaspersky Endpoint Security を使用して、次の種別のネットワーク攻撃に対する保護を管理できます。

- *ネットワークフラッディング*とは、Web サーバーなど、企業のネットワークリソースに対する攻撃を意味します。これは、大量のリクエストを送信し、ネットワークリソースの帯域幅をオーバーロードさせる攻撃です。攻撃されると、ユーザーは企業のネットワークリソースにアクセスできなくなります。

- *ポートのスキャン*とは、コンピューターの UDP ポート、TCP ポート、ネットワークサービスをスキャンする攻撃を意味します。これにより、攻撃者がコンピューターの脆弱性を把握して、より悪質な攻撃を仕掛けることができるようになります。また、コンピューターのオペレーティングシステムを識別し、そのオペレーティングシステムに適したネットワーク攻撃を行うためにポートがスキャンされることもあります。

- *MAC スプーフィング攻撃*では、ネットワークデバイス（ネットワークカード）の MAC アドレスを変更します。その結果、攻撃者はデバイスに送信されたデータを別のデバイスにリダイレクトし、このデータにアクセスすることができます。Kaspersky Endpoint Security で MAC スプーフィング攻撃をブロックし、攻撃に関する通知を管理者に送信できます。

一部の許可されるアプリケーションがこのような攻撃と似た動作を行う場合は、これらの検知機能を無効にすることができます。これにより誤検知を減らすことができます。

既定では、Kaspersky Endpoint Security はネットワークフラッディングおよびポートのスキャン、MAC スプーフィング攻撃を監視しません。

Microsoft Hyper-V インフラストラクチャ内の仮想マシンで MAC スプーフィング対策を有効にすることは推奨しません。Microsoft Hyper-V プラットフォームの特性により、誤検知の結果、Kaspersky Industrial CyberSecurity for Nodes がハイパーバイザーをブロックする可能性があります。

管理コンソール（MMC）で種別ごとのネットワーク脅威対策を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］の順に選択します。

4. これらの攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］を使用します。

   この機能を有効にすると、Kaspersky Endpoint Security は、ポートスキャンとネットワークフラッディングのためにネットワークトラフィックを監視します。このような動作が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。アプリケーションは、リクエストを行っているコンピューターに関する情報を提供します。この情報はタイムリーな応答のために必要です。しかし、Kaspersky Endpoint Security は、このようなトラフィックが企業ネットワーク上で通常発生する可能性があるため、リクエストを行っているコンピューターをブロックしません。

5. ［**MAC スプーフィング対策モード**］ブロックで、以下のオプションのいずれかを選択します：

   - **MAC スプーフィングを監視しない**
   - **通知する**
   - **ブロックする**

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで種別ごとのネットワーク脅威対策を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ネットワーク脅威対策**］に移動します。

5. これらの攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］を使用します。

   この機能を有効にすると、Kaspersky Endpoint Security は、ポートスキャンとネットワークフラッディングのためにネットワークトラフィックを監視します。このような動作が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。アプリケーションは、リクエストを行っているコンピューターに関する情報を提供します。この情報はタイムリーな応答のために必要です。しかし、Kaspersky Endpoint Security は、このようなトラフィックが企業ネットワーク上で通常発生する可能性があるため、リクエストを行っているコンピューターをブロックしません。

6. これらの攻撃の検知を有効にするには、［**ネットワーク脅威対策は有効です**］を使用します。

7. 変更内容を保存します。

製品インターフェイスで種別ごとのネットワーク脅威対策を設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ネットワーク脅威対策**］を選択します。



ネットワーク脅威対策の設定

3. これらの攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］トグルスイッチを使用します。

   この機能を有効にすると、Kaspersky Endpoint Security は、ポートスキャンとネットワークフラッディングのためにネットワークトラフィックを監視します。このような動作が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。アプリケーションは、リクエストを行っているコンピューターに関する情報を提供します。この情報はタイムリーな応答のために必要です。しかし、Kaspersky Endpoint Security は、このようなトラフィックが企業ネットワーク上で通常発生する可能性があるため、リクエストを行っているコンピューターをブロックしません。

4. これらの攻撃の検知を有効または無効にするには、［**MAC スプーフィング対策**］トグルスイッチを使用します。
5. ［**MAC スプーフィング攻撃の検知時の処理**］ブロックで、以下のオプションのいずれかを選択します：
   - **通知する**
   - **ブロック**
6. 変更内容を保存します。

ファイアウォール

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

ネットワークエージェントは Kaspersky Security Center との連携に使用されます。ファイアウォールは本製品とネットワークエージェントが正常に動作するために、自動でネットワークルールを作成します。その結果、ファイアウォールはコンピューターのいくつかのポートを開きます。どのポートが開かれるかは、ディストリビューションポイントなど、コンピューターの役割により異なります。コンピューターで開かれるポートについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

ネットワークルール

次の情報に基づいてネットワークルールを構成できます：

- *ネットワークパケットルール*：ネットワークパケットルールでは、アプリケーションに関係なく、ネットワークパケットに制限が適用されます。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。Kaspersky Endpoint Security には、カスペルスキーのエキスパートが推奨する権限を持つネットワークパケットルールが事前に定義されています。

- *アプリケーションネットワークルール*：アプリケーションネットワークルールでは、特定のアプリケーションのネットワークアクティビティに制限が適用されます。このルールでは、ネットワークパケットの特徴だけでなく、このネットワークパケットの宛先またはネットワークパケットを発行する特定のアプリケーションも考慮されます。

オペレーティングシステムのリソース、プロセス、および個人データへのアプリケーションの制御されたアクセスは、*アプリケーション権限*を使用することにより、ホスト侵入防止によって提供されます。

アプリケーションの最初の起動時に、ファイアウォールは次の動作を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。

2. Kaspersky Security Network での製品のセキュリティを確認する

   ファイアウォールがより効果的に機能するように、Kaspersky Security Network に参加することを推奨します。

3. *信頼済み*、*弱い制限付き*、*強い制限付き*、*ブロック*のうちいずれかの信頼グループにアプリケーションを配置します。

   信頼グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は ホスト侵入防止の設定に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じて、アプリケーションのネットワーク動作をブロックします。たとえば、*強い制限付き*の信頼グループのアプリケーションは、ネットワーク接続を使用できません。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のネットワークルールをそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

ネットワークルールの優先度

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ネットワーク動作が複数のルールに追加された場合、ファイアウォールは最も優先度の高いルールに従ってネットワーク動作を制限します。

ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。同じ種類のネットワークアクティビティに、ネットワークパケットルールとアプリケーションのネットワークルールの両方が指定されている場合、そのネットワークアクティビティはネットワークパケットルールに従って処理されます。

アプリケーションのネットワークルールは特定の方法で動作します。アプリケーションのネットワークルールには、*パブリックネットワーク*、*プライベートネットワーク*、*信頼するネットワーク*のネットワークステータスに基づいたアクセスルールが含まれます。例えば、*強い制限付き*の信頼グループのアプリケーションは、既定ではすべてのステータスのネットワーク内でネットワークアクティビティが許可されません。個別のアプリケーション（親アプリケーション）にネットワークルールが指定されている場合、他のアプリケーションの子プロセスは、親アプリケーションのネットワークルールに基づいて実行されます。アプリケーションにネットワークルールが指定されていない場合は、子プロセスはアプリケーションの信頼グループのネットワークアクセスルールに基づいて実行されます。

例えば、ブラウザー X 以外のすべてのアプリケーションのすべてのステータスのネットワークアクティビティを禁止したとします。その後ブラウザー X（親アプリケーション）からブラウザー Y（子プロセス）のインストールを開始した場合、ブラウザー Y のインストーラはネットワークにアクセスし、必要なファイルをダウンロードします。インストール後、ブラウザー Y はファイアウォールの設定により、すべてのネットワーク接続を拒否します。子プロセスとしてのブラウザー Y のネットワークアクティビティを禁止するには、ブラウザー Y のインストーラに対してネットワークルールを設定する必要があります。

ネットワーク接続の種別

ファイアウォールを使用すると、ネットワーク接続の種別に応じてネットワーク動作を制御できます。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムからネットワーク接続の種別を受け取ります。オペレーティングシステムでのネットワーク接続の種別は、接続のセットアップ時にユーザーが設定します。Kaspersky Endpoint Security の設定でネットワーク接続の種別を変更できます。ファイアウォールは、オペレーティングシステムではなく Kaspersky Endpoint Security の設定に指定されたネットワーク種別に応じてネットワーク動作を監視します。

利用可能なネットワーク接続の種別は次のとおりです：

- **パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。

  既定では、ファイアウォールは、［*パブリックネットワーク*］種別をインターネットに割り当てます。インターネットの種別は変更できません。

- **プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。

- **信頼するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。

ファイアウォールの有効化または無効化

既定では、ファイアウォールは有効化され、最適なモードで機能します。

管理コンソール（MMC）でファイアウォールを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
4. ［**ファイアウォール**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでファイアウォールを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ファイアウォール**］の順に選択します。

5. ［**ファイアウォールは有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. 変更内容を保存します。

製品インターフェイスでファイアウォールを有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。

3. ［**ファイアウォール**］トグルスイッチを使用して機能を有効または無効にします。

4. 変更内容を保存します。

この結果、ファイアウォールが有効になっていると、Kaspersky Endpoint Security はネットワークの動作をコントロールし、コンピューターへの不正なネットワーク接続や、コンピューター上のアプリケーションの不正なネットワーク活動もブロックします。ネットワーク動作はネットワーク脅威対策機能によってもコントロールされます。ネットワーク脅威対策コンポーネント（侵入検知システム、IDS とも呼ばれます）は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視します。

Kaspersky Endpoint Security は、ファイアウォールの設定にかかわらず、ネットワーク攻撃イベントをレポートに記録します。ファイアウォールがルールを使用してネットワーク接続をブロックしてネットワーク攻撃を防いだ場合でも、ネットワーク脅威対策はネットワーク攻撃イベントを登録します。お客様の組織のコンピューターでのネットワーク攻撃に関する統計情報を生成するために必要な情報となります。

ネットワーク接続種別の変更

既定では、ファイアウォールは、［*パブリックネットワーク*］種別をインターネットに割り当てます。インターネットの種別は変更できません。

ネットワーク接続種別を変更するには：

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。

3. ［**使用可能なネットワーク**］をクリックします。

4. 種別を変更するネットワーク接続を選択します。

5. ［**ネットワーク種別**］列で、ネットワーク接続の種別を選択します。

   - **パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。

   - **プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。

   - **信頼するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。

6. 変更内容を保存します。

ネットワークパケットルールの管理

ネットワークパケットルールの管理では、次の操作を実行できます：

- 新しいネットワークパケットルールを作成する。

  新しいネットワークパケットルールを作成するには、ネットワークパケットとデータストリームに適用する一連の条件と処理を作成します。

- ネットワークパケットルールを有効化または無効化する。

  既定では、ファイアウォールによって作成されるすべてのネットワークパケットルールのステータスが「*有効*」になります。ネットワークパケットルールが有効な場合、ファイアウォールはこのルールを適用します。

  ネットワークパケットルールのリストで選択した任意のネットワークパケットルールを無効にすることができます。ネットワークパケットルールが無効な場合、ファイアウォールはこのルールを一時的に適用しません。

  > 既定では、新しいカスタムネットワークパケットルールは、「*有効*」ステータスでネットワークパケットルールのリストに追加されます。

- 既存のネットワークパケットルールの設定を編集する。

  新しいネットワークパケットルールの作成後、必要時にはいつでもそのルールに戻って設定を編集したり、変更を加えたりすることができます。

- ネットワークパケットルールに適用するファイアウォールの処理を変更する。

  ネットワークパケットルールのリストで、特定のネットワークパケットルールに一致するネットワークの動作の検知時にファイアウォールが実行する処理を編集することができます。

- ネットワークパケットルールの優先度を変更する。

  リストから選択したネットワークパケットルールの優先度を変更することができます。

- ネットワークパケットルールを削除する。

ネットワークパケットルールを削除して、ファイアウォールがネットワークの動作の検知時にこのルールを適用しないようにしたり、ネットワークパケットルールのリストにこのルールが「*無効*」ステータスで表示されないようにしたりすることができます。

ネットワークパケットルールの作成

ファイアウォールは、ネットワークパケットルールに従って、コンピューター上のすべてのネットワーク動作をフィルタリングします。ネットワークパケットルールには、ファイアウォールがコンピューターのネットワーク接続を制御するために適用する条件（方向、プロトコルなど）が含まれます。ネットワークパケットルールでは、ルールに一致する接続に対してファイアウォールが実行する処理（接続の許可またはブロック）も指定されます。

ネットワークパケットルールを作成するための推奨事項

IP アドレスまたは IP アドレスの範囲を指定して、ネットワーク動作をフィルタリングできます。DNS 名を指定することもできますが、IP アドレスと IP アドレス範囲を使用することを推奨します。DNS サーバーの所有者は DNS レコードのパラメータを変更できるため、ネットワークパケット名に DNS 名を使用すると安全でない可能性があります。悪意のある攻撃者は、DNS メッセージを偽装して、ファイアウォールルールを回避することもできます。

ユーザーは、ウェブコントロールルールを使用して DNS 名でネットワーク接続を制御することができます。ファイアウォールルールで DNS 名を指定する必要がある場合：

- 企業の LAN のセキュリティを確保します。
- キャッシュ DNS サーバーと権威 DNS サーバーのセキュリティを確保します。
- DNS レコードの変更に対する保護を有効にします。

ネットワークパケットルールを作成するときには、アプリケーションのネットワークルールに優先するということに留意する必要があります。

ネットワークパケットルールの作成方法

次の方法でネットワークパケットルールを作成できます：

- ネットワークモニターツールを使用する。

  *ネットワークモニター*は、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。ルールを設定する必要がないため便利です。一部のファイアウォールの設定はネットワークモニターのデータから自動的に挿入されます。ネットワークモニターは製品のインターフェイスのみで使用できます。

- ファイアウォールを設定する。

  ファイアウォールの設定を詳細に調整できます。その時点でネットワークの操作がない場合にも、ネットワークの動作に関してルールを作成できます。

製品のインターフェイスでネットワークモニターツールを使用してネットワークパケットルールを作成する方法

1. 製品のメインウィンドウの［**監視**］で、［**ネットワークモニター**］をクリックします。
2. ［**ネットワークの動作**］タブを選択します。
   ［**ネットワークの動作**］タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。
3. ネットワーク接続のコンテキストメニューで、［**ネットワークパケットルールを作成する**］を選択します。
   ネットワークルールのプロパティが開きます。
4. パケットルールに［**有効**］を設定します。
5. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。
6. ネットワークルールを設定します（下記の表を参照）。
   ［**ネットワークルールテンプレート**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。
   ネットワークルール設定は自動で入力されます。
7. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。
8. ［**保存する**］をクリックします。
   新しいネットワークルールがリストに追加されます。
9. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。
10. 変更内容を保存します。

製品のインターフェイスでファイアウォールの設定を使用してネットワークパケットルールを作成する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**パケットルール**］をクリックします。
   ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
4. ［**追加する**］ドロップダウンリストを使用して、リスト内でのルールの場所（リストの上部、リストの下部、または選択されたルールの横）を選択します。
   リスト内でのルールの場所によって、ルールの優先度が決まります。リストの先頭にあるルールが最も優先されます。
5. パケットルールに［**有効**］を設定します。
6. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。
7. ネットワークルールを設定します（下記の表を参照）。
   ［**ネットワークルールテンプレート**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。
   ネットワークルール設定は自動で入力されます。

8. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。

9. ［**保存する**］をクリックします。
   新しいネットワークルールがリストに追加されます。

10. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。

11. 変更内容を保存します。

管理コンソール（MMC）でネットワークパケットルールを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。

4. ［**ファイアウォールの設定**］ブロックの［**設定**］をクリックします。
   ネットワークパケットルールおよびアプリケーションネットワークルールのリストが表示されます。

5. ［**ネットワークパケットルール**］タブを選択します。
   ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。

6. ［**追加**］ドロップダウンリストを使用して、リスト内でのルールの場所（リストの上部、リストの下部、または選択されたルールの横）を選択します。
   リスト内でのルールの場所によって、ルールの優先度が決まります。リストの先頭にあるルールが最も優先されます。

7. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。

8. ネットワークルールを設定します（下記の表を参照）。
   ボタン（）をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。
   ネットワークルール設定は自動で入力されます。

9. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。

10. 新しいネットワークルールを保存します。

11. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。

12. 変更内容を保存します。

ファイアウォールはルールに従ってネットワークパケットを制御します。パケットルールをリストから削除しなくても、ファイアウォールの操作からパケットルールを無効にすることができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

Web コンソールと Cloud コンソールでネットワークパケットルールを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ファイアウォール**］の順に選択します。

5. ［**ネットワークパケットルール**］タブを選択します。
   ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。

6. ［**追加**］をクリックします。
   これにより、新しいネットワークルールのフォームが開きます。

7. ［**ルール名**］フィールドに、ネットワークサービスの名前を手動で入力します。

8. ネットワークルールを設定します（下記の表を参照）。
   ［**ルールのテンプレートを選択してください**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。
   ネットワークルール設定は自動で入力されます。

9. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。

10. ネットワークルールを保存します。
    新しいネットワークルールがリストに追加されます。

11. ［**移動する**］を使用してネットワークルールの優先度を設定します。

12. 変更内容を保存します。

ファイアウォールはルールに従ってネットワークパケットを制御します。パケットルールをリストから削除しなくても、ファイアウォールの操作からパケットルールを無効にすることができます。［**ステータス**］列のトグルスイッチを使用してパケットルールを有効または無効にします。

ネットワークパケットルールの設定

パラメータ	説明
処理	**許可** **ブロック** **アプリケーションルールに準拠**：このオプションを選択すると、ファイアウォールはネットワーク接続にアプリケーションネットワークルールを適用します
プロトコル	選択したプロトコル（TCP、UDP、ICMP、ICMPv6、IGMP および GRE）に対してネットワークの動作を制御します。 ICMP または ICMPv6 プロトコルを選択すると、ICMP パケットの種類とコードを定義できます。 TCP または UDP をプロトコルの種類として選択すると、接続が監視されるローカルコンピューターとリモートコンピューターのポートをカンマ区切りで指定できます。
通信方向	**受信（パケット）**：ファイアウォールはすべての受信ネットワークパケットにネットワークルールを適用します。 **受信**：リモートコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。 **受信 / 送信**：ネットワーク接続を開始したのがユーザーのコンピューターかリモートコンピューターか関係なく、送受信ネットワークパケットにネットワークルールが適用されます。 **送信（パケット）**：ファイアウォールはすべての送信ネットワークパケットにネットワークルールを適用します。 **送信**：ユーザーのコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。
ネットワークアダプター	ネットワークパケットを送信または受信することができるネットワークアダプターです。ネットワークアダプターの設定を行うことで、同じ IP アドレスのネットワークアダプターによって送受信されるネットワークパケットを区別できます。
最大生存時間（TTL）	ネットワークパケットのコントロールをその有効期間（最大生存時間、TTL）によって制限します。

パラメータ	説明
リモートアドレス	ネットワークパケットを送信または受信するリモートコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のリモートネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めることも、IP アドレスの範囲を指定することも、IP アドレスごとに別のリストを作成することも、または許可するネットワーク、ローカルネットワーク、パブリックネットワークなどのサブネットを選択することもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。 ネットワークパケットルールで IP アドレスが特定できない DNS 名を追加した場合、Kaspersky Endpoint Security は警告を表示します。Web コンソールのネットワークパケットルールのリストに、列がエラーの説明とともに追加されます。管理コンソール（MMC）では、エラーの説明は使用できません。このようなパケットルールは色で強調されます。
ローカルアドレス	ネットワークパケットを送信または受信するコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のローカルネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めたり、IP アドレスごとに別のリストを作成したり、IP アドレスの範囲を指定したりすることもできます。 本製品は、リモートアドレスのリストが指定されている場合にのみ、ローカルアドレスを保存します。つまり、［**リモートアドレス**］に対して［**設定したネットワークアドレス**］の値が選択されて、少なくとも1つのアドレスが追加されている場合です。 アプリケーションのローカルアドレスが取得できない場合があります。この場合、このパラメータは無視されます。

ネットワークパケットルールの有効化または無効化

ネットワークパケットルールを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**パケットルール**］をクリックします。
   ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。
4. リストから、目的のネットワークパケットルールを選択します。
5. ［**ステータス**］列のトグルスイッチを使用してルールを有効または無効にします。
6. 変更内容を保存します。

ネットワークパケットルールに対するファイアウォール処理の変更

ネットワークパケットルールに適用するファイアウォールの処理を変更するには、次の手順を実行します：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。

3. ［**パケットルール**］をクリックします。
   ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。

4. ネットワークパケットルールのリストからルールを選択し、［**編集**］をクリックします。

5. ［**処理**］で、この種類のネットワークの動作が検知されたときにファイアウォールによって実行される次のいずれかの処理を選択します：

   - **許可**
   - **ブロック**
   - **アプリケーションルールに準拠**：このオプションを選択すると、ファイアウォールはネットワーク接続にアプリケーションネットワークルールを適用します

6. 変更内容を保存します。

ネットワークパケットルールの優先順位の変更

ネットワークパケットルールの優先順位は、ネットワークパケットルールのリスト内の位置で決定されます。ネットワークパケットルールリストの最上位にあるルールの優先順位が最も高くなります。

手動で作成したネットワークパケットルールは、ネットワークパケットルールリストの末尾に追加され、その優先順位は最も低くなります。

ファイアウォールでは、ネットワークパケットルールはネットワークパケットルールリストの上から順に実行されます。ファイアウォールでは、特定のネットワーク接続に適用される処理済みの各ネットワークパケットルールに従って、そのネットワーク接続の設定で指定されているアドレスおよびポートへのネットワークアクセスが許可またはブロックされます。

ネットワークパケットルールの優先順位を変更するには：

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。

3. ［**パケットルール**］をクリックします。
   ファイアウォールによって設定される既定のネットワークパケットルールのリストが表示されます。

4. リストで、優先順位を変更するネットワークパケットルールを選択します。

5. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。

6. 変更内容を保存します。

ネットワークパケットルールのエクスポートおよびインポート

ネットワークパケットルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のルールをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ネットワークパケットルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）でネットワークパケットルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
4. ［**ファイアウォールの設定**］ブロックの［**設定**］をクリックします。
   ネットワークパケットルールおよびアプリケーションネットワークルールのリストが表示されます。
5. ［**ネットワークパケットルール**］タブを選択します。
6. ネットワークパケットルールのリストをエクスポートするには：
   a. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
      ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
   b. ［**エクスポート**］リンクをクリックします。
   c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。
      Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
7. ネットワークパケットルールのリストをインポートするには：
   a. ［**インポート**］リンクをクリックします。
      表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
   b. ファイルを開きます。
      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
8. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでネットワークパケットルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**ファイアウォール**］の順に選択します。

5. ［**ネットワークパケットルール**］ブロックでルールのリストをエクスポートするには：

   a. エクスポートするルールを選択します。

   b. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

6. ［**ネットワークパケットルール**］ブロックでルールのリストをインスポートするには：

   a. → ［**インポート**］を選択します。

      表示されたウィンドウで、ルールのリストをインポートする JSON ファイルを選択します。

   b. ファイルを開きます。

      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

XML でのネットワークパケットルールの定義

ファイアウォールでは、ネットワークパケットルールを XML 形式でエクスポートできます。これにより、例えば同じ種別の多数のルールをファイルを編集して追加することができます。

XML ファイルには、`Rules` と `Resources` の 2 つの主要なノードが含まれています。`Rules` ノードにはネットワークパケットルールの一覧が表示されます。このノードには既定で設定されているルール（*事前定義済みのルール*）とユーザーによって定義されたルール（*カスタムルール*）があります。

ネットワークパケットルールのマークアップ

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

パラメータ	説明	値
`<key name="0000">`	ルールの優先度。値が小さいほど優先度が高くなります。	整数 優先度の値は 4 桁の数字で成り立っている必要があります。XML ファイル内のノードは「`0000`」で始まる優先度の値の順で並んでいます。
`RuleId`	ルールの ID。	**定義済みのルール** `100` – **TCP 経由の DNS サーバーへの要求** `101` – **UDP 経由の DNS サーバーへの要求** `102` – **メールの送信** `110` – **任意のネットワーク動作**（信頼するネットワーク） `125` – **任意のネットワーク動作**（プライベートネットワーク） `130` – **リモートデスクトップのネットワーク動作** `131` – **ローカルポート経由の TCP 接続** `132` – **ローカルポート経由の UDP 接続** `133` – **TCP ストリームの受信** `134` – **UDP ストリームの受信** `137` – **ICMP「宛先到達不可能」応答の受信** `138` – **ICMP エコー応答の受信パケット** `140` – **ICMP「時間切れ通知」応答の受信** `142` – **ICMP ストリームの受信** `266` – **ICMPv6 エコー要求の受信パケット**
`RuleState`	ルールのステータス。	`0` – 定義済みのルールが無効 `1` – 定義済みのルールが有効 `2` – カスタムルールが無効 `3` – カスタムルールが有効
`RuleTypeId`	ルール種別の ID。	`4` – ネットワークパケットルール
`AppIdEx`	ネットワークパケットルールが属するアプリケーションの ID。	ネットワークパケットルールがどのアプリケーションにも属さない場合は、値は「`0`」になります。
`ResIdEx`	ルール設定のあるリソースのメイン ID。この ID を使用して［`Resources`］ノードでルール設定のブロックを配置できます。	整数
`ResIdEx2`	ネットワーク種別の ID。	`0` – **すべてのアドレス** `50` – **信頼するネットワーク** `51` – **プライベートネットワーク** `52` – **パブリックネットワーク** `<Network Identifier>` – **リストからのアドレス**（アドレスは手動で定義します）
`AccessFlag`	**処理**パラメータの値。	`0` – **許可** `2` – **アプリケーションルールに準拠** `3` – **ブロック** `4` – **許可**および**イベントを記録** `6` – **アプリケーションルールに準拠**および**イベントを記録** `7` – **ブロック**および**イベントを記録**
`</key>`		

［Resources］ノードにはネットワークパケットルールの設定が含まれます。カスタムネットワークパケットルールの設定は <key name="0004"> ブロックに表示されます。

カスタムネットワークパケットルールのマークアップ

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

カスタムネットワークパケットルールの設定

パラメータ	説明	値
<key name="Data">	パラメータブロックの ID。	整数
RemotePorts	**リモートポート**パラメータの値。	リモートポート範囲のリスト。
LocalPorts	**ローカルポート**パラメータの値。	ローカルポート範囲のリスト。

パラメータ	説明	値
`AdapterBindings`	**ネットワークアダプター**パラメータの値。	`IpAddresses` – **IP アドレス**パラメータの値。 `MacAddresses` – **MAC アドレス**パラメータの値。 `AdapterName` – ネットワークアダプターの名前。 `InterfaceType` – **インターフェイス種別**パラメータの値： • `0` – **その他** • `1` – **ループバック** • `2` – **有線 LAN（イーサネット）** • `3` – **無線ネットワーク（Wi-Fi）** • `4` – **トンネル** • `5` – **PPP 接続** • `6` – **PPPoE 接続** • `7` – **VPN 接続** • `8` – **モデム接続**
`unique`	構造の内部 ID。	整数 このパラメータは変更しないことを推奨します。
`Proto`	**プロトコル**パラメータの値。	`0` – 無効 `1` – ICMP `2` – IGMP `6` – TCP `17` – UDP `47` – GRE `58` – ICMPv6
`Direction`	**通信方向**パラメータの値。	`1` – **受信（パケット）** `2` – **送信（パケット）** `3` – **受信 / 送信** `4` – **受信** `5` – **送信**

パラメータ	説明	値
`IcmpType`	**ICMP 種別**パラメータの値。	**ICMP プロトコル** `0` – **エコー応答**（ICMP）または無効 `3` – **宛先到達不能**（ICMP） `4` – **ソースクエンチ（送信元抑制）** `5` – **リダイレクト** `6` – **代替ホストアドレス** `8` – **エコー要求** `9` – **ルーター広告** `10` – **ルーター要請** `11` – **時間切れ** `12` – **パラメータ問題** `13` – **タイムスタンプ** `14` – **タイムスタンプ応答** `15` – **情報要求** `16` – **情報応答** `17` – **アドレスマスク要求** `18` – **アドレスマスク応答** `30` – **トレースルート** `31` – **データグラム変換エラー** `32` – **移動体ホストのリダイレクト** `33` – **IPv6 位置確認要求** `34` – **IPv6 位置確認応答** `35` – **移動体登録要求** `36` – **移動体登録応答** `37` – **ドメイン名要求** `38` – **ドメイン名応答** `40` – **Photuris** **ICMPv6 プロトコル** `1` – **宛先到達不能** `2` – **パケット過大** `3` – **時間切れ** `4` – **パラメータ問題** `128` – **エコー要求** `129` – **エコー応答** `130` – **マルチキャストリスナーのクエリ** `131` – **マルチキャストリスナーのレポート** `132` – **マルチキャストリスナーの完了** `133` – **ルーター要請** `134` – **ルーター広告** `135` – **近隣要請** `136` – **近隣広告** `137` – **リダイレクトメッセージ** `138` – **ルーターナンバリング** `139` – **ICMP ノード情報問い合わせ** `141` – **逆近隣探索要請メッセージ** `142` – **逆近隣探索広告メッセージ** `143` – **バージョン 2 マルチキャストリスナーレポート**

パラメータ	説明	値
		144 – **ホームエージェントアドレス発見要求メッセージ** 145 – **ホームエージェントアドレス発見応答メッセージ** 146 – **モバイルプレフィックス要請** 147 – **モバイルプレフィックス広告** 148 – **証明書パス要請メッセージ** 149 – **証明書パス広告メッセージ** 151 – **マルチキャストルーター広告** 152 – **マルチキャストルーター要請** 153 – **マルチキャストルーター終了**
`IcmpCode`	**ICMP コード**パラメータの値。	`0` – **コード 0** または無効 `1` – **コード 1** `2` – **コード 2**
`Flags`	構造体属性ポインタ。	整数 このパラメータは変更しないことを推奨します。
`TTL`	**最大生存時間（TTL）**パラメータの値。	秒単位の値。無効になっている場合、値は `0` です。
`</key>`		
`Id`	リソースのメイン ID（`[Rules]` ノードを確認してください）。	整数
`ParentID`	親グループの ID。	整数 このパラメータは変更しないことを推奨します。
`Flags`	ルールのステータス。	`6` – ルールが無効 `38` – ルールが有効
`Name`	ネットワークパケットルールの名前。	文字列

アプリケーションネットワークルールの管理

既定では、Kaspersky Endpoint Security はファイルまたはネットワークの動作が監視対象となっているソフトウェアの開発元名別に、コンピューターにインストールされているすべてのアプリケーションをグループ化します。アプリケーショングループは信頼グループに分類されます。すべてのアプリケーションとアプリケーショングループは、アプリケーションコントロールルールプロパティ、アプリケーションネットワークルールプロパティ、実行優先順プロパティを親グループから継承します。

［ホスト侵入防止］と同様に、ファイアウォールは、グループ内にあるすべてのアプリケーションのネットワークの動作をフィルターする際に、アプリケーショングループに対してネットワークルールを適用するように既定で設定されています。アプリケーションネットワークルールでは、グループ内のアプリケーションによる異なるネットワーク接続へのアクセス権限が定義されます。

既定では、ファイアウォールは、Kaspersky Endpoint Security がコンピューター上で検知した各アプリケーショングループに対してネットワークルールを作成します。既定で作成されたアプリケーショングループのネットワークルールに適用されるファイアウォールの処理は変更できます。既定で作成されているアプリケーショングループのネットワークルールの優先度を編集、削除、無効化、変更することはできません。

個別のアプリケーションに対するネットワークルールも作成できます。そのルールは、アプリケーションが属するグループに対するネットワークルールよりも優先度が高くなります。

アプリケーションネットワークルールの作成

既定では、アプリケーションの動作は、ネットワークルールによってコントロールされます。このルールは、Kaspersky Endpoint Security が初めて起動したときにアプリケーションを割り当てた信頼グループに定義されます。必要に応じて、信頼グループ全体、個別のアプリケーション、あるいは信頼グループ内に定義されているアプリケーショングループのネットワークルールを作成できます。

手動で定義されたネットワークルールは、信頼グループに定義されたネットワークルールより優先されます。言い換えると、手動で定義されたアプリケーションルールが信頼グループに定義されたアプリケーションルールと異なる場合、ファイアウォールはそのアプリケーションに対して手動で定義されたルールに従って操作を制御します。

既定では、ファイアウォールは各アプリケーションに対して次のネットワークルールを作成します：

- 許可するネットワーク内のネットワークの動作。
- ローカルネットワーク内のネットワークの動作。
- パブリックネットワーク内のネットワークの動作。

Kaspersky Endpoint Security は以下のように事前定義されたネットワークに従ってアプリケーションのネットワークの動作を制御します：

- 信頼および弱い制限付き：すべてのネットワーク動作が許可されます。
- 強い制限付きおよびブロック：すべてのネットワーク動作がブロックされます。

事前定義されたアプリケーションルールは編集または削除することはできません。

次の方法でアプリケーションネットワークルールを作成できます：

- ネットワークモニターツールを使用する。

  ネットワークモニターは、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。ルールを設定する必要がないため便利です。一部のファイアウォールの設定はネットワークモニターのデータから自動的に挿入されます。ネットワークモニターは製品のインターフェイスのみで使用できます。

- ファイアウォールを設定する。

  ファイアウォールの設定を詳細に調整できます。その時点でネットワークの操作がない場合にも、ネットワークの動作に関してルールを作成できます。

アプリケーションネットワークルールを作成する際、ネットワークパケットルールはアプリケーションネットワークルールより優先されることに注意してください。

製品のインターフェイスでネットワークモニターツールを使用してアプリケーションネットワークルールを作成する方法

1. 製品のメインウィンドウの［**監視**］で、［**ネットワークモニター**］をクリックします。
2. ［**ネットワークの動作**］または［**開いているポート**］タブを選択します。

   ［**ネットワークの動作**］タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。

   ［**開いているポート**］タブには、コンピューターで開いているネットワークポートがすべて表示されます。
3. ネットワーク接続のコンテキストメニューで、［**アプリケーションネットワークルールを作成する**］を選択します。

   アプリケーションルールおよびプロパティのウィンドウが開きます。
4. ［**ネットワークルール**］タブを選択します。

   ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
5. ［**追加する**］をクリックします。

   ネットワークルールのプロパティが開きます。
6. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。
7. ネットワークルールを設定します（下記の表を参照）。

   ［**ネットワークルールテンプレート**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。

   ネットワークルール設定は自動で入力されます。
8. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。
9. ［**保存する**］をクリックします。

   新しいネットワークルールがリストに追加されます。
10. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。
11. 変更内容を保存します。

製品のインターフェイスでファイアウォールの設定を使用してアプリケーションネットワークルールを作成する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。

3. ［**アプリケーションのルール**］をクリックします。
   ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。
4. アプリケーションのリストで、ネットワークルールを作成するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、［**詳細とルール**］を選択します。
   アプリケーションルールおよびプロパティのウィンドウが開きます。
6. ［**ネットワークルール**］タブを選択します。
7. ［**追加する**］をクリックします。
   ネットワークルールのプロパティが開きます。
8. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。
9. ネットワークルールを設定します（下記の表を参照）。
   ［**ネットワークルールテンプレート**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。
   ネットワークルール設定は自動で入力されます。
10. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。
11. ［**保存する**］をクリックします。
    新しいネットワークルールがリストに追加されます。
12. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。
13. 変更内容を保存します。

管理コンソール（MMC）でアプリケーションネットワークルールを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
4. ［**ファイアウォールの設定**］ブロックの［**設定**］をクリックします。
   ネットワークパケットルールおよびアプリケーションネットワークルールのリストが表示されます。
5. ［**アプリケーションネットワークルール**］タブを選択します。
6. ［**追加**］をクリックします。
7. 表示されたウィンドウで、ネットワークルールを作成するアプリケーションを検索する条件を入力します。
   アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。
8. ［**更新**］をクリックします。
   Kaspersky Endpoint Security は管理対象コンピューター上にインストールされたアプリケーションのリストから該当するアプリケーションを検索します。検索条件を満たすアプリケーションのリストが表示されます。

9. 必要なアプリケーションを選択します。

10. ［**選択したアプリケーションを次の信頼グループに追加**］で、［**既定のグループ**］を選択し、［OK］をクリックします。

    アプリケーションが既定のグループに追加されます。

11. 対象のアプリケーションを選択して、アプリケーションのコンテキストメニューから［**アプリケーション権限**］を選択します。

    アプリケーションルールおよびプロパティのウィンドウが開きます。

12. ［**ネットワークルール**］タブを選択します。

    ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。

13. ［**追加**］をクリックします。

    ネットワークルールのプロパティが開きます。

14. ［**名前**］フィールドに、ネットワークサービスの名前を手動で入力します。

15. ネットワークルールを設定します（下記の表を参照）。

    ボタン（）をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。

    ネットワークルール設定は自動で入力されます。

16. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。

17. 新しいネットワークルールを保存します。

18. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。

19. 変更内容を保存します。

Web コンソールと Cloud コンソールでアプリケーションネットワークルールを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

    ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**ファイアウォール**］の順に選択します。

5. ［**アプリケーション権限と保護対象のリソース**］セクションで、［**アプリケーション権限**］をクリックします。

    アプリケーション権限の設定ウィンドウおよび保護対象のリソースのリストが開きます。

6. ［**アプリケーション権限**］タブを選択します。

    ウィンドウの左側に信頼グループのリスト、右側にそのプロパティが表示されます。

7. ［**アプリケーション**］ブロックの［**追加**］をクリックします。

    ウィザードがアプリケーションを信頼グループに追加します。

8. アプリケーションに対して適切な信頼グループを選択します。

9. **アプリケーション**の種別を選択します。次の手順に進みます。

   複数のアプリケーションのネットワークルールを作成する場合は、［**グループ**］を選択してアプリケーショングループの名前を定義します。

10. アプリケーションのリストで、ネットワークルールを作成するアプリケーションを選択します。

    フィルターを使用します。アプリケーションの名前または製造元の名前を入力できます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

11. ウィザードを終了します。

    アプリケーションが信頼グループに追加されます。

12. ウィンドウの左側で、アプリケーションを選択します。

13. ウィンドウの右側で、ドロップダウンリストから［**ネットワークルール**］を選択します。

    ファイアウォールによって設定される既定のネットワークルールのリストが表示されます。

14. ［**追加**］をクリックします。

    アプリケーションルールのプロパティが開きます。

15. ［**ルール名**］フィールドに、ネットワークサービスの名前を手動で入力します。

16. ネットワークルールを設定します（下記の表を参照）。

    ［**ルールのテンプレートを選択してください**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続に関する説明があります。

    ネットワークルール設定は自動で入力されます。

17. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。

18. ネットワークルールを保存します。

    新しいネットワークルールがリストに追加されます。

19. ［**移動する**］を使用してネットワークルールの優先度を設定します。

20. 変更内容を保存します。

アプリケーションネットワークルールの設定

パラメータ	説明
処理	**許可** **ブロック**
プロトコル	選択したプロトコル（TCP、UDP、ICMP、ICMPv6、IGMP および GRE）に対してネットワークの動作を制御します。 ICMP または ICMPv6 プロトコルを選択すると、ICMP パケットの種類とコードを定義できます。 TCP または UDP をプロトコルの種類として選択すると、接続が監視されるローカルコンピューターとリモートコンピューターのポートをカンマ区切りで指定できます。
通信方向	**受信** **受信 / 送信** **送信**

パラメータ	説明
リモートアドレス	ネットワークパケットを送信または受信するリモートコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のリモートネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めることも、IP アドレスの範囲を指定することも、IP アドレスごとに別のリストを作成することも、または許可するネットワーク、ローカルネットワーク、パブリックネットワークなどのサブネットを選択することもできます。また、IP アドレスの代わりにコンピューターの DNS 名を指定することも可能です。LAN コンピューターまたは内部サービスに対しては DNS 名のみを使用してください。Microsoft Azure のようなクラウドサービスやその他のインターネットリソースとの連携については、Web コントロール機能で処理してください。 ネットワークパケットルールで IP アドレスが特定できない DNS 名を追加した場合、Kaspersky Endpoint Security は警告を表示します。Web コンソールのネットワークパケットルールのリストに、列がエラーの説明とともに追加されます。管理コンソール（MMC）では、エラーの説明は使用できません。このようなパケットルールは色で強調されます。
ローカルアドレス	ネットワークパケットを送信または受信するコンピューターのネットワークアドレスです。ファイアウォールでは、指定した範囲のローカルネットワークアドレスにネットワークルールが適用されます。すべての IP アドレスをネットワークに含めたり、IP アドレスごとに別のリストを作成したり、IP アドレスの範囲を指定したりすることもできます。 本製品は、リモートアドレスのリストが指定されている場合にのみ、ローカルアドレスを保存します。つまり、［**リモートアドレス**］に対して［**設定したネットワークアドレス**］の値が選択されて、少なくとも 1 つのアドレスが追加されている場合です。 アプリケーションのローカルアドレスが取得できない場合があります。この場合、このパラメータは無視されます。

アプリケーションネットワークルールの有効化と無効化

アプリケーションネットワークルールを有効または無効にするには、次の手順を実行します：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**アプリケーションのルール**］をクリックします。
   アプリケーションルールのリストのテーブルが開きます。
4. アプリケーションのリストで、ネットワークルールを作成または編集するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、［**詳細とルール**］を選択します。
   アプリケーションルールおよびプロパティのウィンドウが開きます。
6. ［**ネットワークルール**］タブを選択します。
7. アプリケーショングループのネットワークルールのリストで、目的のネットワークルールを選択します。
   ［ネットワークルールのプロパティ］ウィンドウが表示されます。
8. ネットワークルールに［**有効**］または［**無効**］を設定します。
   ファイアウォールによって既定で作成されたアプリケーショングループのネットワークルールは、無効にできません。
9. 変更内容を保存します。

アプリケーションネットワークルールのファイアウォール処理の変更

アプリケーションまたはアプリケーショングループに対して既定で作成されたすべてのネットワークルールに適用されているファイアウォール処理を変更したり、アプリケーションまたはアプリケーショングループに対するカスタムネットワークルールのファイアウォール処理を変更したりできます。

アプリケーションまたはアプリケーショングループに対するすべてのネットワークルールに適用するファイアウォールの処理を変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**アプリケーションのルール**］をクリックします。
   アプリケーションルールのリストのテーブルが開きます。
4. 既定で作成されるすべてのネットワークルールに適用するファイアウォールの処理を変更するには、リストでアプリケーションまたはアプリケーショングループを選択します。手動で作成されたネットワークルールは変更されません。
5. 右クリックでコンテキストメニューを開き、［**ネットワークルール**］を選択し、割り当てる操作を選択します：
   - **継承**
   - **許可する**
   - **ブロックする**
6. 変更内容を保存します。

アプリケーションまたはアプリケーショングループに対する単一のネットワークルールに適用するファイアウォールの処理を変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**アプリケーションのルール**］をクリックします。
   アプリケーションルールのリストのテーブルが開きます。
4. リストで、単一のネットワークルールに対する処理を変更するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、［**詳細とルール**］を選択します。
   アプリケーションルールおよびプロパティのウィンドウが開きます。
6. ［**ネットワークルール**］タブを選択します。
7. ファイアウォールの処理を変更するネットワークルールを選択します。

8. ［**権限**］列で右クリックして、コンテキストメニューを表示し、割り当てる処理を次のいずれかから選択します：

   - **継承**
   - **許可する**
   - **ブロック**
   - **イベントを記録**

9. 変更内容を保存します。

アプリケーションネットワークルールの優先度の変更

ネットワークルールの優先度は、ネットワークルールのリスト内の位置によって決まります。ファイアウォールでは、アプリケーションネットワークルールはネットワークルールリストの上から順に実行されます。ファイアウォールでは、特定のネットワーク接続に適用される処理済みネットワークルールに従って、そのネットワーク接続の設定で示されているアドレスおよびポートへのネットワークアクセスが許可またはブロックされます。

手動で作成されたネットワークルールの優先度は、既定のネットワークルールよりも高くなります。

既定で作成されているアプリケーショングループのネットワークルールの優先度を変更することはできません。

ネットワークルールの優先度を変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**脅威対策**］→［**ファイアウォール**］を選択します。
3. ［**アプリケーションのルール**］をクリックします。
   アプリケーションルールのリストのテーブルが開きます。
4. アプリケーションのリストで、ネットワークルールの優先度を変更するアプリケーションまたはアプリケーションのグループを選択します。
5. 右クリックしてコンテキストメニューを表示し、［**詳細とルール**］を選択します。
   アプリケーションルールおよびプロパティのウィンドウが開きます。
6. ［**ネットワークルール**］タブを選択します。
7. 優先度を変更するネットワークルールを選択します。
8. ［**上へ**］と［**下へ**］を使用してネットワークルールの優先度を設定します。
9. 変更内容を保存します。

ネットワークモニター

*ネットワークモニター*は、ユーザーのコンピューターのネットワーク動作に関する情報をリアルタイムで表示するように設計されたツールです。

ネットワークモニターを開始するには：

製品のメインウィンドウの［**監視**］で、［**ネットワークモニター**］をクリックします。

［ネットワークモニター］ウィンドウが表示されます。このウィンドウの次の 4 つのタブに、コンピューターのネットワークの動作に関する情報が表示されます：

- ［**ネットワークの動作**］タブには、コンピューターで現在有効なネットワーク接続がすべて表示されます。送信および受信の両方のネットワーク接続が表示されます。このタブでは、ファイアウォールの操作のためのネットワークパケットルールを作成することができます。
- ［**開いているポート**］タブには、コンピューターで開いているネットワークポートがすべて表示されます。このタブでは、ファイアウォールの操作のためのネットワークパケットルールおよびアプリケーションルールを作成することができます。
- ［**トラフィック**］タブには、ユーザーが現在接続しているネットワークにおける、クライアントコンピューターと他のコンピューターの間の送受信ネットワークトラフィックの量が表示されます。
- ［**ブロック中のコンピューター**］タブには、ネットワーク攻撃の試行元として検知された後にネットワーク脅威対策によってネットワークの動作がブロックされたリモートコンピューターの IP アドレスが表示されます。

脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとすると、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。

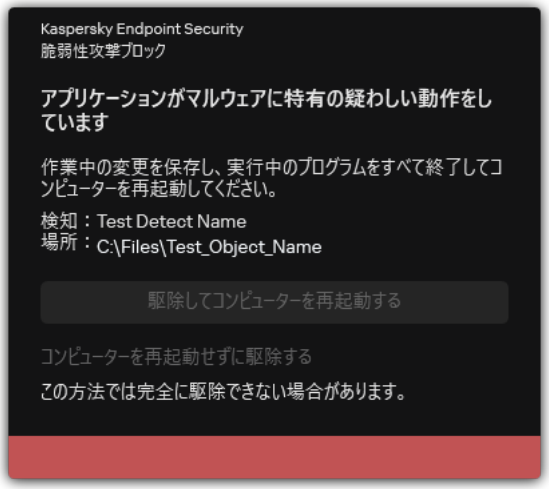
さらに、脆弱性攻撃ブロックは、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

脆弱性攻撃ブロックの有効化と無効化

既定では、脆弱性攻撃ブロックは有効化され、最適なモードで機能します。Kaspersky Endpoint Security は、脆弱性があるアプリケーションによって実行される実行ファイルを監視します。脆弱性があるアプリケーションのファイルが、そのユーザー以外によって使用されていることを検知した場合、本製品は操作をブロックするなど、選択されている処理を行います。

管理コンソール（MMC）で脆弱性攻撃ブロックを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**脆弱性攻撃ブロック**］の順に選択します。
4. ［**脆弱性攻撃ブロック**］を使用して機能を有効または無効にします。
5. ［**攻撃を検知したとき**］ブロックで関連する操作を選択します。
   - **ブロックする**：この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。
   - **通知する**：この項目を選択した場合、攻撃が検知されると、攻撃に関する情報がログに記録され、攻撃に関する情報がアクティブな脅威のリストに追加されます。



アクティブな脅威についての通知

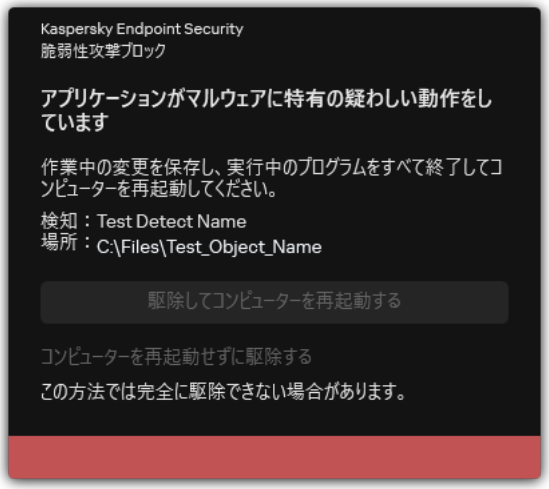
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで脆弱性攻撃ブロックを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**脆弱性攻撃ブロック**］に移動します。
5. ［**脆弱性攻撃ブロックは有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。

- **ブロックする**：この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。
- **通知または手動選択**：この項目を選択した場合、攻撃が検知されると、攻撃に関する情報がログに記録され、攻撃に関する情報がアクティブな脅威のリストに追加されます。



アクティブな脅威についての通知

7. 変更内容を保存します。

製品インターフェイスで脆弱性攻撃ブロックを有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**脆弱性攻撃ブロック**］を選択します。



脆弱性攻撃ブロックの設定

3. ［**脆弱性攻撃ブロック**］トグルスイッチを使用して機能を有効または無効にします。
4. ［**攻撃を検知したとき**］ブロックで関連する操作を選択します。
   - **ブロックする**：この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。
   - **通知する**：この項目を選択した場合、攻撃が検知されると、攻撃に関する情報がログに記録され、攻撃に関する情報がアクティブな脅威のリストに追加されます。
5. 変更内容を保存します。

システムプロセスのメモリ保護

既定では、システムプロセスのメモリ保護は有効です。Kaspersky Endpoint Security は、システムプロセスへのアクセスを取得しようとする外部プロセスをブロックします。

管理コンソール（MMC）でシステムプロセスのメモリ保護を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**脆弱性攻撃ブロック**］の順に選択します。
4. ［**システムプロセスのメモリ保護を有効にする**］を使用してオプションを有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでシステムプロセスのメモリ保護を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**脆弱性攻撃ブロック**］に移動します。
5. ［**システムプロセスのメモリ保護は有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでシステムプロセスのメモリ保護を有効または無効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**脆弱性攻撃ブロック**］を選択します。



脆弱性攻撃ブロックの設定

3. ［**システムプロセスのメモリ保護を有効にする**］トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

ふるまい検知

ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures（BSS）を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

さらに、ふるまい検知は、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

既定では、ふるまい検知は有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されています。悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルが削除されます。

ふるまい検知を無効にすると、保護機能のパフォーマンスが低下するため、絶対に必要な場合を除いて無効にしないでください。脅威を検知するために、保護機能がふるまい検知によって収集されたデータを要求する場合があります。

管理コンソール（MMC）でふるまい検知を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**先進の脅威対策**］→［**ふるまい検知**］の順に選択します。
5. ［**ふるまい検知**］を使用して機能を有効または無効にします。
6. ［**マルウェア活動の検知時の処理**］ブロックで関連する操作を選択します。
   - **削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロック**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。
   - **通知**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。
7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでふるまい検知を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ふるまい分析**］→［**ふるまい検知**］に移動します。
5. ［**ふるまい検知は有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。

   - **削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。
   - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。

7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

製品インターフェイスでふるまい検知を有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**ふるまい検知**］を選択します。



ふるまい検知の設定

3. ［**ふるまい検知**］トグルスイッチを使用して機能を有効または無効にします。

4. ［**マルウェア活動の検知時の処理**］ブロックで関連する操作を選択します。

   - **削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。
   - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。

5. 変更内容を保存します。

ふるまい検知が有効になっていると、Kaspersky Endpoint Security はオペレーティングシステム内で行われるアプリケーションの動作を、Behavior Stream Signatures を使用して分析します。

アンチクリプター

Kaspersky Endpoint Security 12.12 for Windows 以降、以前はふるまい検知コンポーネントの一部であった外部からの暗号化に対する共有フォルダの保護は、現在は独立したコンポーネント（アンチクリプター）になっています。

このコンポーネントは、NTFS ファイルシステムを使用しており EFS で暗号化されていない大容量ストレージデバイスに保存されたファイルに対する操作のみを監視します。

アンチクリプターコンポーネントは共有フォルダ内の動作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。

アンチクリプターコンポーネントが機能するように、ふるまい検知コンポーネントを有効にする必要があります。

共有フォルダーにあるファイルを変更する試行が検知されると、次の処理が実行されます：

- 悪意のある操作を開始したセッションがファイル変更へアクセスするのをブロックします（ファイルは読み取り専用になります）。
- 変更されようとしているファイルのバックアップコピーを作成します。
- ローカルの製品インターフェイスレポートに項目を追加して、検知された悪意のある動作に関する情報を Kaspersky Security Center に送信します。
- また、修復エンジンがオンの場合、変更されたファイルがバックアップコピーから復元されます。

外部からの暗号化に対する共有フォルダーの保護の有効化または無効化

既定では、カスペルスキーの専門家が推奨するように、外部からの暗号化に対する共有フォルダーの保護が有効になり、機能しています。この機能を設定するには、保護範囲を作成して、必要に応じて除外リストを設定します。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダー内のファイルの動作を監視します。共有フォルダー内のファイルを外部から暗号化する試行が検知されると、Kaspersky Endpoint Security はリモートユーザーのセッションを 1 時間（既定）ブロックします。

Kaspersky Endpoint Security のインストール後、コンピューターを再起動するまでは、外部からの暗号化に対する共有フォルダーの保護は制限されます。

管理コンソール（MMC）で外部からの暗号化に対する共有フォルダーの保護を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］の順に選択します。
4. ［**アンチクリプター**］を使用して、外部からの暗号化を示唆する操作の検知を有効または無効にします。
5. 共有フォルダーにあるファイルを変更する試行が検知された際に、本製品が実行する関連する処理を選択します：
   - **接続をブロックする時間**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする時間**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、この試みに関する情報がアクティブな脅威のリストに追加され、ローカルの製品インターフェイスレポートに項目が追加されて、検知された悪意のある活動に関する情報が Kaspersky Security Center に送信されます。
6. 必要に応じて、保護範囲を編集し、除外リストを定義します。
7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで外部からの暗号化に対する共有フォルダーの保護を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。

5. ［**アンチクリプターは有効です**］を使用して、外部からの暗号化を示唆する操作の検知を有効または無効にします。

6. 共有フォルダーにあるファイルを変更する試行が検知された際に、本製品が実行する関連する処理を選択します：

   - **接続をブロックする時間（分）**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする時間（分）**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知する**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、この試みに関する情報がアクティブな脅威のリストに追加され、ローカルの製品インターフェイスレポートに項目が追加されて、検知された悪意のある活動に関する情報が Kaspersky Security Center に送信されます。

7. 必要に応じて、保護範囲を編集し、除外リストを定義します。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで外部からの暗号化に対する共有フォルダーの保護を有効または無効にする方法

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］を選択します。

3. ［**外部からの暗号化に対する共有フォルダーの保護**］を使用して、外部からの暗号化を示唆する操作の検知を有効または無効にします。

4. ［**外部からの暗号化に対する共有フォルダーの保護**］を使用して、外部からの暗号化を示唆する操作の検知を有効または無効にします。

5. 共有フォルダーにあるファイルを変更する試行が検知された際に、本製品が実行する関連する処理を選択します：

   - **接続をブロックする時間（分）**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする時間（分）**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知する**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、この試みに関する情報がアクティブな脅威のリストに追加され、ローカルの製品インターフェイスレポートに項目が追加されて、検知された悪意のある活動に関する情報が Kaspersky Security Center に送信されます。

6. 必要に応じて、保護範囲を編集し、除外リストを定義します。

7. 変更内容を保存します。

信頼できないコンピューターのブロック期間の設定

*信頼できないコンピューター*とは、悪意のある動作やデータ暗号化に関与しているリモートコンピューターです。既定では、Kaspersky Endpoint Security はリモートユーザーのセッションを1時間ブロックします。ブロック期間が終了すると、Kaspersky Endpoint Security はコンピューターをブロックリストから削除し、共有フォルダーへのアクセスを復元します。

管理コンソール（MMC）で信頼できないコンピューターのブロック期間を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］の順に選択します。

4. ［**脅威の検知時の処理**］ブロックで、［**接続をブロックする時間N 分**］を選択します。

5. 悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

6. 変更内容を保存します。

Web コンソールと Cloud コンソールで信頼できないコンピューターのブロック期間を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。

5. ［**脅威の検知時の処理**］で、悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

6. 変更内容を保存します。

製品インターフェイスで信頼できないコンピューターのブロック期間を設定する方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］を選択します。

3. ［**脅威の検知時の処理**］ブロックで、［**接続をブロックする時間（分）**］を選択します。

4. 悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

5. 変更内容を保存します。

これにより、リモートコンピューターがロックされます。リモートコンピューターのロックを解除するには、Kaspersky Endpoint Security を再起動します。

保護範囲の編集

*保護範囲*は、Kaspersky Endpoint Security がファイルの動作を監視する共有フォルダーへのパスのリストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダー内のファイルの動作を監視します。

組織で、共有フォルダーを使用したファイルの交換時にデータ暗号化が使用されている場合、保護範囲からフォルダーを除外することで誤検知の量を減らすことができます。例えば、ユーザーが共有フォルダーで拡張子 ENC のファイルを使用していると、ふるまい検知で誤検知の量が増えることがあります。このような操作は、外部からの暗号化攻撃に典型的な動作と一致します。データを保護するために共有フォルダーでファイルを暗号化した場合は、そのフォルダーを除外リストに追加します。

> 外部からの暗号化に対する処理を実行しないコンピューターを除外することもできます。

管理コンソール（MMC）で保護範囲を編集する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］の順に選択します。

4. ［**保護範囲**］ブロックで、［**指定した共有フォルダーのみ**］を選択します。

5. フォルダーのリストで、［**追加**］をクリックします。

6. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

   > 共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

7. ［OK］をクリックします。

8. 必要に応じて、保護範囲の除外リストを定義します：

   a. ［**信頼するオブジェクト**］ブロックの［**マスク**］をクリックします。

   b. 表示されたウィンドウで、［**追加**］をクリックします。

c. 表示されたウィンドウで、`*.<file extension>` の形式でファイルの拡張子を指定するか、フォルダーパスを指定します。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。

本製品では、いくつかのファイルの拡張子は除外用としてサポートされていません。したがって、除外は、`*.docx` または `**\Folder\**` として指定できます。

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

9. 変更内容を保存します。

Web コンソールと Cloud コンソールで保護範囲を編集する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。
5. ［**保護範囲**］ブロックで、［**指定した共有フォルダーのみ**］を選択します。
6. フォルダーのリストで、［**追加**］をクリックします。
7. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

   > 共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

8. ［**OK**］をクリックします。
9. 必要に応じて、保護範囲の除外リストを定義します：

   a. ウィンドウの上部で、［**信頼するオブジェクト**］リンクをクリックします。

   b. 表示されたウィンドウで、［**追加**］をクリックします。

   c. 表示されたウィンドウで、`*.<file extension>` の形式でファイルの拡張子を指定するか、フォルダーパスを指定します。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。

   本製品では、いくつかのファイルの拡張子は除外用としてサポートされていません。したがって、除外は、`*.docx` または `**\Folder\**` として指定できます。

   保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。
10. 変更内容を保存します。

製品インターフェイスで保護範囲を編集する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］を選択します。
3. ［**保護範囲**］ブロックで、［**指定した共有フォルダーのみ**］を選択します。
4. フォルダーのリストで、［**追加する**］をクリックします。
5. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

   > 共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

6. ［OK］をクリックします。
7. 必要に応じて、保護範囲の除外リストを定義します：
   a. ウィンドウの上部で、［**マスクによる除外**］リンクをクリックします。
   b. 表示されたウィンドウで、［**追加する**］をクリックします。
   c. 表示されたウィンドウで、`*.<file extension>` の形式でファイルの拡張子を指定するか、フォルダーパスを指定します。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
      本製品では、いくつかのファイルの拡張子は除外用としてサポートされていません。したがって、除外は、`*.docx` または `**\Folder\**` として指定できます。

   保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。
8. 変更内容を保存します。

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。
3. ［**除外リスト**］セクションで、［**除外リストの管理**］をクリックします。
4. ［**追加**］をクリックします。
5. ［**参照**］をクリックして共有フォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Endpoint Security では、マスクの入力時の文字「*」および「?」がサポートされます。

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「?:\Users*\Folder\」と入力できます。

6. ［**保護機能**］ブロックで、［**ふるまい検知**］コンポーネントを選択します。

7. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

8. 信頼するオブジェクトのステータスに［**有効**］を選択します。
   このトグルスイッチを使用していつでも除外を停止することができます。

9. 変更内容を保存します。

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**信頼ゾーン**］に移動します。

5. 表示されたウィンドウで、［**マルウェアスキャンの除外リスト**］をクリックします。

6. 組織内のすべてのコンピューターの除外リストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。

7. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。

8. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも 1 つの信頼するオブジェクトをカテゴリに追加します。

   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。

   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。

9. 除外を追加する方法［**ファイルまたはフォルダーのパス**］を選択します。

10. 共有フォルダーへのパスを入力します。

    手動でパスを入力することもできます。Kaspersky Endpoint Security では、マスクの入力時の文字「`*`」および「`?`」 がサポートされます。

    - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

    - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

    ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`C:\Users\*\Folder\`」と入力できます。

11. ［**除外を次に適用する**］ブロックで、［**ふるまい検知**］コンポーネントを選択します。

12. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

13. 信頼するオブジェクトのステータスに［**除外リストに追加する**］を選択します。

    このトグルスイッチを使用していつでも除外を停止することができます。

14. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。

4. ［**信頼するオブジェクトとアプリケーション**］→［**信頼するオブジェクト**］ブロックの［**設定**］をクリックします。

   除外リストを含むウィンドウが開きます。

5. 組織内のすべてのコンピューターの除外リストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。

6. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。

7. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも 1 つの信頼するオブジェクトをカテゴリに追加します。

   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。

   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。

8. ［**追加**］をクリックします。

9. ［**プロパティ**］ブロックで、［**ファイルまたはフォルダー**］をオンにします。

10. ［**信頼するオブジェクトの説明（下線部をクリックして編集します）**］ブロックの［**ファイルまたはフォルダーの選択**］リンクをクリックして、［**ファイルまたはフォルダーの名前**］ウィンドウを開きます。

11. ［**参照**］をクリックして共有フォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Endpoint Security では、マスクの入力時の文字「*」および「?」がサポートされます。

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「?:\Users*\Folder\」と入力できます。

12. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

13. ［**信頼するオブジェクトの説明（下線部をクリックして編集します）**］ブロックのリンクをクリックして、［**保護機能**］ウィンドウを開きます。

14. ［**ふるまい検知**］コンポーネントの横にあるチェックボックスをオンにします。

15. 変更内容を保存します。

外部データ暗号化用の信頼できるコンピューターの追加

所属する組織がファイル交換ワークフローで外部データ暗号化を使用する場合、信頼できるコンピューターのリストを作成する必要があります。Kaspersky Endpoint Security では、信頼できるコンピューターによるデータ暗号化は監視されません。

外部からの暗号化に対する共有フォルダーの保護から除外するアドレスを設定するには、ログオンの監査サービスを有効にしておく必要があります。既定では、ログオンの監査サービスは無効です（ログオンの監査サービスの有効化に関する詳細な情報については、Microsoft の Web サイトを参照してください）。

共有フォルダーの保護からアドレスを除外する機能は、Kaspersky Endpoint Security が開始する前から動作しているリモートコンピューターに対しては適用されません。Kaspersky Endpoint Security が開始した後でリモートコンピューターを再起動することで、そのリモートコンピューターに対して共有フォルダーの保護からアドレスを除外する機能が有効になります。

管理コンソール（MMC）で外部データ暗号化用の信頼できるコンピューターを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］の順に選択します。
4. ［**信頼するオブジェクト**］ブロックの［**名前または IP アドレス**］をクリックします。
5. 表示されたウィンドウで、［**名前または IP アドレス**］をクリックします。
6. 外部からの暗号化に対する処理を実行しない IP アドレス、IP アドレスの範囲、またはコンピューター名を入力します。
   例：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
7. 変更内容を保存します。

Web コンソールと Cloud コンソールで外部データ暗号化用の信頼できるコンピューターを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。
5. ウィンドウの上部で、［**名前または IP アドレスによる除外リスト**］リンクをクリックします。
6. 表示されたウィンドウで、［**追加**］をクリックします。
7. 外部からの暗号化に対する処理を実行しない IP アドレス、IP アドレスの範囲、またはコンピューター名を入力します。
   例：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. 変更内容を保存します。

製品インターフェイスで外部データ暗号化用の信頼できるコンピューターを追加する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］を選択します。
3. ウィンドウの上部で、［**名前または IP アドレスによる除外リスト**］リンクをクリックします。
4. 表示されたウィンドウで、［**追加**］をクリックします。
5. 外部からの暗号化に対する処理を実行しない IP アドレス、IP アドレスの範囲、またはコンピューター名を入力します。

   例：

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. 変更内容を保存します。

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

除外リストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で除外リストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**アンチクリプター**］の順に選択します。
4. ［**信頼するオブジェクト**］ブロックの［**名前または IP アドレス**］をクリックします。

5. ルールのリストをエクスポートするには：

   a. エクスポートする除外リストを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

   除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。

   b. → ［**エクスポート**］を選択します。

   c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

   Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。

6. 除外リストをインポートするには：

   a. → ［**インポート**］を選択します。

   b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

   c. ファイルを開きます。

   コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで除外リストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。

5. ［**名前または IP アドレスによる除外リスト**］リンクをクリックします。

6. ルールのリストをエクスポートするには：

   a. エクスポートする除外リストを選択します。

   b. → ［**エクスポート**］を選択します。

   Kaspersky Endpoint Security は既定のダウンロードフォルダーに除外リストを JSON ファイルでエクスポートします。

7. 除外リストをインポートするには：

   a. → ［**インポート**］を選択します。

   表示されたウィンドウで、除外リストをインポートする JSON ファイルを選択します。

b. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

修復エンジン

修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックするとき、次の種別のマルウェアの動作に対して処理を実行します：

- **ファイルの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
  - マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
  - マルウェアによって変更または削除されたファイルを復元します。

  ファイルの修復機能にはいくつかの制限事項があります。

- **レジストリの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによって作成されたレジストリキーを削除します。
  - マルウェアによって変更または削除されたレジストリキーは復元されません。

- **システムの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによって開始されたプロセスを終了します。
  - 悪意のあるアプリケーションによって侵入されたプロセスを終了します。
  - マルウェアによって停止されたプロセスは再開しません。

- **ネットワークの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによるネットワーク動作をブロックします。
  - マルウェアが侵入したプロセスによるネットワーク動作をブロックします。

マルウェアの動作のロールバックは、ファイル脅威対策またはふるまい検知から開始するか、マルウェアのスキャン中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピューターデータの整合性に悪影響を与えません。

管理コンソール（MMC）で修復エンジンを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**修復エンジン**］の順に選択します。
4. ［**修復エンジン**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで修復エンジンを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**修復エンジン**］に移動します。
5. ［**修復エンジンは有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスで修復エンジンを有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**修復エンジン**］を選択します。
3. ［**修復エンジン**］トグルスイッチを使用して機能を有効または無効にします。
4. 変更内容を保存します。

修復エンジンを有効にすると、悪意のあるアプリケーションが検知された場合、そのアプリケーションによるオペレーティングシステム内での動作がロールバックされます。

Kaspersky Security Network

コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

KSN 機能は、アメリカ合衆国内にある本製品ではご利用いただけなくなる可能性があります。

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

Kaspersky Security Network の使用は任意です。本製品の初期設定中に、KSN を使用するかどうか尋ねられます。KSN への参加はいつでも開始または中止できます。

KSN に参加している間に生成されたカスペルスキー統計情報の送信や、そのような情報の保存と破棄について詳しくは、KSN 声明およびカスペルスキーの Web サイトを参照してください。Kaspersky Security Network 声明のテキストが含まれたファイル ksn_<言語 ID>.txt は製品配信キットに含まれています。

カスペルスキーの評価データベースのインフラストラクチャ

Kaspersky Endpoint Security は、カスペルスキーの評価データベースと連携する、次のインフラストラクチャソリューションをサポートします：

- ほとんどのカスペルスキー製品で使用されるのが *Kaspersky Security Network (KSN)* です。KSN の参加者は、カスペルスキーから情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、評価データベースと統計情報のデータベースに追加されます。

- *Kaspersky Private Security Network (KPSN)* は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。KPSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：

  - コンピューターがインターネットに接続されていない。

  - 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

Kaspersky Security Network の使用の有効化と無効化

既定では、拡張 KSN モードが使用されます。*拡張 KSN モード*は、カスペルスキーに詳細なデータを送信するモードです。

管理コンソール（MMC）で KSN の使用を有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。

4. ［**Kaspersky Security Network**］トグルスイッチを使用して機能を有効または無効にします。

   KSN の使用を有効にすると、Kaspersky Endpoint Security に、Kaspersky Security Network に関する声明が表示されます。Kaspersky Security Network（KSN）に関する声明の条項に同意する場合は、内容を確認した上で同意してください。

5. 必要に応じて、［**拡張 KSN モードを有効にする**］をオフにします。

6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで KSN の使用を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。

5. ［**Kaspersky Security Network（KSN）の使用は有効です**］トグルスイッチを使用して機能を有効または無効にします。

   KSN の使用を有効にすると、Kaspersky Endpoint Security に、Kaspersky Security Network に関する声明が表示されます。Kaspersky Security Network（KSN）に関する声明の条項に同意する場合は、内容を確認した上で同意してください。

6. 必要に応じて、［**拡張 KSN モードを使用する**］をオフにしてください。

7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで KSN の使用を有効または無効にする方法

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**Kaspersky Security Network**］を選択します。

3. ［**Kaspersky Security Network**］トグルスイッチを使用して機能を有効または無効にします。

   KSN の使用を有効にすると、Kaspersky Endpoint Security に、Kaspersky Security Network に関する声明が表示されます。Kaspersky Security Network（KSN）に関する声明の条項に同意する場合は、内容を確認した上で同意してください。

4. 必要に応じて、［**拡張 KSN モードを有効にする**］をオフにしてください。

5. 変更内容を保存します。

KSN の使用を有効にすると、Kaspersky Endpoint Security は Kaspersky Security Network から受け取ったファイル、Web リソース、アプリケーションの評価に関する情報を使用します。

Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。Kaspersky Private Security Network は、オブジェクト（ファイルまたは Web アドレス）の評価をチェックするためのローカルの評価データベースです。ローカルの評価データベースに追加されたオブジェクトの評価は KSN または KPSN に追加されたものより優先度は高くなります。たとえば、Kaspersky Endpoint Security がコンピューターをスキャン中に KSN または KPSN に評価を要求したとします。あるファイルに対して、ローカルの評価データベースに「*ブロック*」という評価があり、KSN または KPSN に「*信頼済み*」という評価があった場合、Kaspersky Endpoint Security はファイルを「*ブロック*」と判断して検出し、検知された脅威に対して定義された操作を実行します。

しかし、Kaspersky Endpoint Security が KSN または KPSN にオブジェクトの評価を要求しないこともあります。この場合、Kaspersky Endpoint Security KPSN のローカル評価データベースからデータを受け取りません。Kaspersky Endpoint Security は次の理由で KSN または KPSN にオブジェクトの評価を要求しないことがあります：

- カスペルスキー製品がオフラインの評価データベースを使用している。オフラインの評価データベースは、カスペルスキー製品の動作中にリソースの最適化をするため、またコンピューター上の特に重要なオブジェクトを保護するために設計されています。オフライン評価データベースは、Kaspersky Security Network のデータに基づいてカスペルスキーによって作成されています。カスペルスキー製品は特定のアプリケーションの定義データベースがアップデートされる際にあわせてオフラインの評価データベースをアップデートします。オフラインの評価データベースにスキャンされるオブジェクトに関する情報が存在する場合、製品は KSN または KPSN にこのオブジェクトの評価を要求しません。

- スキャンの除外リスト（信頼ゾーン）は製品の設定で指定されます。該当する場合、製品はローカルの評価データベースのオブジェクトの評価を判断に使用しません。

- 製品が iSwift または iChecker などのスキャンの最適化技術を使用している、または KSN / KPSN への評価の要求をキャッシュしている場合。この場合は製品が以前にスキャンしたオブジェクトの評価を要求しません。

- 負荷を最適化するため、本製品は特定の形式またはサイズのファイルのみスキャンします。対応する形式およびサイズの制限はカスペルスキーによって定義されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。たとえば、ファイル脅威対策機能など、スキャンの最適化の設定を製品インターフェイスから設定することも可能です。

- Light Agent モードの Kaspersky Endpoint Security は、KSN プロキシサーバーを介して KSN サーバーと通信します。KSN との直接通信には対応していません。

保護機能のクラウドモードの有効化と無効化

*クラウドモード*で動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用しての本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。

Kaspersky Private Security Network を使用する場合、クラウドモードは Kaspersky Private Security Network 3.0 以降で使用できます。

本製品が Light Agent モードで動作している場合、クラウドモードは使用できません。

管理コンソール（MMC）で保護機能のクラウドモードを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。
4. ［**クラウドモードを有効にする**］を使用して機能を有効または無効にします。
5. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールで保護機能のクラウドモードを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。
5. ［**クラウドモードを使用**］トグルスイッチを使用して機能を有効または無効にします。
6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで保護機能のクラウドモードを有効または無効にする方法

1. メインウィンドウで、をクリックします。
2. 本製品の設定ウィンドウで、［**先進の脅威対策**］→［**Kaspersky Security Network**］を選択します。

3. ［**クラウドモードを有効にする**］トグルスイッチを使用して機能を有効または無効にします。

4. 変更内容を保存します。

次のアップデートから、Kaspersky Endpoint Security は軽量なバージョンの定義データベースをダウンロードします。

軽量なバージョンの定義データベースが使用できない場合、通常のバージョンの定義データベースに自動的に切り替えられます。

KSN プロキシ設定

Kaspersky Security Center 管理サーバーによって管理されるクライアントコンピューターは、KSN プロキシサービス経由で KSN と連携できます。

本製品が Light Agent モードで実行されている場合、KSN との直接通信はサポートされません。Kaspersky Endpoint Security は、KSN プロキシサーバーを介して KSN サーバーと通信します。

KSN プロキシサービスは次の機能を提供します：

- クライアントコンピューターはインターネットに直接アクセスしなくても、KSN にクエリを実行し、情報を送信できます。
- KSN プロキシは処理データをキャッシュすることにより、外部ネットワークとの通信チャネルの負荷を軽減し、クライアントコンピューターによって要求される情報の受信を高速化します。

既定では、KSN を有効にして KSN 声明に同意すると、本製品はプロキシサーバーを使用して Kaspersky Security Network. に接続します。本製品が使用するプロキシサーバーは TCP ポート 13111 を介した Kaspersky Security Center 管理サーバーです。このため、KSN プロキシが使用できない場合は、次の項目を検証する必要があります：

- 管理サーバーで *ksnproxy* サービスが実行されている。
- コンピューターのファイアウォールがポート 13111 をブロックしていない。

KSN プロキシの使用は、KSN プロキシを有効または無効にする、また接続のポートを設定することで設定することができます。設定するためには管理サーバーのプロパティを表示する必要があります。KSN プロキシの設定について詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。Kaspersky Endpoint Security のポリシーで個別のコンピューターに対して KSN プロキシを有効または無効にすることも可能です。

管理コンソール（MMC）で KSN プロキシを有効または無効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。
4. ［**KSN プロキシ設定**］ブロックで、［**管理サーバーを KSN プロキシサーバーとして使用する**］チェックボックスを使用して、KSN プロキシを有効または無効にします。

5. 必要に応じて、［**KSN プロキシサーバーを使用できない場合は、Kaspersky Security Network サーバーを使用する**］をオンにします。

   このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

6. 変更内容を保存します。

Web コンソールで KSN プロキシを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。

5. ［**管理サーバーを KSN プロキシサーバーとして使用する**］を使用して KSN プロキシを有効または無効にします。

6. 必要に応じて、［**KSN プロキシサーバーを使用できない場合は、Kaspersky Security Network サーバーを使用する**］をオンにします。

   このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

7. 変更内容を保存します。

KSN プロキシのアドレスが管理サーバーのアドレスと一致します。管理サーバーのドメイン名が変更された場合は、KSN プロキシアドレスを手動で更新する必要があります。

KSN プロキシのアドレスを設定するには：

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

3. **インストールパッケージ**のコンテキストメニューから［**プロパティ**］を選択します。

4. 表示されたウィンドウの［**全般**］タブで、KSN プロキシサーバーの新しいアドレスを指定します。

5. 変更内容を保存します。

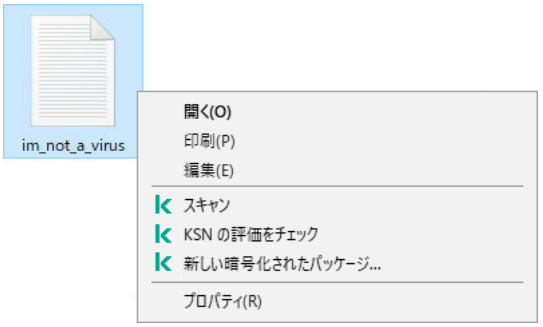
Kaspersky Security Network でのファイルの評価の確認

ファイルのセキュリティに疑問がある場合は、Kaspersky Security Network でその評判を確認できます。

Kaspersky Security Network に関する声明の条件に同意した場合、ファイルの評価を確認できます。

Kaspersky Security Network でのファイルの評価を確認するには：

ファイルコンテキストメニューを開き、**KSN の評価を見る**オプションを選択します（下の図を参照）。



ファイルコンテキストメニュー

Kaspersky Endpoint Security は、ファイルの評価を表示します：

信頼済み（Kaspersky Security Network）。次の条件の 1 つ以上をファイルが満たす場合、信頼できるものと見なされます。

- 信頼できる開発元によってデジタル署名されている。
- Kaspersky Security Network で信頼できるという評価を受けている。
- ユーザーがファイルを「許可」グループに配置した。

ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェアです。悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアについて詳しくは、カスペルスキーのウイルス百科事典を参照してください。これらのアプリケーションを信頼するリストに追加できます。

ブロック（Kaspersky Security Network）：脅威をもたらすウイルスまたはその他のアプリケーション。

不明（Kaspersky Security Network）：Kaspersky Security Network には、ファイルに関する情報はありません。定義データベースを使用して、ファイルをスキャンできます（コンテキストメニューの［**スキャン**］オプション）。

Kaspersky Endpoint Security は、ファイルの評価を決定するために使用された KSN ソリューションを表示します：*Kaspersky Security Network* または*Kaspersky Private Security Network*。

Kaspersky Endpoint Security は、ファイルに関する追加情報も表示します（下の図を参照）。



Kaspersky Security Network でのファイルの評価

暗号化された接続のスキャン

インストール後、Kaspersky Endpoint Security は、信頼する証明書のシステムストレージ（Windows 証明書ストア）に Kaspersky 証明書を追加します。Kaspersky Endpoint Security は暗号化された接続のスキャンにこの証明書を使用します。Kaspersky Endpoint Security には、Firefox および Thunderbird の信頼する証明書のシステムストレージを使用して、これらのアプリケーションのトラフィックをスキャンする機能も含まれています。

ウェブコントロール、メール脅威対策、ウェブ脅威対策、ふるまい検知および脆弱性攻撃ブロックでは、次のプロトコルで暗号化された接続を使用して送受信されるネットワークトラフィックを復号化しスキャンできます：

- SSL 3.0
- TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3

暗号化された接続のスキャンの有効化

既定では、Kaspersky Endpoint Security は暗号化された接続を常にスキャンするのではなく、保護機能によって要求された場合にのみスキャンします。

管理コンソール（MMC）で暗号化された接続のスキャンを有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。

5. ［**暗号化された接続のスキャン**］ブロックで、暗号化された接続のスキャンモードを選択します：

   - **暗号化された接続をスキャン**：Kaspersky Endpoint Security は「`https://`」で始まるアドレスの Web サイトのコンテンツにアクセスしません。
   - **保護機能の要求時に暗号化された接続をスキャンする**：Kaspersky Endpoint Security はウェブ脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。
   - **常に暗号化された接続をスキャンする**：Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。

   トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。

6. 必要に応じて、信頼するオブジェクトを追加します。

7. 暗号化された接続のスキャンに関する設定を指定します（下記の表を参照）。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（  ）。

Web コンソールと Cloud コンソールで暗号化された接続のスキャンを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**ネットワーク設定**］に移動します。

5. ［**暗号化された接続のスキャン**］で、［**暗号化された接続のスキャンは有効です**］をオンにします。
   このトグルスイッチをオフにすると、Kaspersky Endpoint Security は「`https://`」で始まるアドレスの Web サイトのコンテンツにアクセスしません。

6. ［**設定**］をクリックして、暗号化された接続のスキャンモードを選択します：

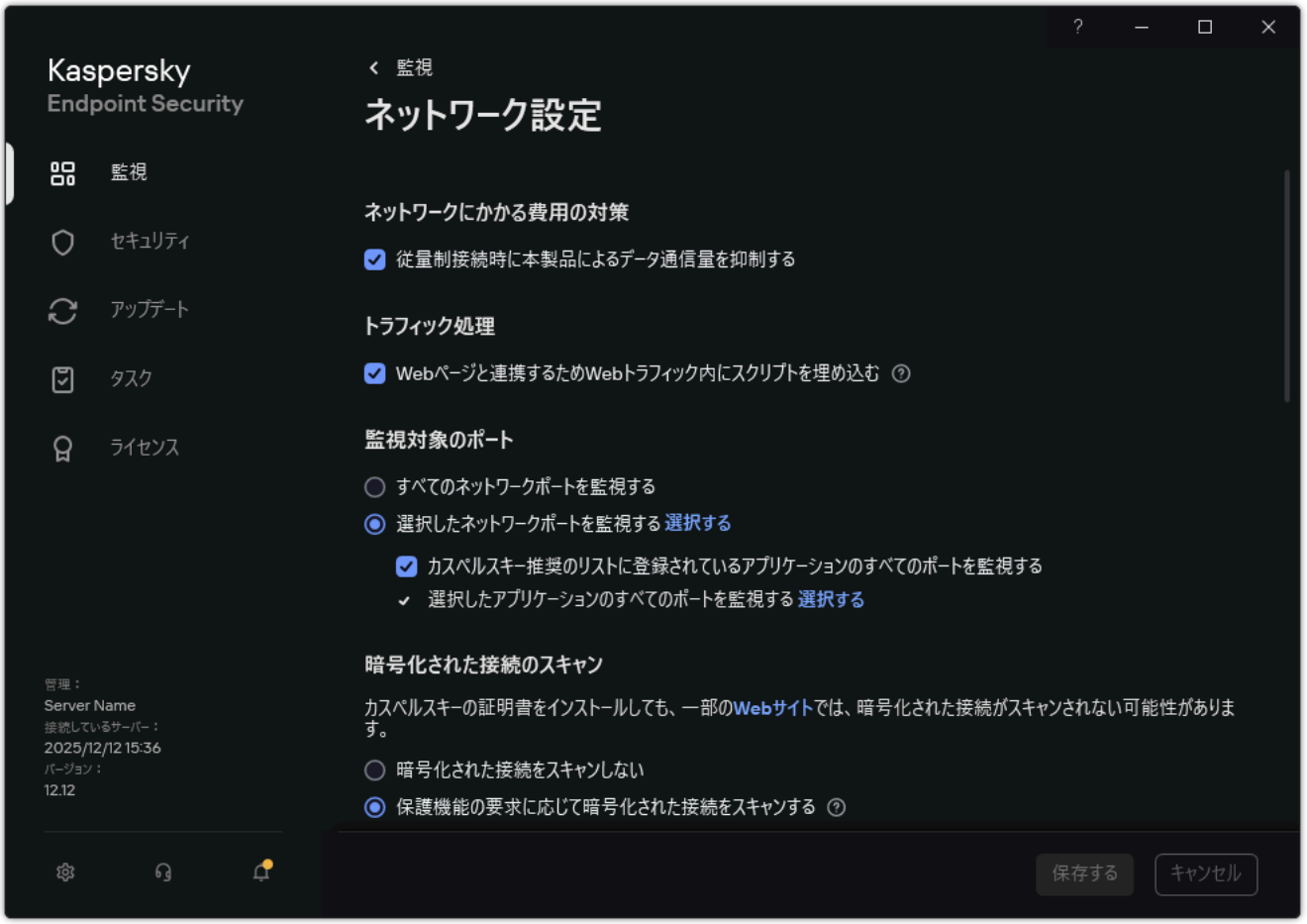
   - **保護機能の要求時に暗号化された接続をスキャンする**：Kaspersky Endpoint Security はウェブ脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。
   - **常に暗号化された接続をスキャンする**：Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。

トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。

7. 必要に応じて、信頼するオブジェクトを追加します。
8. 暗号化された接続のスキャンに関する設定を指定します（下記の表を参照）。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスで暗号化された接続のスキャンを有効にする方法

1. メインウィンドウで、 をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。



暗号化された接続のスキャンの設定

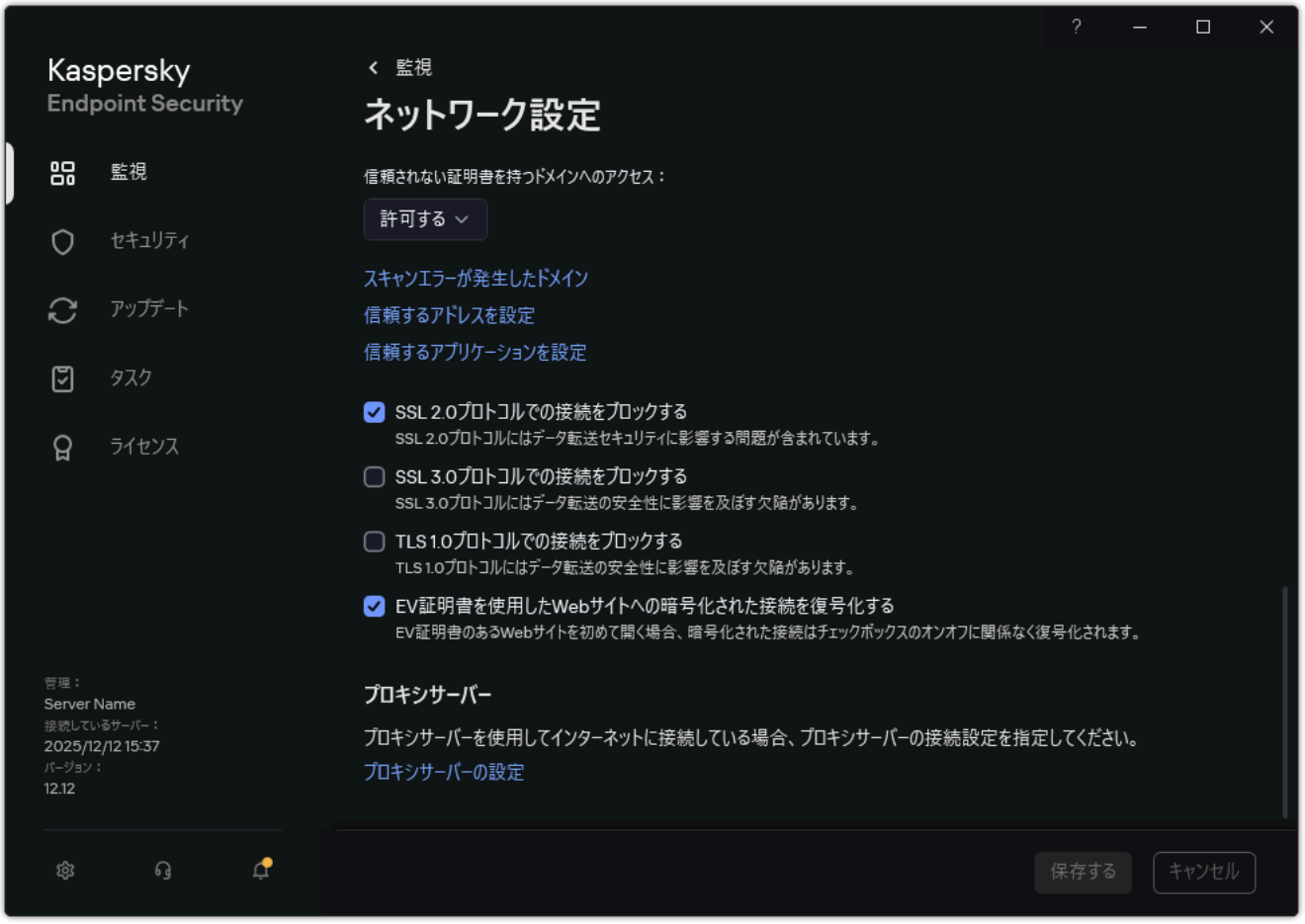
3. ［**暗号化された接続のスキャン**］ブロックで、暗号化された接続のスキャンモードを選択します：

   - **暗号化された接続をスキャンしない**：Kaspersky Endpoint Security は「`https://`」で始まるアドレスの Web サイトのコンテンツにアクセスしません。
   - **保護機能の要求に応じて暗号化された接続をスキャンする**：Kaspersky Endpoint Security はウェブ脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。
   - **常に暗号化された接続をスキャンする**：Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。

   トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。

4. 必要に応じて、信頼するオブジェクトを追加します。

5. 暗号化された接続のスキャンに関する設定を指定します（下記の表を参照）。



暗号化された接続のスキャン向けの追加設定

6. 変更内容を保存します。

パラメータ	説明
信頼するルート証明書	信頼するルート証明書のリストです。新しい認証局を導入する場合などに、Kaspersky Endpoint Security を使用してユーザーのコンピューターに信頼済みのルート証明書をインストールすることができます。本製品を使用して、Kaspersky Endpoint Security の証明書ストアに証明書を追加できます。この場合、証明書は Kaspersky Endpoint Security に対してのみ信頼済みと認識されます。言い換えると、ユーザーは新しい証明書を持つ Web サイトにブラウザーでアクセスできます。別のアプリケーションが Web サイトにアクセスしようとすると、証明書の問題により接続エラーが発生します。システムの証明書ストアに追加するには、Active Directory のグループポリシーを使用できます。
信頼されない証明書を持つドメインへのアクセス	• **許可する**：信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続を許可します。 信頼されていない証明書を持つドメインをブラウザーで開こうとすると、Kaspersky Endpoint Security は、警告とそのドメインにアクセスすることが推奨されない理由が記載された HTML ページを表示します。ユーザーは HTML 警告ページのリンクをクリックすることで、要求された Web リソースにアクセスできます。 サードパーティの製品またはサービスが信頼されていない証明書を持つドメインと接続を確立した場合、Kaspersky Endpoint Security はトラフィックをスキャンするために固有の証明書を作成します。新しい証明書のステータスは *ブロック*になっています。HTML ページはこの場合表示できず、接続はバックグラウンドモードで確立可能であるため、サードパーティの製品に信頼されていない接続に関して通知するためにこのようになっています。 • **ブロックする**：信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続をブロックします。信頼されていない証明書を持つドメインをブラウザーで開こうとすると、Kaspersky Endpoint Security は、そのドメインがブロックされる理由が記載された HTML ページを表示します。
暗号化された接続のスキャンでエラーが発生するドメインへのアクセス	• **ブロックする**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はネットワーク接続をブロックします。 • **許可して除外リストにドメインを追加する**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はエラーが発生したドメインを［スキャンエラーの発生したドメイン］リストに追加し、このドメインへのアクセスでの暗号化されたネットワークトラフィックを監視しません。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。リストに含まれる内容を消去して空にするには、［**ブロックする**］を選択する必要があります。Kaspersky Endpoint Security は、暗号化された接続のスキャンエラーのイベントを生成します。
SSL 2.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、SSL 2.0 プロトコルで確立されたネットワーク接続が監視されてブロックされます。 このチェックボックスをオフにすると、SSL 2.0 プロトコルで確立されたネットワーク接続はブロックされません。ただし、このプロトコル経由のネットワークトラフィックが監視されなくなります。
SSL 3.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、SSL 3.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、SSL 3.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。
TLS 1.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、TLS 1.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、TLS 1.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。
EV証明書を使用したWebサイトへの暗号化された接続を復号化する	EV 証明書（Extended Validation Certificate）は、Web サイトの信頼性を示すためのもので、接続のセキュリティを向上させます。Web サイトで EV 証明書が使用されている場合、ブラウザーのアドレスバーの鍵アイコンでそのことが示されます。また、アドレスバーの全体や一部の色が緑色に変わるブラウザーもあります。 このチェックボックスをオンにすると、EV 証明書を使用している Web サイトの暗号化された接続を復号化して監視します。 このチェックボックスをオフにすると、本製品は HTTPS トラフィックの通信内容にアクセスできません。そのため、HTTPS トラフィックは「`https://bing.com`」などの URL のみに基づいて監視されます。 EV 証明書を使用している Web サイトに最初にアクセスするときには、チェックボックスがオンかオフかにかかわらず、接続が復号されます。

信頼するルート証明書のインストール

新しい認証局を導入する場合などに、Kaspersky Endpoint Security を使用してユーザーのコンピューターに信頼済みのルート証明書をインストールすることができます。本製品を使用して、Kaspersky Endpoint Security の証明書ストアに証明書を追加できます。この場合、証明書は Kaspersky Endpoint Security に対してのみ信頼済みと認識されます。言い換えると、ユーザーは新しい証明書を持つ Web サイトにブラウザーでアクセスできます。別のアプリケーションが Web サイトにアクセスしようとすると、証明書の問題により接続エラーが発生します。システムの証明書ストアに追加するには、Active Directory のグループポリシーを使用できます。

管理コンソール（MMC）で信頼するルート証明書をインストールする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。
4. ［**信頼するルート証明書**］ブロックの［**追加**］をクリックします。
5. 表示されたウィンドウで、信頼するルート証明書を選択します。
   Kaspersky Endpoint Security では、拡張子 PEM、DER および CRT の証明書がサポートされます。
6. 変更内容を保存します。

Web コンソールまたは Cloud コンソールで信頼するルート証明書をインストールする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. ［**信頼するルート証明書**］リンクをクリックします。
6. 表示されたウィンドウで、［**追加**］をクリックして信頼するルート証明書を選択します。
   Kaspersky Endpoint Security では、拡張子 PEM、DER および CRT の証明書がサポートされます。
7. 変更内容を保存します。

製品インターフェイスで信頼するルート証明書をインストールする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**暗号化された接続のスキャン**］ブロックの［**証明書を表示する**］をクリックします。
4. 表示されたウィンドウで、［**追加する**］をクリックして信頼するルート証明書を選択します。
   Kaspersky Endpoint Security では、拡張子 PEM、DER および CRT の証明書がサポートされます。
5. 変更内容を保存します。

この結果、トラフィックをスキャンする際、システム証明書ストアに加えて、Kaspersky Endpoint Security は固有の証明書ストアを使用するようになります。

信頼されていない証明書を持つ暗号化された接続のスキャン

インストール後、Kaspersky Endpoint Security は、信頼する証明書のシステムストレージ（Windows 証明書ストア）に Kaspersky 証明書を追加します。Kaspersky Endpoint Security は暗号化された接続のスキャンにこの証明書を使用します。信頼されない証明書を持つドメインにアクセスする際は、ドメインへのユーザーのアクセスを許可またはブロックできます（以下の手順を参照してください）。

信頼されていない証明書を持つドメインへのユーザーのアクセスを許可した場合、Kaspersky Endpoint Security は次の処理を実行します：

- *ブラウザー*で信頼されない証明書を持つドメインにアクセスする場合は、Kaspersky Endpoint Security はカスペルスキーの証明書を使用してトラフィックをスキャンします。Kaspersky Endpoint Security は、警告とそのドメインへのアクセスが推奨されない理由に関する情報が記載された HTML ページを表示します（下図を参照してください）。ユーザーは HTML 警告ページのリンクをクリックすることで、要求された Web リソースにアクセスできます。このリンクを使用して対象の Web リソースにアクセスした後 1 時間の間は、同じドメインの他のリソースへのアクセス時に、信頼されない証明書に関する警告は表示されません。また、信頼されていない証明書を持つ暗号化された接続の確立に関するイベントも生成されます。

  場合によっては、Kaspersky Endpoint Security はブラウザーに警告の HTML ページを表示することが技術的にできません（下の図を参照）。例えば、Web リソースが古いバージョンのネットワークプロトコルや非標準のポートを使用している場合などです。このような場合、Kaspersky Endpoint Security はこのドメインへのアクセスをブロックし、ブラウザーには標準の `ERR_CONNECTION_RESET` ウィンドウが表示されます。Web リソースにアクセスするには、除外リストにドメインを追加するか、信頼する証明書を使用します。

- *サードパーティの製品またはサービス*が信頼されていない証明書を持つドメインと接続を確立した場合、Kaspersky Endpoint Security はトラフィックをスキャンするために固有の証明書を作成します。新しい証明書のステータスは*ブロック*になっています。HTML ページはこの場合表示できず、接続はバックグラウンドモードで確立可能であるため、サードパーティの製品に信頼されていない接続に関して通知するためにこのようになっています。このため、サードパーティの製品に組み込みの証明書検証ツールがあった場合は、接続が終了されることがあります。この場合、ドメインの所有者に問い合わせて信頼する接続を設定する必要があります。信頼する接続の設定ができない場合は、そのサードパーティの製品を信頼するアプリケーションのリストに追加することができます。また、信頼されていない証明書を持つ暗号化された接続の確立に関するイベントも生成されます。

管理コンソール（MMC）で信頼されていない証明書を持つ暗号化された接続のスキャンを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。
4. ［**暗号化された接続のスキャン**］ブロックの［**詳細設定**］をクリックします。
5. 表示されたウィンドウで、信頼済みでない証明書を持つドメインにアクセスした際の本製品の動作モードを［**許可する**］または［**ブロックする**］から選択します。
6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで信頼されていない証明書を持つ暗号化された接続のスキャンを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. ［**暗号化された接続のスキャン**］セクションで、［**設定**］をクリックします。
6. 表示されたウィンドウで、信頼済みでない証明書を持つドメインにアクセスした際の本製品の動作モードを［**接続を許可する**］または［**接続をブロックする**］から選択します。
7. 変更内容を保存します。

製品のインターフェイスで信頼されていない証明書を持つ暗号化された接続のスキャンを設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**暗号化された接続のスキャン**］ブロックで、信頼済みでない証明書を持つドメインにアクセスした際の本製品の動作モードを［**許可する**］または［**ブロックする**］から選択します。
4. 変更内容を保存します。



信頼されない証明書を持つドメインへのアクセスに関する警告

独自の証明書ストアにカスペルスキーの証明書を追加する

ブラウザーとメールクライアントは、証明書を使用して Web リソースのセキュリティと信頼性を検証します。この証明書は、Web リソースとユーザーの間のデータ暗号化も実現します。ほとんどのブラウザーとメールクライアントでは、信頼済み証明書ストア（Windows 証明書ストア）が使用されます。該当するのは、Google Chrome などです。一部のブラウザーとメールクライアントでは、Windows 証明書ストアではなく、独自の証明書ストアが既定で使用されます。該当するのは、Firefox や Thunderbird などです。

インストール後、Kaspersky Endpoint Security は、信頼する証明書のシステムストレージ（Windows 証明書ストア）に Kaspersky 証明書を追加します。Kaspersky Security Center がお客様の組織で配備され、ポリシーがコンピューターに適用されている場合、Kaspersky Endpoint Security はブラウザーやメールクライアントでの Windows 証明書ストアの使用を自動的に有効にして、これらのアプリケーションのトラフィックのスキャンを実行します。ポリシーがコンピューターに適用されていない場合は、ブラウザーやメールクライアントが使用する証明書ストアを選択することができます。独自の証明書ストアを選択した場合は、このストアにカスペルスキーの証明書を手動で追加します。これにより、HTTPS トラフィックで作業中のエラーを回避することができます。

Mozilla Firefox のブラウザーおよび Thunderbird メールクライアントでトラフィックをスキャンするには、暗号化された接続のスキャンを有効にする必要があります。暗号化された接続のスキャンが無効になっている場合、Mozilla Firefox ブラウザーおよび Thunderbird メールクライアントでのトラフィックはスキャンされません。MyOffice Mail および R7-Office Organizer メールクライアントのトラフィックをスキャンするには、暗号化された接続のスキャンも有効にする必要があります。

ブラウザーまたはメールエージェントの固有の証明書ストアに証明書を追加する前に、Windows コントロールパネル（インターネットプロパティ）からカスペルスキーの証明書をエクスポートします。カスペルスキーの証明書のエクスポートについて詳しくは、テクニカルサポートサイトのナレッジベースの記事を参照してください。ストアに証明書を追加する詳細な方法については、Mozilla テクニカルサポートの Web サイトなどをご覧ください。

本製品のローカルインターフェイス内でのみ証明書ストアを選択することができます。

ブラウザーやメールクライアントでの暗号化された接続のスキャンに使用する証明書ストアを選択するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**暗号化された接続のスキャン**］ブロックで、［**固有の証明書ストアを使用してMozilla製品内で暗号化された接続をスキャンする場合、次を使用する**］をオンにします。

4. 証明書ストアを選択します：

   - **Windowsの証明書ストア（推奨）**：カスペルスキーのルート証明書は Kaspersky Endpoint Security のインストール中にこのストアに追加されます。

   - **固有の証明書ストア**：Mozilla Firefox および Thunderbird は独自の証明書ストアを使用します。Mozilla 証明書ストアが選択されている場合、カスペルスキーのルート証明書をブラウザーのプロパティを使用してこのストアに手動で追加する必要があります。

     MyOffice Mail および R7-Office Organizer メールクライアントも、独自の証明書ストアを使用します。

5. 変更内容を保存します。

暗号化された接続をスキャンから除外する

Web リソースの多くは暗号化された接続を使用しています。カスペルスキーは［暗号化された接続のスキャン］を有効にすることを推奨します。暗号化された接続のスキャンが業務に関連したアクティビティを妨げる場合などに、Web サイトを［*信頼するアドレス*］を参照する例外に追加します。この場合 Kaspersky Endpoint Security は、ウェブ脅威対策、メール脅威対策、ウェブコントロールが動作している間は信頼する URL の HTTPS トラフィックはスキャンしません。

信頼するアプリケーションが暗号化された接続を使用している場合は、このアプリケーションの暗号化された接続のスキャンを無効にすることができます。例えば、独自の認証で 2 ファクタ認証を使用するクラウドストレージアプリケーションなどに対して暗号化された接続のスキャンを無効にできます。

管理コンソール（MMC）で暗号化された接続のスキャンから Web アドレスを除外する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。
4. ［**暗号化された接続のスキャン**］ブロックの［**信頼するアドレスを設定**］をクリックします。
5. ［**追加**］をクリックします。
6. Kaspersky Endpoint Security がドメインにアクセスするときに確立された暗号化された接続をスキャンしないようにする場合は、ドメイン名、または IP アドレスを入力します。

   Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「`*`」をサポートします。

   > Kaspersky Endpoint Security は IP アドレスで記号「`*`」をサポートしません。サブネットマスクを使用して IP アドレス範囲を選択することができます（例：198.51.100.0/24）。

例：

- 「`domain.com`」と入力すると次のアドレスが含まれます：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。サブドメイン（例：`subdomain.domain.com`）は含まれません。
- 「`subdomain.domain.com`」と入力すると次のアドレスが含まれます：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。「`domain.com`」ドメインは含まれません。
- 「`*.domain.com`」と入力すると次のアドレスが含まれます：`https://movies.domain.com`、`https://images.domain.com/page123`。「`domain.com`」ドメインは含まれません。

7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで暗号化された接続のスキャンから Web アドレスを除外する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. ［**暗号化された接続のスキャン**］ブロックの［**信頼するドメイン**］をクリックします。
6. ［**追加**］をクリックします。
7. Kaspersky Endpoint Security がドメインにアクセスするときに確立された暗号化された接続をスキャンしないようにする場合は、ドメイン名、または IP アドレスを入力します。
   Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「`*`」をサポートします。

   > Kaspersky Endpoint Security は IP アドレスで記号「`*`」をサポートしません。サブネットマスクを使用して IP アドレス範囲を選択することができます（例：198.51.100.0/24）。

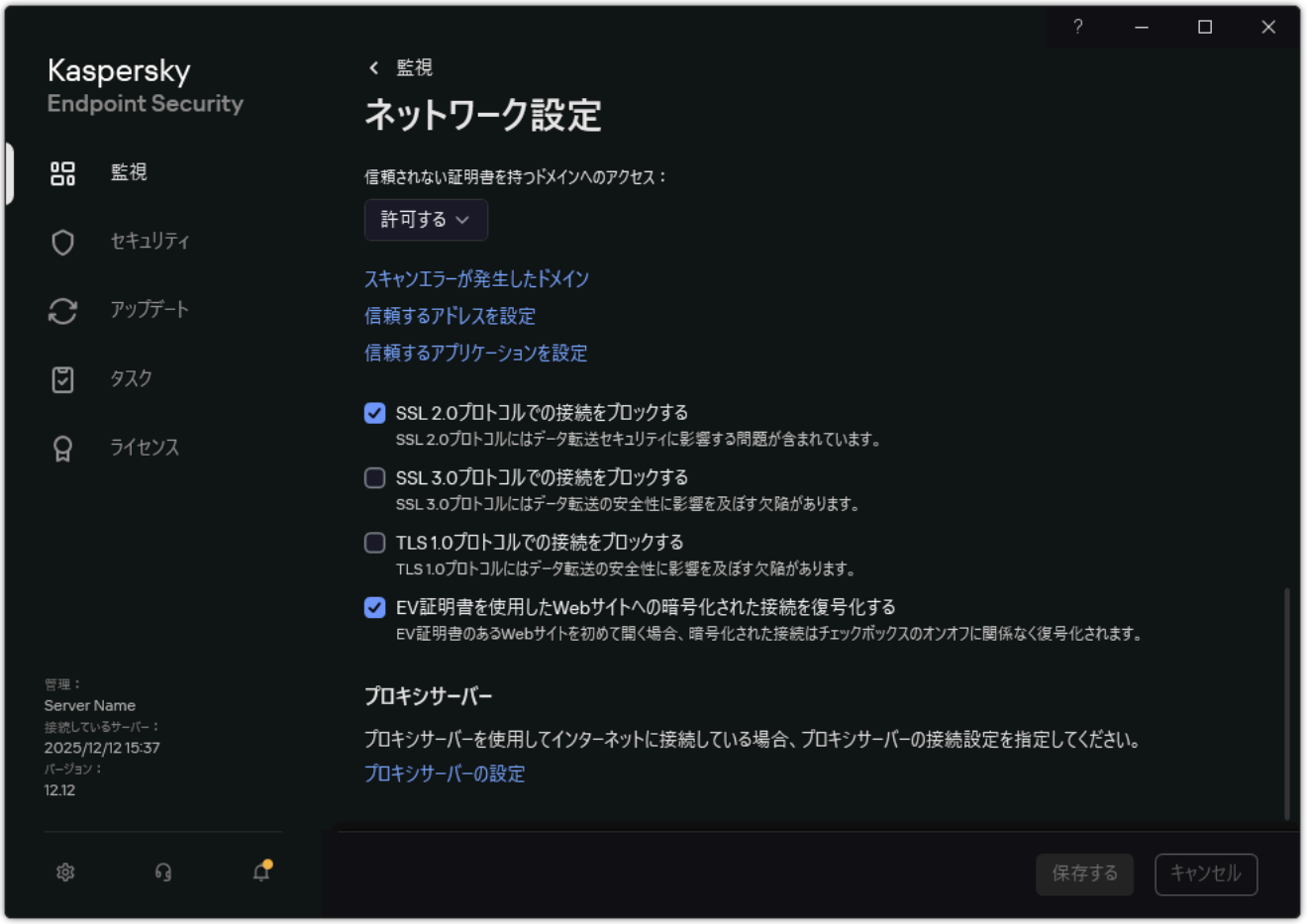
   例：

   - 「`domain.com`」と入力すると次のアドレスが含まれます：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。サブドメイン（例：`subdomain.domain.com`）は含まれません。
   - 「`subdomain.domain.com`」と入力すると次のアドレスが含まれます：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。「`domain.com`」ドメインは含まれません。
   - 「`*.domain.com`」と入力すると次のアドレスが含まれます：`https://movies.domain.com`、`https://images.domain.com/page123`。「`domain.com`」ドメインは含まれません。

8. 変更内容を保存します。

製品インターフェイスで暗号化された接続のスキャンから Web アドレスを除外する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。



製品のネットワーク設定

3. ［**暗号化された接続のスキャン**］ブロックの［**信頼するアドレスを設定**］をクリックします。
4. ［**追加**］をクリックします。
5. Kaspersky Endpoint Security がドメインにアクセスするときに確立された暗号化された接続をスキャンしないようにする場合は、ドメイン名、または IP アドレスを入力します。

   Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「`*`」をサポートします。

   > Kaspersky Endpoint Security は IP アドレスで記号「`*`」をサポートしません。サブネットマスクを使用して IP アドレス範囲を選択することができます（例：198.51.100.0/24）。

例：

- 「`domain.com`」と入力すると次のアドレスが含まれます：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。サブドメイン（例：`subdomain.domain.com`）は含まれません。
- 「`subdomain.domain.com`」と入力すると次のアドレスが含まれます：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。「`domain.com`」ドメインは含まれません。
- 「`*.domain.com`」と入力すると次のアドレスが含まれます：`https://movies.domain.com`、`https://images.domain.com/page123`。「`domain.com`」ドメインは含まれません。

6. 変更内容を保存します。

既定では、Kaspersky Endpoint Security はエラーが発生した場合は暗号化された接続のスキャンを行わず、［*スキャンエラーの発生したドメイン*］のリストに追加します。Kaspersky Endpoint Security は各ユーザーごとにリストを作成し、Kaspersky Security Center にはデータを送信しません。スキャンエラーが発生したときに接続をブロックすることができます。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。

スキャンエラーが発生したドメインのリストを表示するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**暗号化された接続のスキャン**］ブロックの［**スキャンエラーが発生したドメイン**］をクリックします。

スキャンエラーの発生したドメインのリストが開きます。リストをリセットするには、ポリシー内でスキャンエラーが発生した場合の接続のブロックを有効にし、ポリシーを適用してからパラメータを初期値にリセットしてからポリシーを再度適用します。

カスペルスキーは、Kaspersky Endpoint Security が製品の設定に関係なくチェックの対象外にする*グローバル除外リスト*を作成しています。

暗号化されたトラフィックのスキャンのグローバル除外リストを表示するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**暗号化された接続のスキャン**］ブロックの信頼済み Web サイトのリンクのリストをクリックします。

カスペルスキーによりまとめられた Web サイトのリストが開きます。Kaspersky Endpoint Security はこのリストに記載された Web サイトとの保護された接続はスキャンしません。このリストは、Kaspersky Endpoint Security の定義データベースとモジュールがアップデートされたときに更新される可能性があります。

データの消去

Kaspersky Endpoint Security では、タスクを使用してユーザーのコンピューターからデータをリモート消去できます。

Kaspersky Endpoint Security は次の方法でデータを削除します：

- サイレントで実行
- ハードディスクおよびリムーバブルドライブのデータが対象
- コンピューター上のすべてのユーザーアカウントが対象

Kaspersky Endpoint Security は、使用しているライセンスの種別に関わりなく、ライセンスの有効期限が切れている場合でも、*データの消去*タスクを実行します。

データ消去で利用できるモード

このタスクでは、次のいずれかのモードでデータを削除できます：

- 即座にデータを削除

  このモードは、ディスク上の空き容量を確保するために古くて不要になったデータを削除する用途などで使用できます。

- 接続が一定期間なかったときにデータを削除

  このモードは、ノート PC の紛失や盗難時に、ノート PC のデータが流出しないように保護する目的などで使用できます。社内ネットワークの外に持ち出されたノート PC が、長期間 Kaspersky Security Center に接続しなかった場合にデータを自動的に削除するように設定できます。

タスクのプロパティでデータを削除するスケジュールを設定することはできません。データを削除するタイミングは、「タスクを手動で開始した直後」または「Kaspersky Security Center と接続していないまま一定期間が経過した場合」のいずれかのかたちでのみ指定できます。

制限事項

データ消去には次の制限事項があります：

- Kaspersky Security Center の管理者のみが、*データの消去*タスクを管理できます。Kaspersky Endpoint Security のローカルインターフェイスでは、タスクの開始を設定できません。
- NTFS ファイルシステムの場合、Kaspersky Endpoint Security はメインデータストリームの名前のみ削除します。代替データストリーム名は削除できません。
- シンボリックリンクファイルを削除すると、Kaspersky Endpoint Security はシンボリックリンクでパスが指定されているファイルも削除します。

データの消去タスクの作成

ユーザーのコンピューター上でデータを削除するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**データの消去**］を選択します。
   c. ［**タスク名**］に「*データの消去（盗難対策として）*」などの簡潔な名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。

   タスクの範囲内の管理グループに新しいコンピューターが追加された場合、即座にデータを消去するタスクについては、タスクが完了してから 5 分以内にコンピューターが追加された場合にのみ、この新しいコンピューターでもタスクが実行されます。

5. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
6. Kaspersky Endpoint Security の **データの消去**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
7. ［**アプリケーション設定**］タブを選択します。
8. データの削除方法を選択します：
   - **OS の機能で削除する**：Kaspersky Endpoint Security は OS の機能を使用して、ファイルをごみ箱には送らずに削除します。
   - **完全に削除し、復元できないようにする**：Kaspersky Endpoint Security はランダムなデータを使用してファイルを上書きします。削除後にデータを復元することは、事実上不可能です。
9. 接続が一定期間なかったときにデータを削除する場合、［**Kaspersky Security Center への接続がない期間が次を超えた場合、自動的にデータを削除する**］をオンにします。日数を指定します。

   接続が一定期間なかったときにデータを削除するタスクは、Kaspersky Security Center に接続されていない期間が指定した期間を超えるたびに毎回実行されます。

接続が一定期間なかった場合のデータの削除を設定する場合は、従業員の業務スケジュールが異なる可能性があることに留意してください。また、オフラインでコンピューターを使用するユーザーなどの業務スケジュールも考慮に入れてください。オフラインのコンピューターとモバイルユーザーについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

コンピューターの電源がオフになっており、設定された期間よりも長く接続されていない場合、コンピューターの電源がオンになった直後にデータが削除されることはありません。本製品は、1時間待機してから Kaspersky Security Center と同期します。これは、たとえば休暇に出かける前にコンピューターの電源をオフにしたユーザーのコンピューターで、データが許可なく削除されるのを防ぐために必要になります。

チェックボックスをオフにすると、Kaspersky Security Center と同期されたタイミングで即座にタスクが実行されます。

10. 削除するオブジェクトのリストを作成します：

- **フォルダー**：Kaspersky Endpoint Security は、指定したフォルダーとそのサブフォルダーに含まれるファイルをすべて削除します。マスクや環境変数を使用してのフォルダーのパスの指定はサポートされません。
- **ファイルの拡張子による指定**：Kaspersky Endpoint Security は、リムーバブルドライブも含めたコンピューター上のすべてのドライブで、指定した拡張子のファイルを検出します。複数の拡張子を指定するには、区切り文字として「`;`」または「`,`」を使用してください。
- **定義済みの範囲**：次の領域からファイルが削除されます。
  - **ドキュメント**：オペレーティングシステムの標準の［ドキュメント］フォルダー内のファイルとそのサブフォルダー。
  - **Cookie**：ユーザーがアクセスした Web サイトのデータ（ユーザー認証データなど）をブラウザーが保存するファイル。
  - **デスクトップ**：オペレーティングシステムの標準の［デスクトップ］フォルダー内のファイルとそのサブフォルダー。
  - **Internet Explorer の一時ファイル**：Web ページ、画像、メディアファイルのコピーなど、Internet Explorer の動作に関連する一時ファイル。
  - **一時ファイル**：コンピューターにインストールされたアプリケーションの動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。
  - **Outlook ファイル**：Outlook メールクライアントの動作に関連するファイル (データファイル (PST)、オフラインデータファイル (OST)、オフラインアドレス帳ファイル (OAB)、および個人のアドレス帳ファイル (PAB))。
  - **ユーザープロファイル**：ローカルユーザーアカウントのオペレーティングシステム設定を保存している一連のファイルおよびフォルダー。

各タブで削除するオブジェクトのリストを作成できます。Kaspersky Endpoint Security は、統合リストを作成し、タスクの完了時にこのリストからファイルを削除します。

Kaspersky Endpoint Security の動作に関連するファイルは削除できません。

11. 変更内容を保存します。

12. タスクの横にあるチェックボックスをオンにします。

13. ［**開始**］をクリックします。

選択したモードに応じて、ユーザーのコンピューターのデータが削除されます（即座にまたは一定期間接続がなかったときに）。ユーザーがファイルを使用中だったなどの理由で、一部のファイルを Kaspersky Endpoint Security が削除できなかった場合、これらのファイルの削除が再試行されることはありません。データの削除を完了するには、タスクをもう一度実行してください。

コンピューターのコントロール

ウェブコントロール

ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します（下図を参照）。

ウェブコントロールを使用するには、本製品の初期設定を完了する必要があります。

- HTTPS トラフィックを監視するには、 暗号化された接続のスキャンを有効にします（既定では有効になっています）。
- Kaspersky Endpoint Security が監視する必要があるポートを選択します（既定では、本製品はすべてのポートを監視します）。
- Kaspersky Endpoint Security がトラフィックを監視するアプリケーションを選択します。ほとんどのブラウザーは、カスペルスキーが推奨するアプリケーションのリストに含まれています。ブラウザーがリストにない場合は、手動で追加してください。
- Web トラフィックに Web ページとの連携スクリプトを埋め込むことを推奨します（既定では、スクリプトの挿入は無効になっています）。このスクリプトにより、ウェブコントロールのイベントをアプリケーションイベントログ、OS イベントログ、レポートに登録できるようになります。

Web サイトへのアクセスの管理方法

ウェブコントロールでは、次の設定を使用して Web サイトへのアクセスを管理できます：

- **Web サイトのカテゴリ**：Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。たとえば、「*SNS*」カテゴリまたはその他のカテゴリのサイトに対してユーザーのアクセスを制限することができます。
- **データ種別**：Web サイトのデータへのユーザーのアクセスを制限して、画像を表示できないようにするなどの使い方ができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。

  圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「*アーカイブ*」として識別し、「*グラフィック*」とは識別しません。

- **個別のアドレス**：URL を入力したり、マスクを使用して Web アドレスを指定できます。

Web サイトへのアクセスを管理するために、複数の設定を同時に組み合わせて使用できます。たとえば、Web サイトのカテゴリが「*Web メール*」の場合にのみ「*Office アプリケーションのファイル*」へのアクセスを制限するような使い方ができます。

Web サイトへのアクセスルール

ウェブコントロールは、*アクセスルール*を使用して Web サイトへのユーザーアクセスを管理します。Web サイトへのアクセスルールでは、次のような詳細設定を指定できます。

- ルールを適用するユーザー：

  ブラウザーによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。

- ルールのスケジュール：

  ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

アクセスルールの優先順位：

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。適用例として、たとえば、Kaspersky Endpoint Security によって企業ポータルが「ソーシャルネットワーク」サイトと判定されているケースを考えます。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「*SNS*」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 2 つのルールを作成します。この場合、企業ポータルへのアクセスルールには、ソーシャルネットワークカテゴリへのアクセルルールよりも高い優先順位を割り当てる必要があります。





ウェブコントロールによって表示されるメッセージ

Web リソースへのアクセスルールの追加

*Web リソースアクセスルール*は、一連のフィルターと、Web リソースにユーザーがアクセスした時に、Kaspersky Endpoint Security によって適用される一連の処理で構成されています。アクセスルールには、ルールのスケジュールを含めることができます。

1000 件を超える Web リソースアクセスルールを作成することは避けてください。システムが不安定になる可能性があります。

Web リソースアクセスルールは一連のフィルターと、ルールスケジュールに示されている期間中、ルールで指定されている Web リソースにユーザーがアクセスしたときに、Kaspersky Endpoint Security によって実行される一連の処理で構成されています。フィルターを使用することで、ウェブコントロールによってアクセスが管理される Web リソースの対象範囲を正確に指定できます。

次のフィルターを使用できます：

- **コンテンツによるフィルター**：ウェブコントロールでは、Web リソースがコンテンツとデータの種類で分類されます。これらのカテゴリにあてはまるコンテンツとデータの種類を含む Web リソースへのユーザーアクセスを管理できます。選択したコンテンツカテゴリまたはデータ種別カテゴリに属する Web リソースにユーザーがアクセスすると、ルールで指定された処理が実行されます。

- **Web リソースアドレスによるフィルター**：すべての Web リソースアドレス、個別の Web リソースアドレス、Web リソースのアドレスグループのユーザーアクセスを管理できます。

  コンテンツによるフィルターと Web リソースアドレスによるフィルターの両方を指定していて、指定した Web リソースアドレスまたは Web リソースのアドレスグループが、選択したコンテンツカテゴリやデータ種別カテゴリに属しているときには、両方のフィルターの条件を満たす Web リソースへのアクセスが制限されます。選択したコンテンツカテゴリやデータ種別カテゴリに属するすべての Web リソースへのアクセスが制限されるわけではありません。代わりに、指定した Web リソースアドレスまたは Web リソースアドレスグループに限定してアクセスが制限されます。

- **ユーザー名またはユーザーグループ名によるフィルター**：ルールによって管理される Web リソースへのアクセス権を持つユーザーまたはユーザーグループの名前を指定できます。

- **ルールのスケジュール**：ルールのスケジュールを指定できます。ルールのスケジュールは、Kaspersky Endpoint Security がルールによってカバーされた Web リソースへのアクセスを監視する期間を決定します。

Kaspersky Endpoint Security のインストール後、ウェブコントロールのルールリストは空ではありません。［*既定のルール*］がプリセットされています。このルールは他のルールの対象範囲に含まれないすべての Web リソースに適用され、すべてのユーザーによるこれらの Web リソースへのアクセスを許可またはブロックします。

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。適用例として、たとえば、Kaspersky Endpoint Security によって企業ポータルが「ソーシャルネットワーク」サイトと判定されているケースを考えます。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「*SNS*」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 2 つのルールを作成します。この場合、企業ポータルへのアクセスルールには、ソーシャルネットワークカテゴリへのアクセルルールよりも高い優先順位を割り当てる必要があります。

管理コンソール（MMC）で Web リソースアクセスルールを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。

4. ［**ウェブコントロール**］チェックボックスをオンにします。

5. ［**ウェブコントロール設定**］ブロックの［**追加**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが表示されます。

6. Web リソースアクセスルールを設定します（下の表を参照）。

7. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

   > ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

   チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

8. 変更内容を保存します。

Web コンソールと Cloud コンソールで Web リソースアクセスルールを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**ウェブコントロール**］に移動します。

5. ［**ウェブコントロールは有効です**］をオンにします。

6. ［**ルールリスト**］ブロックの［**追加**］をクリックします。

7. Web リソースアクセスルールを設定します（下の表を参照）。

8. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

   > ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

   チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

9. 変更内容を保存します。

製品のインターフェイスで Web リソースアクセスルールを追加する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**ウェブコントロール**］をオンにします。

4. ［**設定**］ブロックの［**Web リソースへのアクセスルール**］をクリックします。

5. 表示されたウィンドウで、［**追加**］をクリックします。

［**Web リソースへのアクセスルール**］ウィンドウが表示されます。

6. Web リソースアクセスルールを設定します（下の表を参照）。

7. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

8. 変更内容を保存します。

これにより、新しいウェブコントロールルールがリストに追加されます。必要に応じて、ウェブコントロールルールの優先度を変更します。リストから削除しなくても、トグルスイッチを使用していつでも Web リソースアクセスルールを無効にすることもできます。

ウェブコントロールルールのパラメータ

パラメータ	説明
ルール名	ウェブコントロールルールの名前。
状態	• **オン** • **オフ** トグルスイッチを使用していつでも Web リソースのアクセスルールを無効にすることができます。
処理	• **許可**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。 • **ブロック**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。 • **警告する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。
フィルターの内容	• **コンテンツカテゴリ**：Web リソースへのユーザーのアクセスをカテゴリ（たとえば *SNS* カテゴリなど）で制御することができます。 • **データ種別**：Web リソースへのユーザーのアクセスを公開されているデータの特定の種別（たとえばグラフィックなど）で制御することができます。
適用するアドレス	• **すべてのアドレス**：Web リソースをアドレスでフィルターしません。 • **個別のアドレス**：リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。 暗号化された接続のスキャンがオフの場合、HTTPS プロトコルについてはサーバー名でのみフィルターできます。
ユーザー	• **すべてのユーザー**：Web リソースを特定のユーザーでフィルターしません。 • **個別のユーザーまたはグループ**：Web リソースを特定のユーザーでのみフィルターします。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。
ルールのスケジュール	ルールのスケジュールは、Kaspersky Endpoint Security がルールによってカバーされた Web リソースへのアクセスを監視する期間を決定します。ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

Web リソースアドレスによるフィルター

個々の Web リソースへのアクセスを制御するには、ウェブコントロールルールを作成し、Web アドレスのリストを作成し、ウェブコントロールの処理を選択する必要があります。Web アドレスのリストを作成する際は、URL アドレスを入力することも、マスクを使用することもできます。

ルールには、ルールのスケジュールと、ルールが適用されるユーザーのリストを含めることができます。たとえば、Web サイトへのアクセスを就業時間中のみに限定したり、特定のグループのユーザーに対して Web サイトへのアクセスを許可したりできます。

管理コンソール（MMC）で Web リソースアドレスフィルターを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。
4. ［**ウェブコントロール**］チェックボックスをオンにします。
5. ［**ウェブコントロール設定**］ブロックの［**追加**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが表示されます。
6. Web リソースアクセスルールを設定します：
   a. ［**名前**］にルール名を入力します。
   b. ［**適用するアドレス**］から［**個別のアドレス**］を選択します。
   c. Web リソースのアドレスのリストを作成します。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。

      暗号化された接続のスキャンがオフの場合、HTTPS プロトコルについてはサーバー名でのみフィルターできます。

   d. ［**適用するユーザー**］ドロップダウンリストで、関連するユーザーのフィルターを選択します：
      - **すべてのユーザー**：Web リソースをアドレスでフィルターしません。
      - **個別のユーザーまたはグループ**：リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

e. ［**処理**］ドロップダウンリストで、オプションを選択します：

- **許可**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
- **ブロック**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
- **警告する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

f. ［**ルールのスケジュール**］ドロップダウンリストで、スケジュールを選択するか、新しいスケジュールを作成します。

7. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

8. 変更内容を保存します。

Web コンソールと Cloud コンソールで Web リソースアドレスフィルターを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**ウェブコントロール**］に移動します。
5. ［**ウェブコントロールは有効です**］をオンにします。
6. ［**ルールリスト**］ブロックの［**追加**］をクリックします。
7. Web リソースアクセスルールを設定します：
   a. ［**ルール名**］にルール名を入力します。
   b. Web リソースのアクセスルールに［**有効**］を選択します。
      リストから削除しなくても、トグルスイッチを使用していつでも Web リソースアクセスルールを無効にすることができます。

c. ［**処理**］ブロックで、関連するオプションを選択します。

- **許可する**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
- **ブロックする**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
- **通知する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

d. ［**範囲**］で、［**個別の Web サイト**］を選択します。

e. コンテンツフィルターを設定します。

- **個別のアドレス**：Web リソースのアドレスのリストを作成します。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。

  > 暗号化された接続のスキャンがオフの場合、HTTPS プロトコルについてはサーバー名でのみフィルターできます。

- **データ種別**：Web リソースへのユーザーのアクセスを公開されているデータの特定の種別（たとえばグラフィックなど）で制御することができます。

f. ［**ユーザーまたはグループ**］で、ウェブコントロールでルールを適用するユーザーを選択します。

リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

g. ［**アクセススケジュール**］ブロックで、スケジュールを選択するか、新しいスケジュールを作成します。

8. 変更内容を保存します。

アプリケーションインターフェイスで Web リソースアドレスフィルターを有効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**設定**］ブロックの［**Web リソースへのアクセスルール**］をクリックします。
4. 表示されたウィンドウで、［**追加**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが表示されます。
5. ［**ルール名**］にルール名を入力します。
6. Web リソースのアクセスルールに［**オン**］を選択します。
   トグルスイッチを使用していつでも Web リソースのアクセスルールを無効にすることができます。
7. ［**処理**］ブロックで、関連するオプションを選択します。

   - **許可**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
   - **ブロック**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
   - **警告する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

8. ［**適用するアドレス**］で、［**個別のアドレス**］を選択します。

   Web リソースのアドレスのリストを作成します。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。

   > 暗号化された接続のスキャンがオフの場合、HTTPS プロトコルについてはサーバー名でのみフィルターできます。

9. ［**ユーザー**］ブロックで、ユーザーのフィルターを選択します。

   - **すべてのユーザー**：Web リソースを特定のユーザーでフィルターしません。
   - **個別のユーザーまたはグループ**：リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

10. ［**ルールのスケジュール**］ドロップダウンリストで、スケジュールを選択するか、新しいスケジュールを作成します。

11. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

    > ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

    チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

12. 変更内容を保存します。

これにより、新しいウェブコントロールルールがリストに追加されます。必要に応じて、ウェブコントロールルールの優先度を変更します。リストから削除しなくても、トグルスイッチを使用していつでも Web リソースアクセスルールを無効にすることもできます。

Web リソースコンテンツによるフィルター

Web リソースコンテンツでアクセスを制御するために、ウェブコントロールにはカテゴリフィルターとデータ種別フィルターが用意されています。

Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。たとえば、「*SNS*」カテゴリまたはその他のカテゴリのサイトに対してユーザーのアクセスを制限することができます。

画像を非表示にするなど、データ種別に基づいて、Web サイトへのユーザーのアクセスを制限することができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。ウェブコントロールは、次のデータ種別を識別します：

- 映像
- 音声
- Office アプリケーションのファイル
- 実行ファイル
- アーカイブ
- グラフィック
- スクリプト

圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「*アーカイブ*」として識別し、「グラフィック」とは識別しません。

ルールには、ルールのスケジュールと、ルールが適用されるユーザーのリストを含めることができます。たとえば、Web サイトへのアクセスを就業時間中のみに限定したり、特定のグループのユーザーに対して Web サイトへのアクセスを許可したりできます。

管理コンソール（MMC）で Web リソースコンテンツフィルターを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。
4. ［**ウェブコントロール**］チェックボックスをオンにします。
5. ［**ウェブコントロール設定**］ブロックの［**追加**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが表示されます。
6. Web リソースアクセスルールを設定します：
   a. ［**名前**］にルール名を入力します。
   b. ［**コンテンツのフィルタリング**］ドロップダウンリストで、関連するコンテンツフィルターを選択します：
      - **コンテンツカテゴリ**：Web リソースへのユーザーのアクセスをカテゴリ（たとえば *SNS* カテゴリなど）で制御することができます。
      - **データ種別**：Web リソースへのユーザーのアクセスを公開されているデータの特定の種別（たとえばグラフィックなど）で制御することができます。
      - **コンテンツカテゴリとデータ種別**：コンテンツカテゴリとデータ種別によるフィルターが有効になります。

フィルターを選択したら、フィルターのパラメータを設定します。

c. ［**適用するユーザー**］ドロップダウンリストで、関連するユーザーのフィルターを選択します：

- **すべてのユーザー**：Web リソースをアドレスでフィルターしません。
- **個別のユーザーまたはグループ**：リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

d. ［**処理**］ドロップダウンリストで、オプションを選択します：

- **許可**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
- **ブロック**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
- **警告する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

e. ［**ルールのスケジュール**］ドロップダウンリストで、スケジュールを選択するか、新しいスケジュールを作成します。

7. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

> ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

8. 変更内容を保存します。

Web コンソールと Cloud コンソールで Web リソースコンテンツフィルターを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**ウェブコントロール**］に移動します。
5. ［**ウェブコントロールは有効です**］をオンにします。
6. ［**ルールリスト**］ブロックの［**追加**］をクリックします。

7. Web リソースアクセスルールを設定します：

a. ［**ルール名**］にルール名を入力します。

b. Web リソースのアクセスルールに［**有効**］を選択します。

トグルスイッチを使用していつでも Web リソースのアクセスルールを無効にすることができます。

c. ［**処理**］ブロックで、関連するオプションを選択します。

- **許可する**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
- **ブロックする**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
- **通知する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

d. ［**範囲**］で、［**コンテンツカテゴリ**］を選択します。

e. コンテンツフィルターを設定します。

- **コンテンツカテゴリ**：Web リソースへのユーザーのアクセスをカテゴリ（たとえば *SNS* カテゴリなど）で制御することができます。
- **データ種別**：Web リソースへのユーザーのアクセスを公開されているデータの特定の種別（たとえばグラフィックなど）で制御することができます。

f. ［**ユーザーまたはグループ**］で、ウェブコントロールでルールを適用するユーザーを選択します。

リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

g. ［**アクセススケジュール**］ブロックで、スケジュールを選択するか、新しいスケジュールを作成します。

8. 変更内容を保存します。

アプリケーションインターフェイスで Web リソースコンテンツフィルターを有効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**設定**］ブロックの［**Web リソースへのアクセスルール**］をクリックします。
4. 表示されたウィンドウで、［**追加**］をクリックします。
   ［**Web リソースへのアクセスルール**］ウィンドウが表示されます。
5. ［**ルール名**］にルール名を入力します。
6. Web リソースのアクセスルールに［**オン**］を選択します。
   トグルスイッチを使用していつでも Web リソースのアクセスルールを無効にすることができます。
7. ［**処理**］ブロックで、関連するオプションを選択します。

   - **許可**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスが許可されます。
   - **ブロック**：ウェブコントロールによって、ルールのパラメータに一致する Web リソースへのアクセスがブロックされて、Web サイトへのアクセスが拒否されたというメッセージが表示されます。
   - **警告する**：ユーザーがルールに一致する Web リソースへのアクセスを取得しようとすると、ウェブコントロールによって、その Web リソースへのアクセスは推奨されないという警告が表示されます。ユーザーは警告メッセージのリンクを使用して、要求された Web リソースにアクセスできます。

8. ［**フィルターの内容**］で、関連するコンテンツフィルターを選択します。

   - **コンテンツカテゴリ**：Web リソースへのユーザーのアクセスをカテゴリ（たとえば *SNS* カテゴリなど）で制御することができます。
   - **データ種別**：Web リソースへのユーザーのアクセスを公開されているデータの特定の種別（たとえばグラフィックなど）で制御することができます。

   コンテンツフィルターを設定するには：

   a. ［**設定**］リンクをクリックします。

   b. 目的のコンテンツカテゴリまたはデータ種別名の横にあるチェックボックスをオンにします。

   コンテンツカテゴリまたはデータ種別名の横にあるチェックボックスをオンにすると、Kaspersky Endpoint Security はこのルールを適用して、選択したコンテンツカテゴリまたはデータ種別に属する Web リソースへのアクセスを管理します。

   c. Web リソースのアクセスルールを設定するウィンドウに戻ります。

9. ［**ユーザー**］ブロックで、ユーザーのフィルターを選択します。

   - **すべてのユーザー**：Web リソースをアドレスでフィルターしません。
   - **個別のユーザーまたはグループ**：リストにある Web リソースのアドレスのみをフィルターします。URL を入力したり、マスクを使用して Web アドレスを指定できます。また、Web リソースのアドレスのリストをテキストファイルでエクスポートすることもできます。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。ルールを適用するユーザーのリストを作成するには：

     a. ［**追加**］をクリックします。

     b. 表示されたウィンドウで、Web リソースのアクセスルールを適用するユーザーまたはユーザーグループを選択します。

     c. Web リソースのアクセスルールを設定するウィンドウに戻ります。

10. ［**ルールのスケジュール**］で、目的のスケジュール名を選択するか、選択したルールスケジュールに基づく新しいスケジュールを作成します。次の手順に従います：

    a. ［**編集または新規追加**］をクリックします。

    b. 表示されたウィンドウで、［**追加**］をクリックします。

    c. 表示されたウィンドウで、ルールスケジュール名を入力します。

    d. ユーザーの Web リソースのアクセスのスケジュールを設定します。

    e. Web リソースのアクセスルールを設定するウィンドウに戻ります。

11. ウェブコントロールを使用して、ポリシーの適用直後に、禁止された Web リソースとの接続を終了する場合は、［**ルール適用後にアクティブなブラウザーセッションを終了する**］をオンにします。

ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。

チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。

12. 変更内容を保存します。

これにより、新しいウェブコントロールルールがリストに追加されます。必要に応じて、ウェブコントロールルールの優先度を変更します。リストから削除しなくても、トグルスイッチを使用していつでも Web リソースアクセスルールを無効にすることもできます。

Web リソースへのアクセスルールのテスト

ウェブコントロールの設定時に、ユーザーの作業で必要になる Web リソースへのアクセスを誤ってブロックしてしまうことがあるかもしれません。どのウェブコントロールルールが Web リソースへのアクセスをブロックしているのかを確認するために、*ウェブコントロールルールの診断*ツールを使用することができます。ウェブコントロールルールの診断は、Kaspersky Endpoint Security のインターフェイスでのみ使用可能です。Kaspersky Security Center コンソールでは、特定のリソースがどのウェブコントロールルールに含まれているかを確認することはできません。

Web リソースのブロックが誤検知だと考えられる場合は、Web リソースのブロックを通知するメッセージのリンクをクリックすると、あらかじめ作成されたメッセージを企業ネットワークの管理者に送信できます。

Web リソースへのアクセスルールをテストするには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



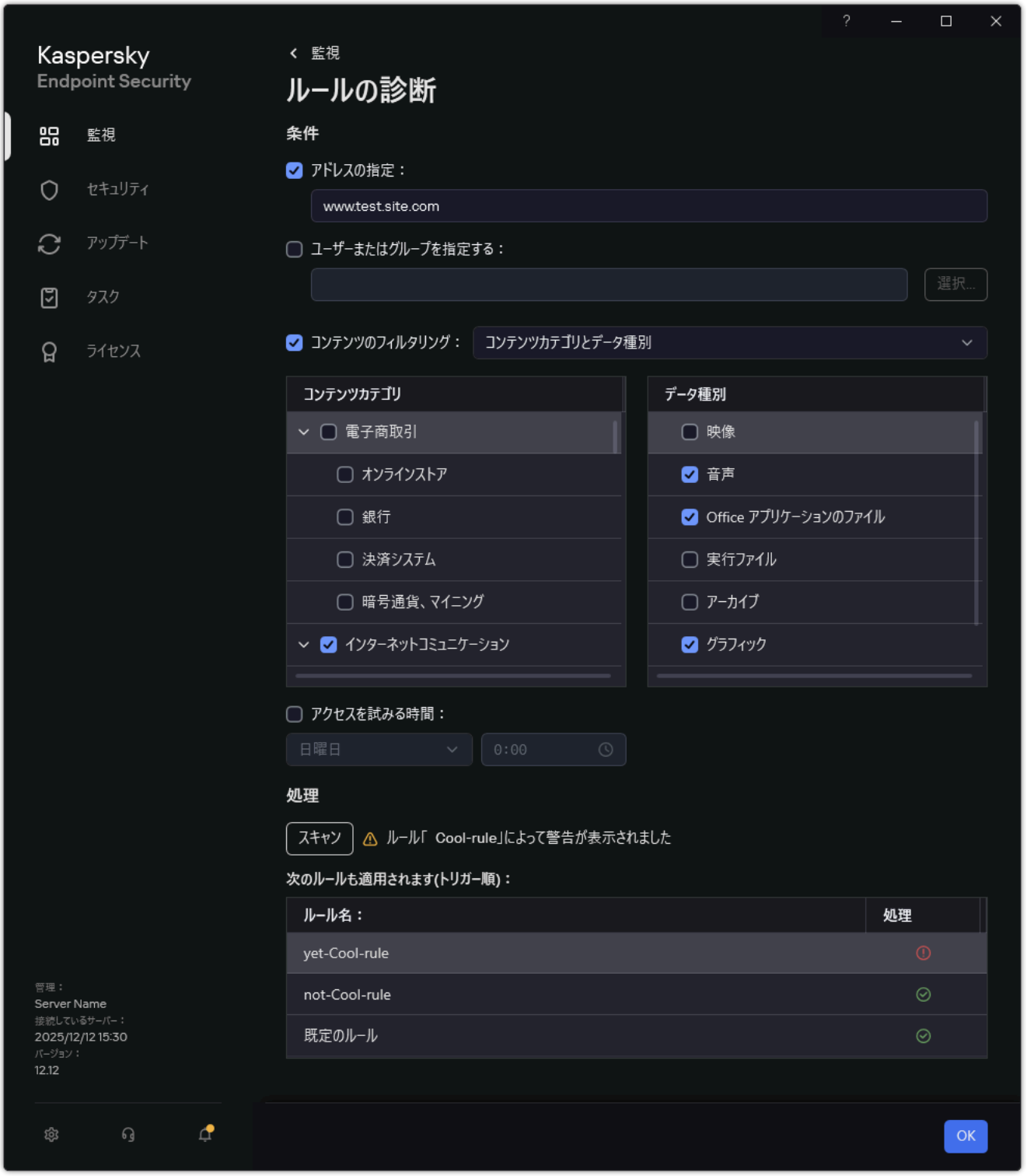
ウェブコントロールの設定

3. ［**設定**］セクションで、［**ルールの診断**］をクリックします。
   ［**ルールの診断**］ウィンドウが表示されます。
4. 特定の Web リソースへのアクセスを管理するルールをテストするには、［**アドレスの指定**］をオンにします。下のフィールドに Web リソースアドレスを入力します。
5. 特定のユーザーおよびユーザーグループ、またはそのいずれかに対して Web リソースへのアクセスを管理するルールをテストするには、ユーザーおよびユーザーグループのリストを指定します。
6. 特定のコンテンツカテゴリまたはデータ種別カテゴリの Web リソースへのアクセスを管理するルールをテストするには、［**コンテンツのフィルタリング**］から、［**コンテンツカテゴリ**］、［**データ種別**］、または［**コンテンツカテゴリとデータ種別**］を選択します。

7. ルール診断条件で指定された Web リソースへのアクセス試行の時間と曜日に関するルールをテストするには、［**アクセスを試みる時間**］をオンにします。次に、曜日と時間を指定します。

8. ［**スキャン**］をクリックします。

テストの完了後、特定の Web リソースへのアクセス試行時に適用される最初のルールに従って、Kaspersky Endpoint Security によって実行された処理に関する情報を含むメッセージが表示されます（許可、ブロック、または警告）。最初に適用されるルールは、ウェブコントロールルールのリストにおいて、診断条件に合っている中で最上位に位置しているルールです。メッセージは、［**スキャン**］の右側に表示されます。次のテーブルには、Kaspersky Endpoint Security が実行した処理を指定する、適用されたルールの残りをリスト表示します。ルールは優先度の高い順に表示されます。



Web リソースへのアクセスのテスト結果

ウェブコントロールルールのエクスポートおよびインポート

ウェブコントロールルールを XML または JSON ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数のアドレスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ウェブコントロールルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で信頼するウェブコントロールルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。
4. ウェブコントロールルールのリストをエクスポートするには：
   a. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
      ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
   b. ［**エクスポート**］リンクをクリックします。
   c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。
      Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
5. ウェブコントロールルールのリストをインポートするには：
   a. ［**インポート**］リンクをクリックします。
      表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
   b. ファイルを開きます。
      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでウェブコントロールルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**ウェブコントロール**］に移動します。

5. ［**ルールリスト**］ブロックでルールのリストをエクスポートするには：

   a. エクスポートするルールを選択します。

   b. → ［**エクスポート**］を選択します。

   Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

6. ［**ルールリスト**］ブロックでルールのリストをインスポートするには：

   a. → ［**インポート**］を選択します。

   表示されたウィンドウで、ルールのリストをインポートする JSON ファイルを選択します。

   b. ファイルを開きます。

   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

ウェブコントロールルールの Web リソースアドレスのエクスポートおよびインポート

Web リソースアクセスルールで Web リソースアドレスのリストを作成した場合は、次のファイルにエクスポートできます：

- 管理コンソール（MMC）で TXT 形式のファイル
- 製品インターフェイスで CSV 形式のファイル

その後、リストをこのファイルからインポートすることで、アクセスルールを設定するときに新しい Web リソースアドレスのリストを手動で作成する必要がなくなります。Web リソースアドレスのリストのエクスポートおよびインポートオプションは、類似したパラメータを使用してアクセスルールを作成する場合などに便利です。

個々のルールの Web リソースアドレスだけでなく、すべてのウェブコントロールルールをエクスポートまたはインポートすることもできます。

> Web コンソールと Cloud コンソールでは、ウェブコントロールルールの Web リソースアドレスをエクスポートすることもインポートすることもできません。

管理コンソール（MMC）でウェブコントロールルールの Web リソースアドレスをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。

4. ［**ウェブコントロール設定**］ブロックで、ファイルにインポートまたはエクスポートする Web リソースアドレスのリストを含むルールを選択します。

   ウェブコントロールルールのプロパティが表示されます。

5. Web リソースのリストをエクスポートするには、アドレスリストで次の操作を行います：

   a. エクスポートするアドレスを選択します。

      アドレスが何も選択されていない場合、すべてのアドレスがエクスポートされます。

   b. を選択します。

   c. 表示されたウィンドウで、Web リソースのアドレスのリストをエクスポートする TXT ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

      Web リソースのアドレスのリストがテキストファイルでエクスポートされます。

6. Web リソースのリストをインポートするには、アドレスリストで次の操作を行います：

   a. を選択します。

      表示されたウィンドウで、Web リソースのリストをインポートする TXT ファイルを選択します。

   b. ファイルを開きます。

      コンピューターにアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、TXT ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

製品インターフェイスでウェブコントロールルールの Web リソースアドレスをエクスポートおよびインポートする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**設定**］ブロックの［**Web リソースへのアクセスルール**］をクリックします。
4. ファイルにインポートまたはエクスポートする Web リソースアドレスのリストを含むルールを選択します。
5. 信頼する URL のリストをエクスポートするには、［**適用するアドレス**］ブロックで次の操作を行います：
   a. エクスポートするアドレスを選択します。
      アドレスが何も選択されていない場合、すべてのアドレスがエクスポートされます。
   b. ［**エクスポート**］をクリックします。
   c. 表示されたウィンドウで、Web リソースのアドレスのリストをエクスポートする CSV ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。
      Web リソースのアドレスのリストが CSV ファイルでエクスポートされます。

6. Web リソースのリストをインスポートするには、［**適用するアドレス**］ブロックで次の操作を行います：

   a. ［**インポート**］をクリックします。

      表示されたウィンドウで、Web リソースのリストをインポートする CSV ファイルを選択します。

   b. ファイルを開きます。

      コンピューターにアドレスのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、CSV ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

ユーザーが行っているインターネット活動の監視

Kaspersky Endpoint Security では、許可されている Web サイトも含めて、すべての Web サイトへのユーザーのアクセスに関するデータをログに記録できます。この機能により、ブラウザーでのすべての閲覧履歴を取得できます。Kaspersky Endpoint Security は、Kaspersky Security Center、Kaspersky Endpoint Security のローカルログ、Windows イベントログのそれぞれに、ユーザーの活動に関するイベント情報を送信できます。Kaspersky Security Center でイベントを受信するには、管理コンソールまたは Web コンソールを使用して、イベントに関するポリシー設定を指定する必要があります。ウェブコントロールイベントのメールによる通知と、ユーザーのコンピューター画面上への通知の表示も設定できます。

監視機能をサポートするブラウザー：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。ユーザーの操作履歴の監視はその他のブラウザーでは動作しません。

Kaspersky Endpoint Security では、ユーザーのインターネット活動に関して次のイベントが作成されます：

- Web サイトのブロック（*緊急* ステータス）。
- 望ましくない Web サイトへのアクセス（*警告*ステータス）。
- 許可されている Web サイトへのアクセス（*情報*ステータス）。

ユーザーのインターネット活動の監視を有効にする前に、以下の項目を実行してください：

- Web トラフィックへの Web ページと相互作用するスクリプトの埋め込み（下の手順を参照）。スクリプトはウェブントロールのイベントの登録を有効にします。
- HTTPS トラフィックをスキャンするには、暗号化された接続のスキャンを有効にする必要があります。

Web サイトと相互作用するスクリプトの埋め込み

管理コンソール（MMC）で Web サイトと相互作用するスクリプトを Web トラフィックに埋め込む方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。

4. ［**暗号化された接続のスキャン**］ブロックで、［**Web ページと連携するため Web トラフィック内にスクリプトを埋め込む**］をオンにします。

5. 変更内容を保存します。

Web コンソールと Cloud コンソールで Web サイトと相互作用するスクリプトを Web トラフィックに埋め込む方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。

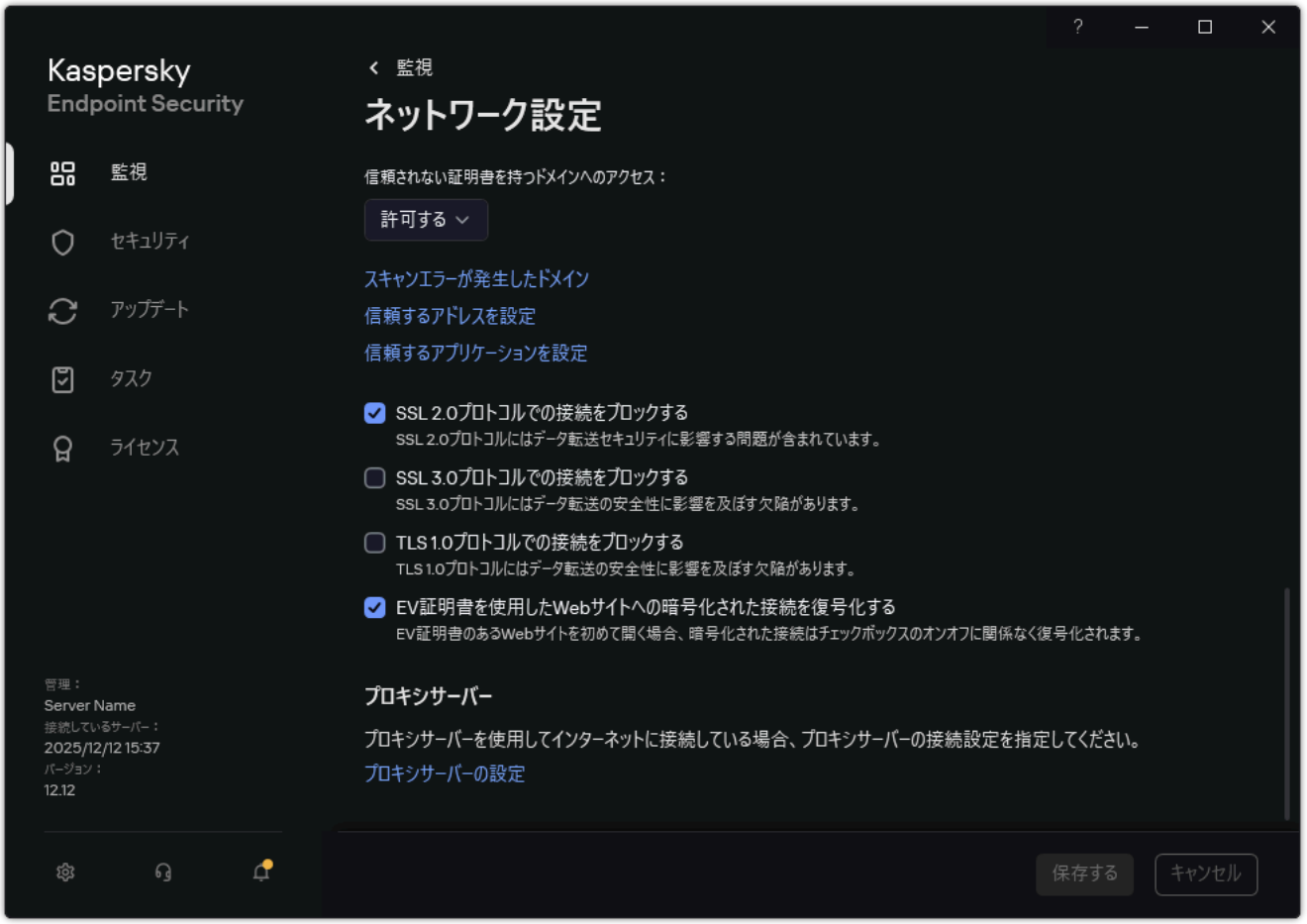
5. ［**インターネット接続の監視**］で、［**インターネット接続の監視は有効です**］をオンにします。

6. 変更内容を保存します。

Web サイトと相互作用するスクリプトを Web トラフィックに埋め込む方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。



製品のネットワーク設定

3. ［**トラフィック処理**］ブロックで、［**Webページと連携するためWebトラフィック内にスクリプトを埋め込む**］をオンにします。

4. 変更内容を保存します。

Kaspersky Endpoint Security は Web トラフィックに Web ページと相互作用するスクリプトを埋め込みます。このスクリプトにより、ウェブコントロールのイベントをアプリケーションイベントログ、OS イベントログ、レポートに登録できるようになります。

ウェブコントロールイベントのログ記録の設定

ユーザーのコンピューター上で発生したウェブコントロールイベントに関する情報の保存を設定するには：

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。

3. ［**通知**］ブロックの［**通知の設定**］をクリックします。

4. 表示されたウィンドウで、［**ウェブコントロール**］セクションを選択します。

   ウェブコントロールイベントと通知方法のリストが表示されます。

5. それぞれのイベントの通知方法を指定します（**ローカルレポートに保存**または**Windows イベントログに保存**）。

   許可されている Web サイトへのアクセスイベントもログに記録するには、ウェブコントロールの設定も編集する必要があります（下記の手順を参照）。

   イベントのリストで、画面上の通知とメール通知を有効にすることもできます。メールによる通知を送信するには、SMTP サーバー設定を指定する必要があります。メールによる通知の送信について詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。

6. 変更内容を保存します。

これにより、ユーザーのインターネット活動に関する情報のログへの記録が始まります。

ウェブコントロールは、ユーザーの活動に関するイベント情報を次のように Kaspersky Security Center に送信します：

- Kaspersky Security Center を使用している場合、ウェブコントロールは Web ページを構成するすべてのオブジェクトのイベントを送信します。そのため、1 つの Web ページがブロックされたときに複数のイベントが作成される場合があります。たとえば、「http://www.example.com」という URL のページをブロックしたときに、Kaspersky Endpoint Security によって「http://www.example.com」「http://www.example.com/icon.ico」「http://www.example.com/file.js」などのオブジェクトに対するイベントが作成される可能性があります。

- Kaspersky Security Center Cloud コンソールを使用している場合、ウェブコントロールはイベントをグループ化し、Web サイトのプロトコルとドメインのみを送信します。たとえば、ユーザーが望ましくない Web ページ http://www.example.com/main、http://www.example.com/contact、および http://www.example.com/gallery を開いた場合、http://www.example.com オブジェクトを持つイベントを 1 つだけ送信します。

許可されている Web サイトへのアクセス時のイベントのログ記録

許可されている Web サイトへのアクセス時にイベントのログ記録を有効にするには：

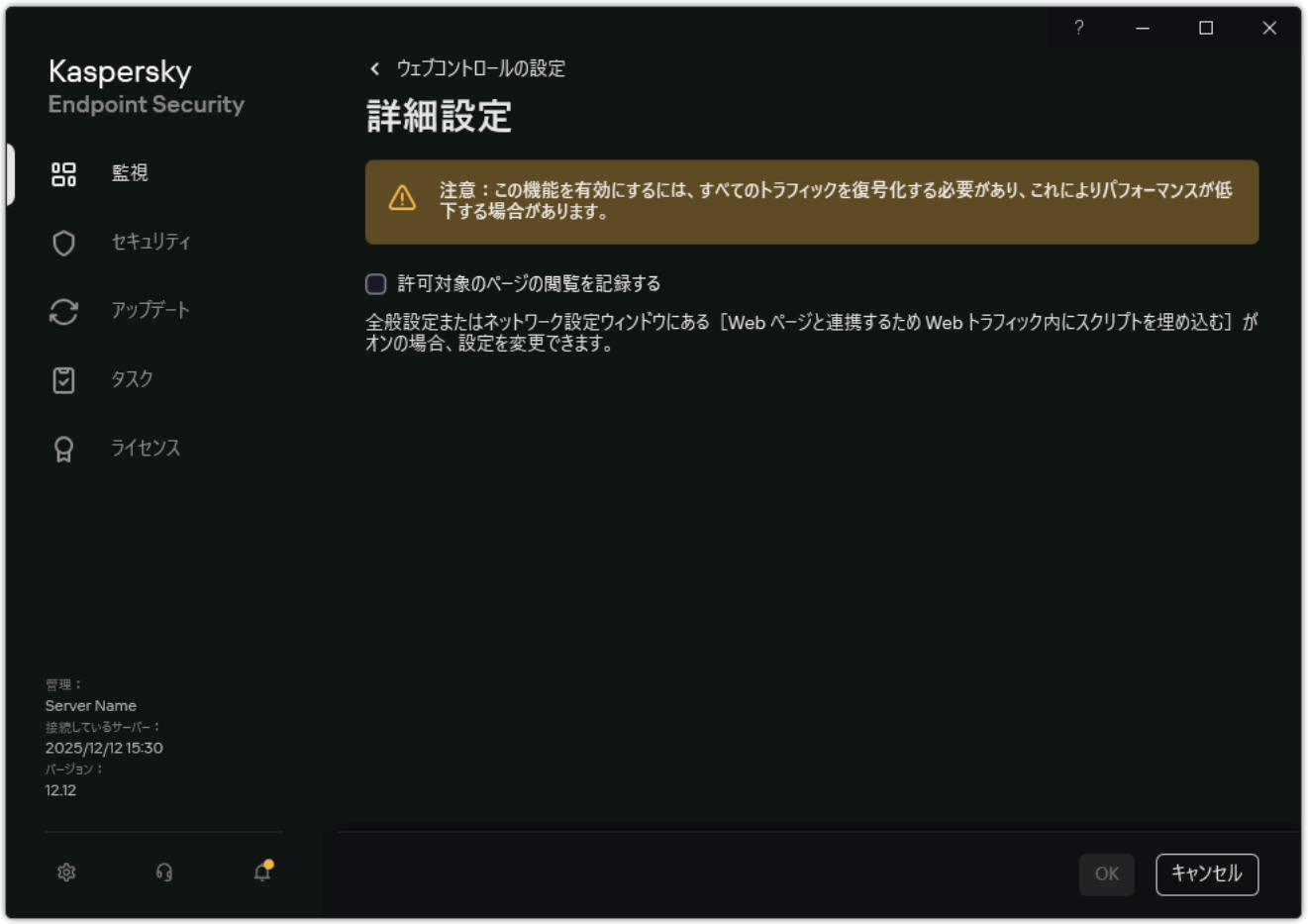
1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**詳細**］ブロックの［**詳細設定**］をクリックします。

4. 表示されたウィンドウで、［**許可対象のページの閲覧を記録する**］をオンにします。



ウェブコントロールの詳細設定

5. 変更内容を保存します。

これにより、ブラウザーでのすべての閲覧履歴を確認できるようになります。

ウェブコントロールメッセージのテンプレートの編集

ユーザーがインターネットリソースへのアクセスを試みると、Kaspersky Endpoint Security ではウェブコントロールルールのプロパティで指定された処理の種類に応じて次の種類のいずれかのメッセージが表示されます（アプリケーションでは HTTP サーバー応答の代わりにメッセージを含む HTML ページが使用されます）：

- 警告メッセージ：このメッセージは、Web リソースの閲覧が推奨されないか企業ポリシーに違反することをユーザーに警告します。Kaspersky Endpoint Security では、この Web リソースを説明するルールの設定の［**警告する**］が選択されている場合に警告メッセージが表示されます。

  警告が誤検知だと考えられる場合は、警告のリンクをクリックすると、あらかじめ作成されたメッセージを企業ネットワークの管理者に送信できます。

- Web リソースのブロックを通知するメッセージ：Kaspersky Endpoint Security では、この Web リソースを説明するルールの設定の［**ブロック**］を選択すると、Web リソースがブロックされたことを通知するメッセージが表示されます（下図を参照）。

Web リソースのブロックが誤検知だと考えられる場合は、Web リソースのブロックを通知するメッセージのリンクをクリックすると、あらかじめ作成されたメッセージを企業ネットワークの管理者に送信できます。



Web リソースのブロックに関するメッセージ

警告メッセージ、Web リソースのブロックを通知するメッセージ、LAN 管理者に送信するメッセージの専用テンプレートがあります。メッセージのテンプレートの管理用に特別な変数が用意されています（例：`%USER_NAME%`）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。

管理コンソール（MMC）でウェブコントロールのメッセージのテンプレートを変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。
4. ［**メッセージのテンプレートの設定**］ブロックの［**テンプレート**］をクリックします。
5. ウェブコントロールのメッセージのテンプレートを設定します。

- **警告**：この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。
- **ブロックに関するメッセージ**：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。
- **管理者に送信するメッセージ**：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**Web ページへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

［**既定**］を使用して既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでウェブコントロールのメッセージのテンプレートを変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**ウェブコントロール**］に移動します。

5. ［**メッセージのテンプレート**］ブロックで、［**Web サイトのブロックに関するメッセージ**］をクリックして、ウェブコントロールのメッセージのテンプレートを設定します。

   - **警告**：この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。

   - **ブロックに関するメッセージ**：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。

   - **管理者へのメッセージ**：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**Web ページへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**既定値にリセット**］を使用して既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

製品インターフェイスでウェブコントロールのメッセージのテンプレートを変更する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］を選択します。



ウェブコントロールの設定

3. ［**テンプレート**］ブロックで、ウェブコントロールのメッセージのテンプレートを設定します。

   - **警告**：この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。
   - **ブロックに関するメッセージ**：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。
   - **管理者に送信するメッセージ**：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**Web ページへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**リセット**］を使用して既定のテンプレートテキストを復元することもできます。

4. 変更内容を保存します。

Web リソースアドレスマスクの編集

Web リソースアドレスマスク（「アドレスマスク」とも呼ばれます）は、Web リソースアクセスルールを作成する際に、多数の類似の Web リソースアドレスを入力する必要がある場合に役立つことがあります。アドレスマスクを適切に作成すると、多数の Web リソースアドレスを置換できます。

アドレスマスクの作成時には、次のルールに従います：

1. `*` 文字はゼロ文字以上の文字を含むすべての文字シーケンスを置換します。

   たとえば、`*abc*` アドレスマスクを入力した場合、アクセスルールは文字シーケンス `abc` を含むすべての Web リソースに適用されます。例：`http://www.example.com/page_0-9abcdef.html`

2. 連続する `*.` 文字（*ドメインマスク*）を使用してアドレスのドメインをすべて選択することができます。ドメインマスク `*.` はすべてのドメイン名、サブドメイン名、空白行を意味します。

   例：マスク `*.example.com` は次のアドレスを表します：

   - `http://pictures.example.com`：ドメインマスク `*.` は `pictures.` を表しています。
   - `http://user.pictures.example.com`：ドメインマスク `*.` は`pictures.` および `user.` を表しています。
   - `http://example.com`：ドメインマスク `*.` は空白を表しています。

3. アドレスマスクの頭にある `www.` 文字シーケンスは `*.` シーケンスとして解釈されます。

   例：`www.example.com` のアドレスマスクは `*.example.com` として解釈されます。このマスクは `www2.example.com` および `www.pictures.example.com` を表します。

4. アドレスマスクの先頭文字が `*` ではない場合は、アドレスマスクの内容は `*.` プリフィックスと同じになります。

5. アドレスマスクの末尾の文字が `/` または `*` 以外の場合、アドレスマスクの内容は `/*` ポストフィックスと同じになります。

   例：アドレスマスク `http://www.example.com` には `http://www.example.com/abc` などのアドレスも含まれます（`a`、`b`、`c` は任意の文字です）。

6. アドレスマスクの末尾の文字が `/` の場合、アドレスマスクの内容は `/*` ポストフィックスと同じになります。

7. アドレスマスクの末尾にある文字シーケンス `/*` は、`/*` または空文字列として解釈されます。

8. Web リソースアドレスは、プロトコル（http または https）を考慮しながら、アドレスマスクに対して検証されます。

   - アドレスマスクにネットワークプロトコルがない場合は、このアドレスマスクにはすべてのネットワークプロトコルのアドレスが含まれます。

     例：アドレスマスク `example.com` には、アドレス `http://`example.com と `https://`example.com が含まれます。

- アドレスマスクにネットワークプロトコルがある場合は、このアドレスマスクにはそのアドレスマスクと同じネットワークプロトコルのアドレスのみが含まれます。

  例：アドレスマスク `http://*.example.com` には `http://www.example.com` が含まれますが、`https://www.example.com` は含まれません。

9. 二重引用符で囲まれているアドレスマスクがアドレスマスクに最初に含まれている場合は、`*` 文字が存在しない限り、その他の文字は考慮されません。ルール 5 および 7 は、「""」で囲まれたアドレスマスクには適用されません（下の表の例 14 – 18 を参照）。

10. Web リソースアドレスマスクと比較するときには、ユーザー名とパスワード、接続ポート、大文字と小文字の区別は考慮されません。

アドレスマスク作成ルールの使用例

番号	アドレスマスク	検証する Web リソースアドレス	アドレスがアドレスマスクに含まれるか	コメント
1	*.example.com	http://www.123example.com	含まれない	ルール 1 を参照
2	*.example.com	http://www.123.example.com	含まれる	ルール 2 を参照
3	*example.com	http://www.123example.com	含まれる	ルール 1 を参照
4	*example.com	http://www.123.example.com	含まれる	ルール 1 を参照
5	http://www.*.example.com	http://www.123example.com	含まれない	ルール 1 を参照
6	www.example.com	http://www.example.com	含まれる	ルール 1、3、2 を参照。
7	www.example.com	https://www.example.com	含まれる	ルール 1、3、2 を参照。
8	http://www.*.example.com	http://123.example.com	含まれる	ルール 1、3、4 を参照。
9	www.example.com	http://www.example.com/abc	含まれる	ルール 1、3、5 を参照。
10	example.com	http://www.example.com	含まれる	ルール 1、3 を参照
11	http://example.com/	http://example.com/abc	含まれる	ルール 6 を参照
12	http://example.com/*	http://example.com	含まれる	ルール 7 を参照
13	http://example.com	https://example.com	含まれない	ルール 8 を参照
14	"example.com"	http://www.example.com	含まれない	ルール 9 を参照
15	"http://www.example.com"	http://www.example.com/abc	含まれない	ルール 9 を参照
16	"*.example.com"	http://www.example.com	含まれる	ルール 9、1 を参照
17	"http://www.example.com/*"	http://www.example.com/abc	含まれる	ルール 9、1 を参照
18	"www.example.com"	http://www.example.com、https://www.example.com	含まれる	ルール 8、9 を参照
19	www.example.com/abc/123	http://www.example.com/abc	含まれない	アドレスマスクには Web リソースのアドレス以外の情報も含まれます。

仮想マシンのウェブコントロール

ウェブコントロールは、コンピューター上のトラフィックだけでなく、コンピューターにローカルに配備された仮想マシン上のトラフィックも制御します。機能させるために、ローカルの仮想マシンに Kaspersky Endpoint Security アプリケーションをインストールする必要はありません。つまり、ウェブコントロールルールでブロックされている Web サイトをユーザーが*仮想*マシン上のブラウザーで開こうとすると、*コンピューター*のホストオペレーティングシステムにインストールされた本製品が、その Web サイトへのアクセスを拒否します。

ウェブコントロールは仮想マシンによって動作が異なります。

Oracle VM VirtualBox

Kaspersky Endpoint Security は、Oracle VM VirtualBox 仮想マシン上のウェブコントロールルールを無制限でサポートします。本製品により仮想マシンのすべてのトラフィックを制御できます。ユーザーによるフィルターがウェブコントロールルールに設定されている場合、仮想マシンのすべてのプロセスはローカルユーザーによって起動されるため、本製品は正常に動作します。

VMware Workstation

Kaspersky Endpoint Security は、VMware Workstation 仮想マシン上のウェブコントロールルールを制限付きでサポートします。本製品は、ユーザーによるフィルターが設定されたルールをサポートしません。仮想マシンプロセスはシステムユーザー（SYSTEM）で実行されます。このため、仮想マシン上で Web サイトを開こうとしているユーザーを識別することができません。

Microsoft Hyper-V

Kaspersky Endpoint Security は、Microsoft Hyper-V 仮想マシン上のウェブコントロールルールをサポートしません。

ウェブコントロールのメッセージテンプレートの変数

ユーザーメッセージテンプレートまたは管理者メッセージテンプレートでは、次の変数を使用できます。

- **ユーザー**：`%USER_NAME%`

  メッセージが生成されたコンピュータ上の現在のユーザーアカウントの名前。形式：`<device name>\<user alias>`（例： `DESKTOP-123\John.Smith`）。

- **Web リソースアドレス**：`%CANONIC_REQUEST_URL%`

  ブロックされた Web リソースのアドレス。

- **ルール名**：%RULE%

  Web リソースをブロックしたルールの名前。

- **メッセージを送信するメール**：%COMPLAIN_EMAIL%

  Web リソースのブロックに関する連絡用のメールアドレス。メールアドレスをクリックすると、ユーザーが管理者にメッセージを書き込むことができるウィンドウが開きます。

- **コンテンツカテゴリ名**：%CONTENT_CATEGORY_LIST%

  ブロックされたリソースが属する Web サイトのカテゴリ（例：*決済システム*）。

- **データ種別カテゴリ名**：%TYPE_CATEGORY_LIST%

  ブロックされた Web リソース上のデータ種別のカテゴリ（例：*グラフィックファイル*）。

- **要求された Web リソースへのリンク**：%CONTINUE_PAGE%

  要求された Web ページへのリンク（例：`http://www.example.com/pagename.html`）。

- **Web サイトへのリンク**：%CONTINUE_SITE%

  要求された Web ページを含む Web サイトへのリンク（例：`http://www.example.com/`）。

- **ドメインへのアクセス用リンク**：%CONTINUE_DOMAIN%

  クリックしてドメイン名の既存のすべての Web ページにアクセスできるリンク。たとえば、ブロックされた Web ページのアドレスが `http://www.example.com` だった場合、変数 %CONTINUE_DOMAIN% は `http://*.example.com` リンクに置換されます。このリンクをクリックすると、基本ドメイン名 `http://www.example.com/` のすべての Web アドレス（サブドメインを含む）にアクセスできます。例えば、`http://start.example.com/*` や `http://domain.domain.example.com/*` などです。ここで、文字「*」は任意の文字列（空白の文字列を含む）を表します。

デバイスコントロール

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。

デバイスコントロールが有効になると、本製品は接続されているデバイスの情報を Kaspersky Security Center に渡します。接続されたデバイスのリストは Kaspersky Security Center の［**詳細**］→［**リポジトリ**］→［**ハードウェア**］フォルダーで表示できます。

デバイスへのアクセスの判定基準

デバイスコントロールは、次の情報に基づいてアクセスをコントロールできます。

- **デバイス種別**：プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。

  次のようにデバイスアクセスを設定できます：

  - 許可：✓
  - ブロック：⊘

- ルールに準拠（プリンターとポータブルデバイスのみ）：
- 接続バスに依存（Wi-Fi 以外）：
- 例外を除きブロック（Wi-Fi のみ）：

- **接続バス**：*接続*バスとは、コンピューターへのデバイスの接続に使用されるインターフェイスです（例：USB、FireWire）。デバイス種別に対して**接続バスに依存**モードが選択されている場合、本製品は接続インターフェイス（USB など）に応じてデバイスへのアクセスを許可または拒否します。

  次のようにデバイスアクセスを設定できます：

  - 許可：
  - ブロック：

- **信頼するデバイス**：「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

  次のデータに基づいて信頼するデバイスを追加できます。

  - **ID によるデバイス**：各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。

  - **モデルによるデバイス**：各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：`VID_1234&PID_5678`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。

  - **ID マスクによるデバイス**：ID が類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`WDC_C*`」。

  - **モデルマスクによるデバイス**：同一の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`VID_05AC&PID_*`」。

デバイスコントロールは、*アクセスルール*を使用してデバイスへのユーザーアクセスを管理します。デバイスコントロールでは、デバイスの接続や切断のイベントを保存することもできます。イベントを保存するには、ポリシー内でイベントの記録を設定する必要があります。

デバイスへのアクセスが接続バスに依存する場合（ステータスの場合）、Kaspersky Endpoint Security ではデバイスの接続イベントと切断イベントが保存されません。Kaspersky Endpoint Security でデバイスの接続イベントと切断イベントを保存するには、デバイスへのアクセスを許可する（ステータス）か、デバイスを信頼リストに追加します。

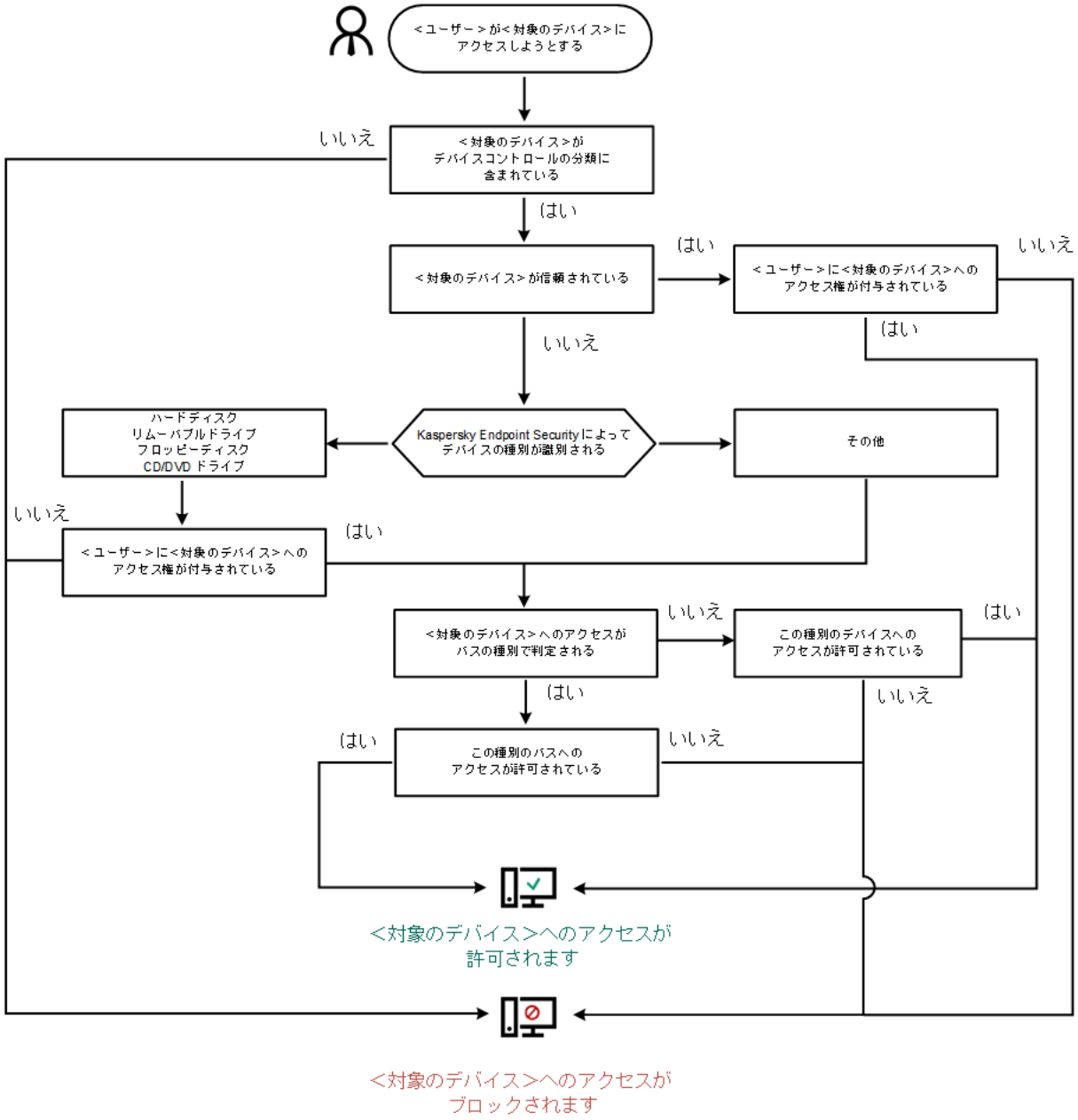
デバイスコントロールでブロックされているデバイスがコンピューターに接続された場合、Kaspersky Endpoint Security はアクセスをブロックし通知を表示します（以下の図を参照）。



デバイスコントロールの通知

デバイスコントロールの動作アルゴリズム

ユーザーがデバイスをコンピューターに接続すると、Kaspersky Endpoint Security はデバイスへのアクセスを許可するかどうかを決定します（以下の図を参照）。



デバイスコントロールの動作アルゴリズム

デバイスが接続されてアクセスが許可されている状況で、アクセスをブロックするようにアクセスルールを編集できます。この場合、（フォルダーの内容の表示や、読み取りまたは書き込みの実行など）次にデバイスへのアクセスが試行されたときに、Kaspersky Endpoint Security はアクセスをブロックします。ファイルシステムのないデバイスは、次回デバイスが接続されたときにのみブロックされます。

Kaspersky Endpoint Security がインストールされているコンピューターのユーザーが、誤ってブロックされたと考えられるデバイスへのアクセスを要求できるようにするには、アクセス要求の手順を伝えます。

アクセスルールの概要

*デバイスアクセスルール*は、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを定義する複数の設定項目です。これらの設定には特定のデバイス、アクセススケジュール、読み取りまたは書き込み権限へのアクセスが含まれます。デバイスコントロールの分類に含まれていないデバイスを追加することはできません。これらのデバイスへのアクセスはすべてのユーザーに対して許可されます。

デバイスアクセスルール

アクセスルールで設定できる項目は、対象となるデバイスの種別に応じて異なります。詳しくは次の表を参照してください。

アクセスルールの設定

デバイス	アクセスコントロール	デバイスへのアクセスのスケジュール	ユーザーまたはユーザーのグループの割り当て	優先度	読み取り／書き込み権限
ハードディスク	✓	✓	✓	✓	✓
リムーバブルドライブ（USB フラッシュドライブを含む）	✓	✓	✓	✓	✓
フロッピーディスク	✓	✓	✓	✓	✓
CD/DVD ドライブ	✓	✓	✓	✓	✓
ポータブルデバイス（MTP）	✓	✓	✓	✓	✓
ローカルプリンター	✓	–	✓	✓	–
ネットワークプリンター	✓	–	✓	✓	–
モデム	✓	–	–	–	–
テープデバイス	✓	–	–	–	–
多機能デバイス	✓	–	–	–	–
スマートカードリーダー	✓	–	–	–	–
Windows CE USB ActiveSync デバイス	✓	–	–	–	–
外部ネットワークアダプター	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
カメラとスキャナー	✓	–	–	–	–

Wi-Fi ネットワークのアクセスルール

Wi-Fi ネットワークのアクセスルールでは、Wi-Fi ネットワークへの接続を許可するか（ステータス）、あるいはブロックするか（ステータス）を指定します。ルールに［*信頼する Wi-Fi ネットワーク*］（ステータス）を追加できます。信頼する Wi-Fi ネットワークは制限なく使用が許可されます。既定では、Wi-Fi ネットワークのアクセスルールはすべての Wi-Fi ネットワークへのアクセスが許可されます。

接続バスアクセスルール

デバイス種別のアクセスルールに［**接続バスに依存**］の値が選択されている場合、本製品は接続インターフェイスに応じてそのデバイスへのアクセスを許可または拒否します。バスへのアクセスを許可するルールは、デバイスコントロールの分類時に存在するすべての接続バスに対して既定で作成されます。

接続バスアクセスルールでは、デバイスの接続を許可するか（ステータス）、あるいはブロックするか（ステータス）を指定します。デバイス種別アクセスルールの優先度は、接続バスアクセスルールの優先度よりも高くなります。

キーボードとマウスはデバイスコントロールを使用してロックできません。USB 接続バスへのアクセスを禁止した場合も、ユーザーは引き続き USB 経由で接続されたキーボードやマウスを使用できます。有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードを模倣してコンピューターに接続するのを防ぐように設計されています。

種別ごとのデバイスへのアクセスの管理

デバイスコントロールを使用すると、種別ごとにデバイスへのアクセスを管理できます。デバイスの種別は、デバイスの接続時にオペレーティングシステムによって決定されます。オペレーティングシステムに組み込まれているデバイスマネージャーツールを使用して、デバイス種別を調べることができます。デバイスへのアクセスを管理するには、ルールを設定する必要があります。*デバイスアクセスルール*は、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを定義する複数の設定項目です。これらの設定には特定のデバイス、アクセススケジュール、読み取りまたは書き込み権限へのアクセスが含まれます。デバイスコントロールの分類に含まれていないデバイスを追加することはできません。これらのデバイスへのアクセスはすべてのユーザーに対して許可されます。

既定では、デバイスコントロールは、すべてのユーザーのすべてのデバイスへのアクセスを許可します。

デバイスへのアクセスは次のように設定できます：

- **許可**

  すべてのユーザーにデバイスへのフルアクセス権が付与されます。

- **ブロック**

  デバイスの接続がブロックされます。信頼するデバイスのみ接続できます。

- **接続バスに依存**

  Kaspersky Endpoint Security がデバイスの接続インターフェイスを判別し、接続バスのステータスに応じてデバイスへのアクセスを制限します。信頼するデバイスの接続も許可されます。

- **ルールに準拠**

  一部のデバイス種別に対して、デバイスの使用、デバイスへのアクセスのスケジュールの設定、読み取り権限および書き込み権限の設定が許可される個々のユーザーまたはユーザーグループを指定することができます。信頼するデバイスの接続も許可されます。

［**ハードディスク**］種別のデバイスへのアクセスを設定する際は注意してください。システムディスクへのアクセスをブロックすると、オペレーティングシステムの起動時にクラッシュ（BSOD）が発生する可能性があります。

デバイスがデバイスコントロールの分類スキームの範囲外にある場合、そのようなデバイスへのアクセスを制限することはできません。

管理コンソール（MMC）で種別ごとのデバイスへのアクセスを管理する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
6. デバイスのアクセスルールを設定します：
   a. アクセスモード（［**許可**］、［**ブロック**］、［**接続バスに依存**］、［**ルールに準拠**］）を選択します。
      ［**ルールに準拠**］のアクセスモードを選択するには、ダブルクリックしてアクセスルールのプロパティを開く必要があります。
   b. ［**接続バスに依存**］のアクセスモードを選択した場合は、［**接続バス**］タブに移動して、接続インターフェイスのアクセスルールを設定します。
   c. ストレージ機器（リムーバブルメディアなど）の場合は、個々のユーザーのアクセス権限を設定できます。デバイスへのアクセスのスケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。
      デバイスを信頼するリストに追加できます。「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。
   d. 必要に応じて、印刷ルールを設定します。
   e. 必要に応じて、Bluetooth デバイスのアクセスルールを設定します。
   f. 必要に応じて、コンピューターの Wi-Fi 接続ルールを設定します。
7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（  ）。

Web コンソールおよび Cloud コンソールで種別ごとのデバイスへのアクセスを管理する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。
5. ［**デバイスアクセスルール**］で、［**デバイスと Wi-Fi ネットワーク**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。

6. デバイスのアクセスルールを設定します：

   a. アクセスモード（[**許可する**]、[**ブロックする**]、[**バスに依存**]、[**カスタム**]）を選択します。

      ドロップダウンメニューにアクセスモードが表示されない場合は、デバイス種別をダブルクリックしてアクセスルールのプロパティを開きます。

   b. ［**バスに依存**］のアクセスモードを選択した場合は、［**接続バス**］タブに移動して、接続インターフェイスのアクセスルールを設定します。

   c. ストレージ機器（リムーバブルメディアなど）の場合は、個々のユーザーのアクセス権限を設定できます。デバイスへのアクセスのスケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。

      デバイスを信頼するリストに追加できます。「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

   d. 必要に応じて、印刷ルールを設定します。

   e. 必要に応じて、Bluetooth デバイスのアクセスルールを設定します。

   f. 必要に応じて、コンピューターの Wi-Fi 接続ルールを設定します。

7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

製品インターフェイスでデバイスへのアクセスを管理する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］セクションで、［**デバイスと Wi-Fi ネットワーク**］をクリックします。

   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。

4. デバイスのアクセスルールを設定します：

   a. アクセスモード（[**許可**]、[**ブロック**]、[**接続バスに依存**]、[**ルールに準拠**]）を選択します。

      ドロップダウンメニューにアクセスモードが表示されない場合は、デバイス種別をダブルクリックしてアクセスルールのプロパティを開きます。

   b. ［**接続バスに依存**］のアクセスモードを選択した場合は、［**接続バス**］タブに移動して、接続インターフェイスのアクセスルールを設定します。

   c. ストレージ機器（リムーバブルメディアなど）の場合は、個々のユーザーのアクセス権限を設定できます。デバイスへのアクセスのスケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。

      デバイスを信頼するリストに追加できます。「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

   d. 必要に応じて、印刷ルールを設定します。

   e. 必要に応じて、Bluetooth デバイスのアクセスルールを設定します。

   f. 必要に応じて、コンピューターの Wi-Fi 接続ルールを設定します。

5. 変更内容を保存します。

これにより、ユーザーがデバイスへのアクセスを取得しようとすると、ルールに従ってアクセスがブロックされます。さらに、対応するイベントがログに記録されます。個々のデバイスへのアクセスを許可する場合は、それらのデバイスを信頼するデバイスのリストに追加することができます。

接続バスによるデバイスへのアクセスの管理

接続バスアクセスルールを編集するには、次の手順を実行します：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**接続バス**］をクリックします。
   ウィンドウに、デバイスコントロールの分類に含まれるすべての接続バスのアクセスルールが表示されます。
4. 編集するアクセスルールを選択します。
5. ［**アクセス**］列で、接続バスへのアクセスを許可するかどうかを選択します：**許可**または**ブロック**。

   接続バス［**シリアルポート**］（COM）または［**パラレルポート**］（LPT）のアクセスを変更した場合、アクセスルールを有効にするにはコンピューターを再起動する必要があります。
6. 変更内容を保存します。

デバイスに対するユーザーアクセス権の区別

デバイス種別ごとにユーザーアクセス権を設定することも、信頼するデバイスに対してユーザーアクセス権を設定することもできます。

デバイス種別ごとのユーザーアクセス権の区別

デバイスコントロールでは、*ストレージ機器*上のデータへのユーザーアクセス権を設定できます。このようなデバイスに対して、書き込み権限と読み取り権限を設定できます。デバイスコントロールは、次の種別の*ストレージ機器*をサポートします：

- ハードディスク
- リムーバブルドライブ（USB フラッシュドライブを含む）
- フロッピーディスク
- CD/DVD ドライブ
- ポータブルデバイス（MTP）ポータブルデバイス（MTP）には、モバイルデバイス、写真用カメラ、メディアプレーヤーなどが含まれます。

この方法により、たとえば、リムーバブルメディアの使用を管理者グループのみに許可することができます。その他のデバイス種別に対し、すべてのユーザーのアクセスを拒否または許可できます。また、プリンターを使用するためのユーザーアクセス権を設定することもできます。

管理コンソール（MMC）でストレージ機器上のデータへのユーザーアクセス権を設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。

   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
6. ストレージ機器のアクセスルールを設定するには、ルールのリストをダブルクリックして開きます。
7. ストレージ機器のアクセスルールを設定します：

   a. ［**アクセスルール**］ブロックの［**追加**］をクリックします。

      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。

   b. ［**ルールの優先度**］フィールドで、*ルールの書き込み*優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**ユーザーとグループのルール**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

   d. ［OK］をクリックします。
8. ［**選択されたアクセスルールのスケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。

   たとえば、ユーザーに対して、勤務時間中にのみストレージ機器の使用を許可できます。
9. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。
10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールと Cloud コンソールでストレージ機器上のデータへのユーザーアクセス権を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。

5. ［**デバイスアクセスルール**］ブロックのアクセスルールテーブルで、ストレージ機器のアクセスルールのプロパティを開きます。

6. ［**デバイスアクセスルール**］ブロックで、［**カスタム**］を選択します。

7. ストレージ機器のアクセスルールを設定します：

   a. ［**ユーザーとその権限**］ブロックの［**追加**］をクリックします。

      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。

   b. ［**優先度**］フィールドで、*ルールの書き込み*優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**ユーザーまたはグループ**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

   d. ［**アクセススケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。

      たとえば、ユーザーに対して、勤務時間中にのみストレージ機器の使用を許可できます。

   e. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。

   f. ［**保存**］をクリックします。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

製品インターフェイスでストレージ機器上のデータへのユーザーアクセス権を設定する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］セクションで、［**デバイスと Wi-Fi ネットワーク**］をクリックします。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
4. ストレージ機器のアクセスルールを設定するには、右クリックしてルールのリストを開きます。
5. ストレージ機器のアクセスルールを設定します：
   a. ［**ユーザーの権限**］ブロックの［**追加する**］をクリックします。
      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。
   b. ［**優先度**］フィールドで、*ルールの書き込み*優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。
      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。
      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。
      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。
   c. ［**ユーザー**］で、ユーザーまたはユーザーグループを選択します。Active Directory でユーザーを選択することも、ローカルユーザー名を手入力することもできます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。
   d. ［OK］をクリックします。
6. ［**デバイスへのアクセスのスケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。
   たとえば、ユーザーに対して、勤務時間中にのみストレージ機器の使用を許可できます。
7. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。
8. 変更内容を保存します。

信頼するデバイスに対するユーザーアクセス権の区別

「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。信頼するデバイスで作業するには、個々のユーザー、ユーザーグループ、または組織内のすべてのユーザーにアクセス権を付与できます。信頼するデバイスのプロパティでユーザーアクセス権を設定することができます。

モバイルデバイスへのアクセスの管理

Kaspersky Endpoint Security を使用して、Android および iOS を実行しているモバイルデバイスのデータへのアクセスをコントロールできます。モバイルデバイスはポータブルデバイス（MTP）のカテゴリに分類されます。そのため、モバイルデバイスのデータへのアクセスを設定するには、ポータブルデバイス（MTP）のアクセス設定を編集する必要があります。

モバイルデバイスがコンピューターに接続されると、コンピューターのオペレーティングシステムがデバイスの種別を識別します。ADB（Android Debug Bridge）または iTunes（または同等のアプリケーション）がコンピューターにインストールされている場合、コンピューターのオペレーティングシステムはモバイルデバイスを ADB デバイスまたは iTunes デバイスとして認識します。それ以外の場合、オペレーティングシステムはモバイルデバイスを、ファイル転送用のポータブルデバイス（MTP）や画像転送用の PTP デバイス（カメラ）などの別のデバイスとして認識します。判定されるデバイスの種別は、モバイルデバイスの機種および選択された USB 接続モードによって異なります。Kaspersky Endpoint Security を使用して、ADB アプリケーション、iTunes またはファイルマネージャーでモバイルデバイスのデータへの個別のアクセス権を設定できます。その他のケースでは、デバイスコントロールを使用してポータブルデバイス（MTP）アクセスルールに従ってモバイルデバイスへのアクセスを許可します。

モバイルデバイスへのアクセス

モバイルデバイスはポータブルデバイス（MTP）のカテゴリに分類されるので、設定も同一となります。モバイルデバイスへのアクセスには、次のモードのうち 1 つを選択します：

- **許可**（）：Kaspersky Endpoint Security はモバイルデバイスへのフルアクセスを許可します。ユーザーはファイルマネージャー、ADB および iTunes を使用してモバイルデバイス上でファイルを開いたり、作成、編集、コピーまたは削除することができます。モバイルデバイスをコンピューターの USB ポートに接続してデバイスのバッテリーを充電することもできます。

- **ブロック**（）：Kaspersky Endpoint Security はファイルマネージャー、ADB および iTunes アプリケーションでモバイルデバイスへのアクセスを制限します。信頼するモバイルデバイスのみアクセスが許可されます。モバイルデバイスをコンピューターの USB ポートに接続してデバイスのバッテリーを充電することもできます。

- **接続バスに依存**（）：Kaspersky Endpoint Security はモバイルデバイスへの接続を USB 接続のステータス（［**許可**］（）または［**ブロック**］（））に応じて許可します。

- **ルールに準拠**（）：Kaspersky Endpoint Security はルールに従ってモバイルデバイスへのアクセスを制限します。ルールでは、アクセス（読み取り/書き込み）を設定したり、モバイルデバイスにアクセスできるユーザーまたはユーザーグループを選択したり、モバイルデバイスへのアクセススケジュールを設定したりすることができます。また、ADB および iTunes アプリケーションを使用してデバイスのデータへのアクセスを制限することもできます。

モバイルデバイスのアクセスルールの設定

ポータブルデバイス（MTP）、ADB デバイスおよび iTunes デバイスへのアクセスルールの設定は異なります。ポータブルデバイス（MTP）および ADB デバイスについては、個別のユーザーまたはユーザーグループに対してルールを設定し、ルールが適用されるスケジュールを作成することができます。iTunes デバイスに関してはこのようなことはできません。すべてのユーザーに対して iTunes アプリケーションを介してデータへのアクセスを許可または拒否することのみ可能です。

管理コンソール（MMC）でモバイルデバイスのアクセスルールを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
4. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
5. デバイス種別［**ポータブルデバイス（MTP）**］のコンテキストメニューで、 モバイルデバイスのアクセスモード（［**許可**］（）、［**ブロック**］（）、または［**接続バスに依存**］（））を設定します。
6. モバイルデバイスのアクセスルールを設定するには、ルールのリストをダブルクリックして開きます。
7. モバイルデバイスのアクセスルールを設定します：
   a. ［**アクセスルール**］ブロックの［**追加**］をクリックします。
      新しいモバイルデバイスへのアクセスルールを追加するウィンドウが開きます。
   b. ［**優先度**］フィールドで、ルールの書き込み優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み/ADB アクセス）、優先度。
      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。
      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。
      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。
   c. ［**ユーザーとグループのルール**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。
   d. ［**OK**］をクリックします。

8. ［**選択されたアクセスルールのスケジュール**］で、ユーザーのデバイスアクセススケジュールを設定します。

ADB デバイスに対して別のスケジュールを設定することはできません。ADB デバイスとポータブルデバイス（MTP）に共通のスケジュールを設定します。

9. ファイルマネージャーで、ユーザーのモバイルデバイスへのアクセス権を設定します（**読み取り / 書き込み**）。

10. ［**ADB 経由でアクセス**］を使用して ADB アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

チェックボックスがオフの場合は、モバイルデバイスが接続されると、ADB アプリケーションではデバイスの検出がブロックされます。

11. ［**iTunes 経由でアクセス**］で、iTunes アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

Kaspersky Endpoint Security では、すべてのユーザーに対して iTunes アプリケーションを介したモバイルデバイスへのアクセスの設定が適用されます。iTunes デバイスで個別のスケジュールを設定することはできません。

12. 変更内容を保存します。

Web コンソールと Cloud コンソールでモバイルデバイスのアクセスルールを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。

5. ［**デバイスアクセスルール**］セクションで、［**デバイスと Wi-Fi ネットワーク**］をクリックします。

表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。

6. ［**ポータブルデバイス（MTP）**］デバイス種別を選択します。

ポータブルデバイス（MTP）のアクセス権が表示されます。

7. モバイルデバイスのアクセスモードを設定します：［**許可する**］、［**ブロックする**］、［**バスに依存**］、または［**カスタム**］。

8. ［**iTunes 経由のすべてのユーザーのアクセスは有効です**］スイッチを使用して、iTunes アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

Kaspersky Endpoint Security では、すべてのユーザーに対して iTunes アプリケーションを介したモバイルデバイスへのアクセスの設定が適用されます。iTunes デバイスで個別のスケジュールを設定することはできません。

9. ［**カスタム**］モードを選択すると、デバイスに対してアクセスルールを設定する必要があります。アクセスルールを設定するには、［**ユーザーとその権限**］で、［**追加**］をクリックしてモバイルデバイスアクセスルールを設定します：

   a. ［**優先度**］フィールドで、ルールの書き込み優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み/ADB アクセス）、優先度。

   ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

   例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

   ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   b. ［**ユーザーまたはグループ**］で、モバイルデバイスにアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

   c. ［**アクセススケジュール**］で、ユーザーのデバイスアクセススケジュールを設定します。

   > ADB デバイスに対して別のスケジュールを設定することはできません。ADB デバイスとポータブルデバイス（MTP）に共通のスケジュールを設定します。

   d. ファイルマネージャーで、ユーザーのモバイルデバイスへのアクセス権を設定します（**読み取り / 書き込み**）。

   e. ［**ADB 経由でアクセス**］を使用して ADB アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

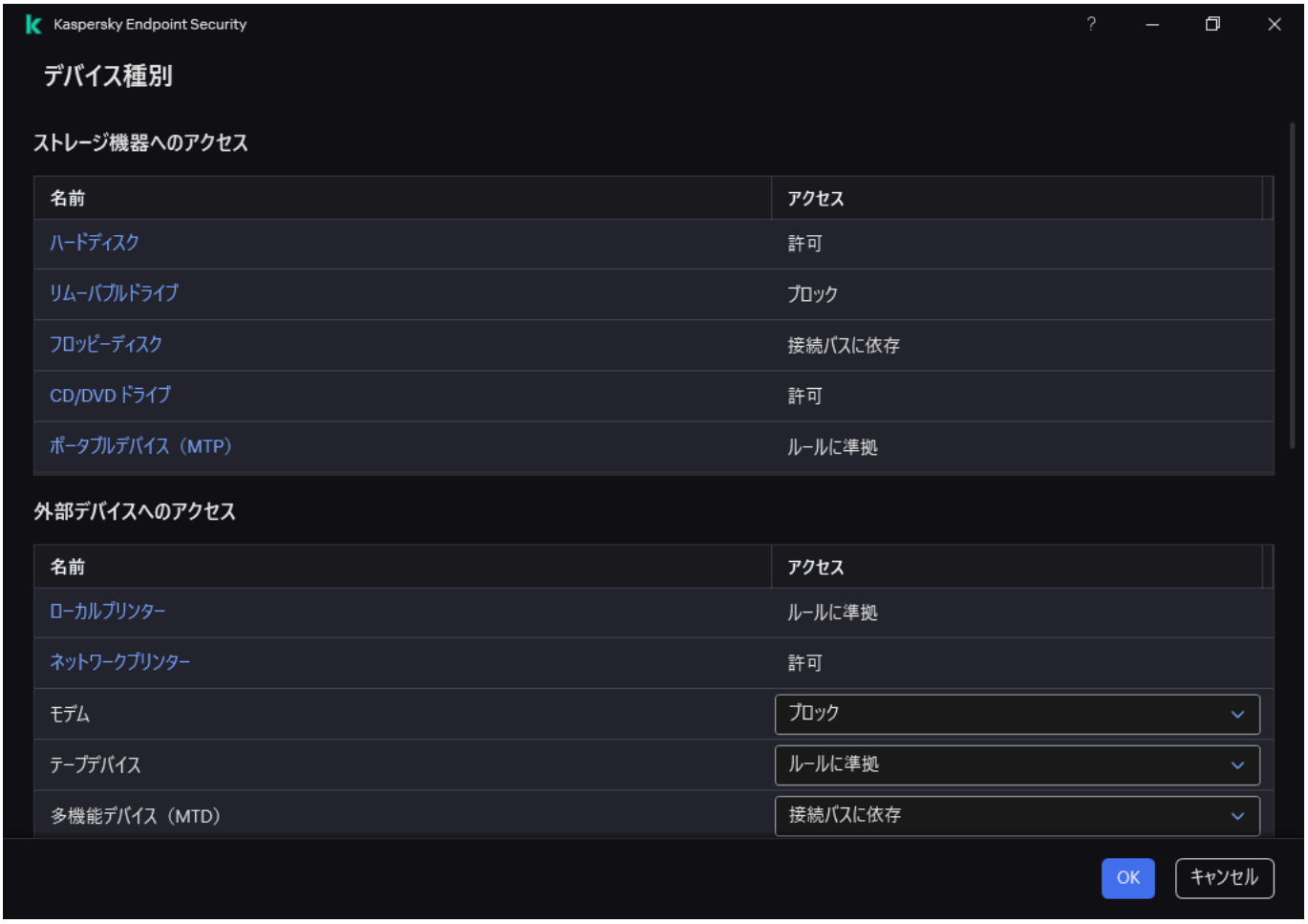
   チェックボックスがオフの場合は、モバイルデバイスが接続されると、ADB アプリケーションではデバイスの検出がブロックされます。

10. 変更内容を保存します。

製品インターフェイスでモバイルデバイスのアクセスルールを設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**デバイスと Wi-Fi ネットワーク**］をクリックします。

ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。



デバイスコントロールコンポーネントのデバイス種別

4. ［**ストレージ機器へのアクセス**］セクションで、［**ポータブルデバイス（MTP）**］をクリックします。
   ポータブルデバイス（MTP）のアクセスルールのウィンドウが表示されます。

5. ［**アクセス**］で、モバイルデバイスのアクセスモードを設定します：［**許可**］、［**ブロック**］、［**接続バスに依存**］、または［**ルールに準拠**］。

6. ［**ルールに準拠**］モードを選択すると、デバイスに対してアクセスルールを設定する必要があります：

   a. ［**ユーザーの権限**］ブロックの［**追加する**］をクリックします。
      新しいモバイルデバイスへのアクセスルールを追加するウィンドウが開きます。

   b. ［**優先度**］フィールドで、ルールの書き込み優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み/ADB アクセス）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

c. ［**状態**］で、モバイルデバイスのアクセスルールをオンにします。

d. ［**アクセスルール**］で、ユーザーのモバイルデバイスへのアクセス権限を設定します。

- ファイルマネージャーで、ユーザーのモバイルデバイスへのアクセス権を設定します（**読み取り / 書き込み**）。
- ［**ADB 経由でアクセス**］を使用して ADB アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

  チェックボックスがオフの場合は、モバイルデバイスが接続されると、ADB アプリケーションではデバイスの検出がブロックされます。

e. ［**ユーザー**］で、モバイルデバイスにアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

f. ［**デバイスへのアクセスのスケジュール**］で、ユーザーのデバイスアクセススケジュールを設定します。

> ADB デバイスに対して別のスケジュールを設定することはできません。ADB デバイスとポータブルデバイス（MTP）に共通のスケジュールを設定します。

g. ［**iTunes 経由でアクセス**］で、iTunes アプリケーションを介したモバイルデバイスのデータへのアクセスを設定します。

> Kaspersky Endpoint Security では、すべてのユーザーに対して iTunes アプリケーションを介したモバイルデバイスへのアクセスの設定が適用されます。iTunes デバイスで個別のスケジュールを設定することはできません。

7. 変更内容を保存します。

これにより、ユーザーのモバイルデバイスへのアクセスはルールに従って制限されます。ADB および iTunes アプリケーションでのモバイルデバイスへのアクセスを禁止した場合は、モバイルデバイスを接続した際に、ADB および iTunes アプリケーションはモバイルデバイスの検出ができなくなります。

信頼するモバイルデバイス

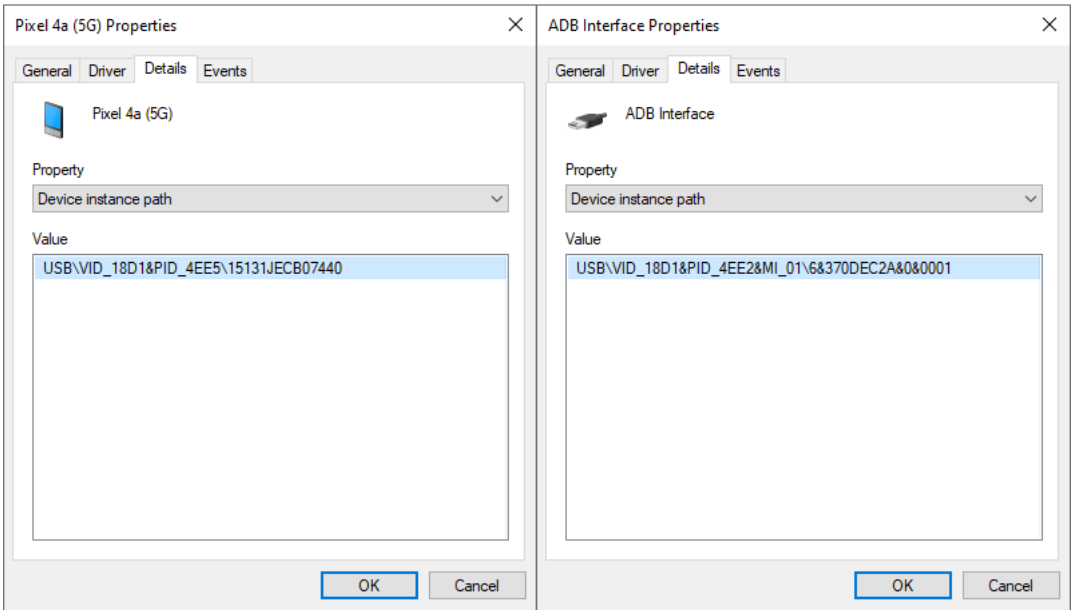
「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

信頼するモバイルデバイスを追加する手順は、信頼するデバイスの他の種別を追加する手順と同じです。モバイルデバイスは ID またはデバイスの機種で追加できます。

ID で信頼するモバイルデバイスを追加するには、一意な ID（ハードウェア ID、Hardware ID – HWID）が必要になります。ID は、オペレーティングシステムツールを使用してデバイスのプロパティ内で表示することができます（下図を参照）。デバイスマネージャーツールを使用すると、プロパティを表示できます。ポータブルデバイス（MTP）および ADB、iTunes デバイスの ID は、同一のモバイルデバイスであっても異なります。ポータブルデバイス（MTP）の ID は「`15131JECB07440`」のように表示されます。ADB デバイスの ID は「`6&370DEC2A&0&0001`」のように表示されます。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。マスクを使用することもできます。

デバイスをコンピューターに接続してから ADB または iTunes アプリケーションをインストールした場合は、デバイスの固有 ID がリセットされる場合があります。つまり、このデバイスは新しいデバイスとして認識されます。デバイスが信頼されている場合は、デバイスを信頼リストに再度追加します。

デバイスの機種で信頼するモバイルデバイスを追加するには、製造元 ID（Vendor ID – VID）および製品 ID（Product ID – PID）が必要です。ID は、オペレーティングシステムツールを使用してデバイスのプロパティ内で表示することができます（下図を参照）。VID および PID の入力用テンプレート：`VID_18D1&PID_4EE5`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。



デバイスマネージャー内のデバイス ID

Bluetooth デバイスへのアクセスの管理

Kaspersky Endpoint Security では、Bluetooth デバイスへのアクセスを管理できます。Bluetooth デバイスには、ワイヤレスキーボード、マウス、ヘッドセット、プリンターなどがあります。また、モバイルデバイスとの通信などにも Bluetooth を使用できます。

Bluetooth デバイスが接続または接続解除されると、本製品がそのデバイスについて複数のイベントを作成することがあります。その理由は、オペレーティングシステムが Bluetooth デバイスを異なる種別の複数のデバイスとして検出する可能性があるためです。Kaspersky Endpoint Security は、そのデバイスの接続に使用されている Bluetooth アダプターも別のデバイスとして管理します。そのため、本製品は検出されたデバイスごとにイベントを作成します。

Bluetooth デバイスへのアクセスには、次のモードのうち 1 つを選択します：

- **許可（ログ記録なし）**：Kaspersky Endpoint Security は、あらゆる Bluetooth デバイスの接続を許可し、接続に関する情報をイベントログに保存しません。Bluetooth 入力デバイス（キーボード、マウスなど）の接続、Bluetooth 経由でのデータ送信、その他の Bluetooth デバイス（ヘッドセット、ヘッドフォンなど）の管理が可能です。

- **許可**：Kaspersky Endpoint Security は、あらゆる Bluetooth デバイスの接続を許可します。Bluetooth 入力デバイス（キーボード、マウスなど）の接続、Bluetooth 経由でのデータ送信、その他の Bluetooth デバイス（ヘッドセット、ヘッドフォンなど）の管理が可能です。

- **ブロック**：Kaspersky Endpoint Security は Bluetooth デバイスへのアクセスを制限します。Bluetooth 入力デバイス（Human Interface Devices クラス）のみの接続を許可することができます。これらのデバイスには、キーボード、マウスデバイス、ジョイスティックなどが含まれます。

信頼する Bluetooth デバイスのリストを作成することはできません。Bluetooth デバイスへのアクセスを制限している場合、接続できるのは Bluetooth 入力デバイスのみです。

管理コンソール（MMC）で Bluetooth デバイスのアクセスルールを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
4. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
5. デバイス種別［**Bluetooth**］のコンテキストメニューで、Bluetooth デバイスのアクセスモード（［**許可**］（ ）、［**ブロック**］（ ）、［**許可（ログ記録なし）**］（ ））を設定します。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールで Bluetooth デバイスのアクセスルールを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。
5. ［**デバイスアクセスルール**］セクションで、［**デバイスと Wi-Fi ネットワーク**］をクリックします。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
6. ［**Bluetooth デバイス**］デバイス種別を選択します。
   Bluetooth デバイスのアクセス設定が開きます。

7. Bluetooth デバイスのアクセスモード（[**許可する**]、[**ブロックする**]、[**許可（ログ記録なし）**]）を設定します。

8. [**ブロックする**] モードを選択した場合、Bluetooth 入力デバイス（キーボード、マウスなど）への接続のみを許可することができます。これを行うには、[**除外リスト**] の下で [**入力デバイス（マウスとキーボード）**] をオンにします。

9. 変更内容を保存します。

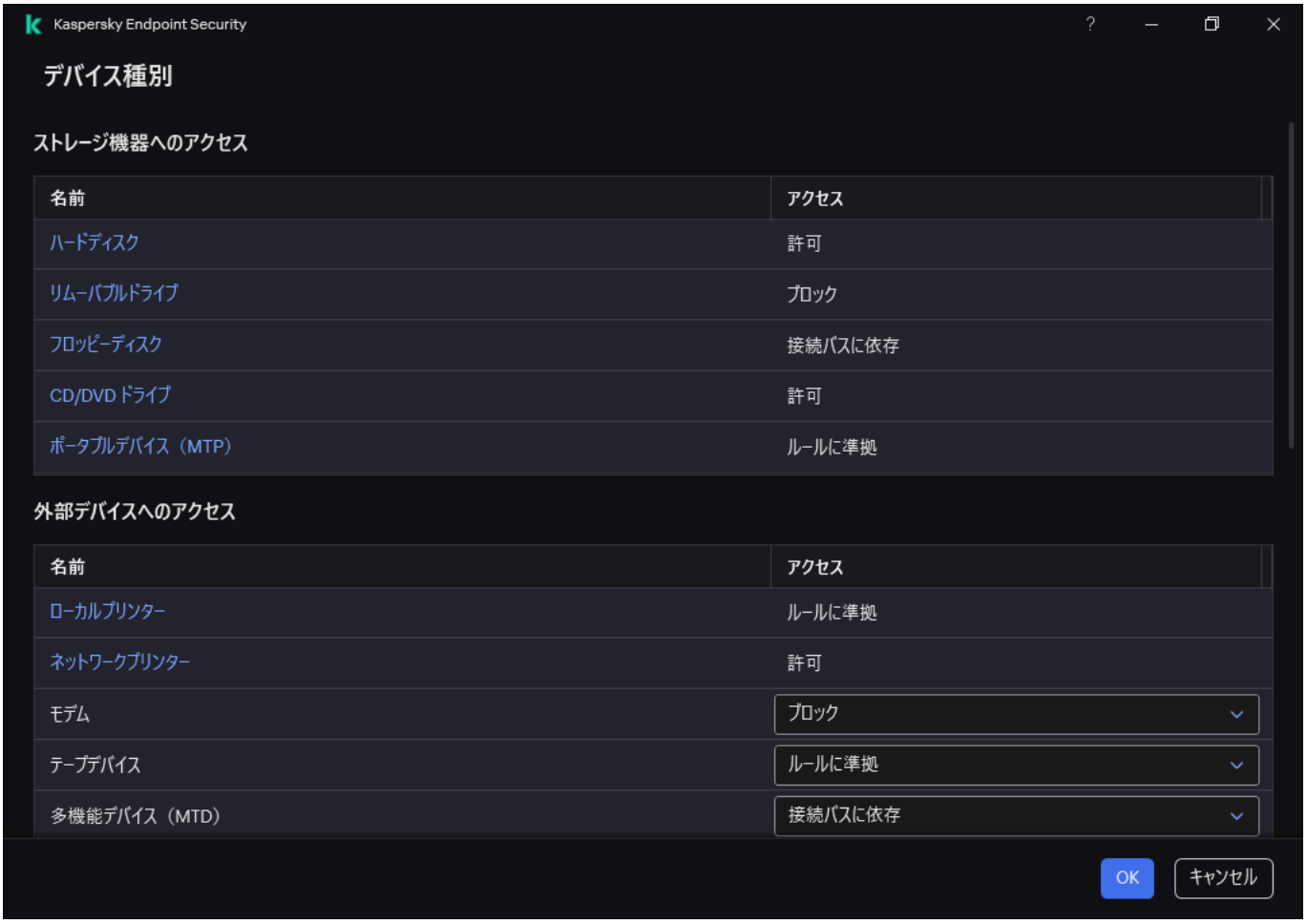
製品インターフェイスで Bluetooth デバイスのアクセスルールを設定する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、[**セキュリティコントロール**] → [**デバイスコントロール**] を選択します。

3. [**アクセスの設定**] ブロックの [**デバイスと Wi-Fi ネットワーク**] をクリックします。

   ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。



デバイスコントロールコンポーネントのデバイス種別

4. [**外部デバイスへのアクセス**] セクションで、[**Bluetooth**] をクリックします。

   Bluetooth デバイスのアクセス設定が開きます。

5. [**アクセス**] で、Bluetooth デバイスのアクセスモード（[**許可**]、[**ブロック**]、[**許可（ログ記録なし）**]）を設定します。

6. ［**ブロック**］モードを選択した場合、Bluetooth 入力デバイス（キーボード、マウスなど）への接続のみを許可することができます。これを行うには、［**除外リスト**］の下で［**入力デバイス（マウスとキーボード）**］をオンにします。

7. 変更内容を保存します。

プリンターのコントロール

ローカルおよびネットワークプリンターへのユーザーアクセスを設定できます。

ローカルプリンターの管理

Kaspersky Endpoint Security では、*接続*および*印刷*の 2 つのレベルでローカルプリンターへのアクセスを設定できます。

Kaspersky Endpoint Security は次のバス経由でローカルプリンターへの接続を管理します：［USB］、［シリアルポート］（COM）、［パラレルポート］（LPT）。

> Kaspersky Endpoint Security はローカルプリンターの COM および LPT ポートへの接続をバスの 1 レベルにおいてのみコントロールします。つまり COM および LPT ポートへのプリンターの接続をブロックするには、ローカルプリンターに［接続バスに依存］アクセスモードを選択し、COM および LPT バスへの接続を禁止する必要があります。

USB に接続されたプリンターについては、本製品はデバイス種別（ローカルプリンター）および接続バス（USB）の 2 レベルをコントロールします。

USB 経由でのローカルプリンターへのアクセスモードは、以下のいずれかから選択することができます：

- **許可**（）：Kaspersky Endpoint Security はすべてのユーザーにローカルプリンターへの完全アクセスを許可します。ユーザーはオペレーティングシステムが提供する方法を使用してプリンターにアクセスして文書を印刷することができます。
- **ブロック**（）：Kaspersky Endpoint Security はローカルプリンターへの接続をブロックします。接続が許可されるのは信頼済みのプリンターのみです。
- **接続バスに依存**（）：Kaspersky Endpoint Security はローカルプリンターへの接続を USB 接続バスのステータス（［**許可**］（）または［**ブロック**］（））に応じて許可します。
- **ルールに準拠**（）：印刷を管理するには、*印刷ルール*を設定する必要があります。ルールでは、ローカルプリンター上での文書の印刷へのアクセスを許可またはブロックするユーザーまたはユーザーグループを選択できます。

ネットワークプリンターの管理

Kaspersky Endpoint Security では、ネットワークプリンター上での印刷へのアクセスを設定することができます。次のネットワークプリンターのアクセスモードのうち1つを選択することができます：

- ［**許可（ログ記録なし）**］（）：Kaspersky Endpoint Security はネットワークプリンターでの印刷をコントロールしません。すべてのユーザーに印刷へのアクセスが許可され、イベントログに印刷に関する情報は保存されません。
- ［**許可**］（）：Kaspersky Endpoint Security はすべてのユーザーにネットワークプリンターでの印刷へのアクセスを許可します。
- ［**ブロック**］（）：Kaspersky Endpoint Security はすべてのユーザーに対してネットワークプリンターへのアクセスを制限します。アクセスが許可されるのは信頼済みのプリンターのみです。
- ［**ルールに準拠**］（）：Kaspersky Endpoint Security は印刷ルールに従って印刷のアクセス権を付与します。ルールでは、ネットワークプリンター上での文書の印刷を許可またはブロックするユーザーまたはユーザーのグループを選択することができます。

プリンターの印刷ルールを追加する

管理コンソール（MMC）で印刷ルールを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
4. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
5. 端末種別［**ローカルプリンター**］および［**ネットワークプリンター**］のコンテキストメニューで、関連するプリンターのアクセスモードを設定します：［**許可**］（）、［**ブロック**］（）、［**許可（ログ記録なし）**］（）（ネットワークプリンターのみ）または［**接続バスに依存**］（）（ローカルプリンターのみ）。
6. ローカルまたはネットワークプリンターの印刷ルールを設定するには、ルールのリストをダブルクリックして開きます。
7. プリンターのアクセスモードとして［**ルールに準拠**］を選択します。
8. 印刷ルールを適用するユーザーまたはユーザーグループを選択します。
   a. ［**追加**］をクリックします。
      新しい印刷ルールを追加するウィンドウが開きます。
   b. ルールの優先度を割り当てます。ルールの項目にはユーザーアカウント、操作（許可またはブロック）、優先度の属性が含まれます。

ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

c. ［**処理**］で、ユーザーのプリンターを使用した印刷へのアクセスを設定します。

d. ［**ユーザーとグループ**］をクリックして、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

e. ［**OK**］をクリックします。

9. 変更内容を保存します。

Web コンソールと Cloud コンソールで印刷ルールを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。

5. ［**デバイスアクセスルール**］セクションで、［**デバイスと Wi-Fi ネットワーク**］をクリックします。

   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。

6. ［**ローカルプリンター**］または［**ネットワークプリンター**］デバイス種別を選択します。

   プリンターのアクセスルールが表示されます。

7. 対応するプリンターのアクセスモードを設定します：［**許可する**］、［**ブロックする**］、［**許可（ログ記録なし）**］（ネットワークプリンターのみ）、［**バスに依存**］（ローカルプリンターのみ）または［**カスタム**］。

8. ［**カスタム**］モードを選択すると、ローカルまたはネットワークプリンターに対して印刷ルールを設定する必要があります。設定するには、印刷ルールの表で［**追加**］をクリックします。

   ネットワーク印刷ルールの設定が開きます。

9. ルールの優先度を割り当てます。ルールの項目にはユーザーアカウント、操作（許可またはブロック）、優先度の属性が含まれます。

   ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

10. ［**処理**］で、ユーザーのプリンターを使用した印刷へのアクセスを設定します。

11. ［**ユーザーまたはグループ**］で、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

12. 変更内容を保存します。

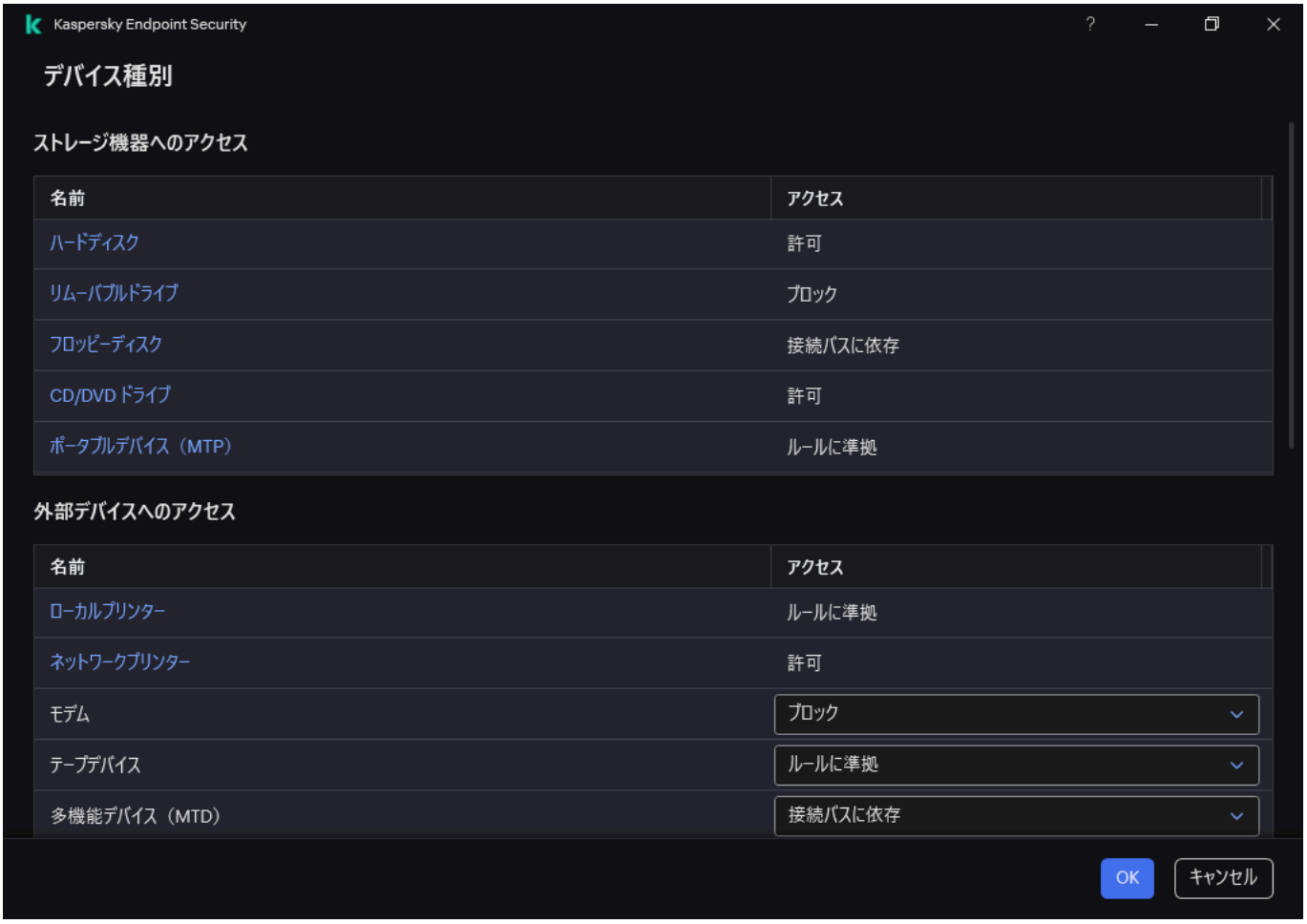
製品インターフェイスで印刷ルールを追加する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。

3. ［**アクセスの設定**］ブロックの［**デバイスと Wi-Fi ネットワーク**］をクリックします。

   ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。



デバイスコントロールコンポーネントのデバイス種別

4. ［**外部デバイスへのアクセス**］で、［**ローカルプリンター**］または［**ネットワークプリンター**］をクリックします。

   プリンターのアクセスルールのウィンドウが表示されます。

5. ［**ローカルプリンターへのアクセス**］または［**ネットワークプリンターへのアクセス**］で、対応するプリンターのアクセスモードを設定します：［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］（ネットワークプリンターのみ）、［**接続バスに依存**］（ローカルプリンターのみ）または［**ルールに準拠**］。

6. ［**ルールに準拠**］モードを選択すると、プリンターに対して印刷ルールを設定する必要があります。印刷ルールを適用するユーザーまたはユーザーグループを選択します。

   a. ［**追加する**］をクリックします。

      新しい印刷ルールを追加するウィンドウが開きます。

   b. ルールの優先度を割り当てます。ルールの項目にはユーザーアカウント、権限（許可またはブロック）、優先度の属性が含まれます。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Endpoint Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Endpoint Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      ブロックルールの優先度は、許可ルールの優先度よりも高くなります。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Endpoint Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**処理**］で、ユーザーの印刷へのアクセス権限を設定します。

   d. ［**ユーザーとグループ**］で、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

7. 変更内容を保存します。

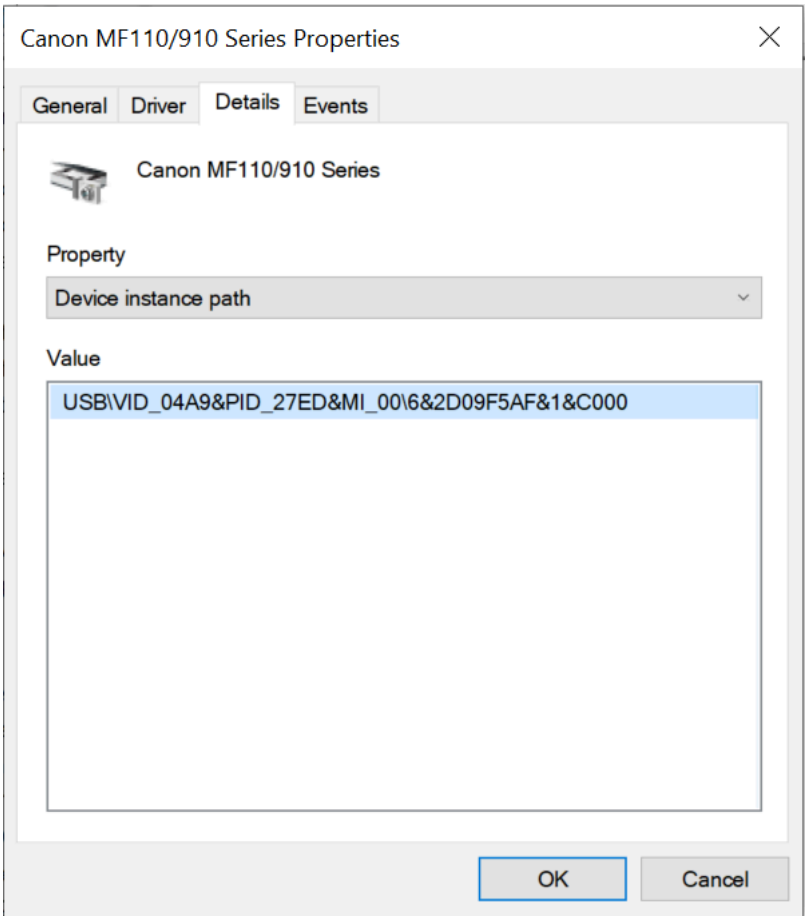
信頼するプリンター

「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

信頼するプリンターを追加する手順は、信頼するデバイスの他の種別を追加する手順と同じです。ローカルプリンターは ID またはデバイスの機種で追加できます。ネットワークプリンターはデバイスの ID によってのみ追加できます。

ID で信頼するローカルプリンターを追加するには、一意な ID（ハードウェア ID、Hardware ID – HWID）が必要になります。ID は、オペレーティングシステムツールを使用してデバイスのプロパティ内で表示することができます（下図を参照）。デバイスマネージャー（Device Manager）ツールを使用すると、プロパティを表示できます。ローカルプリンターの ID は「`6&2D09F5AF&1&C000`」のように表示されます。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。マスクを使用することもできます。

デバイスの機種で信頼するローカルプリンターを追加するには、製造元 ID（Vendor ID – VID）および製品 ID（Product ID – PID）が必要です。ID は、オペレーティングシステムツールを使用してデバイスのプロパティ内で表示することができます（下図を参照）。VID および PID の入力用テンプレート：`VID_04A9&PID_27FD`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。



デバイスマネージャー内のデバイス ID

信頼するネットワークプリンターを追加するには、このデバイス ID が必要です。ネットワークプリンターについては、デバイス ID にはプリンターのネットワーク名（共有プリンターの名前）、プリンターの IP アドレス、プリンターの URL を使用できます。

Wi-Fi 接続の制御

デバイスコントロールを使用して、コンピューター（ノート PC）の Wi-Fi 接続を管理することができます。公衆 Wi-Fi ネットワークは安全でないことがあり、このようなネットワークを使用することによりデータ損失など問題が発生する可能性があります。デバイスコントロールを使用すると、ユーザーの Wi-Fi への接続をブロックしたり、信頼済みのネットワークのみに接続を許可することができます。例えば、セキュリティ要件を満たしている企業 Wi-Fi のネットワークにのみ接続を許可することができます。デバイスコントロールは、信頼リストで指定したもの以外のすべての Wi-Fi ネットワークへのアクセスをブロックします。

Windows 11 を実行しているコンピューターでは、Wi-Fi 接続を制御するために位置情報サービスを有効にする必要があります。これを行うには、オペレーティングシステムの設定で**位置情報サービス**を有効にする必要があります（[**設定**] → [**プライバシーとセキュリティ**] → [**位置情報**]）。位置情報サービスが無効になっている場合、Kaspersky Endpoint Security は Wi-Fi ネットワークへの接続を制御しません。

管理コンソール（MMC）で Wi-Fi 接続を制限する方法

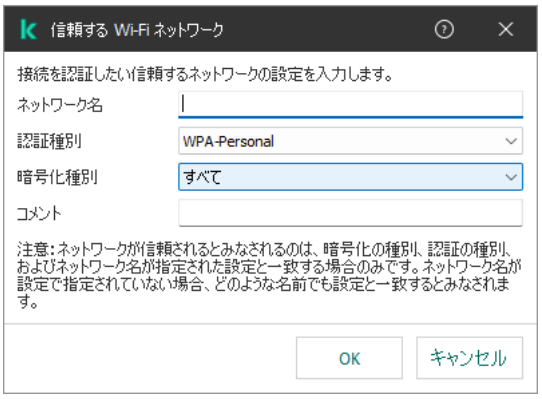
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
4. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
5. 端末種別［**Wi-Fi**］のコンテキストメニューで、［**許可**］（）、［**ブロック**］（）、または［**例外を除きブロック**］（）のいずれかから、デバイスコントロールが Wi-Fi への接続時に実行する操作を選択します。
6. ［**例外を除きブロック**］を選択した場合は、信頼する Wi-Fi ネットワークのリストを作成します。
   a. ダブルクリックして信頼する Wi-Fi ネットワークのリストを開きます。
   b. ［**信頼する Wi-Fi ネットワーク**］ブロックの［**追加**］をクリックします。
   c. 表示されるウィンドウで、信頼する Wi-Fi ネットワークを設定します（下図を参照）。
   - **ネットワーク名**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
   - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。

     Kaspersky Endpoint Security for Windows のバージョン 12.0 から、WPA3 プロトコルのサポートが製品に追加されました。Kaspersky Endpoint Security のバージョン 12.2 のポリシーがコンピューターに適用されている場合、Kaspersky Endpoint Security 11.11.0 以前のバージョンがインストールされたコンピューターには WPA2 プロトコルが選択されます。バージョン 12.0 から 12.1 には WPA2/WPA3 が選択され、12.2 以降のバージョンには WPA3 が選択されます。
   - **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
   - **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

   信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

   すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

7. 変更内容を保存します。



信頼する Wi-Fi ネットワークの設定

Web コンソールおよび Cloud コンソールで Wi-Fi 接続を制限する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。
5. ［**デバイスアクセスルール**］で、［**デバイスと Wi-Fi ネットワーク**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
6. ［**Wi-Fi ネットワーク**］セクションで、［**Wi-Fi**］をクリックします。
7. 表示されたウィンドウで、［**許可する**］、［**ブロックする**］、または［**除外リストを除きブロック**］のいずれかからデバイスコントロールが Wi-Fi 接続時に実行する操作を選択します。
8. ［**除外リストを除きブロック**］を選択した場合は、信頼する Wi-Fi ネットワークのリストを作成します。
   a. ダブルクリックして信頼する Wi-Fi ネットワークのリストを開きます。
   b. ［**信頼する Wi-Fi ネットワーク**］ブロックの［**追加**］をクリックします。
   c. 表示されるウィンドウで、信頼する Wi-Fi ネットワークを設定します（下図を参照）。
      - **名前**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
      - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。

> Kaspersky Endpoint Security for Windows のバージョン 12.0 から、WPA3 プロトコルのサポートが製品に追加されました。Kaspersky Endpoint Security のバージョン 12.2 のポリシーがコンピューターに適用されている場合、Kaspersky Endpoint Security 11.11.0 以前のバージョンがインストールされたコンピューターには WPA2 プロトコルが選択されます。バージョン 12.0 から 12.1 には WPA2/WPA3 が選択され、12.2 以降のバージョンには WPA3 が選択されます。

- **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
- **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

> すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

9. 変更内容を保存します。

製品のインターフェイスで Wi-Fi 接続を制限する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**デバイスと Wi-Fi ネットワーク**］をクリックします。
   ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
4. ［**Wi-Fi ネットワークへのアクセス**］セクションで、［**Wi-Fi**］をクリックします。
   表示されたウィンドウで、Wi-Fi ネットワークのアクセスルールが表示されます。



Wi-Fi のアクセス設定

5. ［**アクセス**］で、［**許可**］、［**ブロック**］、または［**例外を除きブロック**］のいずれかからデバイスコントロールが Wi-Fi 接続時に実行する操作を選択します。

6. ［**例外を除きブロック**］を選択した場合は、信頼する Wi-Fi ネットワークのリストを作成します。

   a. ［**信頼する Wi-Fi ネットワーク**］ブロックの［**追加する**］をクリックします。

   b. 表示されるウィンドウで、信頼する Wi-Fi ネットワークを設定します（下図を参照）。

   - **ネットワーク名**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
   - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。

     Kaspersky Endpoint Security for Windows のバージョン 12.0 から、WPA3 プロトコルのサポートが製品に追加されました。Kaspersky Endpoint Security のバージョン 12.2 のポリシーがコンピューターに適用されている場合、Kaspersky Endpoint Security 11.11.0 以前のバージョンがインストールされたコンピューターには WPA2 プロトコルが選択されます。バージョン 12.0 から 12.1 には WPA2/WPA3 が選択され、12.2 以降のバージョンには WPA3 が選択されます。

   - **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
   - **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

   信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

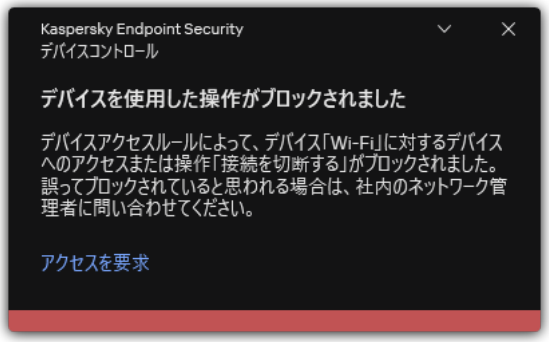
   すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

7. 変更内容を保存します。



信頼する Wi-Fi ネットワークの設定

ユーザーが信頼済みとしてリストに登録されていない Wi-Fi ネットワークに接続しようとした場合、本製品は接続をブロックして通知を表示します（下図を参照）。



デバイスコントロールの通知

リムーバブルドライブの使用状況の監視

リムーバブルドライブの使用状況の監視には以下が含まれます：

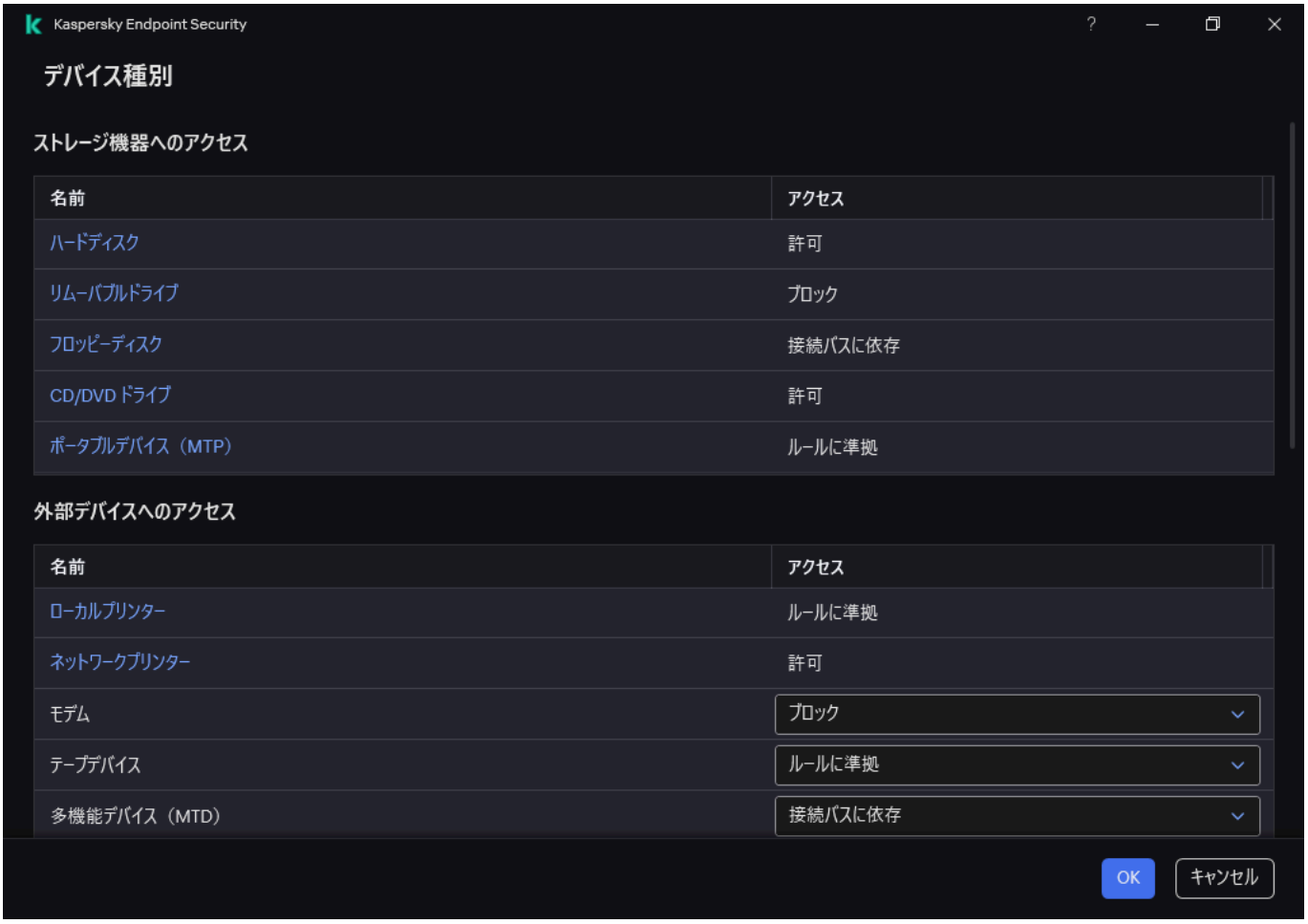
- リムーバブルドライブ上のファイルの操作の監視。
- 信頼済みのリムーバブルドライブの接続および接続解除の監視。

  Kaspersky Endpoint Security を使用して、リムーバブルドライブだけでなくすべての信頼済みデバイスの接続および接続解除を監視できます。イベントの記録はデバイスコントロール機能の通知設定で有効にすることができます。イベントのセキュリティレベルは*情報イベント*です。

リムーバブルドライブの使用状況の監視を有効にするには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**デバイスと Wi-Fi ネットワーク**］をクリックします。

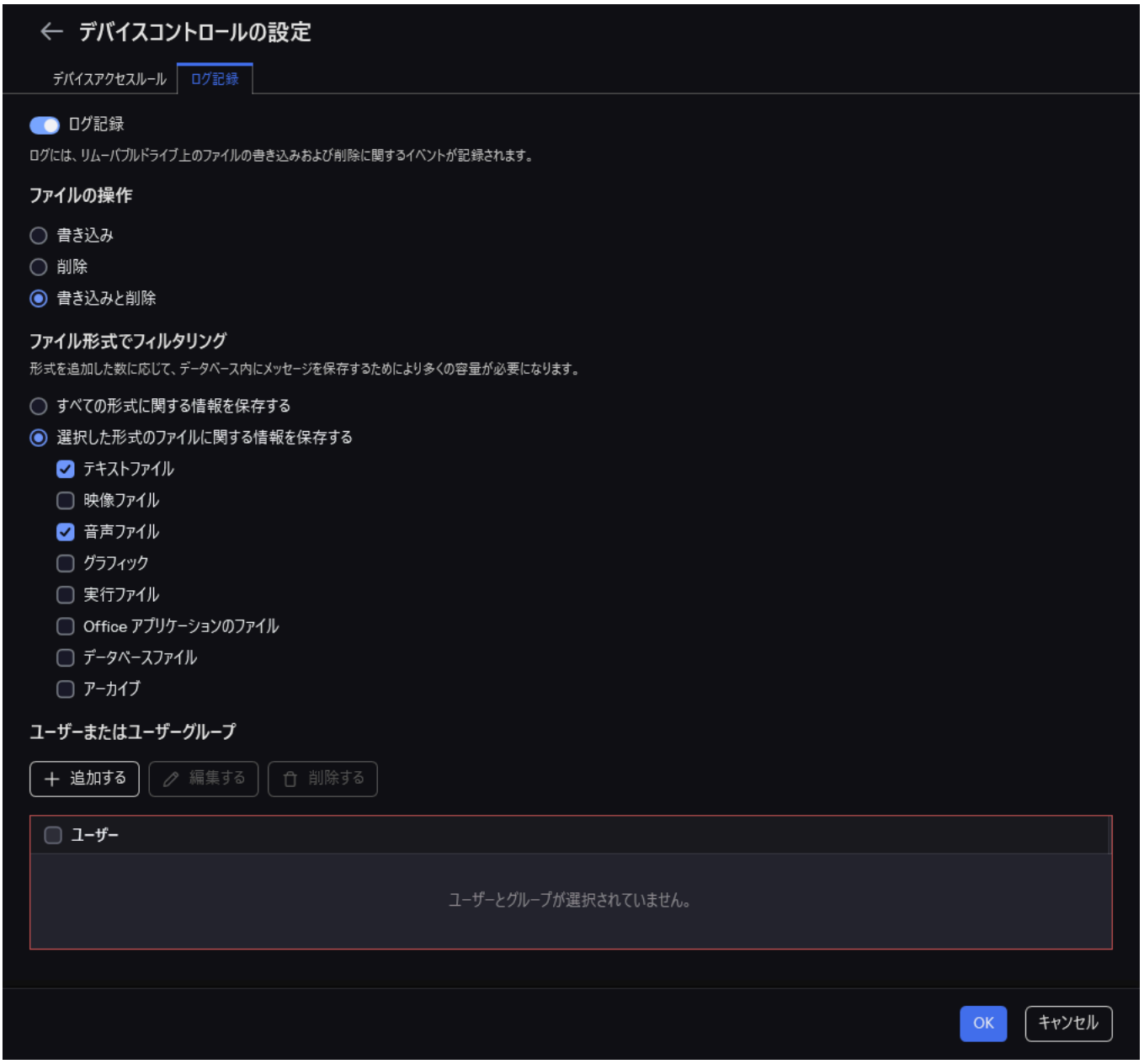
ウィンドウに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。



デバイスコントロールコンポーネントのデバイス種別

4. ［**ストレージ機器へのアクセス**］ブロックで、［**リムーバブルドライブ**］を選択します。

5. 表示されたウィンドウで、**ログ記録**タブを選択します。



リムーバブルドライブの使用監視設定

6. ［**ログ記録**］をオンにします。

7. ［**ファイルの操作**］ブロックで、監視する操作を選択します：**書き込み**、**削除**。

8. ［**ファイル形式でフィルタリング**］ブロックで、デバイスコントロールで記録するファイル形式に関連付けられた操作を選択します。

9. 監視対象のリムーバブルドライブを使用するユーザーまたはユーザーグループを選択します。

10. 変更内容を保存します。

ユーザーが、リムーバブルドライブ上のファイルに書き込みをしたりリムーバブルドライブのファイルを削除すると、その操作に関する情報がイベントログに保存され、Kaspersky Security Center にイベントが送信されます。Kaspersky Security Center の管理コンソールに保存されているリムーバブルドライブのファイルに関するイベントは、［**管理サーバー**］ノードの作業領域内の［**イベント**］タブで確認できます。ローカルの Kaspersky Endpoint Security のイベントログにイベントを表示するには、デバイスコントロールの通知設定で［**ファイルの操作が実行されました**］をオンにしてください。

キャッシュ期間の変更

デバイスコントロール機能は、監視対象デバイスに関連するイベント（デバイスからファイルを読み取り、ファイルをデバイスに書き込む、またその他のイベントのようなデバイスに接続したり接続を解除したりするイベント）を登録します。デバイスコントロールは次に Kaspersky Endpoint Security の設定に従って動作を許可したりブロックしたりします。

デバイスコントロールはキャッシュ*期間*とよばれると口絵の期間イベントに関する情報を保存します。イベントに関する情報がキャッシュされて登録された場合、デバイスへの接続などについて Kaspersky Endpoint Security に関連する情報を通知したり、関連する動作に関してアクセス件を付与するために別のプロンプトを表示する必要はありません。これによりデバイスでの作業がより簡便になります。

次のイベントの設定がキャッシュ内の記録と一致する場合、イベントは重複するイベントとして認識されます：

- デバイス ID
- アクセスを試行したユーザーアカウントの SID
- デバイスカテゴリ
- デバイスに対して実行されら操作
- この操作に関するアプリケーションの権限：許可または拒否
- 操作を実行するために使用されたプロセスのパス
- アクセスされたファイル

キャッシュ期間の変更より前に、Kaspersky Endpoint Security のセルフディフェンスが無効にしてください。キャッシュ期間を変更後、セルフディフェンスを有効にしてください。

キャッシュ期間を変更するには：

1. コンピューター上のレジストリエディタを開きます。
2. レジストリエディタで、次のセクションに移動します：
   - 64 ビットのオペレーティングシステムでは：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - 32 ビットのオペレーティングシステムでは：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. `DeviceControlEventsCachePeriod` を開いて編集します。
4. デバイスコントロールがイベントに関する情報を保存する期間を定義します（分）。

信頼するデバイスを使用した処理

「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。

信頼するデバイスで作業するには、個々のユーザー、ユーザーグループ、または組織内のすべてのユーザーにアクセス権を付与できます。

たとえば、組織でリムーバブルドライブの使用を許可していないが、管理者が仕事でリムーバブルドライブを使用している場合、管理者グループのみにリムーバブルドライブを許可できます。これを行うには、信頼するリストにリムーバブルドライブを追加し、ユーザーのアクセス許可を設定します。

信頼するデバイスを 1000 以上追加すると、システムが不安定になる可能性があるため推奨されません。

Kaspersky Endpoint Security では、次の方法でデバイスを信頼リストに追加できます：

- 組織に Kaspersky Security Center が導入されていない場合、デバイスをコンピューターに接続し、アプリケーション設定の信頼リストに追加できます。信頼するデバイスのリストを組織内のすべてのコンピューターに配布するには、ポリシー内の信頼するデバイスのリストの統合を有効にするか、エクスポート/インポート手順を使用できます。
- 組織に Kaspersky Security Center が導入されている場合、接続されているすべてのデバイスをリモートで検出し、ポリシーで信頼するデバイスのリストを作成できます。信頼するデバイスのリストは、ポリシーが適用されるすべてのコンピューターで利用できます。

Kaspersky Endpoint Security では、信頼済みデバイスの使用をコントロールできます（接続および接続解除）。イベントの記録はデバイスコントロール機能の通知設定で有効にすることができます。イベントのセキュリティレベルは*情報*です。

アプリケーションインターフェイスから信頼リストへのデバイスの追加

既定では、信頼するデバイスのリストにデバイスを追加すると、そのデバイスへのアクセス権がすべてのユーザー（「Everyone」グループに属するユーザー）に付与されます。

製品インターフェイスから信頼リストにデバイスを追加するには、次の操作を行います：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**信頼するデバイス**］をクリックします。
   信頼するデバイスのリストが開きます。
4. ［**選択する**］をクリックします。
   接続されたデバイスのリストが開きます。デバイスのリストは、［**接続されているデバイスの表示**］で選択した値により異なります。

5. デバイスのリストで、信頼するデバイスのリストに追加するデバイスを選択します。

Kaspersky Endpoint Security は、**フロッピーディスク**の種別のデバイスの信頼リストへの追加をサポートしていません。

6. ［**コメント**］フィールドで、その信頼するデバイスに関する情報を入力できます。

7. 信頼するデバイスへのアクセスを許可するユーザーまたはユーザーグループを選択します。

ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

8. 変更内容を保存します。

Kaspersky Security Center から信頼リストへのデバイスの追加

Kaspersky Security Center は、Kaspersky Endpoint Security がコンピューターにインストールされており、かつデバイスコントロールが有効の場合に、デバイスに関する情報を取得します。デバイスに関する情報が Kaspersky Security Center で利用可能でない限り、デバイスを信頼できるリストに追加することはできません。

次のデータに従って、デバイスを信頼リストに追加できます：

- **ID によるデバイス**：各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。

- **モデルによるデバイス**：各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：`VID_1234&PID_5678`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。

- **ID マスクによるデバイス**：ID が類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`WDC_C*`」。

- **モデルマスクによるデバイス**：同一の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`VID_05AC&PID_*`」。

信頼ゾーンは、管理コンソール（MMC）と Web コンソールで異なる方法でグループ化されます。同様に、信頼ゾーンのパラメータ変更を防止する方法も異なります（別の「南京錠」）。本製品の管理には、Web コンソールのみを使用することを推奨します。別のコンソールで信頼ゾーンを設定すると、管理プラグインによって「南京錠」が既定の状態にリセットされる場合があります。

信頼するデバイスのリストにデバイスを追加するには、次の操作を行います：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。
4. ウィンドウの右側で、［**信頼するデバイス**］タブを選択します。
5. 組織内のすべてのコンピューターの信頼するデバイスのリストを作成する場合は［**継承時に値を統合する**］をオンにします。

   親ポリシーおよび子ポリシー内の信頼するデバイスのリストが統合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシー内の信頼するデバイスは子ポリシー内では読み取り専用で表示されます。親ポリシー内の信頼するデバイスは編集または削除することはできません。
6. ［**追加**］をクリックし、デバイスを信頼リストに追加する方法を選択します。
7. デバイスをフィルタリングするには、［**デバイス種別**］ドロップダウンリストで、デバイス種別を選択します（たとえば、［**リムーバブルドライブ**］）。

   Kaspersky Endpoint Security は、**フロッピーディスク**の種別のデバイスの信頼リストへの追加をサポートしていません。
8. ［**名前またはモデル**］フィールドに、選択した追加方法に応じて、ID、モデル（VID および PID）、またはマスクを入力します。

   モデルマスク（VID および PID）によるデバイスの追加は次のように行われます：どのモデルにも一致しないモデルマスクを入力すると、デバイス ID（HWID）がマスクと一致するかどうかがチェックされます。製作元とデバイス種別を識別するデバイス ID の一部のみがチェックされます（`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`）。モデルマスクがデバイス ID の一部と一致する場合、マスクと一致するデバイスがコンピューター上で信頼するデバイスのリストに追加されます。しかし、Kaspersky Security Center のデバイスリストは［**更新**］をクリックすると空のままになります。デバイスリストを正しく表示させるには、デバイス ID マスクを使用してデバイスを追加します。
9. デバイスをフィルタリングするには、［**コンピューター**］フィールドに、デバイスが接続されているコンピューター名またはコンピューター名のマスクを入力します。

   `*` 文字は、任意の文字列を置き換えます。`?` 文字は、任意の 1 文字を置き換えます。
10. ［**更新**］をクリックします。

    テーブルには、定義されたフィルタリング基準を満たすデバイスのリストが表示されます。
11. 信頼するデバイスのリストに追加するデバイス名の横にあるチェックボックスをオンにします。
12. ［**コメント**］フィールドに、デバイスを信頼リストに追加する理由の説明を入力します。
13. ［**許可するユーザーまたはユーザーグループ**］フィールドの右側にある［**選択**］をクリックします。

14. ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

    既定では、信頼するデバイスへのアクセスは Everyone グループに対して許可されます。

15. 変更内容を保存します。

デバイスが接続されると、Kaspersky Endpoint Security は、認証済みユーザーの信頼するデバイスのリストを確認します。デバイスが信頼されている場合は、デバイス種別または接続バスへのアクセスが拒否された場合でも、Kaspersky Endpoint Security は、すべての権限でデバイスへのアクセスを許可します。デバイスが信頼されておらず、アクセスが拒否された場合は、ロックされたデバイスへのアクセス要求ができます。

信頼するデバイスのリストのエクスポート / インポート

信頼するデバイスのリストを組織内のすべてのコンピューターに配布するには、エクスポート/インポート手順を使用できます。

たとえば、信頼するリムーバブルドライブのリストを配布する必要がある場合、次のことを行う必要があります：

1. リムーバブルドライブをコンピューターに順次接続します。
2. Kaspersky Endpoint Security の設定で、リムーバブルドライブを信頼するリストに追加します。必要に応じて、ユーザーのアクセス許可を設定します。たとえば、管理者のみがリムーバブルドライブにアクセスできるようにします。
3. Kaspersky Endpoint Security の設定で信頼するデバイスのリストをエクスポートします（以下の手順を参照）。
4. 信頼するデバイスリストのファイルを組織内の他のコンピューターに配布します。たとえば、ファイルを共有フォルダーに配置します。
5. 組織内の他のコンピューターの Kaspersky Endpoint Security の設定で、信頼するデバイスのリストをインポートします（以下の手順を参照）。

信頼するデバイスのリストをインポートまたはエクスポートするには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**信頼するデバイス**］をクリックします。

    信頼するデバイスのリストが開きます。

4. 信頼するデバイスのリストをエクスポートするには：

    a. 編集する信頼するデバイスを選択します。

    b. ［**エクスポート**］をクリックします。

    c. 表示されたウィンドウで、信頼するデバイスのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. ファイルを保存します。

Kaspersky Endpoint Security は、信頼するデバイスのリスト全体を XML ファイルにエクスポートします。

5. 信頼するデバイスのリストをインポートするには：

a. ［**インポート**］で、関連する操作を選択します：［**インポートして既存に追加**］または［**インポートして既存を置換**］。

b. 表示されたウィンドウで、信頼するデバイスのリストをインポートする XML ファイルを選択します。

c. ファイルを開きます。

6. 変更内容を保存します。

デバイスが接続されると、Kaspersky Endpoint Security は、認証済みユーザーの信頼するデバイスのリストを確認します。デバイスが信頼されている場合は、デバイス種別または接続バスへのアクセスが拒否された場合でも、Kaspersky Endpoint Security は、すべての権限でデバイスへのアクセスを許可します。

ブロックされたデバイスへのアクセスの取得

デバイスコントロールの設定次第では、業務で必要なデバイスを誤ってブロックしてしまう可能性があります。

組織内に Kaspersky Security Center が導入されていない場合、 Kaspersky Endpoint Security のローカルの設定を使用して、デバイスへのアクセスを付与できます。たとえば、そのデバイスを信頼リストに追加したり、デバイスコントロールを一時的に無効にすることができます。

組織内に Kaspersky Security Center が導入されていてコンピューターにポリシーが適用されている場合、管理コンソールを使用して、デバイスへのアクセスを付与できます。

オンラインモードでのアクセス権の付与

ブロックされたデバイスへのオンラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。このコンピューターは管理サーバーに接続できる必要があります。

オンラインモードでのアクセス権が付与される流れは次の通りです：

1. ユーザーが管理者にアクセス要求のメッセージを送信します。

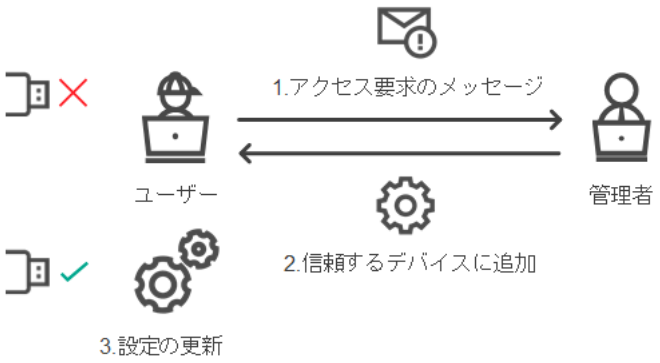
2. 管理者が Kaspersky Security Center コンソールで要求のメッセージを受け取ります。

Kaspersky Security Center コンソールには、ユーザーからのメッセージを確認しやすいよう、プリセットのイベント抽出「*ユーザー要求*」があります。

3. 管理者が、該当するデバイスを信頼リストに追加します。

管理者は、管理グループのポリシーまたは個別のコンピューターのローカルでの製品設定で、信頼するデバイスを追加できます。

4. 管理者が、ユーザーのコンピューター上の Kaspersky Endpoint Security の設定を更新します。



オンラインモードでのデバイスへのアクセス権の付与のプロセス

オフラインモードでのアクセス権の付与

ブロックされたデバイスへのオフラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。ポリシー設定の［**デバイスコントロール**］セクションで、［**一時アクセスの要求を許可する**］がオンになっている必要があります。

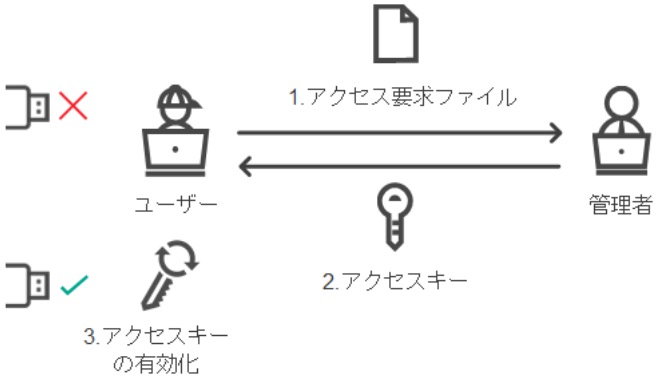
デバイスを信頼リストに追加することはできない状況で、ブロックされているデバイスへの一時的なアクセス権を付与する場合は、デバイスへのオフラインモードでのアクセス権を付与できます。この方法を使用することで、コンピューターがネットワークに接続されていなかったり、企業ネットワークの外で動作している場合でも、ブロックされているデバイスへのアクセス権を付与できます。

オフラインモードでのアクセス権が付与される流れは次の通りです：

1. ユーザーがアクセス要求ファイルを作成し、管理者に送信します。

2. 管理者がアクセス要求ファイルからアクセスキーを作成して、ユーザーに送信します。

3. ユーザーはアクセスキーを有効化します。



オフラインモードでのデバイスへのアクセス権の付与のプロセス

オンラインモードでのアクセス権の付与

ブロックされたデバイスへのオンラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。このコンピューターは管理サーバーに接続できる必要があります。

ユーザーがブロックされたデバイスへのアクセスを要求する方法は次の通りです：

1. コンピューターにデバイスを接続します。

   Kaspersky Endpoint Security によって、このデバイスへのアクセスがブロックされているという通知が表示されます（以下の図を参照）。

2. ［**アクセスを要求**］リンクをクリックします。

   管理者へのメッセージのウィンドウが表示されます。このメッセージには、ブロックされているデバイスの情報が含まれています。

3. ［**送信**］をクリックします。



デバイスコントロールの通知

次に、Kaspersky Security Center コンソールの管理者が［*デバイスへのアクセスブロックに関するメッセージが管理者に送信されました*］イベントを受け取ります。このイベントには、ユーザー名、コンピューター名、ユーザーがアクセスを取得しようとしているデバイスの詳細などの情報が含まれます。メール通知を選択するなど、このようなイベントを管理者に通知する方法を設定できます。Kaspersky Security Center コンソールには、ユーザーからのメッセージを確認しやすいよう、プリセットのイベント抽出「*ユーザー要求*」があります。

アクセスを許可するには、信頼リストにデバイスを追加する必要があります。コンピューターで Kaspersky Endpoint Security の設定を更新したら、ユーザーはデバイスへのアクセスを取得できるようになります。

オフラインモードでのアクセス権の付与

ブロックされたデバイスへのオフラインモードでのアクセス権は、組織内で Kaspersky Security Center を導入済みで対象のコンピューターにポリシーが適用されている場合にのみ付与できます。ポリシー設定の［**デバイスコントロール**］セクションで、［**一時アクセスの要求を許可する**］がオンになっている必要があります。

ユーザーがブロックされたデバイスへのアクセスを要求する方法は次の通りです：

1. コンピューターにデバイスを接続します。

   Kaspersky Endpoint Security によって、このデバイスへのアクセスがブロックされているという通知が表示されます（以下の図を参照）。

2. ［**一時的なアクセスを要求**］リンクをクリックします。

   接続されているデバイスを含むウィンドウが開きます。

3. 接続されているデバイスのリストから、アクセス権を取得するデバイスを選択します。

4. ［**アクセス要求ファイルを生成**］をクリックします。

5. ［**アクセス期間**］で、デバイスにアクセスする期間を指定します。

6. ファイルをコンピューター上に保存します。

これにより、拡張子が「.akey」のアクセス要求ファイルがコンピューターにダウンロードされます。任意の受け渡し方法で、アクセス要求ファイルを企業 LAN の管理者に送信します。



デバイスコントロールの通知

管理コンソール（MMC）で、管理者がブロックされたデバイス向けのアクセスキーを作成する方法

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーの［**管理対象デバイス**］フォルダーで、対象のクライアントコンピューターが属する管理グループの名前のフォルダーを開きます。

3. 作業領域で、［**デバイス**］タブを選択します。

4. クライアントコンピューターのリストで、ブロックされたデバイスへの一時アクセスをユーザーに許可する必要があるコンピューターを選択します。

5. コンピューターのコンテキストメニューで、［**オフラインモードでのアクセスを許可する**］を選択します。

6. 表示されたウィンドウで、**デバイスコントロール**タブを選択します。

7. ［**参照**］をクリックして、ユーザーから受信したアクセス要求ファイルをダウンロードします。

   ユーザーがアクセスを要求した、ブロックされたデバイスの情報が表示されます。

8. 必要に応じて、［**アクセス期間**］設定の値を変更します。

   既定では、［**アクセス期間**］の値は、アクセス要求ファイルの作成時にユーザーが指定した値となります。

9. ［**アクティベーション期限**］設定の値を指定します。

   この設定では、ユーザーがアクセスキーを使用して、ブロックされたデバイスへのアクセスを有効化できる期間を定義します。

10. アクセスキーファイルをコンピューター上に保存します。

Web コンソールまたは Cloud コンソールで、管理者がブロックされたデバイス向けのアクセスキーを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. クライアントコンピューターのリストで、ブロックされたデバイスへの一時アクセスをユーザーに許可する必要があるコンピューターを選択します。

3. コンピューターのリストに上にある省略記号ボタン（ **...** ）をクリックして、［**オフラインモードでのデバイスへのアクセスを許可**］ボタンをクリックします。

4. 表示されたウィンドウで、［**デバイスコントロール**］セクションを選択します。

5. ［**参照**］をクリックして、ユーザーから受信したアクセス要求ファイルをダウンロードします。

   ユーザーがアクセスを要求した、ブロックされたデバイスの情報が表示されます。

6. 必要に応じて、［**アクセス期間（時間）**］設定の値を変更します。

   既定では、［**アクセス期間（時間）**］の値は、アクセス要求ファイルの作成時にユーザーが指定した値となります。

7. デバイス上でのアクセスキーの有効期間を指定します。

   この設定では、ユーザーがアクセスキーを使用して、ブロックされたデバイスへのアクセスを有効化できる期間を定義します。

8. アクセスキーファイルをコンピューター上に保存します。

これにより、ブロックされたデバイスへのアクセスキーファイルがコンピューターにダウンロードされます。アクセスキーファイルの拡張子は「.acode」です。任意の受け渡し方法で、ブロックされたデバイスへのアクセスキーファイルをユーザーに送信します。

ユーザーは次の方法でアクセスキーを有効化します。

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。

3. ［**アクセス要求**］ブロックの［**デバイスへのアクセス要求**］をクリックします。

4. 表示されたウィンドウで、［**アクセスキーの有効化**］をクリックします。

5. 表示されたウィンドウで、企業 LAN 管理者から受け取ったデバイスへのアクセスキーを持つファイルを選択します。

   アクセスの提供に関する情報を確認できるウィンドウが表示されます。

6. ［**OK**］をクリックします。

これにより、管理者が指定した期間、ユーザーにデバイスへのアクセス権が付与されます。ユーザーにはデバイスへのすべてのアクセス権（読み取りと書き込み）が付与されます。キーの有効期限が切れると、デバイスへのアクセスがブロックされます。ユーザーがデバイスへの恒久的なアクセス権を必要としている場合、デバイスを信頼リストに追加します。

デバイスコントロールメッセージのテンプレートの編集

ブロックされているデバイスへのアクセスをユーザーが試行すると、そのデバイスへのアクセスはブロックされていること、またはデバイスの操作はブロックされていることを示すメッセージが表示されます。カスペルスキーのエキスパートは、デバイスへのアクセスがブロックされた理由を説明するメッセージのテンプレートをユーザーに提供します（下の図を参照）。

メッセージのテンプレートの管理用に特別な変数が用意されています（例：`%USER_NAME%`）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。



デバイスコントロールの通知

誤ってデバイスへのアクセスがブロックされているかデバイスの操作がブロックされていると考えられる場合、ユーザーはブロック処理についてのメッセージにあるリンクをクリックして、LAN 管理者にメッセージを送信できます。これを行うには、［**アクセスを要求**］ボタンまたは［**一時的なアクセスを要求**］ボタンをクリックして、状況を説明するメッセージを管理者に送信します。管理者へのメッセージのテンプレートを作成しておき、デバイスへのアクセスを許可するかブロックするかの決定に役立つデータを追加することもできます。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**デバイスへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

管理コンソール（MMC）でデバイスコントロールのメッセージのテンプレートを変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］の順に選択します。

4. ［**メッセージのテンプレートの設定**］ブロックの［**テンプレート**］をクリックします。

5. ウィンドウが表示されるので、そのウィンドウでアプリケーションコントロールのテンプレートを設定します：

   - **ブロックに関するメッセージ**：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。

   - **管理者に送信するメッセージ**：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが LAN 管理者に送信するメッセージのテンプレートが含まれています。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでデバイスコントロールのメッセージのテンプレートを変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**デバイスコントロール**］に移動します。

5. ［**メッセージのテンプレート**］ブロックで、アプリケーションコントロールのメッセージのテンプレートを設定します：

   - **ユーザーへのメッセージ**：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。

   - **管理者へのメッセージ**：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが LAN 管理者に送信するメッセージのテンプレートが含まれています。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

製品インターフェイスでデバイスコントロールのメッセージのテンプレートを変更する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**メッセージのテンプレート**］ブロックで、アプリケーションコントロールのメッセージのテンプレートを設定します：

   - **ブロックに関するメッセージ**：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。
   - **管理者に送信するメッセージ**：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーがLAN管理者に送信するメッセージのテンプレートが含まれています。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   既定のテンプレートテキストを復元することもできます。
4. 変更内容を保存します。

アンチブリッジ

アンチブリッジは、ネットワークブリッジの作成をブロックし、コンピューターで複数のネットワーク接続が同時に確立することを防止します。この機能を使用することで、セキュリティ保護が不十分で接続が許可されていないネットワークから社内ネットワークを保護できます。

アンチブリッジは、*接続ルール*を使用してネットワーク接続の確立を管理します。

以下の定義済みデバイス種別に対して接続ルールが作成されます：

- ネットワークアダプター
- Wi-Fi アダプター
- モデム

接続ルールが有効な場合、以下が実行されます：

- ルールで指定されたデバイス種別が両方の接続で使用されていた場合、新しい接続を確立する際に現在の接続をブロックします。
- 優先順位の低いルールが適用されるデバイス種別を使用して確立された接続をブロックします。

アンチブリッジを有効にする

アンチブリッジは既定で無効です。

アンチブリッジを有効にするには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**アンチブリッジ**］をクリックします。
4. ［**アンチブリッジを有効にする**］トグルスイッチを使用して機能を有効または無効にします。
5. 変更内容を保存します。

アンチブリッジを有効にすると、接続ルールに従って、すでに確立されている接続がブロックされます。

接続ルールのステータスの変更

接続ルールのステータスを変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**アンチブリッジ**］をクリックします。
4. ［**デバイスのルール**］ブロックで、ステータスを変更するルールを選択します。
5. ［**コントロール**］列のトグルスイッチを使用してルールを有効または無効にします。
6. 変更内容を保存します。

接続ルールの優先度の変更

接続ルールの優先度を変更するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**デバイスコントロール**］を選択します。
3. ［**アクセスの設定**］ブロックの［**アンチブリッジ**］をクリックします。
4. ［**デバイスのルール**］ブロックで、優先度を変更するルールを選択します。
5. ［**上へ**］と［**下へ**］を使用して接続ルールの優先度を設定します。

   リスト上の位置が高くなるほど、ルールの優先度が高くなります。アンチブリッジは、最も優先度が高いルールが使用されるデバイス種別によって確立された接続を除くすべての接続をブロックします。
6. 変更内容を保存します。

アダプティブアノマリーコントロール

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「*Office アプリケーションによる Microsoft PowerShell の起動*」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートするのと同様に、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。ルールのアップデートの適用は手動で承認する必要があります。

アダプティブアノマリーコントロールの設定

アダプティブアノマリーコントロールの設定では、次のステップが必要です：

1. アダプティブアノマリーコントロールのトレーニング

   アダプティブアノマリーコントロールを有効にすると、アダプティブアノマリーコントロールルールが*トレーニングモード*で動作します。トレーニング期間中、アダプティブアノマリーコントロールはルールを適用可能な動作が発生するかどうかを監視し、ルールを適用可能な動作が発生したらそのイベントを Kaspersky Security Center に送信します。ルールごとに、設定されているトレーニング期間は異なります。トレーニングモードの継続期間はカスペルスキーのエキスパートが設定しています。通常は、トレーニングモードの継続期間は 2 週間です。

   特定のルールを適用可能な動作がトレーニング期間中に 1 回も発生しなかった場合、アダプティブアノマリーコントロールは、そのルールの対象となる動作は平常時には発生しない動作だと判断します。そのため、トレーニング終了後、該当するルールの適用対象となる動作はすべて Kaspersky Endpoint Security でブロックされるようになります。

   特定のルールを適用可能な動作がトレーニング期間中に発生した場合、Kaspersky Endpoint Security は「ルールの適用のレポート」と［**「スマートトレーニング」ステータスのルール適用条件**］リポジトリにイベントのログ記録を保存します。

2. 「ルールの適用のレポート」の分析

   管理者は「ルールの適用のレポート」または［**「スマートトレーニング」ステータスのルール適用条件**］リポジトリの内容を分析する必要があります。分析結果に基づき、管理者はそれぞれのルールが適用されたときのアダプティブアノマリーコントロールによる処理を、「ブロック」または「許可」から選択します。管理者は、ルールの適用状況に関する情報をさらに収集した上で判断を行うために、トレーニングモードの期間を延長することもできます。また、管理者がルールの適用状況のレポートに対する対応を行わなかった場合も、アダプティブアノマリーコントロールは引き続きトレーニングモードで動作します。トレーニングモードの残り期間もリセットされます。

アダプティブアノマリーコントロールの設定は、リアルタイムで次の方法で設定されます：

- トレーニングモードの期間中に1回も適用可能な動作が発生しなかったルールについては、該当するルールが適用可能な動作をすべてブロックする設定が自動的に行われる。
- 新しいルールの追加や古くなったルールの削除が Kaspersky Endpoint Security によって行われる。
- 管理者がルール適用のレポートまたは**「スマートトレーニング」ステータスのルール適用条件**リポジトリの内容を確認した後、アダプティブアノマリーコントロールによる処理を設定します。ルールの適用に関するレポートと、[**「スマートトレーニング」ステータスのルール適用条件**] ストレージの内容をチェックすることをお勧めします。

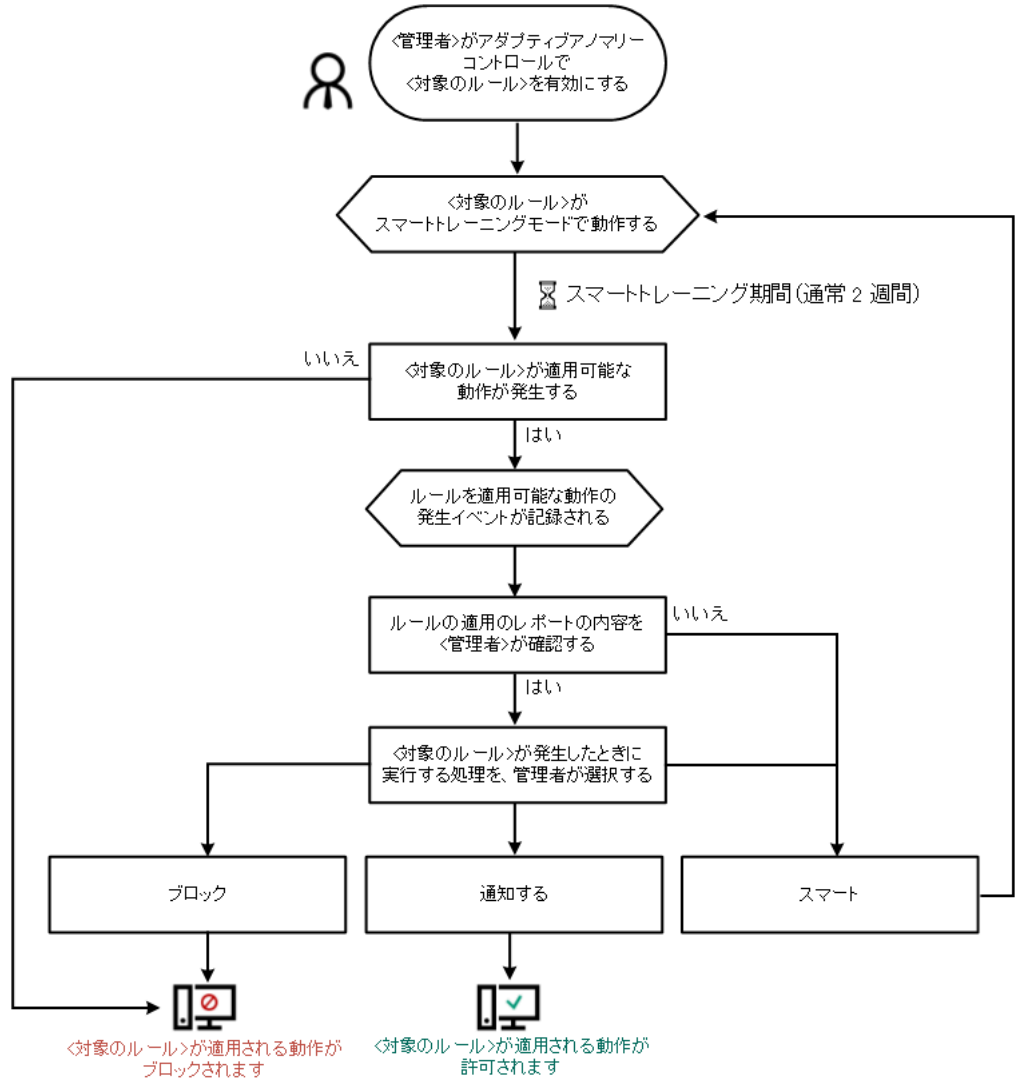
悪意のあるアプリケーションによる動作が検知された場合、Kaspersky Endpoint Security はその動作をブロックし通知を表示します（以下の図を参照）。



アダプティブアノマリーコントロールの通知

アダプティブアノマリーコントロールの動作アルゴリズム

Kaspersky Endpoint Security は次の図のアルゴリズムに従って、ルールの適用対象となる動作の実行を許可するかブロックするかを判定します。



アダプティブアノマリーコントロールの動作アルゴリズム

アダプティブアノマリーコントロールのトレーニング

アダプティブアノマリーコントロールには、一連のルール（ふるまいパターン）が含まれています。アダプティブアノマリーコントロールを有効にすると、アダプティブアノマリーコントロールルールが *トレーニングモード*で動作します。トレーニング期間中、アダプティブアノマリーコントロールはルールを適用可能な動作が発生するかどうかを監視し、ルールを適用可能な動作が発生したらそのイベントを Kaspersky Security Center に送信します。アダプティブアノマリーコントロールは、コンピューター上のアプリケーション動作状況をブロックせず、管理者に通知するだけです。アダプティブアノマリーコントロールのルールの適用時に実行する処理を手動で選択することもできます。

管理コンソール（MMC）でアダプティブアノマリーコントロールのルールのリストを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］の順に選択します。

5. ［**アダプティブアノマリーコントロール**］チェックボックスをオンにします。

6. ［**アダプティブアノマリーコントロールルールの設定**］で、ルールのリストを確認します。
   既定では、すべてのルールは［**スマート**］モードで動作しています。

7. 必要に応じて、アダプティブアノマリーコントロールのルールの更新を確認します。

8. 必要に応じて、アダプティブアノマリーコントロールのルールの適用時の処理を選択します：

   - **ブロック**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

   - **通知**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、ルールの適用対象となった動作の情報がログに記録されます。

9. 必要に応じて、使用しないルールを無効にします。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（  ）。

Web コンソールおよび Cloud コンソールでアダプティブアノマリーコントロールのルールを表示する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］に移動します。

5. ［**アダプティブアノマリーコントロールは有効です**］をオンにします。

6. ［**ルール**］で、ルールのリストを確認します。
   既定では、すべてのルールは［**スマート**］モードで動作しています。

7. 必要に応じて、アダプティブアノマリーコントロールのルールの更新を確認します。

8. 必要に応じて、アダプティブアノマリーコントロールのルールの適用時の処理を選択します：

   - **ブロックする**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

   - **通知する**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、ルールの適用対象となった動作の情報がログに記録されます。

9. 必要に応じて、使用しないルールを無効にします。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

製品インターフェイスでアダプティブアノマリーコントロールのルールのリストを表示する方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。

3. ［**アダプティブアノマリーコントロール**］をオンにします。

4. ［**ルール**］セクションで、［**ルールの編集**］をクリックします。

   アダプティブアノマリーコントロールルールのリストが開きます。既定では、すべてのルールは［**スマート**］モードで動作しています。

5. 必要に応じて、アダプティブアノマリーコントロールのルールの更新を確認します。

6. 必要に応じて、アダプティブアノマリーコントロールのルールの適用時の処理を選択します：

   - **ブロック**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

   - **通知**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、ルールの適用対象となった動作の情報がログに記録されます。

7. 必要に応じて、使用しないルールを無効にします。

8. 変更内容を保存します。

ルールごとに、設定されているトレーニング期間は異なります。トレーニングモードの継続期間はカスペルスキーのエキスパートが設定しています。通常は、トレーニングモードの継続期間は 2 週間です。

トレーニング中にルールが一度も適用されなかった場合、アダプティブアノマリーコントロールはそのようなふるまいを異常と判断し、ルールのステータスを**スマートブロック**に変更します。その後、本製品はこのルールに一致するすべての動作をブロックします。

トレーニング中にルールが適用された場合、このルールに一致する検知された動作に本製品が適用する処理を手動で設定する必要があります。ルールの適用時の処理を選択しない場合、アダプティブアノマリーコントロールは引き続きトレーニングモードで動作します。

アダプティブアノマリーコントロールルールの有効化と無効化

アダプティブアノマリーコントロールルールを有効または無効にするには：

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。

3. ［**ルール**］ブロックの［**ルールの編集**］をクリックします。
   アダプティブアノマリーコントロールルールのリストが開きます。

4. テーブルで、*Office アプリケーションの動作*など、ルールのセットを選択し、展開します。

5. *Office アプリケーションによる Microsoft PowerShell の起動*などのルールを選択します。

6. ［**状態**］列のトグルスイッチを使用してアダプティブアノマリーコントロールルールを有効または無効にします。

7. 変更内容を保存します。

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

アダプティブアノマリーコントロールルールが適用されたときに実行する処理を編集するには：

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。

3. ［**ルール**］ブロックの［**ルールの編集**］をクリックします。
   アダプティブアノマリーコントロールルールのリストが開きます。

4. ルールを選択します。

5. ［**編集する**］をクリックします。
   アダプティブアノマリーコントロールルールのプロパティウィンドウが開きます。

6. ［**処理**］ブロックで、以下のオプションのいずれかを選択します：

   - **スマート**：このオプションを選択した場合、アダプティブアノマリーコントロールルールは、カスペルスキーのエキスパートが定義した期間、スマートトレーニングで動作します。このモードでは、アダプティブアノマリーコントロールルールが適用されると、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、情報が Kaspersky Security Center 管理サーバーの［**「スマートトレーニング」ステータスのルール適用条件**］保管領域にログとして記録されます。スマートトレーニングで動作するよう指定された期間が終了すると、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

   - **ブロック**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作をブロックします。また、ルールの適用対象となった動作の情報がログに記録されます。

   - **通知**：この処理を選択した場合、アダプティブアノマリーコントロールルールが適用されたときに、Kaspersky Endpoint Security はルールの適用対象となる動作を許可します。また、ルールの適用対象となった動作の情報がログに記録されます。

7. 変更内容を保存します。

アダプティブアノマリーコントロールルールの除外の作成

アダプティブアノマリーコントロールルールの除外を 1000 個を超えて作成することはできません。また、200 個を超える除外を作成することも推奨されません。使用する除外の件数を少なくするには、除外の指定時にマスクを使用することが推奨されます。

アダプティブアノマリーコントロールルールの除外には、ソースオブジェクトとターゲットオブジェクトの説明が含まれます。*ソースオブジェクト*とは、処理を実行しているオブジェクトです。*ターゲットオブジェクト*とは、処理が実行されているオブジェクトです。たとえば、「`file.xlsx`」という名前のファイルを開いたとします。このとき、拡張子が DLL のライブラリファイルがコンピューターメモリに読み込まれます。このライブラリがブラウザー（実行ファイル名は「`browser.exe`」）で使用されたとします。この場合、「`file.xlsx`」がソースオブジェクトで、Excel がソースプロセス、「`browser.exe`」がターゲットオブジェクト、ブラウザーがターゲットプロセスになります。

アダプティブアノマリーコントロールルールの除外を作成するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。
3. ［**ルール**］ブロックの［**ルールの編集**］をクリックします。
   アダプティブアノマリーコントロールルールのリストが開きます。
4. ルールを選択します。
5. ［**編集する**］をクリックします。
   アダプティブアノマリーコントロールルールのプロパティウィンドウが開きます。
6. ［**除外リスト**］ブロックの［**追加**］をクリックします。
   除外リストのプロパティウィンドウが表示されます。
7. 除外リストを設定するユーザーを選択します。
   ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

   アダプティブアノマリーコントロールはユーザーグループに対する除外リストをサポートしません。ユーザーグループを選択すると、Kaspersky Endpoint Security は除外リストを適用しません。
8. ［**説明**］に、除外の説明を入力します。
9. ソースオブジェクトまたはオブジェクトが開始したソースプロセスの設定を指定します：
   - **ソースプロセス**：ファイルまたはファイルが含まれているフォルダーのパスまたはパスのマスク（例：「`C:\Dir\File.exe`」または「`Dir\*.exe`」）。
   - **ソースプロセスのハッシュ**：ファイルのハッシュ値。

- **ソースオブジェクト**：ファイルまたはファイルが含まれているフォルダーのパスまたはパスのマスク（例：「`C:\Dir\File.exe`」または「`Dir\*.exe`」）。たとえば、ターゲットプロセスを起動するスクリプトまたはマクロを使用するファイルのパスとして「`document.docm`」を指定します。

  Web アドレス、マクロ、コマンドラインのコマンド、レジストリパスなどのその他の種別のオブジェクトを指定することもできます。「`object://<object>`」という形式でオブジェクトを指定してください。「`<object>`」にはオブジェクト名が入るように、「`object://web.site.example.com`」、「`object://VBA`」、「`object://ipconfig`」、「`object://HKEY_USERS`」などのように指定します。「`object://*C:\Windows\temp\*`」のようにマスクを使用することもできます。

- **ソースオブジェクトのハッシュ**：ファイルのハッシュ値。

指定したオブジェクトが実行した処理、またはオブジェクトによって起動されたプロセスに対しては、アダプティブアノマリーコントロールルールが適用されません。

10. ターゲットオブジェクトまたはオブジェクトが開始したターゲットプロセスの設定を指定します：

    - **ターゲットプロセス**：ファイルまたはファイルが含まれているフォルダーのパスまたはパスのマスク（例：「`C:\Dir\File.exe`」または「`Dir\*.exe`」）。

    - **ターゲットプロセスのハッシュ**：ファイルのハッシュ値。

    - **ターゲットオブジェクト**：ターゲットプロセスを起動するコマンド。「`object://<command>`」という形式で、「`object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`」などのようにコマンドを指定します。「`object://*C:\Windows\temp\*`」のようにマスクを使用することもできます。

    - **ターゲットオブジェクトのハッシュ**：ファイルのハッシュ値。

    指定したオブジェクトに対して実行された処理、またはオブジェクトに対して起動されたプロセスに対しては、アダプティブアノマリーコントロールルールが適用されません。

11. 変更内容を保存します。

アダプティブアノマリーコントロールルールの除外のエクスポートとインポート

選択したルールに除外リストをエクスポートまたはインポートするには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。
3. ［**ルール**］ブロックの［**ルールの編集**］をクリックします。

   アダプティブアノマリーコントロールルールのリストが開きます。
4. ルールのリストをエクスポートするには：

   a. エクスポートする除外リストを含むルールを選択します。

   b. ［**エクスポート**］をクリックします。

c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。

e. ファイルを保存します。

5. ルールのリストをインポートするには：

a. ［**インポート**］をクリックします。

b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

c. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

アダプティブアノマリーコントロールルールへのアップデートの適用

定義データベースがアップデートされたときに、ルールのリストに新しいアダプティブアノマリーコントロールルールを追加したり、ルールのリストから既存のアダプティブアノマリーコントロールルールを削除したりできます。これらのルールへのアップデートが適用されていない場合、Kaspersky Endpoint Security はリストから追加または削除されるアダプティブアノマリーコントロールルールを他のルールから区別します。

アップデートが適用されるまで、アップデートによって削除される予定のアダプティブアノマリーコントロールルールもテーブルに表示されますが、［*無効*］ステータスが割り当てられます。これらのルールの設定は変更できません。

アダプティブアノマリーコントロールルールにアップデートを適用するには：

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。

3. ［**ルール**］ブロックの［**ルールの編集**］をクリックします。

アダプティブアノマリーコントロールルールのリストが開きます。

4. 表示されたウィンドウで、［**アップデートの承認**］をクリックします。

［**アップデートの承認**］は、アダプティブアノマリーコントロールルールで利用可能なアップデートが存在する場合にクリックできます。

5. 変更内容を保存します。

アダプティブアノマリーコントロールのメッセージテンプレートの編集

ユーザーがアダプティブアノマリーコントロールルールによってブロックされている処理を実行しようとすると、有害な可能性のある処理がブロックされることを示すメッセージが表示されます。処理が誤ってブロックされていると思われる場合は、メッセージテキストのリンクを使用して、メッセージをローカルエリアネットワーク管理者に送信できます。

有害な可能性のある処理がブロックされた際に管理者に表示されるメッセージについては、専用テンプレートを使用できます。メッセージのテンプレートの管理用に特別な変数が用意されています（例：`%USER_NAME%`）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。

メッセージテンプレートを編集するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］を選択します。
3. ［**テンプレート**］ブロックで、アダプティブアノマリーコントロールのメッセージのテンプレートを設定します。
   - **ブロックに関するメッセージ**：典型的でない動作をブロックするアダプティブアノマリーコントロールルールが適用された際に表示されるメッセージのテンプレート。
   - **管理者に送信するメッセージ**：ブロックが誤検知だと考えられる場合に、社内のローカルネットワークの管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの動作ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**リセット**］を使用して既定のテンプレートテキストを復元することもできます。
4. 変更内容を保存します。

アダプティブアノマリーコントロールの動作の監視

アダプティブアノマリーコントロールには、いくつかの監視ツールが含まれています。アダプティブアノマリーコントロールを監視する主な目的は、トレーニング中にコンポーネントを設定することです。

アダプティブアノマリーコントロールのレポート

アダプティブアノマリーコントロールでは次のレポートが使用されます：

- **アダプティブアノマリーコントロールルールのステータスに関するレポート**：このレポートには、アダプティブアノマリーコントロールルールのステータスに関する情報（*オフ*、*スマートトレーニング*、*スマートブロック*、*通知*、*ブロック*）が含まれています。このレポートでは、アダプティブアノマリーコントロールのトレーニングレベルを分析して、*スマートトレーニング*モードから通常の操作モード（例：*スマートブロック*）に切り替えられたルールの数を評価することができます。

- **アダプティブアノマリーコントロールルールの適用に関するレポート**：レポートにはルールの適用に関する情報が含まれます。また、レポートには、ルールを適用するモードとして、*ブロック*モード（*スマートブロック*を含む）または*通知*モードが示されます。このレポートにより、ユーザーのコンピューター上のアダプティブアノマリーコントロールの動作を評価できます。

管理コンソール（MMC）でアダプティブアノマリーコントロールレポートを表示する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］の順に選択します。

4. 次のいずれかの手順を実行します：

   - アダプティブアノマリーコントロールルールのステータスに関するレポートを表示するには、［**アダプティブアノマリーコントロールルールのステータスに関するレポート**］をクリックします。

   - アダプティブアノマリーコントロールルールの適用に関するレポートを表示するには、［**アダプティブアノマリーコントロールルールの適用に関するレポート**］をクリックします。

5. レポートの生成プロセスが開始されます。

   レポートが新しいウィンドウに表示されます。

Web コンソールでアダプティブアノマリーコントロールレポートを表示する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アダプティブアノマリーコントロール**］に移動します。

5. ［**ルール**］ブロックで、次のいずれかを実行します：

   - アダプティブアノマリーコントロールルールのステータスに関するレポートを表示するには、［**レポートの表示**］→［**ルールの状態**］の順に選択します。

   - アダプティブアノマリーコントロールルールの適用に関するレポートを表示するには、［**レポートの表示**］→［**検知**］の順に選択します。

6. レポートの生成プロセスが開始されます。

   レポートが新しいウィンドウに表示されます。

Kaspersky Security Center コンソールでレポートを生成するには、管理サーバーへのデータ転送を有効にする必要があります。既定ではデータ転送は有効になっています。

管理コンソール（MMC）でアダプティブアノマリーコントロールのデータ転送を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**レポートと保管領域**］の順に選択します。

4. ［**管理サーバーへのデータ転送**］ブロックの［**設定**］をクリックします。

5. 次のボックスをオンにします：

   - **アダプティブアノマリーコントロールルールのステータスに関するレポート**

   - **アダプティブアノマリーコントロールルールの適用に関するレポート**

6. 変更内容を保存します。

Web コンソールでアダプティブアノマリーコントロールのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**KSC 連携**］に移動します。

5. ［**管理サーバーへのデータ転送**］で、次のチェックボックスをオンにします：

   - **アダプティブアノマリーコントロールルールのステータスに関するレポート**

   - **アダプティブアノマリーコントロールルールの適用に関するレポート**

6. 変更内容を保存します。

「スマートトレーニング」ステータスのルール適用条件の保管領域

トレーニングモードでは、アダプティブアノマリーコントロールは、適用されるルールに関する情報を別のストレージ（[**「スマートトレーニング」ステータスのルール適用条件**]）に送信します。適用されるルールに関する情報は、ストレージ内でイベントのリストとして表されます。アダプティブアノマリーコントロールを調整するには、コンピューター上の異常なふるまいを確認するか、ルールから除外を追加します。

アダプティブアノマリーコントロールのイベント

アダプティブアノマリーコントロールは、*ブロック*モード（*スマートブロック*を含む）または*通知*モードでのルール適用イベントをログに記録します。この目的で、次のイベントが提供されています：

プロセスの処理がブロックされました

プロセスの処理がスキップされました

イベントには、ファイルのチェックサム、関係するユーザー、ルールの適用時刻、コンピューター名など、疑わしい動作に関する情報が含まれます。イベントを分析した後で、動作が正当であると判断した場合は、すぐにルールからの除外を追加できます。

アプリケーションコントロール

アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。

アプリケーションコントロールの設定では、次のステップが必要です：

1. アプリケーションカテゴリの作成

   管理者は、自身が管理するアプリケーションのカテゴリを作成します。アプリケーションのカテゴリは、管理グループに関係なく、企業ネットワーク内のすべてのコンピューターを対象としています。カテゴリを作成するには、KL カテゴリ（ブラウザーなど）、ファイルのハッシュ、アプリケーションの開発元、およびその他の条件を使用できます。

2. アプリケーションコントロールルールの作成

   管理者は、管理グループのポリシーにアプリケーションコントロールルールを作成します。ルールには、アプリケーションのカテゴリと、「ブロック」または「許可」のカテゴリからのアプリケーションの起動ステータスが含まれます。管理者は複数のルールを作成できます。1つのアプリケーションが複数のルールの条件に一致する場合があります。ブロックルールの優先度は、許可ルールの優先度よりも高くなります。Kaspersky Endpoint Security は、アプリケーションが起動されるたびに、ルールに一致するかどうかをチェックします。すべてのアプリケーションコントロールルールに対して、アプリケーションが順次照合されます。

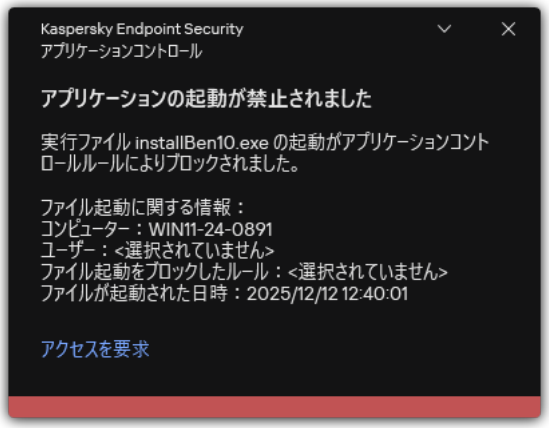
3. アプリケーションコントロールモードの選択

   管理者は、拒否リストまたは許可リストのいずれのルールにも含まれていないアプリケーションを操作するモードを選択します。

ユーザーが禁止されたアプリケーションを起動しようとすると、Kaspersky Endpoint Security はアプリケーションの起動をブロックし、通知を表示します（下の図を参照）。

Application Control の構成を確認するための*テストモード*が用意されています。このモードでは、Kaspersky Endpoint Security は次のことを行います：

- 禁止されているものも含めて、アプリケーションの起動を許可します。
- 禁止されているアプリケーションの起動に関する通知を表示し、ユーザーのコンピューターのレポートに情報を追加します。
- 禁止されたアプリケーションの起動に関するデータを Kaspersky Security Center に送信します。



アプリケーションコントロールの通知

アプリケーションコントロールの操作モード

アプリケーションコントロールは 2 つのモードで動作します。

- **拒否リスト**：このモードでは、アプリケーションコントロールルールで禁止されているアプリケーションを除くすべてのアプリケーションを、ユーザーが起動できます。

  アプリケーションコントロールのこのモードは、規定では有効になっています。

- **許可リスト**：このモードでは、アプリケーションコントロールルールで許可および禁止されていないアプリケーション以外のアプリケーションを、ユーザーが起動できないようにします。

  必要なアプリケーションコントロールの許可ルールをすべて設定すると、LAN 管理者が検証していない新しいアプリケーションの起動はブロックされますが、オペレーティングシステムとユーザーが業務で使用している信頼するアプリケーションの動作は許可されます。

  許可リストモードでは、アプリケーションコントロールルールの設定における推奨事項を確認できます。

アプリケーションコントロールは、Kaspersky Endpoint Security のローカルインターフェイスと Kaspersky Security Center の両方で、これらのモードで動作するように設定できます。

Kaspersky Security Center が提供するツールには、Kaspersky Endpoint Security のローカルインターフェイスで使用できないものもあります。これらは次の用途で必要となります：

- アプリケーションカテゴリの作成

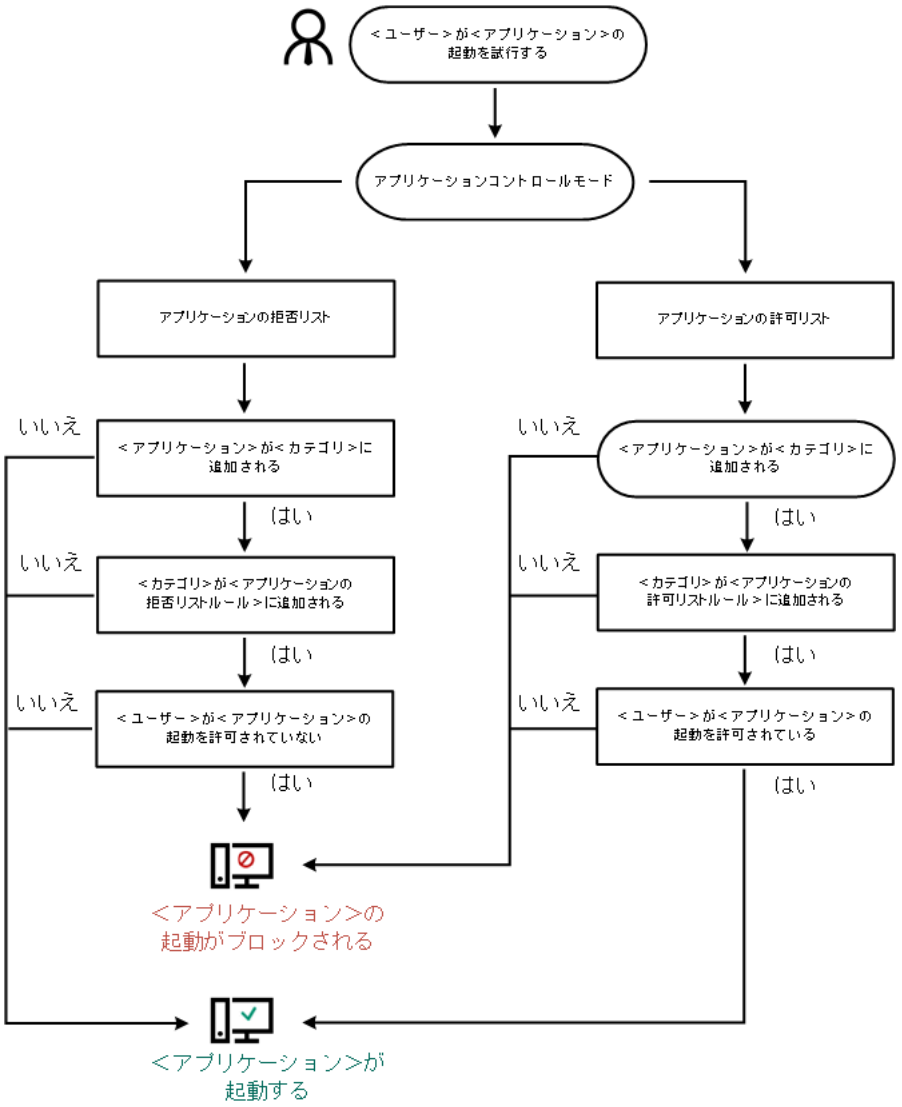
  Kaspersky Security Center の管理コンソールで作成するアプリケーションコントロールルールは、カスタマイズされたアプリケーションカテゴリに基づき、Kaspersky Endpoint Security のローカルインターフェイスでの対象条件や除外条件には基づきません。

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

そのため、アプリケーションコントロールの動作設定には Kaspersky Security Center の使用を推奨します。

アプリケーションコントロールの動作アルゴリズム

Kaspersky Endpoint Security は、アルゴリズムを使用して、アプリケーションの起動に関する決定を下します（下の図を参照）。



アプリケーションコントロールの動作アルゴリズム

アプリケーションコントロールの機能の制限

アプリケーションコントロールの機能には、次のような制限があります：

- 本製品のバージョンをアップグレードするとき、アプリケーションコントロールの設定のインポートはサポートされません。
- KSN サーバーと接続されていない場合、Kaspersky Endpoint Security はアプリケーションとモジュールの評価情報をローカル定義データベースからのみ取得します。

  Kaspersky Endpoint Security が KL カテゴリ［**その他のソフトウェア\アプリケーション、KSN の評価によって信頼済み**］とするアプリケーションのリストは KSN サーバーへの接続が利用可能であるかによって異なることがあります。

- Kaspersky Security Center のデータベースには、処理したファイル 150,000 個分の情報を記録できます。保管されている記録が 150,000 個に到達すると、新しいファイルは処理されなくなります。処理を再開するには、以前 Kaspersky Endpoint Security がインストールされているコンピューターから Kaspersky Security Center のデータベースに保管したファイルを削除してください。
- スクリプトの起動は、スクリプトがコマンドラインを経由してインタープリターに送られる場合を除き、管理されません。

  インタープリターの起動がアプリケーションコントロールルールによって許可されている場合、そのインタープリターから開始されるスクリプトはブロックされません。

  インタープリターのコマンドラインで 1 つ以上のスクリプトの起動がアプリケーションコントロールルールによってブロックされた場合、インタープリターのコマンドラインで指定されたすべてのスクリプトがブロックされます。

- Kaspersky Endpoint Security でサポートされていないインタープリターから開始されるスクリプトは管理されません。

  Kaspersky Endpoint Security は、以下のインタープリターをサポートします：

  - Java
  - PowerShell

  以下の種別のインタープリターがサポートされます：

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe

- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

クライアントコンピューターにインストールされたアプリケーションについての情報の取得

最適なアプリケーション起動コントロールを作成するには、まず、企業のローカルエリアネットワークにあるコンピューターで使用されているアプリケーションを把握します。次の情報を取得できます：

- 企業の LAN で使用されているアプリケーションの開発元、バージョン、およびローカライズ
- アプリケーションアップデートの頻度
- 企業で採用しているアプリケーション使用ポリシー（セキュリティポリシーまたは管理ポリシー）
- アプリケーション配布パッケージの保管場所

アプリケーション情報の表示

インストールされているアプリケーションの情報は、Kaspersky Security Center ネットワークエージェントから提供されます。インストールされているアプリケーションの情報は、Kaspersky Security Center コンソールの［**アプリケーションレジストリ**］フォルダーにあります。ネットワークエージェントは、Kaspersky Security Center との同期のたびに情報を更新します。ネットワークエージェントから送信される情報の詳細については、Kaspersky Security Center ヘルプを参照してください。

アプリケーションレジストリフォルダーでアプリケーションのプロパティウィンドウを開くには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**アプリケーションレジストリ**］の順に選択します。
3. アプリケーションを選択します。
4. アプリケーションのコンテキストメニューから［**プロパティ**］を選択します。

実行ファイルに関する情報の表示

実行ファイルに関する情報を照会する際に、データベースの負荷を軽減できます。これを実現するために、標準セットのソフトウェアがインストールされている複数の参照コンピューターでインベントリタスクを実行することを推奨します。

Kaspersky Endpoint Security のインベントリタスクを使用して実行ファイルのリストを取得できます。実行ファイルのリストは、Kaspersky Security Center コンソールの［**実行ファイル**］フォルダーで確認できます。

インベントリタスクを実行する前に、データベースが Kaspersky Security Center の推奨事項を満たしていることを確認してください。データベースの制限について詳しくは、Kaspersky Security Center ヘルプを参照してください。

管理コンソール（MMC）でインベントリタスクを実行する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**インベントリ**］の順に選択します。

ステップ 2：インベントリ範囲

Kaspersky Endpoint Security が実行ファイルを検索するフォルダーのリストを作成します。インベントリを設定します（下の表を参照）。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスクを実行するアカウントの選択

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

ステップ 5：タスク開始スケジュールの設定

タスクのスケジュールを設定します（たとえば、［手動］など）。

ステップ 6：タスク名の定義

タスクの名前を入力します。たとえば、「*ベースラインインベントリ*」など。

ステップ 7：タスク作成の完了

ウィザードを終了します。必要に応じて、［**ウィザードの終了後にタスクを実行**］をオンにします。タスクのプロパティでタスクの進行状況を監視できます。設定が完了すると、設定されたスケジュールに従ってユーザーのコンピューターで実行ファイルの検索が実行されるようになります。

Web コンソールと Cloud コンソールでインベントリタスクを実行する方法

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

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］から［**インベントリ**］を選択します。

   c. ［**タスク名**］に「*ベースラインインベントリ*」などの短く分かりやすい名前を付けます。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。

5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。

6. ウィザードを終了します。

   タスクのリストに新しいタスクが表示されます。

7. タスクを設定するには、タスクのプロパティに移動します（下の表を参照）。

8. タスクの横にあるチェックボックスをオンにします。

9. ［**開始**］をクリックします。

   タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。設定が完了すると、指定したスケジュールに従ってユーザーのコンピューターで実行ファイルが検索されるようになります。

インベントリ設定

パラメータ	説明
インベントリ範囲	インベントリ範囲を形成するオブジェクトのリスト。
DLL モジュールのインベントリ	Kaspersky Endpoint Security が、インベントリ範囲内で DLL モジュールを検索し、その情報を Kaspersky Security Center に送信します。 DLL モジュールのインベントリを有効にすると、インベントリタスクの完了にかかる時間とデータベースのサイズが大幅に増加します。
スクリプトファイルのインベントリ	Kaspersky Endpoint Security が、インベントリ範囲内でスクリプトを検索し、その情報を Kaspersky Security Center に送信します。 スクリプトファイルのインベントリを有効にすると、インベントリタスクの完了にかかる時間とデータベースのサイズが大幅に増加します。
スクリーンセーバーが無効でコンピューターのロックが解除されている場合は、スケジュールされたスキャンを停止する	コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。
新規作成または変更されたファイルのみスキャン	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
ファイルの最大スキャン時間（秒）	タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

パラメータ	説明
アーカイブのスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配布パッケージをスキャン	サードパーティ製品の配布パッケージをスキャンします。
大きな複合ファイルをスキャンしない	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。

実行ファイルフォルダーにある実行ファイルのプロパティウィンドウを開くには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**実行ファイル**］の順に選択します。
3. 実行ファイルを選択します。
4. 実行ファイルのコンテキストメニューから［**プロパティ**］を選択します。

アプリケーションやその実行ファイル、またアプリケーションがインストールされたコンピューターのリストに関する概要情報を見るには、［**アプリケーションレジストリ**］フォルダーまたは［**実行ファイル**］フォルダーで選択されたアプリケーションのプロパティウィンドウを開いてください。

インストールされているアプリケーションと実行ファイルに関する情報の更新

Endpoint Security 12.3 for Windows より、実行ファイルのデータベースに対するアプリケーションコントロールコンポーネントの動作が最適化されました。Kaspersky Endpoint Security 12.3 for Windows は、ファイルがコンピューターから削除された後でデータベースを更新します。これにより、データベースを最新の状態に保ち、Kaspersky Security Center のリソースを節約できます。

インストールされているアプリケーションのデータベースを最新の状態に保つには、管理サーバーへのアプリケーション情報の送信を有効にする必要があります（既定で有効になっています）。

管理コンソール（MMC）でアプリケーション情報の送信を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**レポートと保管領域**］の順に選択します。
4. ［**管理サーバーへのデータ転送**］ブロックの［**設定**］をクリックします。
5. ［**起動されたアプリケーション**］チェックボックスをオンにします。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールでアプリケーション情報の送信を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**KSC 連携**］に移動します。
5. ［**管理サーバーへのデータ転送**］ブロックの［**詳細設定**］をクリックします。
6. 表示されたウィンドウで、［**起動されたアプリケーションの情報**］をオンにします。
7. 変更内容を保存します。

ブロック対象のアプリケーションモードを有効にする方法

*ブロック対象のアプリケーション*モードでは、アプリケーションコントロールルールで禁止されているアプリケーションを除くすべてのアプリケーションを、ユーザーが起動できます。つまり、拒否ルールが存在しない場合は、アプリケーションコントロールによってアプリケーションの起動が許可されます。アプリケーションコントロールのこのモードは、規定では有効になっています。

*ブロック対象のアプリケーション*モードを有効にする前に、アプリケーションコントロールルールをテストすることを推奨します。この目的で、テストモードを有効にすることができます。

管理コンソール（MMC）でブロック対象のアプリケーションモードを有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。
5. ［**アプリケーションコントロール**］チェックボックスをオンにします。
6. ［**アプリケーションコントロールの設定**］ブロックで、［**コントロールモード**］ドロップダウンリストから［**拒否リスト**］を選択します。
7. ［**処理**］で、アプリケーションコントロールの処理を選択します。
   - **ルールをテスト運用**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。
   - **ルールを適用**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。

8. アプリケーションコントロールルールのステータスを選択します。

- **オン**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
- **オフ**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
- **テスト**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

必要に応じて、新しいアプリケーションコントロールルールを追加します。

9. アプリケーションコントロールの詳細設定を指定します：

- **DLL モジュールの読み込みの監視（システムの負荷が大きくなります）**：このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。

  どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、［アプリケーションコントロール］で、既定の［**ゴールデンイメージ**］ルールまたは［**ゴールデンイメージ\信頼済み証明書**］KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。［**ゴールデンイメージ**］ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。

  Kaspersky Endpoint Security は、［DLL とドライバーを管理］をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。

- **厳密なデジタル署名検証を使用する**：アプリケーションコントロールルールの適用条件として証明書を選択できます。このチェックボックスをオンにすると、Kaspersky Endpoint Security は、信頼するシステム証明書ストアの証明書で署名されたアプリケーションにのみルールを適用します。このような証明書で署名されたアプリケーションは、さらに、マルウェアのスキャンタスクなどの保護機能によって信頼されていると判断されます。ただし、アプリケーションコントロールルールで別のストアの証明書を指定した場合、そのルールは適用されません。

  チェックボックスをオフにすると、Kaspersky Endpoint Security は、Windows の信頼するルート証明書ストア（Trusted Root Certificate Store）の証明書で署名されたアプリケーションにルールを適用します。このようなアプリケーションは信頼ゾーンに含まれません。保護機能により、このようなアプリケーションの動作が監視されます。

- **ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。
- **管理者に送信するメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（  ）。

Web コンソールおよび Cloud コンソールでブロック対象のアプリケーションモードを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。
5. ［**アプリケーションコントロールは有効です**］をオンにします。
6. ［**操作モード**］ブロックで、［**ルールリスト以外をすべて禁止する**］を選択します。
7. ［**処理**］で、アプリケーションコントロールの処理を選択します。
   - **通知する**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。
   - **ルールを適用**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。
8. アプリケーションコントロールルールのステータスを選択します。
   - **有効**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
   - **無効**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
   - **テストモード**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

   必要に応じて、新しいアプリケーションコントロールルールを追加します。
9. アプリケーションコントロールの詳細設定を指定します：
   - **DLL モジュールの読み込みの監視**：このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。

     どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、［アプリケーションコントロール］で、既定の［**ゴールデンイメージ**］ルールまたは［**ゴールデンイメージ\信頼済み証明書**］KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。［**ゴールデンイメージ**］ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。

Kaspersky Endpoint Security は、［DLL とドライバーを管理］をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。

- **厳密なデジタル署名検証を使用する**：アプリケーションコントロールルールの適用条件として証明書を選択できます。このチェックボックスをオンにすると、Kaspersky Endpoint Security は、信頼するシステム証明書ストアの証明書で署名されたアプリケーションにのみルールを適用します。このような証明書で署名されたアプリケーションは、さらに、マルウェアのスキャンタスクなどの保護機能によって信頼されていると判断されます。ただし、アプリケーションコントロールルールで別のストアの証明書を指定した場合、そのルールは適用されません。

  チェックボックスをオフにすると、Kaspersky Endpoint Security は、Windows の信頼するルート証明書ストア（Trusted Root Certificate Store）の証明書で署名されたアプリケーションにルールを適用します。このようなアプリケーションは信頼ゾーンに含まれません。保護機能により、このようなアプリケーションの動作が監視されます。

- **ユーザーへのメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。

- **管理者へのメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスでブロック対象のアプリケーションモードを有効にする方法

1. メインウィンドウで、をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**アプリケーションコントロール**］をオンにします。
4. ［**アプリケーション起動コントロールモード**］ブロックで、［**拒否リスト。ルールリストに登録されているもの以外が許可されます**］を選択します。
5. ［**ルールによりブロックされたアプリケーションの開始時の操作**］で、アプリケーションコントロールの処理を選択します。

   - **報告（テストモード）して、次に記録する**： **レポート**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。

   - **ブロックする**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。

6. アプリケーションコントロールルールのステータスを選択します。

- **有効**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
- **無効**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
- **テストモード**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

必要に応じて、新しいアプリケーションコントロールルールを追加します。

7. アプリケーションコントロールの詳細設定を指定します：

- **DLL モジュールの読み込みを監視する**：このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。

  どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、［アプリケーションコントロール］で、既定の［**ゴールデンイメージ**］ルールまたは［**ゴールデンイメージ\信頼済み証明書**］KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。［**ゴールデンイメージ**］ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。

  Kaspersky Endpoint Security は、［DLL とドライバーを管理］をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。

- **厳密なデジタル署名検証を使用する**：アプリケーションコントロールルールの適用条件として証明書を選択できます。このチェックボックスをオンにすると、Kaspersky Endpoint Security は、信頼するシステム証明書ストアの証明書で署名されたアプリケーションにのみルールを適用します。このような証明書で署名されたアプリケーションは、さらに、マルウェアのスキャンタスクなどの保護機能によって信頼されていると判断されます。ただし、アプリケーションコントロールルールで別のストアの証明書を指定した場合、そのルールは適用されません。

  チェックボックスをオフにすると、Kaspersky Endpoint Security は、Windows の信頼するルート証明書ストア（Trusted Root Certificate Store）の証明書で署名されたアプリケーションにルールを適用します。このようなアプリケーションは信頼ゾーンに含まれません。保護機能により、このようなアプリケーションの動作が監視されます。

- **アプリケーションのブロックに関するメッセージのテンプレートです**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。
- **アプリケーションの起動のブロック時に表示されるメッセージテキストのテンプレートです**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

8. 変更内容を保存します。

その結果、アプリケーションコントロールはブロック対象のアプリケーションをブロックします。Kaspersky Endpoint Security は、［*アプリケーションの起動が禁止されました*］のイベントも生成します。Kaspersky Security Center コンソールで、これらのイベントを使用して、*ブロック対象アプリケーションのレポート*のレポートを生成できます。レポートの概要では、アプリケーションコントロールルールが適用されたアプリケーションとコンピューターのリストを確認できます。

ベースラインコンピューターに基づくアプリケーションコントロール

ベースラインコンピューターを使用して、必要な一連のアプリケーションを含むイメージを作成できます。このイメージを使用して、オペレーティングシステムとアプリケーションを他のコンピューターに導入できます。イメージを常に最新の状態に保つことが常に可能であるとは限りません。アプリケーションコントロールを使用すると、ベースラインコンピューターに基づいて、許可するアプリケーションのリストを管理できます。アプリケーションコントロールは、ベースラインコンピューターにインストールされているアプリケーションを自動的に特定してカテゴリを更新します。このようにして、コンピューターは、許可するアプリケーションの最新のリストを取得します。

ベースラインコンピューターに基づくアプリケーションコントロールを設定するには、次の手順を実行します：

1. 自動で更新されるカテゴリを作成します。新しいカテゴリを作成する場合は、［**特定のフォルダーの実行ファイルを含むカテゴリ**］カテゴリを選択し、ベースラインコンピューターを選択します。

   管理コンソール（MMC）で自動で更新されるカテゴリを作成する方法

   1. Kaspersky Security Center の管理コンソールを開きます。
   2. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**アプリケーションカテゴリ**］の順に選択します。
   3. 作業領域で［**新規カテゴリ**］をクリックします。

      アプリケーションカテゴリの作成ウィザードが開始します。
   4. アプリケーションカテゴリの作成ウィザードの指示に従います。

ステップ 1：カテゴリ種別の選択

［**選択したデバイスの実行ファイルを含むカテゴリ**］をカテゴリ種別として選択します。

ステップ 2：ユーザーカテゴリ名の入力

この手順では、アプリケーションカテゴリの名前を指定します。

ステップ 3：設定

この手順は、［**選択したデバイスの実行ファイルを含むカテゴリ**］カテゴリ種別を選択した場合に使用できます。

この手順では、［**追加**］をクリックしてコンピューターを指定します。そのコンピューターにある実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。［**実行ファイル**］フォルダーに表示される、指定されたコンピューターのすべての実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。

この手順では、以下の設定も指定できます：

- ハッシュ関数の計算アルゴリズム。アルゴリズムを選択するには、以下のチェックボックスを 1 つ以上オンにします：
  - **このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**
  - **このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**
- ［**データを管理サーバーのリポジトリと同期**］チェックボックス：Kaspersky Security Center によって、定期的にアプリケーションカテゴリを空にした後、［**実行ファイル**］フォルダーに表示される、指定されたコンピューターのすべての実行ファイルをアプリケーションカテゴリに追加する場合、このチェックボックスをオンにします。

  ［**データを管理サーバーのリポジトリと同期**］がオフの場合、アプリケーションカテゴリの作成後、Kaspersky Security Center はカテゴリへの変更を行いません。

ステップ 4：フィルター

この手順では、ファイルのフィルターを設定します。

アプリケーションカテゴリを作成するために使用するファイル種別を指定できます。

- **すべてのファイル**：このカテゴリはすべてのファイルに一致します。既定ではこのオプションが選択されます。
- **アプリケーションカテゴリに含まれないファイルのみ**：このカテゴリは、アプリケーションカテゴリ以外のファイルのみに一致します。

アプリケーションカテゴリの作成に使用するファイルが含まれる、選択したコンピューターのフォルダーを指定できます。

- **すべてのフォルダー**：このカテゴリはすべてのフォルダーに一致します。既定ではこのオプションが選択されます。
- **指定フォルダー**：このカテゴリは指定されたフォルダーのみに一致します。このオプションを選択した場合は、フォルダーパスを指定する必要があります。

ステップ 5：カスタムカテゴリの作成

ウィザードを終了します。

Web コンソールおよび Cloud コンソールで自動でコンテンツが追加されるカテゴリを作成する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。
   アプリケーションカテゴリのリストのテーブルが開きます。
2. ［**追加**］をクリックします。
   アプリケーションカテゴリの作成ウィザードが開始します。
3. アプリケーションカテゴリの全般設定を指定します：
   - カテゴリ名。
   - カテゴリの作成方法。［**選択したデバイスの実行ファイルを含むカテゴリ**］をカテゴリ種別として選択します。

   次の手順に進みます。
4. アプリケーションカテゴリの詳細設定を指定します：
   - アプリケーションカテゴリに追加する実行ファイルの入手元のコンピューターを指定します。［**実行ファイル**］フォルダーに表示される、指定されたコンピューターのすべての実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。
   - ハッシュ関数の計算アルゴリズムを選択します。
   - 管理サーバー保管領域とデータを同期する間隔を設定します。
   - ファイルのフィルターを設定します。
5. ウィザードを終了します。

自動で更新されるカテゴリを作成する場合は、ファイルを複数のカテゴリに分割すると便利な場合があります。たとえば、オペレーティングシステムのファイルや Program Files フォルダーのファイルなどです。これを行うには、カテゴリ設定でフィルターを使用して、個々のフォルダーを選択します。

2. アプリケーションコントロールモードを選択します。明示的に許可されていないすべてのアプリケーションの実行をブロックする必要があります。これを行うには、［*ブロック対象のアプリケーション*］モードを選択します。
3. アプリケーションコントロールルールの作成。ルール設定で、ベースラインコンピューターの実行ファイルが属するカテゴリを選択します。

   管理コンソール（MMC）でベースラインコンピューターに基づくアプリケーションコントロールを設定する方法

   1. Kaspersky Security Center の管理コンソールを開きます。
   2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。

5. ［**アプリケーションコントロール**］チェックボックスをオンにします。

6. ［**アプリケーションコントロールの設定**］ブロックで、［**コントロールモード**］ドロップダウンリストから［**拒否リスト**］を選択します。

7. ［**処理**］で、アプリケーションコントロールの処理を選択します。

   - **ルールをテスト運用**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。

   - **ルールを適用**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。

8. アプリケーションコントロールルールのリストで、［**追加**］をクリックします。

   これにより、アプリケーションコントロールルールを追加するためのウィザードが起動します。

9. ［**カテゴリ**］ドロップダウンリストで、ベースラインコンピューターに基づいて自動で更新されるカテゴリを選択します。

10. アプリケーションコントロールルールを適用するユーザーまたはユーザーグループを選択します。

11. アプリケーションコントロールルールの詳細設定を指定します：

    - **他のユーザーを拒否**：本製品は、リストに含まれていないすべてのユーザーに対して、選択したカテゴリに属するアプリケーションの起動をブロックします。

    - **信頼するアップデーター**：選択したカテゴリに含まれるアプリケーションを信頼するアップデーターと判断し、そのアプリケーションが作成する別の実行ファイルの実行を許可します。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールでベースラインコンピューターに基づくアプリケーションコントロールを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

5. ［**アプリケーションコントロールは有効です**］をオンにします。

6. ［**操作モード**］ブロックで、［**ルールリスト以外をすべて禁止する**］を選択します。

7. ［**処理**］で、アプリケーションコントロールの処理を選択します。

   - **通知する**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。

   - **ルールを適用**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。

8. アプリケーションコントロールルールのリストで、［**追加**］をクリックします。

   これにより、アプリケーションコントロールルールを追加するためのウィザードが起動します。

9. ［**カテゴリ / アプリケーション**］で、ベースラインコンピューターに基づいて自動で更新されるカテゴリを選択します。

10. アプリケーションコントロールルールを適用するユーザーまたはユーザーグループを選択します。

11. アプリケーションコントロールルールの詳細設定を指定します：

    - **ユーザー**：本製品は、リストに含まれていないすべてのユーザーに対して、選択したカテゴリに属するアプリケーションの起動をブロックします。

    - **信頼するアップデーター**：選択したカテゴリに含まれるアプリケーションを信頼するアップデーターと判断し、そのアプリケーションが作成する別の実行ファイルの実行を許可します。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

製品インターフェイスでベースラインコンピューターに基づくアプリケーションコントロールを設定する方法

1. メインウィンドウで、 をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。

3. ［**アプリケーションコントロール**］をオンにします。

4. ［**アプリケーション起動コントロールモード**］ブロックで、［**拒否リスト。ルールリストに登録されているもの以外が許可されます**］を選択します。

5. ［**ルールによりブロックされたアプリケーションの開始時の操作**］で、アプリケーションコントロールの処理を選択します。

   - **報告（テストモード）して、次に記録する： レポート**：アプリケーションコントロールは、ルールによって実行が禁止されているアプリケーションをブロックしませんが、これ以外でブロックされるアプリケーションの実行に関するイベントを生成します。

   - **ブロックする**：アプリケーションコントロールは、ブロック対象のアプリケーションをブロックし、対応するイベントを生成します。

6. アプリケーションコントロールルールのリストで、［**追加**］をクリックします。

   これにより、アプリケーションコントロールルールを追加するためのウィザードが起動します。

7. ［**カテゴリ**］で、ベースラインコンピューターに基づいて自動で更新されるカテゴリを選択します。

8. アプリケーションコントロールルールを適用するユーザーまたはユーザーグループを選択します。

9. アプリケーションコントロールルールの詳細設定を指定します：

   - **他のユーザーを拒否**：本製品は、リストに含まれていないすべてのユーザーに対して、選択したカテゴリに属するアプリケーションの起動をブロックします。

   - **信頼するアップデーター**：選択したカテゴリに含まれるアプリケーションを信頼するアップデーターと判断し、そのアプリケーションが作成する別の実行ファイルの実行を許可します。

10. 変更内容を保存します。

アプリケーションコントロールルールの管理

Kaspersky Endpoint Security は、ルールを使用してアプリケーションの起動をコントロールします。アプリケーションコントロールルールは、ルールを適用する条件と、ルールが適用されたときアプリケーションコントロールが実行する処理を指定します（ユーザーによってアプリケーションの起動を許可またはブロックします）。

ルールを適用する条件

ルールを適用する条件には次の相互関係があります：「条件種別 - 条件判定基準 - 条検値」ルールを適用する条件に基づいて、Kaspersky Endpoint Security はルールをアプリケーションに適用します（あるいは適用しません）。

次の条件の種別がルール内で使用されます：

- *対象条件*：アプリケーションが対象条件のうち 1 つ以上を満たす場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用します。

- *除外条件*：アプリケーションが除外条件のうち 1 つ以上を満たしている一方で、どの対象条件も満たさない場合、Kaspersky Endpoint Security はそのアプリケーションにルールを適用しません。

ルールを適用する条件は、基準を使用して作成されます。Kaspersky Endpoint Security では、次の基準を使用してルールが作成されます：

- アプリケーションの実行ファイルが含まれているフォルダーのパス、またはアプリケーションの実行ファイルのパス。

- メタデータ：アプリケーションの実行ファイル名、アプリケーションの実行ファイルバージョン、アプリケーション名、アプリケーションのバージョン、アプリケーションの開発元。

- アプリケーションの実行ファイルのハッシュ。

- 証明書の発行元、発行先、ハッシュ値。

- アプリケーションが KL カテゴリに属しているかどうか。

- リムーバブルドライブ上のアプリケーション実行ファイルの場所。

条件で使用される基準のそれぞれに対して基準値を指定する必要があります。起動されるアプリケーションのパラメータが対象条件で指定されている基準値を満たす場合、ルールが適用されます。この場合、アプリケーションコントロールは、ルールで指定された処理を実行します。アプリケーションパラメータが除外条件で指定されている基準値を満たす場合、アプリケーションコントロールはアプリケーションの起動をコントロールしません。

ルールを適用する条件として証明書を選択した場合、その証明書が信頼するシステムの保管領域に追加されていることを確認し、製品内の信頼するシステム保管領域の使用設定を確認してください。

ルールが適用されたときのアプリケーションコントロールの処理

ルールが適用されると、アプリケーションコントロールはそのルールに従って、ユーザーまたはユーザーグループに対してアプリケーションの起動を許可またはブロックします。ルールが適用されるアプリケーションの起動を許可または許可しないユーザーまたはユーザーグループを選択できます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されるユーザーを指定しないルールを、「*ブロック*」ルールと呼びます。

そのルールの中で、ルールを満たすアプリケーションの起動を許可されないユーザーを指定しないルールを、「*許可*」ルールと呼びます。

ブロックルールの優先度は、許可ルールの優先度よりも高くなります。たとえば、アプリケーションコントロールの許可ルールがユーザーグループに割り当てられていて、アプリケーションコントロールのブロックルールがそのユーザーグループの1人のユーザーに割り当てられている場合、そのユーザーはアプリケーションを起動できません。

ルールの動作ステータス

アプリケーションコントロールルールの動作ステータスは、次のいずれかです：

- **有効**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
- **無効**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
- **テストモード**：このステータスは、ルールが適用されるアプリケーションの起動は許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを示します。

アプリケーションコントロールルールの適用条件の追加

アプリケーションコントロールルールの作成を容易にするため、アプリケーションカテゴリを作成できます。

会社で使用されている標準セットのアプリケーションを網羅する「作業アプリケーション」カテゴリを作成すると有用です。さまざまなユーザーグループが仕事で異なるアプリケーションセットを使用している場合は、ユーザーグループごとに別個のアプリケーションカテゴリを作成できます。

管理コンソールでアプリケーションカテゴリを作成するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**アプリケーションカテゴリ**］の順に選択します。
3. 作業領域で［**新規カテゴリ**］をクリックします。
   ユーザーカテゴリの作成ウィザードが表示されます。
4. ユーザーカテゴリの作成ウィザードの指示に従います。

ステップ 1：カテゴリ種別の選択

この手順では、次のいずれかのアプリケーションカテゴリ種別を選択します：

- 手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します。このカテゴリ種別を選択した場合、「*カテゴリにアプリケーションを含める条件の設定*」ステップと「*カテゴリからアプリケーションを除外する条件の設定*」ステップで、実行ファイルをカテゴリに追加する条件を定義できます。
- 選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されますこのカテゴリ種別を選択した場合、「*設定*」ステップで、カテゴリに自動で追加する実行ファイルのコンピューターを指定できます。
- 特定のフォルダーの実行ファイルを含むカテゴリ：指定されたフォルダーにコピーされたアプリケーションの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されますこのカテゴリ種別を選択した場合、「*リポジトリフォルダー*」ステップで、カテゴリに自動で追加する実行ファイルのフォルダーを指定できます。

自動でコンテンツが追加されるカテゴリを作成すると、Kaspersky Security Center によって、以下の形式のファイルに対してインベントリが実行されます：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX、SCR。

ステップ 2：ユーザーカテゴリ名の入力

この手順では、アプリケーションカテゴリの名前を指定します。

ステップ 3：アプリケーションをカテゴリに含める条件の設定

アプリケーションコントロールルールに多数の条件（例：ファイルハッシュなど）を追加すると、コンピューター リソースの消費量が増加します。条件の総数が 50,000 に達すると、パフォーマンスの問題が発生する可能性があります。パフォーマンスを最適化するには、条件の数を見直して減らすことをお勧めします。

この手順は、［**手動でコンテンツを追加するカテゴリ**］カテゴリ種別を選択した場合に使用できます。

この手順の［**追加**］ドロップダウンリストで、アプリケーションをカテゴリに含める条件を選択します。

- **実行ファイルのリストから**：クライアントデバイス上の実行ファイルのリストからカスタムカテゴリへアプリケーションを追加します。
- **ファイルのプロパティ**：アプリケーションをカスタムカテゴリに追加する条件として、実行ファイルの詳細なデータを指定します。
- **フォルダーのファイルのメタデータ**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダーに含まれるファイルのチェックサム**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダー内のファイルの証明書**：証明書で署名された実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルの証明書が、アプリケーションをカスタムカテゴリに追加する条件として示されます。

  プロパティで［**証明書のフィンガープリント**］パラメータが指定されていない条件の使用は推奨されません。

- **MSI インストーラーファイルのメタデータ**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーに含まれるファイルのチェックサム**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **KL カテゴリから選択**：アプリケーションをカスタムカテゴリに追加する条件として KL カテゴリを指定します。*KL カテゴリ*とは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「*Office アプリケーション*」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。

  すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。
- **アプリケーションのパスを指定（マスクをサポート）**：クライアントデバイス上のフォルダーを選択します。Kaspersky Security Center により、そのフォルダーにある実行ファイルがカスタムカテゴリに追加されます。
- **リポジトリから証明書を選択**：カスタムカテゴリにアプリケーションを追加するための条件として、実行可能ファイルの署名に使用された証明書を選択します。

  プロパティで［**証明書のフィンガープリント**］パラメータが指定されていない条件の使用は推奨されません。

証明書ストアを選択できます。既定では、アプリケーションコントロールは、信頼するシステム証明書ストアの証明書で署名されたアプリケーションに対してのみルールを適用します。これは、［**厳密なデジタル署名検証を使用する**］チェックボックスによって有効になります。

- **ドライブ種別**：アプリケーションをカスタムカテゴリに追加する条件として、ストレージデバイスの種別（すべてのハードディスクとリムーバブルドライブ、またはリムーバブルドライブのみ）を選択します。

ステップ 4：アプリケーションをカテゴリから除外する条件の設定

この手順は、［**手動でコンテンツを追加するカテゴリ**］カテゴリ種別を選択した場合に使用できます。

この手順で指定したアプリケーションは、「アプリケーションをカテゴリに含める条件の設定」ステップで指定されていても、カテゴリから除外されます。

この手順の［**追加**］ドロップダウンリストで、アプリケーションをカテゴリから除外する条件を選択します。

- **実行ファイルのリストから**：クライアントデバイス上の実行ファイルのリストからカスタムカテゴリへアプリケーションを追加します。
- **ファイルのプロパティ**：アプリケーションをカスタムカテゴリに追加する条件として、実行ファイルの詳細なデータを指定します。
- **フォルダーのファイルのメタデータ**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダーに含まれるファイルのチェックサム**：実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **フォルダー内のファイルの証明書**：証明書で署名された実行ファイルを含んだクライアントデバイスのフォルダーを指定します。Kaspersky Security Center により、それらの実行ファイルの証明書が、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーファイルのメタデータ**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのメタデータが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **MSI インストーラーに含まれるファイルのチェックサム**：MSI パッケージを選択します。Kaspersky Security Center により、その MSI パッケージに含まれる実行ファイルのハッシュが、アプリケーションをカスタムカテゴリに追加する条件として示されます。
- **KL カテゴリから選択**：アプリケーションをカスタムカテゴリに追加する条件として KL カテゴリを指定します。*KL カテゴリ*とは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「*Office アプリケーション*」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。

  すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。

- **アプリケーションのパスを指定（マスクをサポート）**：クライアントデバイス上のフォルダーを選択します。Kaspersky Security Center により、そのフォルダーにある実行ファイルがカスタムカテゴリに追加されます。

- **リポジトリから証明書を選択**：カスタムカテゴリにアプリケーションを追加するための条件として、実行可能ファイルの署名に使用された証明書を選択します。

- **ドライブ種別**：アプリケーションをカスタムカテゴリに追加する条件として、ストレージデバイスの種別（すべてのハードディスクとリムーバブルドライブ、またはリムーバブルドライブのみ）を選択します。

ステップ 5：設定

この手順は、［**選択したデバイスの実行ファイルを含むカテゴリ**］カテゴリ種別を選択した場合に使用できます。

この手順では、［**追加**］をクリックしてコンピューターを指定します。そのコンピューターにある実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。［**実行ファイル**］フォルダーに表示される、指定されたコンピューターのすべての実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。

この手順では、以下の設定も指定できます：

- ハッシュ関数の計算アルゴリズム。アルゴリズムを選択するには、以下のチェックボックスを 1 つ以上オンにします：

  - **このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**

  - **このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**

- ［**データを管理サーバーのリポジトリと同期**］チェックボックス：Kaspersky Security Center によって、定期的にアプリケーションカテゴリを空にした後、［**実行ファイル**］フォルダーに表示される、指定されたコンピューターのすべての実行ファイルをアプリケーションカテゴリに追加する場合、このチェックボックスをオンにします。

  ［**データを管理サーバーのリポジトリと同期**］がオフの場合、アプリケーションカテゴリの作成後、Kaspersky Security Center はカテゴリへの変更を行いません。

ステップ 6：［リポジトリ］フォルダー

この手順は、［**特定のフォルダーの実行ファイルを含むカテゴリ**］カテゴリ種別を選択した場合に使用できます。

この手順では、フォルダーを指定すると、Kaspersky Security Center によってそのフォルダー内の実行ファイルが検索され、アプリケーションがアプリケーションカテゴリに自動的に追加されます。

この手順では、以下の設定も指定できます：

- ［**ダイナミックリンクライブラリ（DLL）をこのカテゴリに含める**］チェックボックス：ダイナミックリンクライブラリ（DLL ファイル）をアプリケーションカテゴリに含める場合は、このチェックボックスをオンにします。

  DLL ファイルをアプリケーションカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

- ［**このカテゴリ内のスクリプトデータを含める**］チェックボックス：アプリケーションカテゴリにスクリプトを含める場合は、このチェックボックスをオンにします。

  スクリプトをアプリケーションカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

- ハッシュ関数の計算アルゴリズム。アルゴリズムを選択するには、以下のチェックボックスを 1 つ以上オンにします：

  - **このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**

  - **このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**

- ［**変更のあったフォルダーを強制スキャンする**］チェックボックス：アプリケーションカテゴリへの自動追加に使用されたフォルダーに対して、Kaspersky Security Center によって定期的に実行ファイルを検索する場合、このチェックボックスをオンにします。

  ［**変更のあったフォルダーを強制スキャンする**］がオフの場合、Kaspersky Security Center は、アプリケーションカテゴリへの自動追加に使用されたフォルダーでファイルの追加または削除があった場合のみ、そのフォルダー内の実行ファイルを検索します。

- ［**スキャン間隔（1 - 168時間）**］フィールド：このフィールドで、アプリケーションカテゴリへの自動追加に使用されるフォルダー内の実行ファイルを Kaspersky Security Center が検索する間隔（時間）を指定できます。

  このフィールドは、［**変更のあったフォルダーを強制スキャンする**］をオンにした場合に使用できます。

ステップ 7：カスタムカテゴリの作成

ウィザードを終了します。

製品インターフェイスでアプリケーションコントロールルールの新しい適用条件を追加するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**ブロック対象のアプリケーション**］または［**許可するアプリケーション**］をクリックします。

   アプリケーションコントロールルールのリストのテーブルが開きます。

4. 適用する基準を設定するルールを選択します。

   アプリケーションコントロールルールのプロパティが表示されます。

5. ［**条件：N**］タブまたは［**除外リスト：N**］タブを選択し、［**追加**］をクリックします。

6. アプリケーションコントロールルールの適用条件を選択します。

   - **起動したことがあるアプリケーションのプロパティによる条件設定**：実行中のアプリケーションのリストで、アプリケーションコントロールルールが適用されるアプリケーションを選択することができます。コンピューター上で以前実行されたアプリケーションのリストも表示されます。1つまたは複数のルールを適用する条件の作成に使用する次の条件を選択します：**ファイルのハッシュ**、**証明書**、KL **カテゴリ**、**メタデータ**または**ファイルまたはフォルダーのパス**。

   - **「KL カテゴリ」による条件設定**：*KL カテゴリ*とは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe® Acrobat® などが含まれます。

   - **カスタム条件設定**：アプリケーションのファイルを選択し、ルールを適用する条件を選択できます：**ファイルのハッシュ**、**証明書**、**メタデータ**または**ファイルまたはフォルダーのパス**。

   - **ドライブによる条件設定（リムーバブルドライブ）**：アプリケーションコントロールルールはリムーバブルドライブ上で実行されているファイルにのみ適用されます。

   - **指定されたフォルダー内のファイルのプロパティによる条件設定**：アプリケーションコントロールルールは特定のフォルダーのファイルにのみ適用されます。サブフォルダーのファイルを含めたり除外することもできます。1つまたは複数のルールを適用する条件の作成に使用する次の条件を選択します：**ファイルのハッシュ**、**証明書**、KL **カテゴリ**、**メタデータ**または**ファイルまたはフォルダーのパス**。

7. 変更内容を保存します。

条件を追加する際には、アプリケーションコントロールの次の事項に留意してください：

- Kaspersky Endpoint Security はメタデータ（**File name**、**Application name**、**Vendor**）にマスクを入力するための文字として「`*`」と「`?`」をサポートします。

- Kaspersky Endpoint Security は、MD5 ファイルハッシュ値をサポートせず、MD5 ハッシュに基づいたアプリケーションの起動のコントロールを実行しません。ルールを適用する条件には SHA256 ハッシュが使用されます。

- ルールを適用する条件として［**発行元**］と［**証明書の発行先**］のみを使用することは避けてください。これらの条件は信頼されません。

- ［**ファイルまたはフォルダーのパス**］でシンボリックリンクを使用している場合、アプリケーションコントロールルールが正しく動作するために、シンボリックリンクを解決してください。これを行うには、［**シンボリックリンクを解決する**］をクリックします。

実行ファイルフォルダーからアプリケーションカテゴリへの実行ファイルの追加

［**実行ファイル**］フォルダーに、コンピューター上で検出された実行ファイルが表示されます。Kaspersky Endpoint Security ではインベントリタスクの実行後に実行ファイルのリストが生成されます。

実行ファイルフォルダーからアプリケーションカテゴリに実行ファイルを追加するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**実行ファイル**］の順に選択します。
3. 作業領域で、アプリケーションカテゴリに追加する実行ファイルを選択します。
4. 選択した実行ファイルを右クリックしてコンテキストメニューを開き、［**カテゴリに追加**］を選択します。
5. 表示されたウィンドウで、次の操作を実行します：
   - ウィンドウの上部で、次のいずれかのオプションを選択します：
     - **新規アプリケーションカテゴリへ追加**：新しいアプリケーションカテゴリを作成して実行ファイルを追加する場合、このオプションを選択します。
     - **アプリケーションカテゴリへ追加**：既存のアプリケーションカテゴリを選択して実行ファイルを追加する場合、このオプションを選択します。
   - ［**ルール種別**］ブロックで、次のいずれかを選択します：
     - **除外しない場合のルール**：実行ファイルをアプリケーションカテゴリに追加する条件を作成する場合、このオプションを選択します。
     - **除外に追加する場合のルール**：実行ファイルをアプリケーションカテゴリから除外する条件を作成する場合、このオプションを選択します。
   - ［**条件として使用する情報**］ブロックで、以下のオプションのいずれかを選択します：
     - **証明書の詳細情報（証明書がないファイルの場合 SHA256 ハッシュ）**
     - **証明書の詳細情報（証明書のないファイルはスキップ）**
     - **SHA256 のみ（ハッシュのないファイルはスキップ）**
     - **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**
6. 変更内容を保存します。

イベントに関連した実行ファイルのアプリケーションカテゴリへの追加

アプリケーションコントロールによるイベントに関連する実行ファイルをアプリケーションカテゴリに追加するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**イベント**］タブを選択します。
3. ［**イベントの抽出**］で、アプリケーションコントロールの動作に関連するイベントの抽出を選択します（アプリケーションコントロールの動作によるイベントの表示、アプリケーションコントロールのテスト動作によるイベントの表示）。
4. ［**抽出を実行**］をクリックします。

5. 関連する実行ファイルをアプリケーションカテゴリに追加するイベントを選択します。

6. 選択したイベントを右クリックしてコンテキストメニューを開き、［**カテゴリに追加**］を選択します。

7. 表示されたウィンドウで、アプリケーションカテゴリの設定をします：

   - ウィンドウの上部で、次のいずれかのオプションを選択します：

     - **新規アプリケーションカテゴリへ追加**：新しいアプリケーションカテゴリを作成して実行ファイルを追加する場合、このオプションを選択します。

     - **アプリケーションカテゴリへ追加**：既存のアプリケーションカテゴリを選択して実行ファイルを追加する場合、このオプションを選択します。

   - ［**ルール種別**］ブロックで、次のいずれかを選択します：

     - **除外しない場合のルール**：実行ファイルをアプリケーションカテゴリに追加する条件を作成する場合、このオプションを選択します。

     - **除外に追加する場合のルール**：実行ファイルをアプリケーションカテゴリから除外する条件を作成する場合、このオプションを選択します。

   - ［**条件として使用する情報**］ブロックで、以下のオプションのいずれかを選択します：

     - **証明書の詳細情報（証明書がないファイルの場合 SHA-256 ハッシュ）**

     - **証明書の詳細情報（証明書のないファイルはスキップ）**

     - **SHA-256 のみ（ハッシュのないファイルはスキップ）**

     - **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

8. 変更内容を保存します。

アプリケーションコントロールルールを追加する

Kaspersky Security Center を使用してアプリケーションコントロールルールを追加するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。

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

4. ［**追加**］をクリックします。

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

5. 次のいずれかの手順を実行します：

- 新しいカテゴリを作成する場合：

  a. ［**カテゴリの作成**］をクリックします。
  ユーザーカテゴリの作成ウィザードが表示されます。

  b. ユーザーカテゴリの作成ウィザードの指示に従います。

  c. ［**カテゴリ**］で、作成したアプリケーションカテゴリを選択します。

- 既存のカテゴリを編集する場合：

  a. ［**カテゴリ**］で、編集する既存のアプリケーションカテゴリを選択します。

  b. ［**プロパティ**］をクリックします。

  c. 選択したアプリケーションカテゴリの設定を変更します。

  d. 変更内容を保存します。

  e. ［**カテゴリ**］で、ルール作成のために作成したアプリケーションカテゴリを選択します。

6. ［**ユーザーとその権限**］テーブルで、［**追加**］をクリックします。
ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

7. ［**ユーザーとその権限**］テーブルで、以下を実行します：

- 選択したカテゴリに属するアプリケーションの起動をユーザーまたはユーザーグループに許可する場合、該当する行にある［**許可**］をオンにします。

- 選択したカテゴリに属するアプリケーションの起動をユーザーまたはユーザーグループに許可しない場合、該当する行にある［**ブロック**］をオンにします。

8. ［**ユーザーまたはグループ**］列に表示されておらず、［**ユーザーまたはグループ**］列で指定されているユーザーグループに属していないすべてのユーザーに対して、選択したカテゴリに属するアプリケーションの起動をブロックする場合、［**他のユーザーを拒否**］をオンにします。

9. 選択したアプリケーションカテゴリに含まれるアプリケーションを信頼するアップデーターとみなし、そのアプリケーションが作成する別の実行ファイルの実行を許可するには、［**信頼するアップデーター**］をオンにします。

> Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。

10. 変更内容を保存します。

アプリケーションコントロールルールを追加するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**ブロック対象のアプリケーション**］または［**許可するアプリケーション**］をクリックします。
   アプリケーションコントロールルールのリストのテーブルが開きます。
4. ［**追加**］をクリックします。
   アプリケーションコントロールルールの設定ウィンドウが表示されます。
5. ［**全般設定**］タブでルールの主要な設定を定義します。
   a. ［**ルール名**］にルール名を入力します。
   b. ［**説明**］に、ルールの説明を入力します。
   c. ［**ユーザーとその権限**］テーブルで、［**追加**］をクリックします。
      ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。
      このルールは、既定ですべてのユーザーに適用されます。

      > テーブルでユーザーが指定されていない場合、ルールは保存できません。

   d. ［**ユーザーとその権限**］テーブルで、トグルスイッチを使用してユーザーがアプリケーションを開始する権限を定義します。
   e. ［**他のユーザーを拒否**］をオンにすると、［**ユーザーとその権限**］テーブルに入っておらず、［**ユーザーとその権限**］テーブルのユーザーグループのメンバーでもないユーザーによるルールを適用する条件を満たすプログラムの実行をブロックします。

      > ［**他のユーザーを拒否**］をオフにすると、［**ユーザーとその権限**］テーブルで指定されておらず［**ユーザーとその権限**］テーブルで指定されたユーザーグループに属していないユーザーによるアプリケーションの起動は、管理されません。

   f. ルールを適用する条件に合致するアプリケーションを信頼するアップデーターとして認識するよう設定する場合は、［**信頼するアップデーター**］をオンにします。*信頼するアップデーター*とは、実行ファイルの作成とそのファイルの実行が許可されているアプリケーションです。
      アプリケーションが複数のルールの適用条件に一致する場合、Kaspersky Endpoint Security は次の条件を満たす場合に「*信頼するアップデーター*」フラグを作成します：
      - すべてのルールでアプリケーションの実行が許可されている。
      - ルールのうち少なくとも1つで［**信頼するアップデーター**］がオンになっている。
6. ［**条件：N**］タブで、ルールをトリガする対象条件のリストを作成または編集します。

7. ［**除外リスト：N**］タブで、ルールをトリガする例外条件のリストを作成または編集します。

   Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。

8. 変更内容を保存します。

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

管理コンソールでアプリケーションコントロールルールのステータスを変更するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。

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

4. ［**状態**］列をクリックしてコンテキストメニューを表示し、以下のいずれかを選択します：

   - **オン**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
   - **オフ**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
   - **テスト**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

5. 変更内容を保存します。

製品インターフェイスでアプリケーションコントロールルールのステータスを変更するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**ブロック対象のアプリケーション**］または［**許可するアプリケーション**］をクリックします。

   アプリケーションコントロールルールのリストのテーブルが開きます。

4. ［**ステータス**］列でコンテキストメニューを表示し、以下のいずれかを選択します：

   - **有効**：このステータスは、アプリケーションコントロールが実行されているときにルールが使用されることを示します。
   - **無効**：このステータスは、アプリケーションコントロールが実行されているときにルールが無視されることを示します。
   - **テストモード**：このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

5. 変更内容を保存します。

アプリケーションコントロールルールのエクスポートおよびインポート

アプリケーションコントロールルールを XML ファイルにエクスポートすることができます。また、エクスポートまたはインポート機能を使用して、アプリケーションコントロールルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

アプリケーションコントロールルールをエクスポートまたはインポートする際、次の留意事項にご注意ください：

- Kaspersky Endpoint Security は、有効なアプリケーションコントロールモードのルールのリストのみをエクスポートします。言い換えると、アプリケーションコントロールが拒否リストモードで動作している場合、Kaspersky Endpoint Security はこのモードのルールのみをエクスポートします。許可リストモードのルールのリストをエクスポートするには、モードを変更してエクスポート操作を再度実行してください。
- Kaspersky Endpoint Security はアプリケーションコントロールルールが動作するためにアプリケーションカテゴリを使用します。アプリケーションコントロールルールのリストを別のサーバーに抗する場合、アプリケーションカテゴリのリストも移行する必要があります。アプリケーションカテゴリのエクスポートまたはインポートの詳細については、Kaspersky Security Center ヘルプを参照してください。

管理コンソール（MMC）で信頼するアプリケーションコントロールルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。
4. アプリケーションコントロールルールのリストをエクスポートするには：
   a. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

      ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

   b. ［**エクスポート**］リンクをクリックします。
   c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. ファイルを保存します。

Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

5. アプリケーションコントロールルールのリストをインポートするには：

a. ［**インポート**］リンクをクリックします。

表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

b. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでアプリケーションコントロールルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

5. ［**操作モード**］で、ルールのリストを選択します：アプリケーションの拒否リストまたは許可リスト。

6. ルールのリストをエクスポートするには：

a. エクスポートするルールを選択します。

b. → ［**エクスポート**］を選択します。

Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

7. ルールのリストをインポートするには：

a. → ［**インポート**］を選択します。

表示されたウィンドウで、ルールのリストをインポートする JSON ファイルを選択します。

b. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

アプリケーションコントロールの動作によるイベントの表示

Kaspersky Security Center が受信した、アプリケーションコントロールの動作によるイベントを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**イベント**］タブを選択します。
3. ［**抽出の作成**］をクリックします。
4. 表示されたウィンドウで、［**イベント**］セクションに移動します。
5. ［**すべてクリア**］をクリックします。
6. ［**イベント**］テーブルで、［**アプリケーションの起動が禁止されました**］をオンにします。
7. 変更内容を保存します。
8. ［**イベントの抽出**］で、作成した抽出を選択します。
9. ［**抽出を実行**］をクリックします。

ブロックされたアプリケーションに関するレポートの表示

ブロックされたアプリケーションに関するレポートを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］手順で、［**その他**］→［**ブロック対象アプリケーションのレポート**］の順に選択します。
   新規レポートテンプレートウィザードが完了すると、［**レポート**］タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

アプリケーションコントロールルールのテスト

アプリケーションコントロールルールが業務で必要なアプリケーションをブロックしないことを確認するため、新しくルールを作成したあとでテストを有効にして動作を検証してください。アプリケーションコントロールルールのテストを有効にすると、Kaspersky Endpoint Security は、アプリケーションコントロールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

アプリケーションコントロールルールの動作を検証するには、動作の結果として Kaspersky Security Center に報告されるアプリケーションコントロールのイベントを確認します。テストモードの結果、コンピューターのユーザーの業務に必要なすべてのアプリケーションについて起動ブロックイベントがなければ、適切なルールが作成されています。そうでない場合、作成したルールの設定の変更、追加のルールの作成、既存のルールの削除を行ってください。

既定では、Kaspersky Endpoint Security は、ルールで禁止されているアプリケーションを除くすべてのアプリケーションの起動を許可します。

アプリケーションコントロールルールのテストを有効または無効にする

Kaspersky Security Center でアプリケーションコントロールルールのテストを有効または無効にするには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。

   ウィンドウの右側に、アプリケーションコントロールの設定が表示されます。
4. ［**コントロールモード**］ドロップダウンリストから、次のいずれかを選択します：

   - **拒否リスト**：このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールの条件を満たす場合は除きます。
   - **許可リスト**：このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールの条件を満たす場合は除きます。
5. 次のいずれかの手順を実行します：

   - アプリケーションコントロールルールのテストを有効にする場合、［**ルールをテスト運用**］で［**処理**］を選択します。
   - アプリケーションコントロールを有効にしてユーザーのコンピューター上のアプリケーションの起動を管理する場合は、［**ルールを適用**］を選択します。
6. 変更内容を保存します。

アプリケーションコントロールルールのテストを有効にするか、アプリケーションコントロールのブロック処理を選択するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。
3. ［**ブロック対象のアプリケーション**］または［**許可するアプリケーション**］をクリックします。

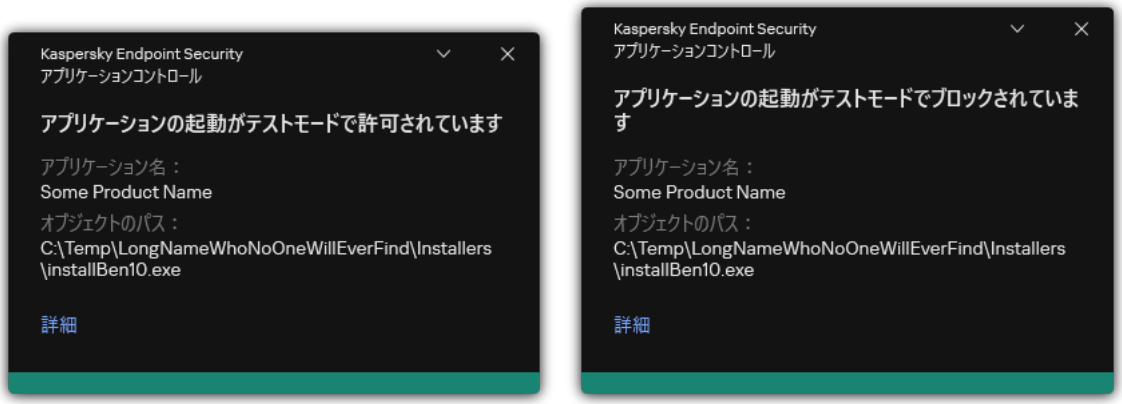
   アプリケーションコントロールルールのリストのテーブルが開きます。

4. ［**ステータス**］列で［**テストモード**］をオンにします。

   このステータスは、ルールが適用されるアプリケーションの起動は常に許可されるが、そのようなアプリケーションの起動についての情報がレポートに記録されることを意味します。

5. 変更内容を保存します。

Kaspersky Endpoint Security は、アプリケーションコントロールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。ユーザーのコンピューターでのルールのテストに関する通知の表示を設定することも可能です（下の図を参照）。



テストモードでのアプリケーションコントロールの通知

テストモードでのブロック対象アプリケーションのレポートの表示

テストモードでのブロック対象アプリケーションのレポートを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。

   新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ステップで、［**その他**］→［**テストモードでのブロック対象アプリケーションのレポート**］の順に選択します。

   新規レポートテンプレートウィザードが完了すると、［**レポート**］タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

アプリケーションコントロールのテスト動作によるイベントの表示

Kaspersky Security Center が受信した、アプリケーションコントロールのテストイベントを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**イベント**］タブを選択します。

3. ［**抽出の作成**］をクリックします。

4. 表示されたウィンドウで、［**イベント**］セクションに移動します。

5. ［**すべてクリア**］をクリックします。

6. ［**イベント**］テーブルで［**アプリケーションの起動がテストモードでブロックされています**］と［**アプリケーションの起動がテストモードで許可されています**］をオンにします。

7. 変更内容を保存します。

8. ［**イベントの抽出**］で、作成した抽出を選択します。

9. ［**抽出を実行**］をクリックします。

アプリケーション動作モニター

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

*アプリケーション動作モニター*は、ユーザーのコンピューターのアプリケーションの動作に関する情報をリアルタイムで表示するように設計されたツールです。

アプリケーション動作モニターを使用するには、アプリケーションコントロールおよびホスト侵入防止のインストールが必要です。これらの機能がインストールされていない場合、メインウィンドウのアプリケーション動作モニターは非表示になります。

アプリケーション動作モニターを開始するには：

製品のメインウィンドウの［**監視**］で、［**アプリケーション動作モニター**］をクリックします。

このウィンドウに、ユーザーのコンピューターのアプリケーションの動作に関する情報が 3 つのタブに分かれて表示されます：

- ［**すべてのアプリケーション**］タブにはコンピューターにインストールされているすべてのアプリケーションに関する情報が表示されます。
- ［**実行中**］タブには、リアルタイムで各アプリケーションによるコンピューターのリソース消費に関する情報が表示されます。このタブから、個別のアプリケーションに関する権限の設定画面に移動することもできます。
- ［**OSの起動時に実行**］タブには、オペレーティングシステムの開始時に起動するアプリケーションのリストが表示されます。

ユーザーのコンピューターでアプリケーション動作モニターの情報を非表示にするには、ユーザーのアプリケーション動作モニターのアクセス権を制限します。

管理コンソール（MMC）を使用して製品インターフェイスでアプリケーション動作モニターを非表示にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**インターフェイス**］の順に選択します。
4. ［**アプリケーション動作モニターセクションを非表示**］を使用してツールへのアクセス権を付与する、もしくはアクセスをブロックします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールを使用して製品インターフェイスでアプリケーション動作モニターを非表示にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**アプリケーション動作モニターセクションを非表示**］を使用してツールへのアクセス権を付与する、もしくはアクセスをブロックします。
6. 変更内容を保存します。

ファイルまたはフォルダーの名前のマスクの作成

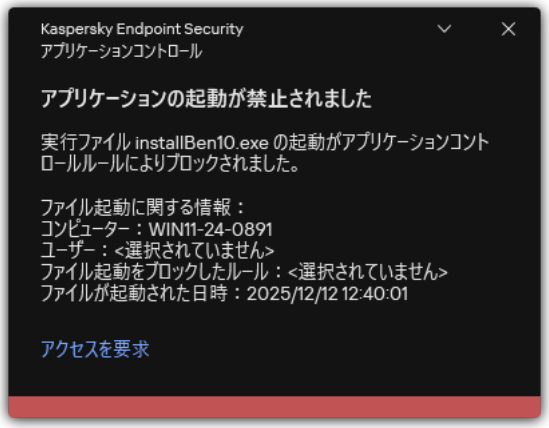
*ファイル名またはフォルダー名のマスク*とは、フォルダー名またはファイルの名前や拡張子を、正規表現を使用して表現したものです。

次の正規表現を使用してファイル名またはフォルダー名のマスクを作成できます：

- 「`*`」（アスタリスク）。任意の文字数の文字列を表します。たとえば、マスク「`C:\*.txt`」は、C: ドライブ上のフォルダーおよびサブフォルダーにある拡張子が `txt` のファイルのパスすべてを含みます。
- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

アプリケーションコントロールのメッセージテンプレートの編集

ユーザーがアプリケーションコントロールルールによってブロックされているアプリケーションを起動しようと試みると、Kaspersky Endpoint Security はアプリケーションの起動がブロックされていることを示すメッセージを表示します。カスペルスキーのエキスパートは、アプリケーションがブロックされた理由を説明するメッセージのテンプレートをユーザーに提供します（下の図を参照）。メッセージのテンプレートの管理用に特別な変数が用意されています（例：%USER_NAME%）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。



アプリケーションコントロールの通知

アプリケーションの起動が誤ってブロックされていると思われる場合は、メッセージテキストのリンクを使用して、メッセージを LAN 管理者に送信できます。これを行うには、［**アクセスを要求**］ボタンをクリックし、状況を説明するメッセージを管理者に送信します。また、管理者へのメッセージのテンプレートを作成しておき、アプリケーションへのアクセスを許可するかブロックするかの決定に役立つデータを追加することもできます。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの起動ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

管理コンソール（MMC）でアプリケーションコントロールのメッセージのテンプレートを変更する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。
4. ［**メッセージのテンプレートの設定**］ブロックの［**テンプレート**］をクリックします。

5. ウィンドウが表示されるので、そのウィンドウでアプリケーションコントロールのテンプレートを設定します：

   - **ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。

     テストモードではアプリケーションコントロールのメッセージテンプレートを設定することはできません。テストモードのアプリケーションコントロールでは、事前定義された通知が表示されます。

   - **管理者に送信するメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**既定**］を使用して既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでアプリケーションコントロールのメッセージのテンプレートを変更する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

5. ［**メッセージのテンプレート**］ブロックで、［**アプリケーションの開始に関するメッセージ**］をクリックして、アプリケーションコントロールのメッセージのテンプレートを設定します。

   - **ユーザーへのメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。

     テストモードではアプリケーションコントロールのメッセージテンプレートを設定することはできません。テストモードのアプリケーションコントロールでは、事前定義された通知が表示されます。

   - **管理者へのメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**既定値にリセット**］を使用して既定のテンプレートテキストを復元することもできます。

6. 変更内容を保存します。

製品インターフェイスでアプリケーションコントロールのメッセージのテンプレートを変更する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］を選択します。

3. ［**アプリケーションのブロックに関するメッセージのテンプレートです**］ブロックで、アプリケーションコントロールのメッセージのテンプレートを設定します：

   - **ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。

     テストモードではアプリケーションコントロールのメッセージテンプレートを設定することはできません。テストモードのアプリケーションコントロールでは、事前定義された通知が表示されます。

   - **管理者に送信するメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数を追加する**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**リセット**］を使用して既定のテンプレートテキストを復元することもできます。

4. 変更内容を保存します。

アプリケーションコントロールのメッセージテンプレートの変数

ユーザーメッセージテンプレートまたは管理者メッセージテンプレートでは、次の変数を使用できます。

- **適用されたルールの名前**：`%RULE%`

  ファイルの実行をブロックしたルールの名前。

- **今日の日付**：`%DATE%`

  ファイルの実行がブロックされた日付（形式：DD.MM.YYYY）。

- **現在の時刻**：`%TIME%`

  ファイルの実行がブロックされた時刻（形式：HH:MM）。

- **ユーザー名**：`%USER_NAME%`

  ファイルの実行がブロックされたコンピュータ上の現在のユーザーアカウントの名前。形式：`<device name>\<user alias>`（例： `DESKTOP-123\John.Smith`）。

- **コンピューター名**：`%COMPUTER_NAME%`

  ファイルの実行がブロックされたコンピューターの名前。

- **実行ファイル名**：`%FILE_NAME%`

  ブロックされたアプリケーションの実行ファイルの名前。

- **実行ファイルの KL カテゴリ**：`%KL_CAT%`

  ブロックされたアプリケーションが属する KL カテゴリ（例： ブラウザー）。

- **実行ファイルのパス**：`%FILE_PATH%`

  ブロックされたアプリケーションの実行ファイルの完全パス。

- **実行ファイルのバージョン**：`%FILE_VERSION%`

  ブロックされたアプリケーションの実行ファイルのバージョン。

- **実行ファイルの元の名前**：%ORIGINAL_FILE_NAME%

  ブロックされたアプリケーションの実行ファイルの元の名前。ファイル名は、アプリケーションの実行ファイルのプロパティで指定されます。

- **製造元**：%FILE_PUBLISHER%

  ブロックされたアプリケーションの製造元。

- **アプリケーション名**：%FILE_PRODUCT_NAME%

  ブロックされたアプリケーションの名前。

- **バージョン**：%PRODUCT_VERSION%

  ブロックされたアプリケーションのバージョン。

- **実行ファイルのハッシュ**：%FILE_HASH%

  ブロックされたアプリケーションの実行ファイルのハッシュ。

- **証明書の発行元**：%CERT_ISSUER%

  実行ファイルが署名されている証明書の発行者。

- **証明書の発行先**：%CERT_SUBJECT%

  実行ファイルが署名されている証明書の発行先。

- **証明書のハッシュ値**：%CERT_THUMBPRINT%

  実行ファイルが署名されている証明書のサムプリント。

許可されるアプリケーションのリストの実装のベストプラクティス

許可されるアプリケーションのリストの実装を計画する場合、以下を実行してください：

1. 以下のグループを作成します：

   - ユーザーグループ：各種アプリケーションの使用を許可するユーザーのグループ。

   - 管理グループ：Kaspersky Security Center によって許可されるアプリケーションのリストを割り当てるコンピューターのグループ。異なる許可リストの設定をグループに対して使用する場合は、複数のコンピューターのリストを作成する必要があります。

2. 起動を許可するアプリケーションのリストを作成します。

   リストを作成する前に、以下を実行してください：

   a. インベントリタスクを実行します。

      インベントリタスクの作成、設定、開始に関する情報は、「タスクの管理」セクションにあります。

   b. 実行ファイルのリストを表示します。

アプリケーションの許可リストモードの設定

許可リストモードを設定する際は、以下の操作を実行してください：

1. 起動を許可するアプリケーションを含むアプリケーションカテゴリを作成します。

   次のいずれかのアプリケーションカテゴリ作成方法を選択できます：

   - **手動でコンテンツが追加されるカテゴリ**：このカテゴリには、以下の条件を使用して手動で追加できます：
     - ファイルのメタデータ：Kaspersky Security Center により、指定されたメタデータを伴うすべての実行ファイルがアプリケーションカテゴリに追加されます。
     - ファイルのハッシュ値。Kaspersky Security Center により、指定されたハッシュを持つすべての実行ファイルがアプリケーションカテゴリに追加されます。

       異なるバージョンのファイルのハッシュは異なるため、この条件を使用すると、アップデートの自動インストールが使用できなくなります。

     - ファイルの証明書：Kaspersky Security Center により、指定された証明書で署名されたすべての実行ファイルがアプリケーションカテゴリに追加されます。
     - KL カテゴリ：Kaspersky Security Center により、指定された KL カテゴリにあるすべてのアプリケーションがアプリケーションカテゴリに追加されます。
     - アプリケーションフォルダー：Kaspersky Security Center により、そのフォルダーにあるすべての実行ファイルがアプリケーションカテゴリに追加されます。

       ［**アプリケーションフォルダー**］条件を使用すると、指定されたフォルダー内の任意のアプリケーションに対して起動が許可されるため、安全でない場合があります。［**アプリケーションフォルダー**］を条件としたアプリケーションカテゴリは、アップデートの自動インストールが許可されているユーザーに対して適用されるルールでのみ使用してください。

   - **特定のフォルダーの実行ファイルを含むカテゴリ**：指定したフォルダーの実行ファイルを、作成されたアプリケーションカテゴリに自動的に割り当てるように設定できます。
   - **選択したデバイスの実行ファイルを含むカテゴリ**：指定したコンピューターのすべての実行ファイルを、作成されたアプリケーションカテゴリに自動的に割り当てるように設定できます。

     この方法でアプリケーションカテゴリを作成すると、Kaspersky Security Center は**実行ファイル**フォルダーからコンピューター上のアプリケーションに関する情報を受け取ります。

2. アプリケーションコントロールの許可リストモードを選択します。

3. 作成したアプリケーションカテゴリを使用してアプリケーションコントロールルールを作成します。

［**ゴールデンイメージ**］ルールおよび［**信頼するアップデーター**］ルールは許可リストモードの初期設定です。アプリケーションコントロールは KL カテゴリに対応しています。「ゴールデンイメージ」KL カテゴリには、オペレーティングシステムの通常の動作を可能にするプログラムが含まれます。「信頼するアップデーター」KL カテゴリには、最も信頼できるソフトウェア開発元のアップデーターが含まれます。また、これらのルールは削除できません。これらのルールの設定は編集できません。既定では、［**ゴールデンイメージ**］ルールが有効で、［**信頼するアップデーター**］ルールは無効です。これらのルールを適用する条件に一致するアプリケーションは、すべてのユーザーが起動できます。

4. アップデートの自動インストールを許可するアプリケーションを特定します。

次のいずれかの方法で、アップデートの自動インストールを許可できます：

- KL カテゴリに属するすべてのアプリケーションの起動を許可することで、許可するアプリケーションのリストを指定する。
- 証明書で署名されたすべてのアプリケーションの起動を許可することで、許可するアプリケーションのリストを指定する。

  証明書で署名されたすべてのアプリケーションの起動を許可するには、証明書に基づく条件のカテゴリを作成し、［**発行先**］パラメータのみを使用して値を「*」にします。
- アプリケーションコントロールルールで［**信頼するアップデーター**］をオンにする。このチェックボックスをオンにすると、ルールに含まれるアプリケーションが信頼するアップデーターとみなされます。ルールに含まれるアプリケーションによってインストールまたはアップデートされたアプリケーションの起動は、ブロックルールが適用されなければ許可されます。

  Kaspersky Endpoint Security の設定を移行すると、信頼するアップデーターによって作成された実行ファイルのリストも移行されます。
- フォルダーを作成し、その中にアップデートの自動インストールを許可するアプリケーションの実行ファイルを置きます。続いて、［**アプリケーションフォルダー**］条件を設定したアプリケーションカテゴリを作成し、フォルダーのパスを指定します。許可ルールを作成し、対象としてこのアプリケーションカテゴリを選択します。

  ［**アプリケーションフォルダー**］条件を使用すると、指定されたフォルダー内の任意のアプリケーションに対して起動が許可されるため、安全でない場合があります。［**アプリケーションフォルダー**］を条件としたアプリケーションカテゴリは、アップデートの自動インストールが許可されているユーザーに対して適用されるルールでのみ使用してください。

許可リストモードのテスト

アプリケーションコントロールルールが業務で必要なアプリケーションをブロックしないことを確認するため、新しくルールを作成したあとでテストを有効にして動作を検証してください。テストを有効にすると、Kaspersky Endpoint Security は、アプリケーションコントロールルールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

許可リストモードをテストする場合、以下を実行してください：

1. テスト期間を決定します（数日間から 2 か月）。
2. アプリケーションコントロールルールのテストを有効にします。
3. アプリケーションコントロールの動作テストによるイベントとテストモードでのブロック対象アプリケーションのレポートを検証することにより、テスト結果を分析します。
4. 分析の結果に基づいて、許可リストモードの設定を変更します。

   特に、テスト結果に基づいて、イベントに関連する実行ファイルをアプリケーションカテゴリに追加できます。

許可リストモードのサポート

アプリケーションコントロールのブロック処理を選択した後、以下を実行して許可リストモードのサポートを継続してください：

- アプリケーションコントロールの動作によるイベントと実行ブロックのレポートを検証することにより、アプリケーションコントロールの有効性を分析します。
- アプリケーションへのアクセスを求めるユーザーからのリクエストを分析します。
- 見慣れない実行ファイルについて、Kaspersky Security Networkで評価を確認して分析します。
- オペレーティングシステムやソフトウェアのアップデートをインストールする前に、アップデートをテストグループのコンピューターにインストールして、アプリケーションコントロールルールでの処理を確認します。
- アプリケーションコントロールルールで使用されているカテゴリに、必要なアプリケーションを追加します。

ネットワークポートの監視

Kaspersky Endpoint Security の動作中、ウェブコントロール、メール脅威対策、ウェブ脅威対策、ふるまい検知および脆弱性攻撃ブロックは、特定のプロトコルで送信される、もしくはコンピューターの開いている TCP および UDP ポートを通過するデータストリームを監視します。たとえば、メール脅威対策は SMTP を使用して送信される情報を分析し、ウェブ脅威対策は HTTP または FTP を使用して送信される情報を分析します。

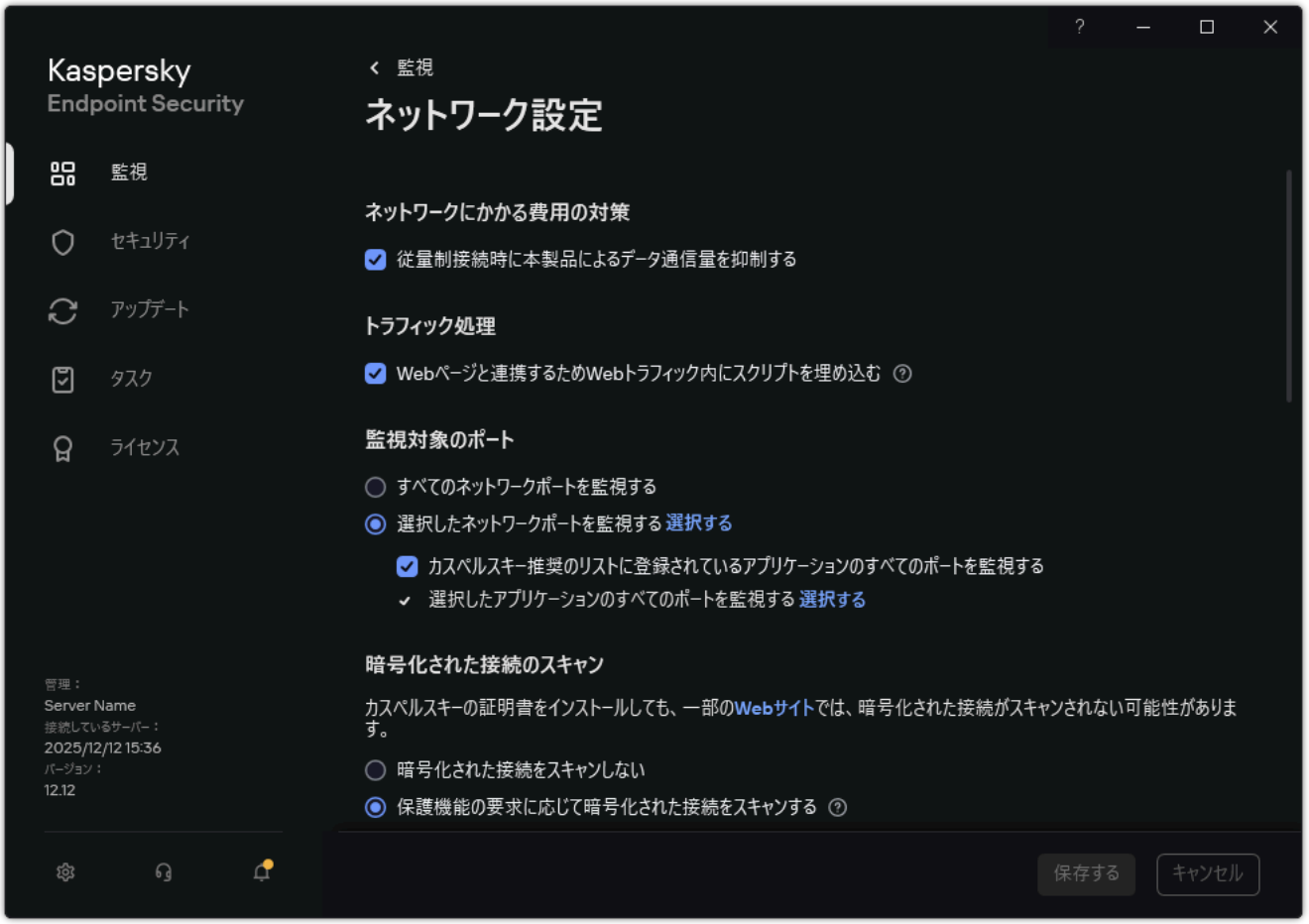
Kaspersky Endpoint Security は、ユーザーのコンピューターの TCP ポートと UDP ポートを、侵害される可能性に応じていくつかのグループに分割します。一部のネットワークポートは、脆弱なサービスのために予約されています。これらのポートはネットワーク攻撃の標的となる可能性が大きいため、より重点的に監視してください。非標準ネットワークポートに依存する非標準サービスを使用する場合も、これらのネットワークポートが攻撃側のコンピューターの標的になる可能性があります。ネットワークポートのリスト、およびネットワークアクセスを要求するアプリケーションのリストを指定できます。こうすると、メール脅威対策とウェブ脅威対策がネットワークトラフィックを監視する際に、これらのポートとアプリケーションに特別な注意がはらわれます。

コンピューターのセキュリティを確保するために、ふるまい検知および脆弱性攻撃ブロックは、ネットワークポートを通過するデータストリームも監視します。これらのコンポーネントは、脅威となる可能性のある個々のプロセスのネットワークトラフィックを継続的に監視します。

すべてのネットワークポートの監視の有効化

すべてのネットワークポートの監視を有効にするには、次の手順を実行します：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。



ネットワークポートの監視設定

3. ［**監視対象のポート**］ブロックで、［**すべてのネットワークポートを監視する**］を選択します。
4. 変更内容を保存します。

監視対象ネットワークポートのリストの作成

監視するネットワークポートのリストを作成するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。
3. ［**監視対象のポート**］ブロックで、［**選択したネットワークポートを監視する**］を選択します。

4. ［**選択する**］をクリックします。

   メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。

5. ［**ステータス**］列のトグルスイッチを使用してネットワークポートの監視を有効または無効にします。

6. 目的のネットワークポートがリストに表示されていない場合は、次の手順を実行してそのポートを追加します：

   a. ［**追加**］をクリックします。

   b. 表示されたウィンドウで、ネットワークポート番号と短い説明を入力します。

   c. ネットワークポートの［**有効**］または［**無効**］を設定します。

7. 変更内容を保存します。

FTP プロトコルがパッシブモードで動作している場合、監視対象のネットワークポートのリストに追加されていないランダムネットワークポートを経由して接続を確立することもできます。接続を保護するには、すべてのネットワークポートの監視を有効化するか、FTP 接続を確立するアプリケーションのネットワークポートの制御を設定します。

すべてのネットワークポートを監視するアプリケーションのリストの作成

Kaspersky Endpoint Security がすべてのネットワークポートを監視するアプリケーションのリストを作成できます。

Kaspersky Endpoint Security がすべてのネットワークポートを監視するアプリケーションのリストに、FTP プロトコル経由でデータを受信または送信するアプリケーションを含めるようにしてください。

すべてのネットワークポートを監視するアプリケーションのリストを作成するには：

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**ネットワーク設定**］を選択します。

3. ［**監視対象のポート**］ブロックで、［**選択したネットワークポートを監視する**］を選択します。

4. ［**カスペルスキー推奨のリストに登録されているアプリケーションのすべてのポートを監視する**］チェックボックスをオンにします。

   このチェックボックスをオンにすると、Kaspersky Endpoint Security は次のアプリケーションのポートすべてを監視します：

   - Adobe Acrobat Reader
   - Apple Application Support
   - Google Chrome

- Microsoft Edge
- Mozilla Firefox
- Internet Explorer
- Java
- mIRC
- Opera
- Pidgin
- Safari
- Mail.ru Agent
- Yandex Browser

5. ［**選択したアプリケーションのすべてのポートを監視する**］チェックボックスをオンにします。
6. ［**選択する**］をクリックします。
   Kaspersky Endpoint Security がネットワークポートを監視するアプリケーションのリストが開きます。
7. ［**ステータス**］列のトグルスイッチを使用してネットワークポートの監視を有効または無効にします。
8. アプリケーションがリストに含まれていない場合は、次の手順に従って追加します：
   a. ［**追加**］をクリックします。
   b. 表示されたウィンドウで、アプリケーションの実行ファイルへのパスおよび短い説明を入力します。
   c. ネットワークポートの［**有効**］または［**無効**］を設定します。
9. 変更内容を保存します。

監視対象のポートのリストのエクスポートまたはインポート

Kaspersky Endpoint Security は次のリストを使用してネットワークポートを監視します：ネットワークポートのリストおよび Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリスト。監視対象のポートのリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ説明を持つ多数のポートをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、監視対象のポートのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

管理コンソール（MMC）で監視対象のポートのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**ネットワーク設定**］に移動します。

5. ネットワークポートのリストをエクスポートするには：

   a. ［**監視対象のポート**］ブロックで、［**選択されたネットワークポートのみを監視する**］を選択します。

   b. ［**選択済み<N> ポート**］をクリックします。

      ［**ネットワークポート**］ウィンドウが表示されます。［**ネットワークポート**］ウィンドウに、メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。

   c. ネットワークポートのリストで、エクスポートするポートを選択します。

   d. ［**エクスポート**］をクリックします。

   e. 表示されたウィンドウで、ネットワークポートのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   f. ファイルを保存します。

      Kaspersky Endpoint Security は、ネットワークポートのリスト全体を XML ファイルにエクスポートします。

6. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをエクスポートするには：

   a. ［**監視対象のポート**］ブロックで、［**選択したアプリケーションのすべてのポートを監視する**］をオンにします。

   b. ［**選択済み<N> アプリケーション**］をクリックします。

   c. アプリケーションのリストで、エクスポートするアプリケーションを選択します。

   d. ［**エクスポート**］をクリックします。

   e. 表示されたウィンドウで、アプリケーションをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   f. ファイルを保存します。

      Kaspersky Endpoint Security は、アプリケーションのリスト全体を XML ファイルにエクスポートします。

7. ネットワークポートのリストをインポートするには：

   a. ネットワークポートのリストで、［**インポート**］をクリックします。

      表示されたウィンドウで、ネットワークポートのリストをインポートする XML ファイルを選択します。

   b. ファイルを開きます。

      コンピューターにネットワークポートのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをインポートするには：

   a. アプリケーションのリストで、［**インポート**］をクリックします。

      表示されたウィンドウで、アプリケーションのリストをインポートする XML ファイルを選択します。

   b. ファイルを開きます。

      コンピューターにアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

9. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**ネットワーク設定**］の順に選択します。

4. ［**監視対象のポート**］ブロックで、［**選択されたネットワークポートのみを監視する**］を選択します。

5. ［**設定**］をクリックします。

   ［**ネットワークポート**］ウィンドウが表示されます。［**ネットワークポート**］ウィンドウに、メールとネットワークトラフィックの送信に通常使用されているネットワークポートのリストが表示されます。ネットワークポートのリストは、Kaspersky Endpoint Security パッケージに含まれています。

6. ネットワークポートのリストをエクスポートするには：

   a. ネットワークポートのリストで、エクスポートするポートを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

      ポートが何も選択されていない場合、すべてのポートがエクスポートされます。

   b. ［**エクスポート**］をクリックします。

   c. 表示されたウィンドウで、ネットワークポートのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

      Kaspersky Endpoint Security は、ネットワークポートのリスト全体を XML ファイルにエクスポートします。

7. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをエクスポートするには：

   a. ［**選択したアプリケーションのすべてのポートを監視する**］チェックボックスをオンにします。

   b. アプリケーションのリストで、エクスポートするアプリケーションを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

      アプリケーションが何も選択されていない場合、すべてのアプリケーションがエクスポートされます。

   c. ［**エクスポート**］をクリックします。

   d. 表示されたウィンドウで、アプリケーションをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

e. ファイルを保存します。

Kaspersky Endpoint Security は、アプリケーションのリスト全体を XML ファイルにエクスポートします。

8. ネットワークポートのリストをインポートするには：

a. ネットワークポートのリストで、［**インポート**］をクリックします。

表示されたウィンドウで、ネットワークポートのリストをインポートする XML ファイルを選択します。

b. ファイルを開きます。

コンピューターにネットワークポートのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

9. Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストをインポートするには：

a. アプリケーションのリストで、［**インポート**］をクリックします。

表示されたウィンドウで、アプリケーションのリストをインポートする XML ファイルを選択します。

b. ファイルを開きます。

コンピューターにアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

10. 変更内容を保存します。

Windows イベントログ監視

このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

バージョン 11.11.0 から、Kaspersky Endpoint Security for Windows には Windows イベントログ監視コンポーネントが含まれるようになりました。Windows イベントログ監視は Windows イベントログの分析に基づいて保護対象環境の整合性を監視します。通常と異なるふるまいを検知した場合、本製品は管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。

Kaspersky Endpoint Security はルールに従って Windows イベントログを分析して違反を検出します。コンポーネントには事前定義済みのルールが含まれます。事前定義済みのルールはヒューリスティック分析によって動作します。独自のルールを追加することもできます（カスタムルール）。ルールが適用されると、本製品は緊急ステータスのイベントを作成します（下図を参照）。

Windows イベントログ監視を使用する場合、監査ポリシーのセキュリティが設定されており、システムが関連するイベントを記録していることを確認してください（詳細については、Microsoft のテクニカルサポートの Web サイトを参照してください）。



Windows イベントログ監視の通知

事前定義済みのルールの設定

事前定義済みのルールには、保護対象コンピューター上における正常でない活動のテンプレートが含まれます。正常でない活動は、攻撃の可能性を示している場合があります。事前定義済みのルールはヒューリスティック分析によって動作します。Windows イベントログ監視には 7 つの事前定義済みのルールが使用できます。いずれのルールを有効または無効にすることができます。事前定義済みのルールを削除することはできません。

次の操作に対するイベントの監視ルールの適用条件を設定できます：

- パスワードのブルートフォース攻撃の検知
- ネットワークログオンの検知

管理コンソール（MMC）で事前定義済みのルールを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**Windows イベントログ監視**］の順に選択します。
4. ［**Windows イベントログ監視**］がオンになっていることを確認してください。
5. ［**事前定義済みのルール**］ブロックの［**設定**］をクリックします。
6. チェックボックスをオンまたはオフにして、事前定義済みのルールを設定します：
   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**

- **Windows イベントログの悪用の可能性を示すパターンがあります**
- **新しくインストールしたサービスに通常と異なる活動が検出されました**
- **明示的な資格情報を使用した通常と異なるログオンが検出されました**
- **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**
- **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**

7. 必要に応じて、［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］ルールを設定します：

   a. ルールの下で［**設定**］をクリックします。

   b. 表示されるウィンドウで、ルールが適用されるパスワードの入力試行の回数と期間を指定します。

   c. ［**OK**］をクリックします。

8. ［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］ルールを選択した場合、設定を構成する必要があります：

   a. ルールの下で［**設定**］をクリックします。

   b. ［**ネットワークログオンの検知**］ブロックで、間隔の開始および終了時間を指定します。

   Kaspersky Endpoint Security はこの定義された間隔で実行されたログオン試行回数を正常でない活動と認識します。

   既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。

   c. 信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）のリストを作成します。

   ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。Kaspersky Endpoint Security はこれらのユーザーおよびコンピューターのログオン試行を監視しません。

   d. ［**OK**］をクリックします。

9. 変更内容を保存します。

Web コンソールと Cloud コンソールで事前定義済みのルールを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**Windows イベントログ監視**］に移動します。
5. ［**Windows イベントログ監視は有効です**］がオンになっていることを確認してください。

6. ［**事前定義済みのルール**］ブロックで、トグルスイッチを使用して事前定義済みのルールをオンまたはオフにします：

   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**
   - **Windows イベントログの悪用の可能性を示すパターンがあります**
   - **新しくインストールしたサービスに通常と異なる活動が検出されました**
   - **明示的な資格情報を使用した通常と異なるログオンが検出されました**
   - **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**

   a. **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**

7. 必要に応じて、［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］ルールを設定します：

   a. ルールの下の［**設定**］をクリックします。

   b. 表示されるウィンドウで、ルールが適用されるパスワードの入力試行の回数と期間を指定します。

   c. ［**OK**］をクリックします。

8. ［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］ルールを選択した場合、設定を構成する必要があります：

   a. ルールの下の［**設定**］をクリックします。

   b. ［**ネットワークログオンの検知**］ブロックで、間隔の開始および終了時間を指定します。

      Kaspersky Endpoint Security はこの定義された間隔で実行されたログオン試行回数を正常でない活動と認識します。

      既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。

   c. ［**除外リスト**］ブロックで、信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）を追加します。

      ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。Kaspersky Endpoint Security はこれらのユーザーおよびコンピューターのログオン試行を監視しません。

   d. ［**OK**］をクリックします。

9. 変更内容を保存します。

製品インターフェイスで事前定義済みのルールを設定する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**Windows イベントログ監視**］を選択します。
3. ［**Windows イベントログ監視**］がオンになっていることを確認してください。
4. ［**事前定義済みのルール**］ブロックの［**設定**］をクリックします。
5. チェックボックスをオンまたはオフにして、事前定義済みのルールを設定します：
   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**
   - **Windows イベントログの悪用の可能性を示すパターンがあります**
   - **新しくインストールしたサービスに通常と異なる活動が検出されました**
   - **明示的な資格情報を使用した通常と異なるログオンが検出されました**
   - **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**

   a. **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**
6. 必要に応じて、［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］ルールを設定します：
   a. ルールの下の［**設定**］をクリックします。
   b. 表示されるウィンドウで、ルールが適用されるパスワードの入力試行の回数と期間を指定します。
7. ［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］ルールを選択した場合、設定を構成する必要があります：
   a. ルールの下の［**設定**］をクリックします。
   b. ［**ネットワークログオンの検知**］ブロックで、間隔の開始および終了時間を指定します。

      Kaspersky Endpoint Security はこの定義された間隔で実行されたログオン試行回数を正常でない活動と認識します。

      既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。
   c. ［**除外リスト**］ブロックで、信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）を追加します。

      ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。Kaspersky Endpoint Security はこれらのユーザーおよびコンピューターのログオン試行を監視しません。
8. 変更内容を保存します。

この結果、ルールがトリガーされると、Kaspersky Endpoint Security は緊急イベントイベントを作成します。

カスタムルールの追加

Windows イベントログ監視のルールトリガー条件を独自に設定することができます。そのためには、イベント ID を入力してイベントソースを選択する必要があります。イベント ID は Microsoft のテクニカルサポートの Web サイト で検索できます。［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。また、サードパーティ製のアプリケーションのログを指定することもできます。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（*Windows PowerShell* ログなど）に保存されています。

本製品は、指定されたログが実際に Windows イベントログ内に存在するかどうかは確認しません。ログの名前に誤りがあった場合は、そのログからのイベントは監視されません。

カスタムルールのリストには、カスペルスキーのエキスパートにより作成された 3 つのルールが含まれています。

管理コンソール（MMC）でカスタムルールを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**Windows イベントログ監視**］の順に選択します。
4. ［**Windows イベントログ監視**］がオンになっていることを確認してください。
5. ［**カスタムルール**］ブロックの［**設定**］をクリックします。
6. 表示されたウィンドウで、有効にするカスタムルールの隣にあるチェックボックスをオンにします。
7. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。
8. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：
   - **ルール名**
   - **ログの名前**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。
   - **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（*Windows PowerShell* ログなど）に保存されています。
   - **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイト で検索できます。
9. 変更内容を保存します。

Web コンソールと Cloud コンソールでカスタムルールを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**Windows イベントログ監視**］に移動します。
5. ［**Windows イベントログ監視は有効です**］がオンになっていることを確認してください。
6. ［**カスタムルール**］ブロックで、編集するカスタムルールを選択します。
7. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。
8. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：
   - **ルール名**
   - **カスタムログ名**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。
   - **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（*Windows PowerShell* ログなど）に保存されています。
   - **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイト で検索できます。
9. 変更内容を保存します。

製品インターフェイスでカスタムルールを追加する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**Windows イベントログ監視**］を選択します。
3. ［**Windows イベントログ監視**］がオンになっていることを確認してください。
4. ［**カスタムルール**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、有効にするカスタムルールの隣にあるチェックボックスをオンにします。
6. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。
7. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：
   - **ルール名**
   - **ログの名前**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。

- **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（*Windows PowerShell* ログなど）に保存されています。

- **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイト で検索できます。

8. 変更内容を保存します。

この結果、ルールがトリガーされると、Kaspersky Endpoint Security は緊急イベントを作成します。

システム変更監視

このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

バージョン 12.6 から、Kaspersky Endpoint Security for Windows には、ファイル変更監視コンポーネント の代わりにシステム変更監視コンポーネントが含まれるようになりました。システム変更監視コンポーネントには、ファイル変更監視のすべての機能が含まれており、さらにレジストリの変更や外部デバイスの接続を監視することもできます。

システム変更監視コンポーネントは、コンピューターのセキュリティ侵害を示す可能性のあるオペレーティングシステムの変更を監視します。そのような変更を検知すると、Kaspersky Endpoint Security は対応するイベントを生成し、管理者に警告します。システム変更監視はリアルタイムモードで動作しますが、オンデマンドでシステム変更チェックを実行することもできます。

リアルタイムシステム変更監視

リアルタイムモードで、システム変更監視は、コンポーネントの範囲（*監視範囲*）に含めたオブジェクトへの変更を追跡します。システム変更監視では、このようなオブジェクトへの不正アクセスをリアルタイムでブロックすることもできます。

オンデマンドのシステム変更チェック

オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。*システム変更チェック*タスクを実行するには、コンポーネントの範囲（*監視範囲*）を設定して、ベースラインを作成します。ベースラインとは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。

ファイル変更監視の設定の移行

Kaspersky Endpoint Security をバージョン 12.6 にアップデートすると、ファイル変更監視の設定が自動的に移行されます。移行の一環として、監視ルールがシステム変更監視に移動されます。ファイル変更監視ルールは、KSWS から KES への移行時にもシステム変更監視に移行されます。

システム変更監視を正しく動作させるには、Kaspersky Endpoint Security のアプリケーションと管理プラグインをバージョン 12.6 にアップデートする必要があります。以前のバージョンの管理プラグインがインストールされている場合は、管理プラグインに［**システム変更監視**］ セクションがないため、システム変更監視を設定することができません。

システム変更監視ルールについて

システム変更監視が機能するには、ルールを少なくとも 1 つ追加する必要があります。*システム変更監視ルール*とは、ファイルおよびレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された*監視範囲*内のファイルとレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の 1 つです。

システム変更監視では、次のオブジェクトを監視できます：

- ファイル
- レジストリ
- 外部デバイス

ファイル監視に関する特別な考慮事項

システム変更監視は、ファイルとフォルダーの変更、および監視範囲に追加されるファイルや監視範囲から削除されるファイルについて監視します。これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。管理者のみがアクセス可能なオブジェクトや、めったに変更されないオブジェクトを追加することを推奨します。これにより、システム変更監視イベントの数を減らすことができます。

システム変更監視では、サーバーの共有フォルダー内のファイルへの変更は監視されません。システム変更監視はローカルでのみ使用できます。

Kaspersky Endpoint Security は、リアルタイムシステム変更監視が動作を開始したときに接続されていたディスク上のファイルとフォルダーの変更のみを監視します。リアルタイムシステム変更監視が動作を開始したときにディスクが接続されていなかった場合、監視範囲にファイルとフォルダーが追加されても、本製品はそのディスク上のファイルとフォルダーの変更を監視しません。

レジストリ監視に関する特別な考慮事項

システム変更監視はレジストリを監視します。これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。

システム変更監視は、レジストリの次のルートキーを監視します：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG（リアルタイムシステム変更監視でのみ使用可能です）
- HKEY_CURRENT_USER（リアルタイムシステム変更監視でのみ使用可能です）

> *システム変更チェック*タスクでは、HKEY_CURRENT_USER キーはサポートされていません。
> HKEY_USERS の下に、HKEY_USERS\<user profile ID>\<key> という形式でキーを指定できます。

外部デバイスの監視に関する特別な考慮事項

システム変更監視は、外部デバイスの接続と接続解除を監視します。これは、それらのデバイスとのファイル交換によって生じる可能性のあるセキュリティ上の脅威からコンピューターを保護するために必要となります。システム変更監視では、外部デバイスへのアクセスを監視せず、ファイル交換もブロックしません。別のアプリケーションコンポーネントのデバイスコントロールを使用してデバイスへのアクセスを設定することができます。

> *ベースラインシステム変更監視*タスクの実行中、外部デバイスがオペレーティングシステムで同じドライブ文字を持つ場合、本製品は外部デバイスの再接続を無視します。ログに記録するには、再接続されるデバイスのドライブ文字が異なっている必要があります。

システム変更監視は、次の種別の外部デバイスの接続を監視します：

- リムーバブルドライブ（USB フラッシュドライブを含む）
- ハードディスク
- 外部ネットワークアダプター

- CD/DVD/Blu-ray ドライブ
- スキャナーとカメラ

リアルタイムシステム変更監視

システム変更監視により、オペレーティングシステムの変更をリアルタイムで追跡できます。コンピューターでのセキュリティ侵害を示す可能性がある変更を追跡することが可能です。このコンポーネントを使用すると、これらの変更をブロックすることも、変更イベントをただログ記録することもできます。

システム変更監視が機能するには、ルールを少なくとも1つ追加する必要があります。*システム変更監視ルール*とは、ファイルおよびレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された*監視範囲*内のファイルとレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の1つです。

リアルタイムシステム変更監視モード

システム変更監視ルールにより、オペレーティングシステムやその他のサービスの機能にとって重要なリソースに対する操作がブロックされないようにするには、テストモードを有効化し、コンポーネントがシステムに与える影響について分析することを推奨します。テストモードをオンにすると、Kaspersky Endpoint Security はルールで禁止されているユーザー動作をブロックせず、代わりに*警告* ⚠イベントを生成します。

リアルタイムシステム変更監視コンポーネントには、次の 2 つのモードがあります：

- ブロックする

  このモードで、システム変更監視はシステムの変更を追跡し、ルールに従って操作を実行します：**許可**または**ブロック**。システム変更監視はまた、対応するイベントを生成し、Kaspersky Security Center コンソールでデバイスのステータスを変更します。

- 通知する

  このモードで、システム変更監視は、監視範囲内のファイルとレジストリキーに対する操作を許可します。ファイルやレジストリに対する操作が禁止されている場合、本製品は次のイベントを生成します：*テストモードで禁止された操作が許可されました*。ルールがシステムにどのような影響を与えるかを分析するには、レポートを確認できます。

リアルタイムシステム変更監視の有効化

管理コンソール（MMC）でリアルタイムシステム変更監視を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. ［**システム変更監視**］チェックボックスをオンにします。

5. ［**ブロックルールの操作モード**］の下で、リアルタイムシステム変更監視のモードを選択します。

   - **ブロックする**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成します。
   - **通知する**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作を許可し、対応するイベントを生成します。

6. ［**リアルタイムシステム変更監視**］ブロックで、［**リアルタイムシステム変更監視**］をオンにします。

7. 外部デバイスの監視を設定します：

   a. ［**デバイスを監視する**］チェックボックスをオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

システム変更監視は、外部デバイスの現在の接続を記録します。アプリケーション設定でコンポーネントを有効にすると、外部デバイスの接続と接続解除の監視が開始されます。その後、外部デバイスが接続または接続解除されると、対応するイベントが生成されます。

8. ファイルとレジストリの監視を設定します：

   a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。

   b. ［**設定**］をクリックします。

   これで、システム変更チェックルールのリストが開きます。

   c. ［**追加**］をクリックします。

   また、**別のソースからルールをインポートする**こともできます。

   システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

> システム変更監視では、*システム変更チェックタスクへの* `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。

4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

      2. ［**エクスポート**］リンクをクリックします。

      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

      4. ファイルを保存します。

         Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

   c. リアルタイムシステム変更監視ルールのリストをインポートするには：

      1. ［**インポート**］リンクをクリックします。

         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

5. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**設定**］をクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

      2. ［**エクスポート**］リンクをクリックします。

      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

      4. ファイルを保存します。

   Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

d. システム変更チェックルールのリストをインポートするには：

1. ［**インポート**］リンクをクリックします。
   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
2. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。
5. ［**Windows**］タブを選択します。
6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：
   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。
   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。
      2. → ［**エクスポート**］を選択します。
         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。
   c. リアルタイムシステム変更監視ルールのリストをインポートするには：
      1. → ［**インポート**］を選択します。
         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。
7. *システム変更チェック*のルールをエクスポートまたはインポートするには：
   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。
   b. ［**ルール**］リンクをクリックします。

c. システム変更チェックルールのリストをエクスポートするには：

1. エクスポートするルールを選択します。

2. → ［**エクスポート**］を選択します。

   Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

d. システム変更チェックルールのリストをインポートするには：

1. → ［**インポート**］を選択します。

   表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

2. ファイルを開きます。

   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

d. システム変更監視のルールを設定します（下の表を参照）。

9. 変更内容を保存します。

Web コンソールでリアルタイムシステム変更監視を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。

5. ［**システム変更監視は有効です**］をオンにします。

6. ［**Windows**］タブを選択します。

7. ［**リアルタイムシステム変更監視**］の下で、リアルタイムシステム変更監視のモードを選択します。

   - **ルールを適用**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成します。

   - **ルールをテスト運用（通知）**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作を許可し、対応するイベントを生成します。

8. ファイルとレジストリの監視を設定します：

   a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。

   b. ［**ルール**］をクリックします。

   これで、システム変更チェックルールのリストが開きます。

c. ［**追加**］をクリックします。

また、**別のソースからルールをインポートする**こともできます。

システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

システム変更監視では、*システム変更チェック*タスクへの HKEY_CURRENT_USER および HKEY_CURRENT_CONFIG のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：
   a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。
   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。
         Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
   c. リアルタイムシステム変更監視ルールのリストをインポートするには：
      1. ［**インポート**］リンクをクリックします。
         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

5. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**設定**］をクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

      2. ［**エクスポート**］リンクをクリックします。

      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

      4. ファイルを保存します。

      Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. ［**インポート**］リンクをクリックします。

         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

      2. ファイルを開きます。

      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。

5. ［**Windows**］タブを選択します。

6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   c. リアルタイムシステム変更監視ルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

d. システム変更監視のルールを設定します（下の表を参照）。

9. 外部デバイスの監視を設定します：

   a. ［**デバイスを監視する**］チェックボックスをオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

   システム変更監視は、外部デバイスの現在の接続を記録します。アプリケーション設定でコンポーネントを有効にすると、外部デバイスの接続と接続解除の監視が開始されます。その後、外部デバイスが接続または接続解除されると、対応するイベントが生成されます。

10. 変更内容を保存します。

本製品のインターフェイスでリアルタイムシステム変更監視を有効にする方法

1. メインウィンドウで、をクリックします。

2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］を選択します。

3. ［**システム変更監視**］をオンにします。

4. ［**ブロックルールの操作モード**］の下で、リアルタイムシステム変更監視のモードを選択します。

   - **ブロックする**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成します。

   - **通知する**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作を許可し、対応するイベントを生成します。

5. ［**リアルタイムシステム変更監視**］ブロックで、［**リアルタイムシステム変更監視**］をオンにします。

6. 外部デバイスの監視を設定します：

   a. ［**デバイスを監視する**］チェックボックスをオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

   システム変更監視は、外部デバイスの現在の接続を記録します。アプリケーション設定でコンポーネントを有効にすると、外部デバイスの接続と接続解除の監視が開始されます。その後、外部デバイスが接続または接続解除されると、対応するイベントが生成されます。

7. ファイルとレジストリの監視を設定します：

   a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。

   b. ［**設定**］をクリックします。

   これで、システム変更チェックルールのリストが開きます。

   c. ［**追加**］をクリックします。

   また、**別のソースからルールをインポートする**こともできます。

システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

システム変更監視では、*システム変更チェック*タスクへの HKEY_CURRENT_USER および HKEY_CURRENT_CONFIG のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：
   a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。
   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。
         Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
   c. リアルタイムシステム変更監視ルールのリストをインポートするには：
      1. ［**インポート**］リンクをクリックします。
         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
5. *システム変更チェック*のルールをエクスポートまたはインポートするには：
   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。
   b. ［**設定**］をクリックします。

c. システム変更チェックルールのリストをエクスポートするには：

1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

   ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

2. ［**エクスポート**］リンクをクリックします。

3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

4. ファイルを保存します。

Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

d. システム変更チェックルールのリストをインポートするには：

1. ［**インポート**］リンクをクリックします。

   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

2. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。

5. ［**Windows**］タブを選択します。

6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

   1. エクスポートするルールを選択します。

   2. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

c. リアルタイムシステム変更監視ルールのリストをインポートするには：

1. → ［**インポート**］を選択します。

   表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

2. ファイルを開きます。

   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

   1. エクスポートするルールを選択します。

   2. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

   1. → ［**インポート**］を選択します。

      表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

   2. ファイルを開きます。

      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

8. システム変更監視のルールを設定します（下の表を参照）。

9. 変更内容を保存します。

リアルタイムシステム変更監視ルールの設定

パラメータ	説明
ルール名	リアルタイムシステム変更監視ルールの名前
レジストリによる操作	• **許可**：システム変更監視は、監視範囲内のファイルとレジストリキーに対する操作を許可します。 • **ブロック**：システム変更監視の挙動は、選択したモードによって異なります。*システム保護モード*を選択した場合、システム変更監視は、監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成して、Kaspersky Security Center コンソールでデバイスのステータスを変更します。*テストモード*を選択した場合、システム変更監視は、監視範囲内のファイルやレジストリキーに対する操作を許可します。

パラメータ	説明
イベントの深刻度	Kaspersky Endpoint Security は、監視範囲内のファイルまたはレジストリキーが変更された場合にファイル変更イベントを記録します。*情報*、*警告*、*緊急* のイベントセキュリティレベルが利用可能です。
監視範囲	• **ファイル**：コンポーネントによって監視されるファイルとフォルダーのリスト。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 マスクを使用する • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 • **レジストリ**：コンポーネントによって監視されるレジストリキーと値のリスト。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
除外リスト	• **ファイル**：監視範囲からの除外リストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。例：「`C:\Folder\Application\*.log`」。除外項目は監視範囲項目よりも優先されます。 マスクを使用する • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 • **レジストリ**：監視範囲からの除外リストです。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。除外項目は監視範囲項目よりも優先されます。
信頼するユーザーまたはユーザーグループ	*信頼済みユーザー*とは、監視範囲内のファイルとレジストリキーに対して操作を実行することが許可されたユーザーです。Kaspersky Endpoint Security が信頼済みユーザーによる操作を検知すると、システム変更監視は*情報*イベントを生成します。 ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。
ファイル操作マーカー / 監視対象の操作	本製品が監視するファイルまたはレジストリキーに対する操作を特徴付けるマーカー。
ハッシュ	編集時にファイルのハッシュを計算します。Kaspersky Endpoint Security は、イベントが生成されるとファイルのハッシュに関する情報を追加します。

オンデマンドのシステム変更チェック

オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。*システム変更チェック*タスクの実行中、本製品は監視範囲に含まれるオブジェクトの現在の状態をベースラインの状態と比較します。リアルタイムシステム変更監視とは対照的に、*システム変更チェック*タスクは、イベントの数を制限し、オペレーティングシステムの変更に関する全体的なレポートを生成するのに役立ちます。

システム変更監視が機能するには、ルールを少なくとも1つ追加する必要があります。*システム変更監視ルール*とは、ファイルおよびレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された*監視範囲*内のファイルとレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の1つです。リアルタイムシステム変更監視と*システム変更チェック*タスクによって共有されるルールを設定するか、タスク用に個別のルールを作成することができます。ベースラインを作成するために、Kaspersky Endpoint Security は*システム変更チェック*タスクの監視範囲を*ベースラインアップデート*タスクに適用します。

ベースラインの作成と更新

*システム変更チェック*タスクが機能するにはベースラインが必要です。*ベースライン*とは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。システムの現在の状態がベースラインに記録されたシステムの状態と異なる場合、Kaspersky Endpoint Security は対応するイベントを生成します。ベースラインは、*ベースラインアップデート*タスクを使用して作成または更新できます。

ベースラインは次のいずれかのモードで更新できます：

- 完全アップデート
  監視範囲内のすべてのオブジェクトを更新します。
- 増分アップデート
  変更されたオブジェクトまたは新規オブジェクトのみを検知して更新します。

管理コンソール（MMC）でベースラインを作成または更新する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**ベースラインアップデート**］の順に選択します。

ステップ2：ベースラインアップデートモードの選択

次のベースラインアップデートモードを選択します：

- **完全アップデート**：監視範囲内のすべてのオブジェクトを更新します。
- **増分アップデート**：変更されたオブジェクトまたは新規オブジェクトのみを検知して更新します。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスク名の定義

「ベースライン *2024*」などのタスクの名前を入力します。

ステップ 5：タスク作成の完了

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

Web コンソールでベースラインを作成または更新する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**ベースラインアップデート**］を選択します。
   c. ［**タスク名**］に「ベースライン *2024*」などの短く分かりやすい名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。
6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。

7. 新しいタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. 次のベースラインアップデートモードを選択します：
   - **完全アップデート**：監視範囲内のすべてのオブジェクトを更新します。
   - **増分アップデート**：変更されたオブジェクトまたは新規オブジェクトのみを検知して更新します。
10. 変更内容を保存します。
11. タスクの横にあるチェックボックスをオンにします。
12. ［**開始**］をクリックします。

システム変更チェックタスク用の監視範囲の設定

既定で、*システム変更チェック*タスクの監視範囲とは、リアルタイムシステム変更監視の監視範囲と同じです。このタスクに対して異なる監視範囲を設定できます。

システム変更監視では、*システム変更チェック*タスクへの `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でシステム変更チェックタスク用に異なる監視範囲を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. ［**システム変更監視**］チェックボックスをオンにします。
5. ［**システム変更チェック**］の下で、タスク設定モード：**カスタム**を選択します。
6. 外部デバイスの監視を設定します：
   a. ［**デバイスを監視する**］チェックボックスをオンにします。
   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報* ⓘ、*警告* ⚠、*緊急* ⓘ。

システム変更監視は、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。*システム変更チェック*タスクの実行中、外部デバイスの接続解除は監視されません。

7. ファイルとレジストリの監視を設定します：

a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。

b. ［**設定**］をクリックします。

これで、システム変更チェックルールのリストが開きます。

c. ［**追加**］をクリックします。

また、**別のソースからルールをインポートする**こともできます。

システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

システム変更監視では、*システム変更チェック*タスクへの `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。

b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

2. ［**エクスポート**］リンクをクリックします。
3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
4. ファイルを保存します。

Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

c. リアルタイムシステム変更監視ルールのリストをインポートするには：

1. ［**インポート**］リンクをクリックします。

表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

2. ファイルを開きます。

   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

5. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**設定**］をクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

      2. ［**エクスポート**］リンクをクリックします。

      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

      4. ファイルを保存します。

      Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. ［**インポート**］リンクをクリックします。

         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

      2. ファイルを開きます。

      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。

5. ［**Windows**］タブを選択します。

6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   c. リアルタイムシステム変更監視ルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

d. システム変更監視のルールを設定します（下の表を参照）。

8. 変更内容を保存します。

Web コンソールでシステム変更チェックタスク用に異なる監視範囲を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。
5. ［**Windows**］タブを選択します。
6. ［**システム変更監視は有効です**］をオンにします。
7. ［**システム変更チェック**］の下で、タスク設定モード：**カスタム**を選択します。
8. 外部デバイスの監視を設定します：
   a. ［**デバイスを監視する**］チェックボックスをオンにします。
   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

   システム変更監視は、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。*システム変更チェック*タスクの実行中、外部デバイスの接続解除は監視されません。
9. ファイルとレジストリの監視を設定します：
   a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。
   b. ［**ルール**］をクリックします。
      これで、システム変更チェックルールのリストが開きます。
   c. ［**追加**］をクリックします。
      また、**別のソースからルールをインポートする**こともできます。

      システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

      システム変更監視では、*システム変更チェック*タスクへの `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：
   a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。
   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。
         Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
   c. リアルタイムシステム変更監視ルールのリストをインポートするには：
      1. ［**インポート**］リンクをクリックします。
         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
5. *システム変更チェック*のルールをエクスポートまたはインポートするには：
   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。
   b. ［**設定**］をクリックします。
   c. システム変更チェックルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。

Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

d. システム変更チェックルールのリストをインポートするには：

1. ［**インポート**］リンクをクリックします。
   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
2. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。
5. ［**Windows**］タブを選択します。
6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。
      2. → ［**エクスポート**］を選択します。
         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   c. リアルタイムシステム変更監視ルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。
         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

d. システム変更監視のルールを設定します（下の表を参照）。

10. 変更内容を保存します。

アプリケーションインターフェイスでシステム変更チェックタスク用に異なる監視範囲を設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］を選択します。
3. ［**システム変更監視**］をオンにします。
4. ［**システム変更チェック**］の下で、タスク設定モード：**カスタム**を選択します。
5. 外部デバイスの監視を設定します：

   a. ［**デバイスを監視する**］チェックボックスをオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報* ⓘ、*警告* ⚠、*緊急* ❗。

システム変更監視は、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。*システム変更チェック*タスクの実行中、外部デバイスの接続解除は監視されません。

6. ファイルとレジストリの監視を設定します：

   a. ［**ファイルとレジストリを監視する**］チェックボックスをオンにします。

   b. ［**設定**］をクリックします。

      これで、システム変更チェックルールのリストが開きます。

   c. ［**追加**］をクリックします。

      また、**別のソースからルールをインポートする**こともできます。

      システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

      システム変更監視では、*システム変更チェック*タスクへの `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

      管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

      1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

      2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

      3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。

      4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

         a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。

         b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

            1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

               ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

            2. ［**エクスポート**］リンクをクリックします。

            3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

            4. ファイルを保存します。

               Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

         c. リアルタイムシステム変更監視ルールのリストをインポートするには：

            1. ［**インポート**］リンクをクリックします。

               表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

2. ファイルを開きます。

   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

5. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**設定**］をクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

      2. ［**エクスポート**］リンクをクリックします。

      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

      4. ファイルを保存します。

      Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. ［**インポート**］リンクをクリックします。

         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

      2. ファイルを開きます。

      コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。

5. ［**Windows**］タブを選択します。

6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

   a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   c. リアルタイムシステム変更監視ルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. *システム変更チェック*のルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

d. システム変更監視のルールを設定します（下の表を参照）。

7. 変更内容を保存します。

パラメータ	説明
ルール名	*システム変更チェックタスクルール*の名前。
イベントの深刻度	Kaspersky Endpoint Security は、監視範囲内のファイルまたはレジストリキーが変更された場合にファイル変更イベントを記録します。*情報*、*警告*、*緊急* のイベントセキュリティレベルが利用可能です。
監視範囲	• **ファイル**：コンポーネントによって監視されるファイルとフォルダーのリスト。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 マスクを使用する • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 • **レジストリ**：コンポーネントによって監視されるレジストリキーと値のリスト。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
除外リスト	• **ファイル**：監視範囲からの除外リストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。例：「`C:\Folder\Application\*.log`」。除外項目は監視範囲項目よりも優先されます。 マスクを使用する • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 • **レジストリ**：監視範囲からの除外リストです。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。除外項目は監視範囲項目よりも優先されます。

システム変更チェックタスクの実行

*システム変更チェックタスク*により、ファイルやレジストリキーの変更を確認したり、外部デバイスの接続を確認したりできます。ファイルの変更を確認するには、*システム変更チェックタスク*を次のいずれかのモードで実行します：

- 簡易スキャン

  ファイルの変更をチェックする際にファイル属性のみをチェックします。ファイルの内容はチェックしません。

- 完全スキャン

  ファイルの変更をチェックする際にすべてのファイル属性とファイルの内容をチェックします。

タスクの実行モードは、レジストリまたは外部デバイスのチェックには影響しません。

管理コンソール（MMC）でシステム変更チェックタスクを実行する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
3. ［**新規タスク**］をクリックします。
   タスクウィザードが起動します。ウィザードの指示に従います。
4. ［**Kaspersky Endpoint Security**］→［**ベースラインシステム変更監視**］の順に選択します。システム変更監視モードを選択します：
   - **完全スキャン**：このモードでは、本製品はファイルのすべての属性とハッシュをチェックします。
   - **簡易スキャン**：このモードでは、本製品はファイルの属性のみをチェックします。
5. タスクを実行するコンピューターを選択します。次の設定方法があります：
   - 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
   - デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。
   - タスクを実行するデバイスの抽出を指定します。
   - 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
6. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。
7. タスクを開始するスケジュールを設定します（手動や、特定の曜日など）。
8. タスクの名前を入力します。
9. ウィザードを終了します。必要に応じて、［**ウィザードの終了後にタスクを実行**］をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

Web コンソールでシステム変更チェックタスクを実行する方法

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

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］から［**システム変更チェック**］を選択します。

   c. ［**タスク名**］に「*週次のシステム変更チェック*」などの短く分かりやすい名前を付けます。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。

5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。

6. ウィザードを終了します。

   タスクのリストに新しいタスクが表示されます。

7. 新しいタスクをクリックします。

   タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. システム変更チェックモードを選択します：

   - **簡易スキャン**：ファイル属性のみをチェックします。ファイルの内容はチェックしません。
   - **完全スキャン**：ファイルの内容だけでなく、すべての属性もチェックします。

10. 変更内容を保存します。

11. タスクの横にあるチェックボックスをオンにします。

12. ［**開始**］をクリックします。

*システム変更チェック*タスクが正常に完了するためには、*システム変更チェック*タスクの監視範囲がベースラインと完全に一致する必要があります。監視範囲が異なる場合、タスクはエラーで終了します。監視範囲を同期するには、*ベースラインアップデート*タスクを新しい監視範囲で実行します。

システム変更監視ルールのエクスポートとインポート

システム変更監視ルールを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の記録をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、システム変更監視ルールのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

システム変更監視では、*システム変更チェック*タスクへの `HKEY_CURRENT_USER` および `HKEY_CURRENT_CONFIG` のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

管理コンソール（MMC）でリシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**セキュリティコントロール**］→［**システム変更監視**］の順に選択します。
4. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：
   a. ［**リアルタイムシステム変更監視**］ブロックの［**設定**］をクリックします。
   b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。
         Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。
   c. リアルタイムシステム変更監視ルールのリストをインポートするには：
      1. ［**インポート**］リンクをクリックします。
         表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
      2. ファイルを開きます。
         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
5. *システム変更チェック*のルールをエクスポートまたはインポートするには：
   a. ［**システム変更チェック**］ブロックで、［**カスタム**］を選択します。
   b. ［**設定**］をクリックします。
   c. システム変更チェックルールのリストをエクスポートするには：
      1. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
         ルールが何も選択されていない場合、すべてのルールがエクスポートされます。
      2. ［**エクスポート**］リンクをクリックします。
      3. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。
      4. ファイルを保存します。

Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

d. システム変更チェックルールのリストをインポートするには：

1. ［**インポート**］リンクをクリックします。
   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
2. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

Web コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**セキュリティコントロール**］→［**システム変更監視**］に移動します。
5. ［**Windows**］タブを選択します。
6. *リアルタイムシステム変更監視*のルールをエクスポートまたはインポートするには：

a. ［**リアルタイムシステム変更監視**］セクションで、［**ルール**］をクリックします。

b. リアルタイムシステム変更監視ルールのリストをエクスポートするには：

1. エクスポートするルールを選択します。
2. → ［**エクスポート**］を選択します。
   Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

c. リアルタイムシステム変更監視ルールのリストをインポートするには：

1. → ［**インポート**］を選択します。
   表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。
2. ファイルを開きます。
   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

7. システム変更チェックのルールをエクスポートまたはインポートするには：

   a. ［**オンデマンドのシステム変更チェック**］ブロックで、［**カスタム**］を選択します。

   b. ［**ルール**］リンクをクリックします。

   c. システム変更チェックルールのリストをエクスポートするには：

      1. エクスポートするルールを選択します。

      2. → ［**エクスポート**］を選択します。

         Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを JSON ファイルでエクスポートします。

   d. システム変更チェックルールのリストをインポートするには：

      1. → ［**インポート**］を選択します。

         表示されたウィンドウで、信頼するアドレスのリストをインポートする JSON ファイルを選択します。

      2. ファイルを開きます。

         コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

システム変更監視レポートの表示

システム変更監視ルールのパフォーマンスを分析するには、本製品で生成されたレポートとイベントを確認できます。Kaspersky Endpoint Security は、コンポーネントに関して次のレポートを生成します：

- 製品インターフェイス内：
  - システム変更監視レポート
  - システム変更チェックレポート
  - ベースラインアップデートレポート

  レポートにはシステム変更監視イベントが含まれます。
- Kaspersky Security Center コンソール内：
  - 監視ルールの適用回数が最も多いコンピューターに関するレポート
  - 適用頻度が最も高い監視ルールに関するレポート

  既定では、レポートの作成日を含む過去 30 日間のレポートが作成されます。

管理コンソール（MMC）でシステム変更監視レポートを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ステップで、システム変更監視レポート（［**その他**］セクション）を選択します：
   - **ファイル変更監視 / システム変更監視ルールの適用回数が多い 10 台のデバイス**
   - **デバイスで適用された回数が多い 10 個のファイル変更監視 / システム変更監視ルール**

   新規レポートテンプレートウィザードが完了すると、［**レポート**］タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

Web コンソールでシステム変更監視レポートを表示する方法

1. Web コンソールのメインウィンドウで、［**監視とレポート**］→［**レポート**］の順に選択します。
2. ［**追加**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。
3. ［**Template type**］の下の［**その他**］セクションで、システム変更監視レポートを選択します。
   - **ファイル変更監視 / システム変更監視ルールの適用回数が多い 10 台のデバイス**
   - **デバイスで適用された回数が多い 10 個のファイル変更監視 / システム変更監視ルール**

   新規レポートテンプレートウィザードが完了すると、テーブルに新しいレポートテンプレートが表示されます。
4. レポートを選択して実行します。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

本製品で生成されたイベントを表示するには、Kaspersky Security Center コンソールのイベント選択を使用することもできます。

システム変更ステータスのリセット

Kaspersky Security Center コンソールでコンピューターのステータスは次のいずれかになります：*OK*、*警告*、または*緊急*。システム変更監視が監視範囲内のファイルまたはレジストリキーの変更を検知すると、コンピューターのステータスは*警告*または*緊急*に変わります。システム変更監視によって割り当てられたステータスを*システム整合性ステータス*と呼びます。検知されたオブジェクトの変更がコンピューターのセキュリティに影響を与えないことが分析によって確実になった場合、システム整合性ステータスをリセットできます。

管理コンソール（MMC）でシステム整合性ステータスをリセットする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**システム変更ステータスのリセット**］の順に選択します。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：タスク開始スケジュールの設定

タスクのスケジュールを設定します（たとえば、［手動］など）。

ステップ 4：タスク名の定義

タスクの名前を入力します（例：*監視範囲の変更後のステータスのリセット*）。

ステップ 5：タスク作成の完了

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

Web コンソールでシステム整合性ステータスをリセットする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**システム変更ステータスのリセット**］を選択します。
   c. ［**タスク名**］フィールドに簡単な説明を入力します（例：*監視範囲の変更後のステータスのリセット*）。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. タスクを実行するアカウントを選択します。既定では、Kaspersky Endpoint Security はローカルユーザーアカウントの権限でタスクを開始します。
6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. タスクの横にあるチェックボックスをオンにします。
8. ［**開始**］をクリックします。

その結果、システム変更監視イベントによってコンピューターのステータスが*警告*または*緊急*に変わった場合、コンピューターのステータスは*OK*にリセットされます。コンピューターのステータスが他のイベントによっても変更された場合、コンピューターのステータスは変更されません。

Cloud Discovery

Cloud Discovery はクラウドサービスへのユーザーアクセスを管理します。クラウドサービスには、Microsoft Teams、Salesforce、Microsoft Office 365 などがあります。クラウドサービスは、*ファイル共有*、*メッセンジャー*、*メール*などのカテゴリに分類されます。カスペルスキーの専門家は、Cloud Discovery のカテゴリと、各カテゴリに分類されたクラウドサービスを定期的に更新します。Kaspersky Endpoint Security は、定義データベースを使用して、カテゴリとクラウドサービスのセットを更新します。つまり、Cloud Discovery は、クラウドサービスの分類に Kaspersky Security Network を使用しません。

Cloud Discovery は、次の機能を備えています：

- クラウドサービスの使用の監視
- クラウドサービスへのユーザーアクセスのブロック

システム要件

Cloud Discovery は次の条件が満たされた場合に使用可能です：

- 本製品が、ワークステーション用の Windows を実行しているコンピューターにインストールされている。
  このコンポーネントは、サーバーには使用できません。
- Kaspersky Security Center のバージョンが 15.1 以降である。
  このコンポーネントは、管理コンソール（MMC）では使用できません。Cloud Discovery は Kaspersky Security Center Web コンソール および Kaspersky Security Center Cloud コンソールで設定できます。
- Kaspersky Next ライセンス。

Cloud Discovery コンポーネントに必要なアプリケーション機能を有効にします：

1. **暗号化された接続をスキャン**これは HTTPS トラフィックを監視するために必要です。この機能は、［**ネットワーク設定**］セクションで管理できます。
2. **Webページと連携するためWebトラフィック内にスクリプトを埋め込む**スクリプトは Cloud Discovery のイベントの登録を有効にします。また、このスクリプトによって、クラウドサービスへのアクセスのブロック機能が完備されます。スクリプトがない場合、アクセスのブロックは、クラウドサービスのドメインによってのみ行われます。この機能は、［**ネットワーク設定**］セクションで管理できます。

［**許可対象のページの閲覧を記録する**］機能を有効にすることもできます。この機能には、ユーザーが同じドメインに属する Web サイトにアクセスした時のイベントのグループ化が含まれています。これにより、ユーザーがクラウドサービスを使用した場合、Cloud Discovery は Web サイトごとの複数のイベントをログに記録するのではなく、1 つのイベントのみをログに記録します。この機能は、［**ウェブコントロール**］セクションで管理できます。

クラウドサービスの監視

ユーザーがクラウドサービスを使用し始めると、Kaspersky Endpoint Security によってそのイベントが登録されて、レポートにエントリが作成されます。Cloud Discovery により、ブラウザーおよび対応するアプリケーションでのクラウドサービスの使用が制御されます。Cloud Discovery は、HTTP および HTTPS 経由のクラウドサービスの使用を制御します。

Cloud コンソールでクラウドサービスの監視を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**コミュニケーションと危険サイトブロック**］→［**Cloud Discovery**］に移動します。

5. ［**Cloud Discovery は有効です**］をオンにします。

6. 変更内容を保存します。

これにより、使用されるクラウドサービスに関する情報が Kaspersky Security Center に転送されます。レポートで、クラウドサービスの使用情報を確認できます。必要に応じて、クラウドサービスへのアクセスをブロックできます。

クラウドサービスへのアクセスのブロック

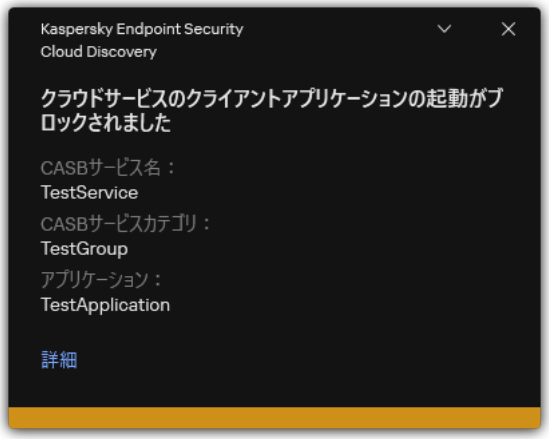
クラウドサービスへのアクセスのブロックは、Kaspersky Next EDR Optimum および XDR Expert ライセンスでのみ使用可能です。この機能は、Kaspersky Next EDR Foundations ライセンスでは利用できません。Kaspersky Next のライセンスタイプ別のアプリケーション機能の比較は、Kaspersky Next のヘルプをご覧ください。

管理者は、Cloud Discovery のカテゴリまたは個々のクラウドサービスへのユーザーアクセスを制限することができます。こうすることで、管理者は、セキュアなクラウドサービスのみを許可し、データ流出を防ぐことができます。Cloud Discovery のクラウドサービスごとに*リスクレベルの情報*が表示されます。リスクレベルは、組織のセキュリティ要件を満たさないサービスを検出するのに役立ちます。

リスクレベルは推定であり、クラウドサービスやその製造元の品質に関する情報を示すものではありません。リスクレベルは、あくまでもカスペルスキーの専門家による推奨です。

クラウドサービスのリスクレベルは、すべての制御されているクラウドサービスのリストにあるポリシーの［**Cloud Discovery**］セクションに表示されます。

その他の Kaspersky Endpoint Security コンポーネントによって、クラウドサービス使用時の脅威からの保護機能と疑わしいユーザーの活動の追跡機能が提供されます。



Cloud Discovery 通知

Kaspersky Endpoint Security よりも前に起動されたクラウドアプリケーションは、Cloud Discovery によってブロックされません。

Cloud コンソールでクラウドサービスへのアクセスをブロックする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**コミュニケーションと危険サイトブロック**］→［**Cloud Discovery**］に移動します。

5. ［**Cloud Discovery は有効です**］をオンにします。

   すべてのクラウドサービスのリストが表示されます。クラウドサービスは、*ファイル共有*、*メッセンジャー*、*メール*などのカテゴリに分類されます。カスペルスキーの専門家は、Cloud Discovery のカテゴリと、各カテゴリに分類されたクラウドサービスを定期的に更新します。Kaspersky Endpoint Security は、定義データベースを使用して、カテゴリとクラウドサービスのセットを更新します。

6. ［**アクセス**］列でトグルスイッチを使用して、クラウドサービスへのアクセスを設定します。

7. 変更内容を保存します。

これにより、ブラウザーおよび対応するアプリケーションでのクラウドサービスの使用が制御されます。

信頼ゾーン

*信頼ゾーン*は Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。

管理者は処理されるオブジェクトとコンピューターにインストールされるアプリケーションの特徴を考慮しながら、信頼ゾーンを個別に定義します。Kaspersky Endpoint Security がアクセスをブロックする特定のオブジェクトやアプリケーションが無害であることが確実なときには、オブジェクトやアプリケーションを信頼ゾーンに含めなければならない場合があります。管理者が、ユーザーが特定のコンピューターに対してローカルの信頼するゾーンを作成するよう許可することも可能です。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。

Kaspersky Endpoint Security 12.5 for Windows から、EDR テレメトリを信頼ゾーンに追加できるようになりました。これにより、アプリケーションが Kaspersky Anti Targeted Attack Platform (EDR) ソリューション向けにテレメトリの収集サーバーに送信するデータを最適化できます。

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。

信頼するオブジェクトの作成

*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。信頼するオブジェクトにより、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアを安全に使用できるようになります。悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェアについて詳しくは、カスペルスキーのウイルス百科事典を参照してください。

このようなアプリケーションは Kaspersky Endpoint Security によってブロックされる場合があります。ブロックしないようにするには、使用している製品を信頼するオブジェクトに設定できます。これを行うには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクを信頼ゾーンに追加します。たとえば、ユーザーがコンピューターのリモート管理用に Radmin アプリケーションを使用しているとします。Kaspersky Endpoint Security はこの処理を疑わしいものとみなして、ブロックする可能性があります。アプリケーションがブロックされないようにするには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクによって信頼するオブジェクトを作成します。

情報を収集し、それを処理するために送信するアプリケーションがコンピューターにインストールされていると、Kaspersky Endpoint Security がそのアプリケーションをマルウェアに分類する可能性があります。それを防ぐために、ヘルプ内で説明する方法で Kaspersky Endpoint Security を設定することで、そのアプリケーションをスキャン対象から除外できます。

システム管理者が設定した以下のコンポーネントとタスクによって信頼するオブジェクトを使用できます：

- ふるまい検知
- 脆弱性攻撃ブロック
- ホスト侵入防止
- ファイル脅威対策
- ウェブ脅威対策
- メール脅威対策
- マルウェアのスキャンタスク

スキャンタスクの開始時にこのオブジェクトを含むドライブやフォルダーがスキャン範囲に含まれている場合、オブジェクトはスキャンされません。ただし、ある特定のオブジェクトについてオブジェクトスキャンタスクが開始された場合、信頼するオブジェクトは適用されません。

信頼ゾーンは、管理コンソール（MMC）と Web コンソールで異なる方法でグループ化されます。同様に、信頼ゾーンのパラメータ変更を防止する方法も異なります（別の「南京錠」）。本製品の管理には、Web コンソールのみを使用することを推奨します。別のコンソールで信頼ゾーンを設定すると、管理プラグインによって「南京錠」が既定の状態にリセットされる場合があります。

管理コンソール（MMC）で信頼するオブジェクトを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
4. ［**信頼するオブジェクトとアプリケーション**］→［**信頼するオブジェクト**］ブロックの［**設定**］をクリックします。

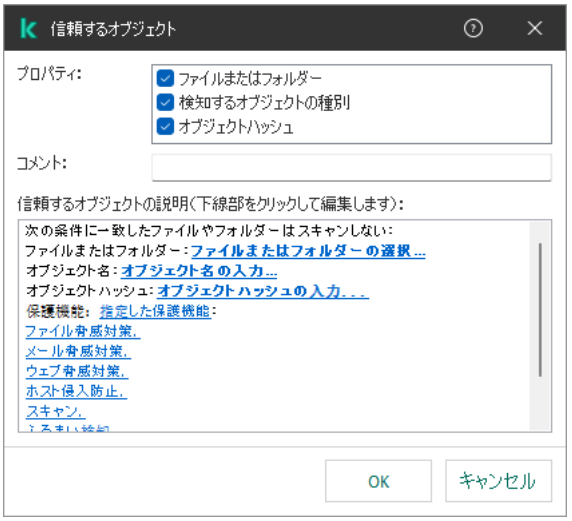
   除外リストを含むウィンドウが開きます。
5. 組織内のすべてのコンピューターの除外リストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。
6. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。

7. ［**追加**］をクリックして、処理を選択します：

- **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも1つの信頼するオブジェクトをカテゴリに追加します。
- **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。
- **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。
- **選択したカテゴリに新しい除外を追加**：新しい信頼するオブジェクトを特定のカテゴリに追加するには、カテゴリを選択します。

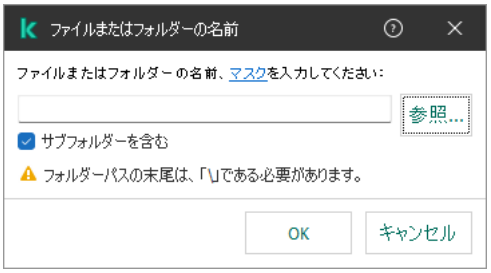
8. ファイルまたはフォルダーをスキャンから除外するには：



除外設定

a. ［**プロパティ**］ブロックで、［**ファイルまたはフォルダー**］をオンにします。

b. 下のブロックのリンクをクリックして、［**ファイルまたはフォルダーの名前**］ウィンドウを開きます。



ファイルまたはフォルダーの選択

a. ファイルまたはフォルダー名あるいはファイルまたはフォルダー名のマスクを指定するか、［**参照**］をクリックしてフォルダーツリーからファイルまたはフォルダーを選択します。

マスクを使用する

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`?:\Users\*\Folder\`」と入力できます。

Kaspersky Endpoint Security は環境変数をサポートしています。

ネットワークフォルダーを除外できます。これを行うには、ネットワークフォルダーのパスを手動で入力します（例：`\\Network Share\*`）。

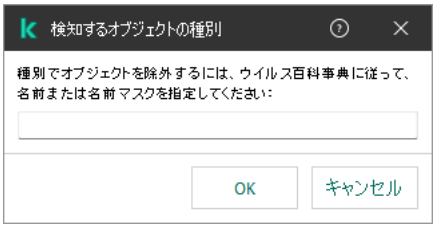
> Kaspersky Security Center コンソールを使用して除外リストを作成する際、環境変数「`%userprofile%`」は Kaspersky Endpoint Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

b. 変更内容を保存します。

9. 特定の名前を持つオブジェクトをスキャンから除外するには：

   a. ［**プロパティ**］ブロックで、［**検知するオブジェクトの種別**］をオンにします。

   b. 下のブロックのリンクをクリックして、［**検知するオブジェクトの種別**］ウィンドウを開きます。



オブジェクトの選択

   a. 「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（例：「`Email-Worm`」、「`Rootkit`」、「`RemoteAdmin`」）。

   任意の1文字を置き換える「`?`」と複数の文字を置き換える「`*`」を使用してマスクを使用することができます。たとえば、マスク「`Client*`」を使用すると、「`Client-IRC`」、「`Client-P2P`」および「`Client-SMTP`」がスキャンから除外されます。

   b. 変更内容を保存します。

10. 個別のファイルをスキャンから除外する場合：

   a. ［**プロパティ**］ブロックで、［**オブジェクトハッシュ**］をオンにします。

   b. 下のブロックのリンクをクリックして、［**オブジェクトハッシュ**］ウィンドウを開きます。



ファイルの選択

   a. ファイルのハッシュを入力するか、［**参照**］をクリックしてファイルを選択します。

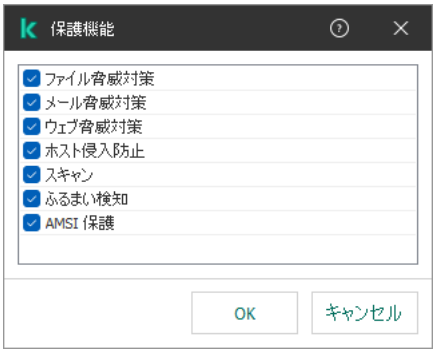
   ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

   b. 変更内容を保存します。

11. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

12. 次の手順に従って、信頼するオブジェクトを使用する Kaspersky Endpoint Security コンポーネントを指定します：

    a. 下のブロックのリンクをクリックして、［**保護機能**］ウィンドウを開きます。



保護機能の選択

    a. スキャンからの除外を適用するコンポーネントの横にあるチェックボックスをオンにします。

    信頼するオブジェクトの設定でコンポーネントが指定されている場合、Kaspersky Endpoint Security のこれらのコンポーネントによるスキャン時にのみ、この信頼するオブジェクトが適用されます。

    信頼するオブジェクトの設定でコンポーネントが指定されていない場合、Kaspersky Endpoint Security のどのコンポーネントによるスキャン時にも、この信頼するオブジェクトが適用されます。

13. ［**OK**］をクリックします。

    新しい信頼するオブジェクトがリストに追加されます。いつでもオブジェクトの横のチェックボックスを使用して信頼するオブジェクトを無効にできます。

14. 変更内容を保存します。

Web コンソールと Cloud コンソールで信頼するオブジェクトを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

    ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**信頼ゾーン**］に移動します。

5. 表示されたウィンドウで、［**マルウェアスキャンの除外リスト**］をクリックします。

6. 組織内のすべてのコンピューターの除外リストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。

7. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

    チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。

8. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも1つの信頼するオブジェクトをカテゴリに追加します。

   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。

   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。

   新しい信頼するオブジェクトを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、［**新しい除外**］オプションを選択します。

9. 除外を追加する方法を選択します：［**ファイルまたはフォルダーのパス**］、［**オブジェクト種別**］または［**オブジェクトハッシュ**］。

10. ファイルまたはフォルダーをスキャンから除外するには、パスを手動で入力してください。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

    - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

    - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。

      ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`?:\Users\*\Folder\`」と入力できます。

      ネットワークフォルダーを除外できます。これを行うには、ネットワークフォルダーのパスを手動で入力します（例：`\\Network Share\*`）。

11. 特定のオブジェクトをスキャンから除外する場合は、［**オブジェクト種別**］フィールドで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（例：「`Email-Worm`」、「`Rootkit`」、「`RemoteAdmin`」）。

    任意の1文字を置き換える「`?`」と複数の文字を置き換える「`*`」を使用してマスクを使用することができます。たとえば、マスク「`Client*`」を使用すると、「`Client-IRC`」、「`Client-P2P`」および「`Client-SMTP`」がスキャンから除外されます。

12. 個別のファイルをスキャンから除外する場合は、［**オブジェクトハッシュ**］フィールドにファイルのハッシュを入力します。

    ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

13. ［**除外を次に適用する**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

14. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

15. ［**OK**］をクリックします。

    新しい信頼するオブジェクトがリストに追加されます。このトグルスイッチを使用していつでも除外を停止することができます。

16. 変更内容を保存します。

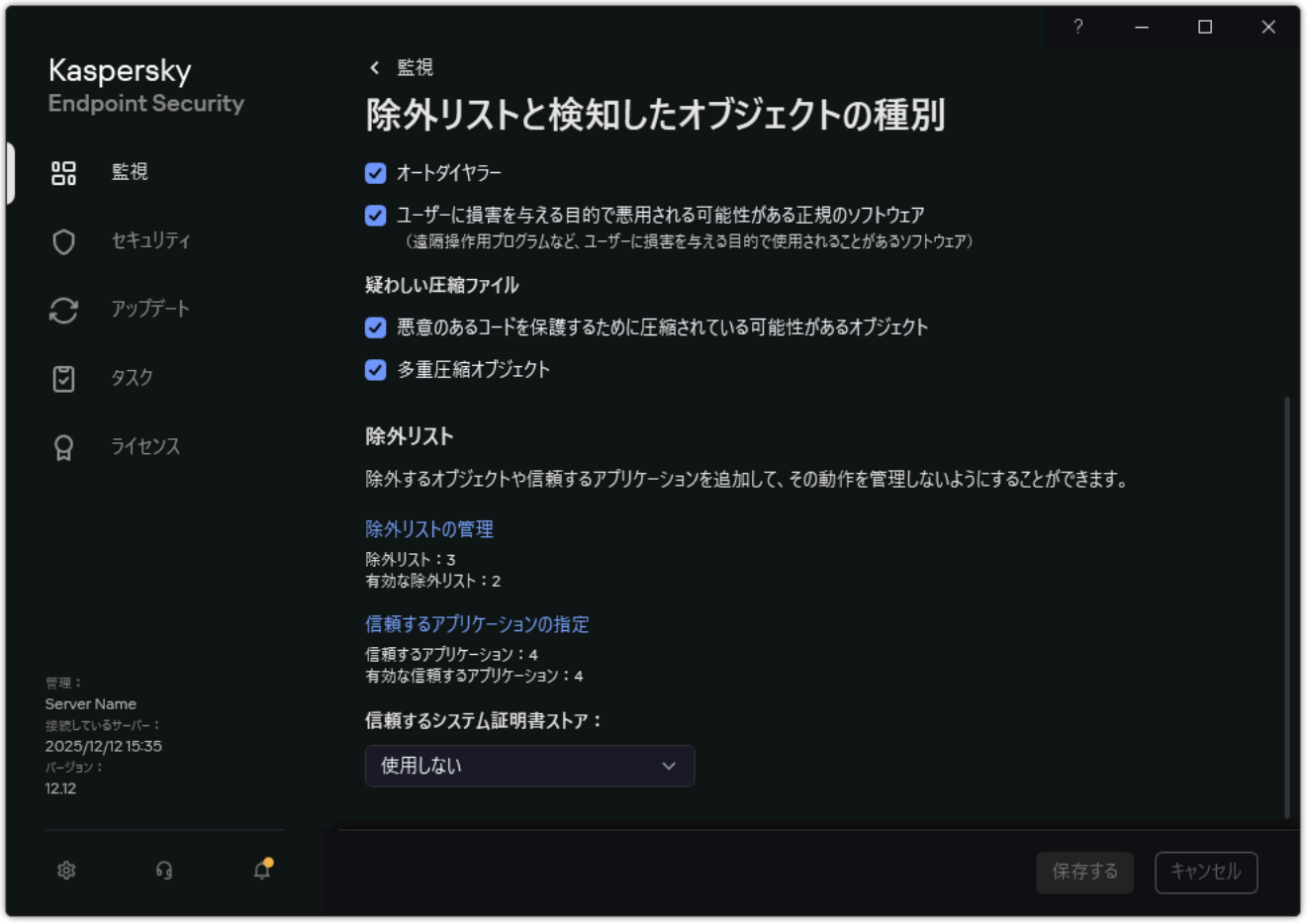
製品インターフェイスで信頼するオブジェクトを作成する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。

3. ［**除外リスト**］セクションで、［**除外リストの管理**］をクリックします。

信頼するオブジェクトの設定がコンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトが禁止されている場合（[**ローカルの除外リストの使用を許可する**]チェックボックスがオフ）は、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。



除外リストの設定

4. [**追加**]をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも1つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **リストから除外を選択してください**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。

   新しい信頼するオブジェクトを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、[**新しい除外**]オプションを選択します。

5. ファイルまたはフォルダーをスキャンから除外する場合は、[**参照**]をクリックしてファイルまたはフォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

  ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「?:\Users*\Folder\」と入力できます。

  ネットワークフォルダーを除外できます。これを行うには、ネットワークフォルダーのパスを手動で入力します（例：\\Network Share*）。

6. 特定のオブジェクトをスキャンから除外する場合は、［**検知するオブジェクトの種別**］フィールドで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、「Rootkit」、「RemoteAdmin」）。

   任意の 1 文字を置き換える「?」と複数の文字を置き換える「*」を使用してマスクを使用することができます。たとえば、マスク「Client*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。

7. 個別のファイルをスキャンから除外する場合は、［**オブジェクトハッシュ**］フィールドにファイルのハッシュを入力します。

   ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

8. ［**保護機能**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

9. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

10. 信頼するオブジェクトのステータスに［**有効**］を選択します。

11. ［**追加する**］をクリックします。

    新しい信頼するオブジェクトがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼するオブジェクトを無効にできます。

12. 変更内容を保存します。



除外リスト

パスマスクの例：

絶対パスではなく相対パスを指定することを推奨します。これにより、ファイルシステムのオブジェクトだけでなく、ファイルレス攻撃の対象オブジェクトも除外できるようになります。例：「`*\Program Files (x86)\Folder\Subfolder`」。

任意のフォルダーにあるファイルへのパス：

- 「`*.exe`」というマスクには、拡張子が「exe」のファイルへのすべてのパスが含まれます。
- 「`example*`」というマスクには、名前が「EXAMPLE」のファイルへのすべてのパスが含まれます。

特定のフォルダーにあるファイルへのパス：

- 「`C:\dir\*.*`」というマスクには、「`C:\dir\`」フォルダーにあるすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\*`」というマスクには、「`C:\dir\`」フォルダーとそのサブフォルダーにあるすべてのファイルへのパスが含まれます。
- 「`C:\dir\`」というマスクには、「`C:\dir\`」フォルダーとそのサブフォルダーにあるすべてのファイルへのパスが含まれます。
- 「`C:\dir\*.exe`」というマスクには、「`C:\dir\`」フォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\test`」というマスクには、「`C:\dir\`」フォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、「`C:\dir\`」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\*\test`」というマスクには、「`C:\dir\`」フォルダーとそのサブフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれます。
- 「`C:\dir1\*\dir3\`」というマスクには、「`C:\dir1\`」からサブフォルダー「dir3」までの間1レベルのすべてのファイルのパスが含まれます。
- 「`C:\dir1\**\dirN\`」というマスクには、「`C:\dir1\`」からサブフォルダー「dirN」までのすべてのレベルにあるファイルすべてのパスが含まれます。

特定の名前のすべてのフォルダーにあるファイルへのパス：

- `dir\*.*`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- `dir\*`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- `dir\`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\*.exe`」というマスクには、名前が「dir」のフォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\test`」というマスクには、名前が「dir」のフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。

検知したオブジェクトの種別による除外リストの作成

Kaspersky Endpoint Security は検知したオブジェクトを次のように分類します：

- **ウイルス、ワーム**

  サブカテゴリ：ウイルスやワーム（Viruses_and_Worms）

  危険度：高

古典的なウイルスやワームは、ユーザーが許可していない処理を実行します。このようなウイルスやワームは、自己複製が可能な自身のコピーを作成することができます。

古典的ウイルス

古典的ウイルスがコンピューターに侵入すると、ファイルに感染して活動を開始し、悪意のある処理を実行し、それ自体のコピーを他のファイルに追加します。

古典的ウイルスは、コンピューターのローカルリソースでしか増殖しないため、自力で他のコンピューターに侵入できません。このウイルスが別のコンピューターに感染するのは、ウイルス自身のコピーを共有フォルダーに保管されているファイルまたは挿入された CD に追加したときや、ユーザーが感染したファイルを添付したメールを転送したときです。

古典的ウイルスのコードはコンピューター、オペレーティングシステム、アプリケーションの各種領域に侵入する可能性があります。環境により、ウイルスは、*ファイルウイルス*、*ブートウイルス*、*スクリプトウイルス*、および *マクロウイルス*に分けられます。

ウイルスはさまざまな技法を駆使してファイルを感染させます。上書き（*Overwriting*）ウイルスは、そのコードを、感染したファイルのコードに上書きして、そのファイルの内容を消去します。感染したファイルは機能しなくなり、復元できません。寄生（*Parasitic*）ウイルスは、ファイルを変更しますが、ファイルが完全にまたは部分的に機能する状態を維持します。コンパニオンウイルス（*Companion*）は、ファイルを変更しませんが、代わりに複製を作成します。感染したファイルが開かれると、ウイルスの複製（実際にはこれがウイルス）が起動します。他にも、次のような種別のウイルスが見つかっています：*Link* ウイルス、*OBJ ウイルス*、*LIB ウイルス*、*ソースコード*ウイルスなど多数。

ワーム

古典的ウイルスのコードと同様に、ワームのコードは、コンピューターに侵入してから活動を開始し、悪意のある処理を実行します。ワームは、コンピューターから別のコンピューターに「這うように移動」し、ユーザーの許可なく多数のデータチャネルを経由してコピーを拡散させることから、この名が付けられました。

さまざまなワームの種類を区別する主な特徴は、その拡散方法です。次のテーブルに、拡散方法によって分類される各種ワームの概要を示します：

ワームの拡散方法

種別	Name	説明
メールワーム	メールワーム	これらのワームはメールを介して広がります。 感染したメールには、ワームのコピーを含んだ添付ファイル、あるいは感染した Web サイトまたは感染させる目的で作成された Web サイトにアップロードされるファイルへのリンクが含まれています。添付ファイルを開くと、ワームが起動します。リンクをクリックし、ファイルをダウンロードして開くと、ワームも悪意のある処理を実行し始めます。その後、ワームは他のメールアドレスを検索して、これらのアドレスに感染メールを送信しながら、自身のコピーを拡散し続けます。
IM ワーム	IM クライアントワーム	インスタントメッセージ（IM）クライアント経由で拡散します。 通常、このようなワームは、ユーザーの連絡先リストを使用して、ワームのコピーに感染した Web サイト上のファイルへのリンクを含んだメールを送信します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。
IRC ワーム	インターネットチャットワーム	このワームは Internet Relay Chats（インターネット上の別のユーザーとリアルタイムで通信できるサービスシステム）を介して拡散します。 この種のワームは、インターネットチャットで自身のコピーを含むファイルまたはそのファイルへのリンクを公開します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。
インターネットワーム（Net-Worm）	ネットワークワーム	これらのワームは、コンピューターネットワークを介して広がります。 通常のネットワークワームは、他の種類のワームと異なり、ユーザーが参加していなくても拡散します。このワームはプライベートネットワークに、脆弱性のあるプログラムがインストールされたコンピューターがないか探します。この操作を行うために、このワームはワームコードまたはその一部を含む特別に形成されたネットワークパケット（エクスプロイト）を送信します。ネットワーク上に「脆弱な」コンピューターが存在すると、そのコンピューターはこのようなネットワークパケットを受信します。ワームが完全にコンピューターに侵入すると、ワームが起動します。

種別	Name	説明
P2P ワーム	ファイル共有ネットワークワーム	peer-to-peer のファイル共有ネットワーク経由で拡散します。 P2P ネットワークに潜入するために、ワームはそれ自身をファイル共有フォルダーにコピーします。このフォルダーは通常、ユーザーのコンピューター上にあります。P2P ネットワークでは、ネットワーク上の感染したファイルをユーザーが他のファイルと同様に「見つけ」、このファイルをダウンロードして開くように、このファイルに関する情報が表示されます。 さらに巧妙なワームは特定の P2P ネットワークのネットワークプロトコルを装って検索クエリに肯定応答を返し、自身のコピーをダウンロードさせます。
ワーム	他の種類のワーム	他の種類のワームには、以下のものがあります： • 自身のコピーをネットワークリソースを介して拡散するワーム。このようなワームは、オペレーティングシステムの機能を使って使用可能なネットワークフォルダーを検索し、インターネット上のコンピューターへ接続し、このコンピューターのディスクドライブへのフルアクセス権を取得しようと試みます。他の種類のワームは上記種類のワームとは異なり、自力で起動するのではなく、ユーザーがワームのコピーを含むファイルを開いたときに起動します。 • 上記のどの拡散方法も使用しないワーム（携帯電話を通じて拡散するワームなど）。

- **トロイの木馬（ランサムウェアを含む）**

  サブカテゴリ：トロイの木馬

  危険度：高

  ワームやウイルスとは異なり、トロイの木馬は自己複製しません。たとえば、ユーザーが感染している Web サイトにアクセスすると、トロイの木馬はメールやブラウザーからコンピューターに侵入します。トロイの木馬は、ユーザーの関与によって起動します。起動直後に、悪意のある処理を実行し始めます。

  トロイの木馬は多種多様で、感染コンピューター上でのふるまいも多岐にわたります。トロイの木馬の主な機能は、情報のブロック、改変、破壊、およびコンピューターまたはネットワークの無効化です。また、トロイの木馬はファイルの送受信、ファイルの実行、画面上へのメッセージの表示、Web サイトの要求、プログラムのダウンロードとインストール、コンピューターの再起動を行うこともできます。

  多くの場合、ハッカーはトロイの木馬の「セット」を使用します。

  次のテーブルでは、トロイの木馬における動作の種類について説明します。

  感染コンピューターにおけるトロイの木馬の動作種類

種別	Name	説明
Trojan-ArcBomb	トロイの木馬 - 「圧縮爆弾」	このアーカイブは、解凍するとコンピューターの動作に影響を与える程度のサイズにまで膨張します。 ユーザーがこのようなアーカイブを解凍しようとすると、コンピューターは処理速度が低下したりフリーズしたりすることがあります。また、ハードディスクが「空の」データで満杯になることがあります。「圧縮爆弾」は、特にファイルサーバーやメールサーバーにとって危険です。サーバーが自動システムを使用して受信情報を処理すると、「圧縮爆弾」によってサーバーが停止することがあります。
バックドア	リモート管理用のトロイの木馬	このプログラムは、トロイの木馬の中でも最も危険なものと考えられます。機能面で、コンピューターにインストールされるリモート管理アプリケーションに似ています。 これらのプログラムは、ユーザーに気付かれずにコンピューターにインストールされるので、侵入者はコンピューターを遠隔管理できます。
トロイの木馬	トロイの木馬	トロイの木馬には、次のような悪意のあるアプリケーションがあります： • **古典的なトロイの木馬**：これらのプログラムはトロイの木馬の主な機能（情報のブロック、改変または破壊、およびコンピューターまたはネットワークの無効化）のみを実行し、テーブルに示す他の種類のトロイの木馬とは異なり、高度な機能を持っていません。 • **多目的なトロイの木馬**：これらのプログラムは、数種類のトロイの木馬に特徴的な先進機能を備えています。
Trojan-Ransom	トロイの木馬型ランサムウェア	このプログラムは、ユーザーの情報を「人質」にとって改変したり、ブロックしたりします。また、ユーザーが情報を使用する能力を喪失するように、コンピューターの動作に影響を与えます。侵入者は、コンピューターのパフォーマンスと保存されていたデータを復元するアプリケーションを送るという約束と引き替えに、ユーザーから身代金を要求します。

種別	Name	説明
Trojan-Clicker	トロイの木馬クリッカー	このプログラムは、ブラウザーにコマンドを送信するか、オペレーティングシステムファイルで指定されている Web アドレスを変更することによって、ユーザーのコンピューターから Web サイトにアクセスします。 侵入者はこのようなプログラムを使用することによって、ネットワーク攻撃を行って Web サイトのアクセス数を増やし、バナー広告の表示回数を増やします。
Trojan-Downloader	トロイの木馬ダウンローダー	これは侵入者の Web サイトにアクセスして、そこから他の悪意のあるアプリケーションをダウンロードし、ユーザーのコンピューターにインストールします。このプログラムには、悪意のあるアプリケーションをダウンロードまたは受信するためにアクセスした Web サイトのファイル名が含まれていることがあります。
Trojan-Dropper	トロイの木馬ドロッパー	このプログラムは他のトロイの木馬を内包しており、この内包されたプログラムがハードディスクにインストールされ、実行されます。 侵入者は、トロイの木馬ドロッパー型プログラムを次のような目的で使用することがあります： • ユーザーに気付かれずに悪意のあるプログラムをインストールする：トロイの木馬ドロッパー型プログラムは、メッセージを表示しないか、たとえば、アーカイブ中にエラーが発生したことやオペレーティングシステムが互換性のないバージョンであることを示すといった偽のメッセージを表示します。 • 既知の悪意のある別のアプリケーションが検知されないようにする：すべてのアンチウイルスのソフトウェアがトロイの木馬ドロッパー型アプリケーション内の悪意のあるアプリケーションを検知できるわけではありません。
Trojan-Notifier	トロイの木馬型ノーティファイア	このプログラムは、感染したコンピューターにアクセスできることを侵入者に教えるため、コンピューターの次のような情報を侵入者に送信します：IP アドレス、開いているポートの番号、メールアドレスなど。このプログラムはこれらの情報をメール、FTP、侵入者の Web サイトへのアクセス、あるいはこれら以外の方法で侵入者に送ります。 トロイの木馬型ノーティファイアプログラムは、多くの場合、複数のトロイの木馬からなるセットとして使用されます。また、このプログラムはトロイの木馬がユーザーのコンピューターにインストールされたことを侵入者に知らせます。
Trojan-Proxy	トロイの木馬型プロキシ	これらのトロイの木馬により、侵入者は、ユーザーのコンピューターを使って匿名で Web サイトにアクセスします。このトロイの木馬はスパムの送信によく利用されます。
Trojan-PSW	パスワード窃盗ソフトウェア	パスワード窃盗ソフトウェアは、ソフトウェア登録データなどのユーザーアカウントを盗むトロイの木馬の一種です。このトロイの木馬はシステムファイルおよびレジストリ内の機密データを見つけ、そのデータを「攻撃者」にメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって送信します。 これらのトロイの木馬のうち、いくつかがこのテーブルに示す種類に分類されます。これらは、銀行のアカウント情報（Trojan-Banker）、メッセンジャークライアントのユーザーのデータ（Trojan-IM）、およびオンラインゲームのユーザーの情報（Trojan-GameThief）を盗むトロイの木馬です。
Trojan-Spy	スパイウェア型トロイの木馬	このトロイの木馬はコンピューター上で動作しながら、ユーザーが行う処理に関する情報を収集して、ユーザーの行動を秘密裏に監視します。このトロイの木馬は、ユーザーがキーボードで入力するデータの傍受、スクリーンショットの撮影、あるいはアクティブなアプリケーションのリストの収集などを行うことがあります。このプログラムが情報を入手すると、その情報をメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。
Trojan-DDoS	トロイの木馬ネットワークアタッカー	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。ハッカーは、1 台のサーバーを多数のコンピューターから同時に攻撃できるように、このプログラムを利用して多数のコンピューターを感染させることがあります。 DoS プログラムは 1 台のコンピューターから、ユーザーに気付かれることなく攻撃を実行します。DDoS（分散 DoS）プログラムは、感染したコンピューターのユーザーに気付かれずに、複数のコンピューターから分散して攻撃を行います。
Trojan-IM	メッセンジャークライアントのユーザーから情報を盗むトロイの木馬	このトロイの木馬は、メッセンジャークライアントのユーザーのアカウント番号とパスワードを盗みます。このプログラムは、データをメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。
ルートキット	ルートキット	ルートキットは、他の悪意のあるアプリケーションやその活動を隠蔽します。そのため、このアプリケーションはオペレーティングシステムに長期間潜入します。また、ルートキットはファイル、感染しているコンピューターのメモリ内のプロセス、または悪意のあるアプリケーションを実行するレジストリキーを隠蔽することもできます。さらにルートキットは、ユーザーのコンピューターにインストールされているアプリケーションとネットワーク上の他のコンピューターにインストールされているアプリケーションの間で行われるデータ交換を隠蔽できます。
Trojan-SMS	SMS メッセージ形式のトロイの木馬	このトロイの木馬は携帯電話を感染させ、高額の通話料が発生する電話番号に SMS メッセージを送信します。

種別	Name	説明
Trojan-GameThief	オンラインゲームのユーザーから情報を盗むトロイの木馬	このトロイの木馬は、オンラインゲームのユーザーのアカウント情報を盗み、このデータを侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。
Trojan-Banker	銀行のアカウント情報を盗むトロイの木馬	このトロイの木馬は、銀行のアカウント情報や電子マネーシステムのデータを盗み、このデータをメールや FTP を使用して侵入者に送信するか、侵入者の Web サイトにアクセスするなどして送信します。
Trojan-Mailfinder	メールアドレスを収集するトロイの木馬	このトロイの木馬は、コンピューターに保存されているメールアドレスを収集し、侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。侵入者が収集したアドレスにスパムを送信することがあります。

- **悪意のあるツール**

  サブカテゴリ：悪意のあるツール

  危険度：中

  悪意のあるツールは、他の種類のマルウェアとは異なり、起動した直後に処理を実行しません。このプログラムはユーザーのコンピューターに安全に侵入し、そこで起動することができます。侵入者は、多くの場合、悪意のあるツールの機能を悪用して、ウイルス、ワーム、トロイの木馬を作成したり、リモートサーバーに対してネットワーク攻撃を仕掛けたりします。

  悪意のあるツールのさまざまな機能を、次のテーブルに示す種類別に分類しています：

  悪意のあるツールの機能

種別	Name	説明
コンストラクター	コンストラクター	このツールを使用して、新しいウイルス、ワームおよびトロイの木馬を作成します。一部のコンストラクターは標準的なウィンドウベースのインターフェイスを備えています。このインターフェイスでは、悪意のあるアプリケーションの種類を選択して、デバッガを無効にする手段やその他の機能を作成できます。
Dos	ネットワーク攻撃	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。
エクスプロイト	エクスプロイト	*エクスプロイト*は、処理されるアプリケーションの脆弱性を利用する一連のデータまたはプログラムコードで、コンピューター上で悪意のある処理を実行します。たとえば、エクスプロイトは、ファイルの書き込みまたは読み取り、あるいは「感染している」Web サイトの要求を行うことができます。 それぞれのエクスプロイトは、さまざまなアプリケーションまたはネットワークサービスの脆弱性を利用します。ネットワークパケットに偽装したエクスプロイトは、ネットワーク経由で多数のコンピューターに送信され、脆弱なネットワークサービスを備えるコンピューターを探します。DOC ファイルのエクスプロイトは、テキストエディターの脆弱性を利用します。このエクスプロイトは、ユーザーが感染したファイルを開いたときに、ハッカーが事前にプログラミングした処理を開始することがあります。メールに組み込まれたエクスプロイトは、メールクライアントの脆弱性を探します。このエクスプロイトは、ユーザーがメールクライアントの感染メールを開くとすぐに悪意のある処理を実行します。 エクスプロイトを使用してネットワーク上に拡散するのがネットワームです。ヌーカー型エクスプロイトは、コンピューターを無効にするネットワークパケットです。
FileCryptor	エンクリプター	このプログラムは、他の悪意のあるアプリケーションを暗号化してアンチウイルス製品から隠蔽します。
Flooder	ネットワークを「汚染する」ためのプログラム	このプログラムは大量のメールをネットワークチャネル上に送信します。この種のツールには、インターネットリレーチャットなどを汚染するプログラムがあります。 Flooder 型ツールには、メール、IM クライアントおよびモバイル通信システムで使用されるチャネルを「汚染する」プログラムは含まれません。これらのプログラムは、テーブルに示す別種（Email-Flooder、IM-Flooder および SMS-Flooder）として区別されます。
HackTool	ハッキングツール	このプログラムは、たとえば、ユーザーの許可なしに新しいシステムアカウントを追加したり、システムログを消去してオペレーティングシステムにおける存在の痕跡を隠蔽したりすることによって、このプログラムがインストールされたコンピューターをハッキングすることや別のコンピューターを攻撃することを可能にします。この種のツールには、パスワードの傍受などの悪意のある機能を特徴とする一部のスニファーが含まれます。スニファーは、ネットワークトラフィックの監視を可能にするプログラムです。

種別	Name	説明
Hoax	デマウイルス	このプログラムはウイルスメッセージに似たメッセージでユーザーに注意を喚起します。具体的には、感染していないファイルで「ウイルスを検知した」というメッセージや、実際にはディスクのフォーマットが発生しなかったのに、ディスクがフォーマットされたというメッセージを表示します。
スプーファ	スプーフィングツール	このツールは、メッセージ要求やネットワーク要求を送信者の偽装アドレスで送信します。たとえば、侵入者はスプーファ型のツールを使用して、ツール本体をメールの実際の送信者として渡します。
VirTool	悪意のあるアプリケーションを改変するツール	このツールを使用すると、他のマルウェアを改変して、アンチウイルス製品から隠蔽することができます。
Email-Flooder	メールアドレスを「汚染する」プログラム	このプログラムはさまざまなメールアドレスに大量のメールを送信して、これらのメールアドレスを「汚染」します。大量の受信メールによって、ユーザーは必要なメールを受信ボックスで表示できなくなります。
IM-Flooder	メッセンジャークライアントのトラフィックを「汚染する」プログラム	IM クライアントのユーザーをメッセージであふれさせます。大量のメールが送られてくるため、ユーザーは必要な受信メールを表示できなくなります。
SMS-Flooder	トラフィックを SMS メッセージで「汚染する」プログラム	このプログラムは携帯電話に大量の SMS メッセージを送信します。

- **アドウェア**

  サブカテゴリ：広告ソフトウェア（アドウェア）

  危険度：中

  アドウェアはユーザーに対して広告情報を表示します。アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。このようなプログラムには、ユーザーに関するマーケティング情報を収集し、それを開発者に送信するものがあります。この情報には、ユーザーが表示した Web サイトの名前や、ユーザーの検索の内容などが含まれます。スパイウェア型のトロイの木馬とは異なり、アドウェアは、このような情報をユーザーの同意を得てから開発者に送ります。

- **オートダイヤラー**

  サブカテゴリ：オートダイヤラー（ダイヤラー）

  危険度：中

  オートダイヤラーはモデムを使用して密かに電話接続を確立できます。

- **ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア**

  サブカテゴリ：ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア。

  危険度：中

  これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

種別	Name	説明
クライアント-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他のコンピューターにインストールされているアプリケーションとどのようにデータをやり取りしているかを監視する）。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理プログラム	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。 合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。
Server-FTP	FTP サーバー	このプログラムは FTP サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP 経由でコンピューターへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnet サーバー	このプログラムは Telnet サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet 経由でコンピューターへのリモートアクセスを開きます。
Server-Web	Web サーバー	このプログラムは Web サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP 経由でコンピューターへのリモートアクセスを開きます。
RiskTool	ローカルコンピューターで動作するツール	このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、コンピューターにインストールされているアプリケーションを起動することできます。
Client-P2P	P2P ネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
クライアント-SMTP	SMTP クライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Web ツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

- **悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト**

  サブカテゴリ：損害を与える可能性がある圧縮ファイル

  危険度：中

ファイルは、マルウェア（ウイルス、ワーム、トロイの木馬）の圧縮に使用される特殊なパッカーを使用して圧縮されます。Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に解凍モジュールがないかスキャンします。

マルウェアをアンチウイルスによる検知から隠すために、ハッカーは特殊なパッカーを使用してマルウェアを圧縮します。カスペルスキーのエキスパートは、ハッカーの間で最も使用されているパッカーを特定しています。

- **多重圧縮オブジェクト**

  サブカテゴリ：多重圧縮ファイル

  危険度：中

  ファイルは1つ以上のパッカーを使用して3回以上圧縮されます。

  マルウェアをアンチウイルスによる検知から隠すために、ハッカーがファイルを複数回圧縮することがあります。Kaspersky Endpoint Security は圧縮されたファイルをスキャンします。

既定では、Kaspersky Endpoint Security はすべての種別のオブジェクトを検知します。コンピューターのセキュリティを向上させるために、すべての種別のオブジェクトの検知を有効のままにしておくことを推奨します。本製品が悪意のあるものとして検知する社内ユーティリティを使用している場合は、これらのユーティリティを除外リストに追加します。ただし、オブジェクトの種別全体の検知を無効にしないでください。

管理コンソール（MMC）で検知可能なオブジェクトの種別を選択する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
5. ［**検知するオブジェクトの種別**］ブロックの［**設定**］をクリックします。
6. 表示されたウィンドウで、チェックボックスを使用して Kaspersky Endpoint Security が検知するオブジェクトの種類を選択します。
7. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（  ）。

Web コンソールと Cloud コンソールで検知可能なオブジェクトの種別を選択する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**検知の設定**］に移動します。

5. ［**その他の種別のオブジェクトの検知**］ブロックで、チェックボックスを使用して Kaspersky Endpoint Security が検知するオブジェクトの種類を選択します。

6. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

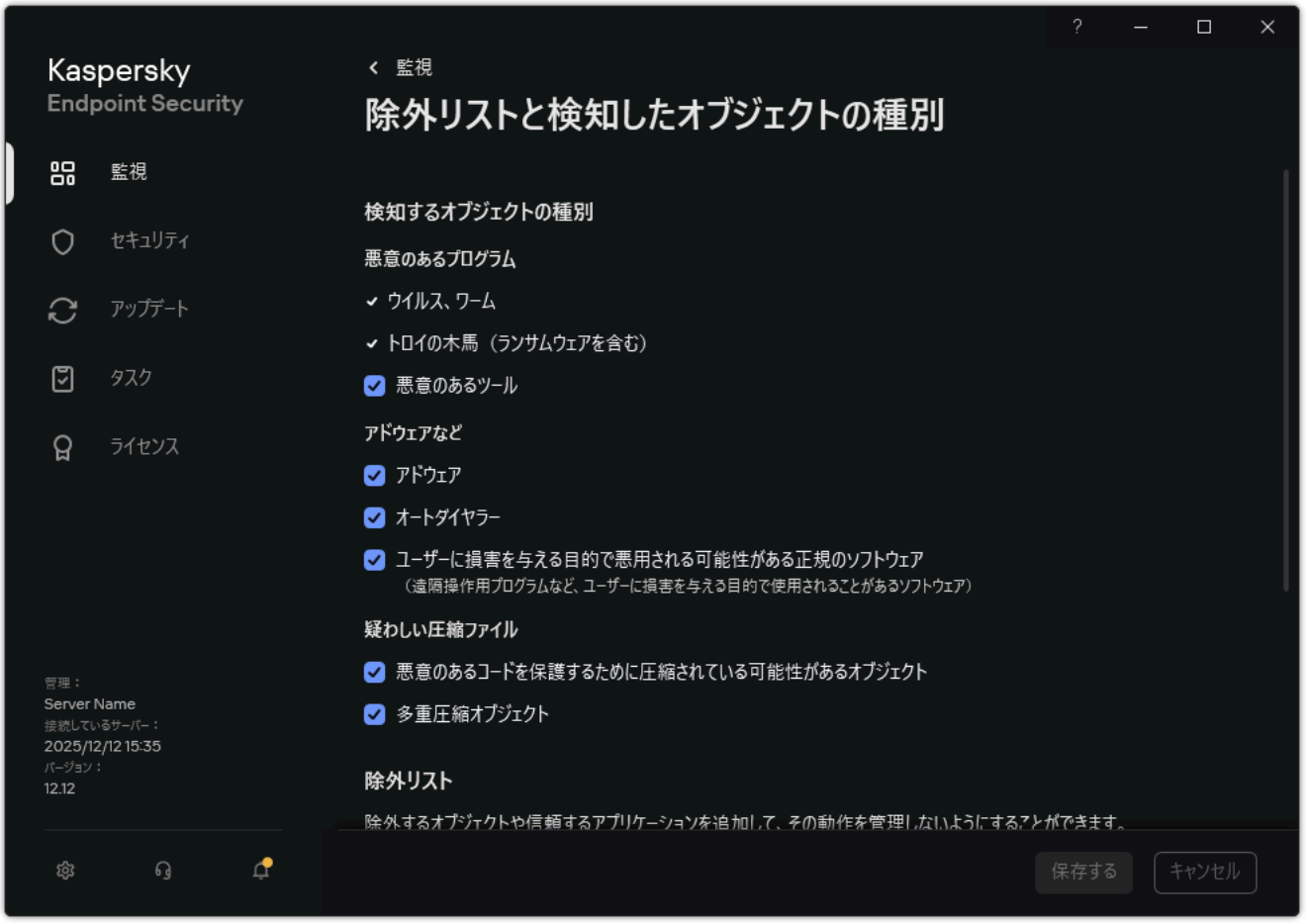
製品インターフェイスで検知可能なオブジェクトの種別を選択する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。

3. ［**検知するオブジェクトの種別**］ブロックで、チェックボックスを使用して Kaspersky Endpoint Security が検知するオブジェクトの種類を選択します。

4. 変更内容を保存します。



検知するオブジェクトの種別

信頼するアプリケーションのリストの編集

*信頼するアプリケーションのリスト*は、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Endpoint Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Endpoint Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトを監視し、すべてのアプリケーションとこのようなアプリケーションが生成するネットワークトラフィックの処理を管理します。アプリケーションが信頼するアプリケーションのリストに追加されると、Kaspersky Endpoint Security はアプリケーションのアクティビティの監視を停止します。

信頼するオブジェクトと信頼するアプリケーションの違いは、信頼するオブジェクトの場合、Kaspersky Endpoint Security はファイルをスキャンしないのに対し、信頼するアプリケーションの場合は、開始されたプロセスを制御しないことです。信頼するアプリケーションが信頼するオブジェクトに含まれていないフォルダーに悪意のあるファイルを作成した場合、Kaspersky Endpoint Security はそのファイルを検知して脅威を排除します。フォルダーが除外リストに追加されている場合、Kaspersky Endpoint Security はこのファイルをスキップします。

たとえば、Microsoft Windows 標準のメモ帳アプリケーションで使用するオブジェクトが安全であり信頼できると考える場合は、Microsoft Windows メモ帳を信頼するアプリケーションのリストに追加し、このアプリケーションが使用するオブジェクトが監視されないようにすることができます。これにより、サーバーアプリケーションで特に重要となるコンピューターのパフォーマンスを高めることができます。

また、特定の処理が Kaspersky Endpoint Security によって疑わしい処理に分類されたとしても、多数のアプリケーションの機能を考慮すると安全な場合があります。たとえば、キーボードで入力したテキストの取得は、自動キーボードレイアウト切り替えプログラム（Punto Switcher など）では通常の処理です。このようなアプリケーションの特性を考慮して、アプリケーション処理を監視対象から除外するために、このようなアプリケーションを信頼するアプリケーションのリストに追加してください。

信頼するアプリケーションは、Kaspersky Endpoint Security と他のアプリケーションとの間の互換性の問題（たとえば、Kaspersky Endpoint Security と他のアンチウイルス製品によるサードパーティ製コンピューターのネットワークトラフィックの二重スキャンなど）を回避するのに役立ちます。

ただし、信頼するアプリケーションの実行ファイルとプロセスのウイルスおよびその他のマルウェアスキャンは実行されます。アプリケーションを Kaspersky Endpoint Security のスキャンから完全に除外するには、信頼するオブジェクトを設定します。

信頼ゾーンは、管理コンソール（MMC）と Web コンソールで異なる方法でグループ化されます。同様に、信頼ゾーンのパラメータ変更を防止する方法も異なります（別の「南京錠」）。本製品の管理には、Web コンソールのみを使用することを推奨します。別のコンソールで信頼ゾーンを設定すると、管理プラグインによって「南京錠」が既定の状態にリセットされる場合があります。

管理コンソール（MMC）の信頼リストにアプリケーションを追加する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
4. ［**信頼するオブジェクトとアプリケーション**］→［**信頼するアプリケーション**］ブロックの［**設定**］をクリックします。

   信頼するアプリケーションのリストを含むウィンドウが開きます。
5. 組織内のすべてのコンピューターの信頼するアプリケーションのリストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の信頼するアプリケーションのリストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの信頼するアプリケーションは子ポリシー内では読み取り専用で表示されます。親ポリシーの信頼するアプリケーションは、変更または削除できません。

6. 信頼するアプリケーションのローカルのリストをユーザーが作成できるようにするには、［**ローカルの信頼するアプリケーションの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された信頼するアプリケーションの全体的なリストに加えて自分のローカルの信頼するアプリケーションのリストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の信頼するアプリケーションの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。

7. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも 1 つカテゴリに追加します。

   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するアプリケーションをリストのルートに追加します。

   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するアプリケーション*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するアプリケーションが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するアプリケーションを選択する必要があります。

   - **選択したカテゴリに新しい除外を追加**：新しい信頼するアプリケーションを特定のカテゴリに追加するには、カテゴリを選択します。

8. 信頼の基準を選択します。

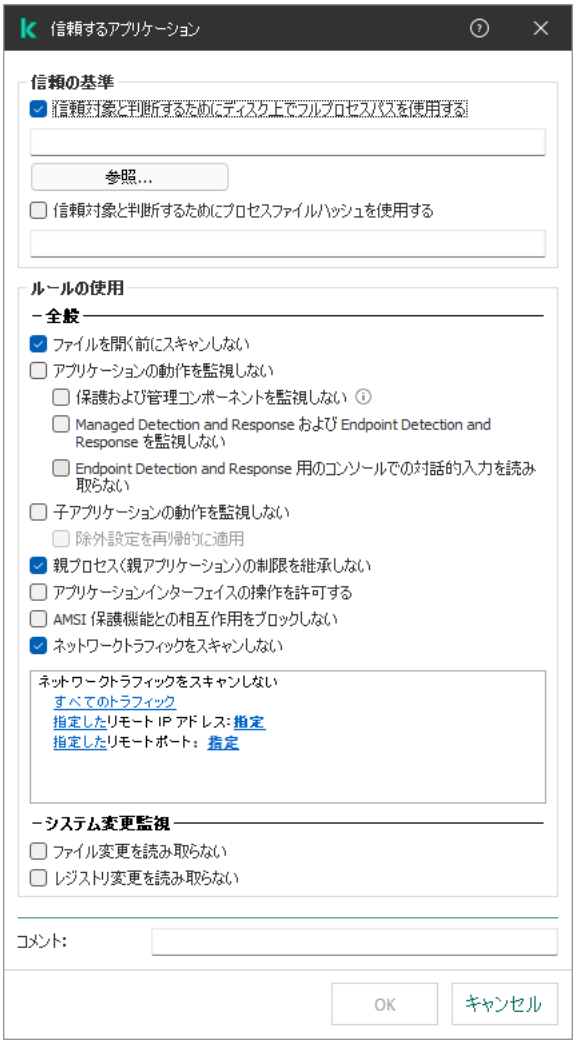
   - **信頼対象と判断するためにディスク上でフルプロセスパスを使用する**：信頼するアプリケーションの実行ファイルのパスを入力します。

     Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

     Kaspersky Endpoint Security は、信頼するアプリケーションのファイル名を、大文字と小文字を区別して扱います。入力したファイル名の大文字と小文字が間違っていると、Kaspersky Endpoint Security は、信頼するアプリケーションを認識しません。

   - **信頼対象と判断するためにプロセスファイルハッシュを使用する**

Kaspersky Security Center コンソールで信頼するアプリケーションのリストを作成する際、環境変数 `%userprofile%` は Kaspersky Endpoint Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「*」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。



信頼するアプリケーションの設定

9. 信頼するアプリケーションの詳細設定を指定します（下の表を参照ください）。

10. ［**OK**］をクリックします。

新しい信頼するアプリケーションがリストに追加されます。いつでもオブジェクトの横のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

11. 変更内容を保存します。



信頼するアプリケーションのリスト

Web コンソールと Cloud コンソールの信頼済みリストにアプリケーションを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**信頼ゾーン**］に移動します。

5. 表示されたウィンドウで、［**アプリケーション**］をクリックします。

   信頼するアプリケーションのリストを含むウィンドウが開きます。

6. 組織内のすべてのコンピューターの信頼するアプリケーションのリストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の信頼するアプリケーションのリストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの信頼するアプリケーションは子ポリシー内では読み取り専用で表示されます。親ポリシーの信頼するアプリケーションは、変更または削除できません。

7. 信頼するアプリケーションのローカルのリストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された信頼するアプリケーションの全体的なリストに加えて自分のローカルの信頼するアプリケーションのリストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の信頼するアプリケーションの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。

8. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも 1 つカテゴリに追加します。
   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するアプリケーションをリストのルートに追加します。
   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するアプリケーション*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するアプリケーションが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するアプリケーションを選択する必要があります。

   新しい信頼するアプリケーションを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、［**新しい除外**］オプションを選択します。

9. 信頼の基準を選択します。

   - **ファイルまたはフォルダーのパス**：信頼するアプリケーションの実行ファイルのパスを入力します。

     Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

     Kaspersky Endpoint Security は、信頼するアプリケーションのファイル名を、大文字と小文字を区別して扱います。入力したファイル名の大文字と小文字が間違っていると、Kaspersky Endpoint Security は、信頼するアプリケーションを認識しません。
   - **アプリケーションのハッシュ**

   > Kaspersky Security Center console で信頼するアプリケーションのリストを作成する際、環境変数 %userprofile% は Kaspersky Endpoint Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

10. 信頼するアプリケーションの詳細設定を指定します（下の表を参照ください）。

11. ［**OK**］をクリックします。

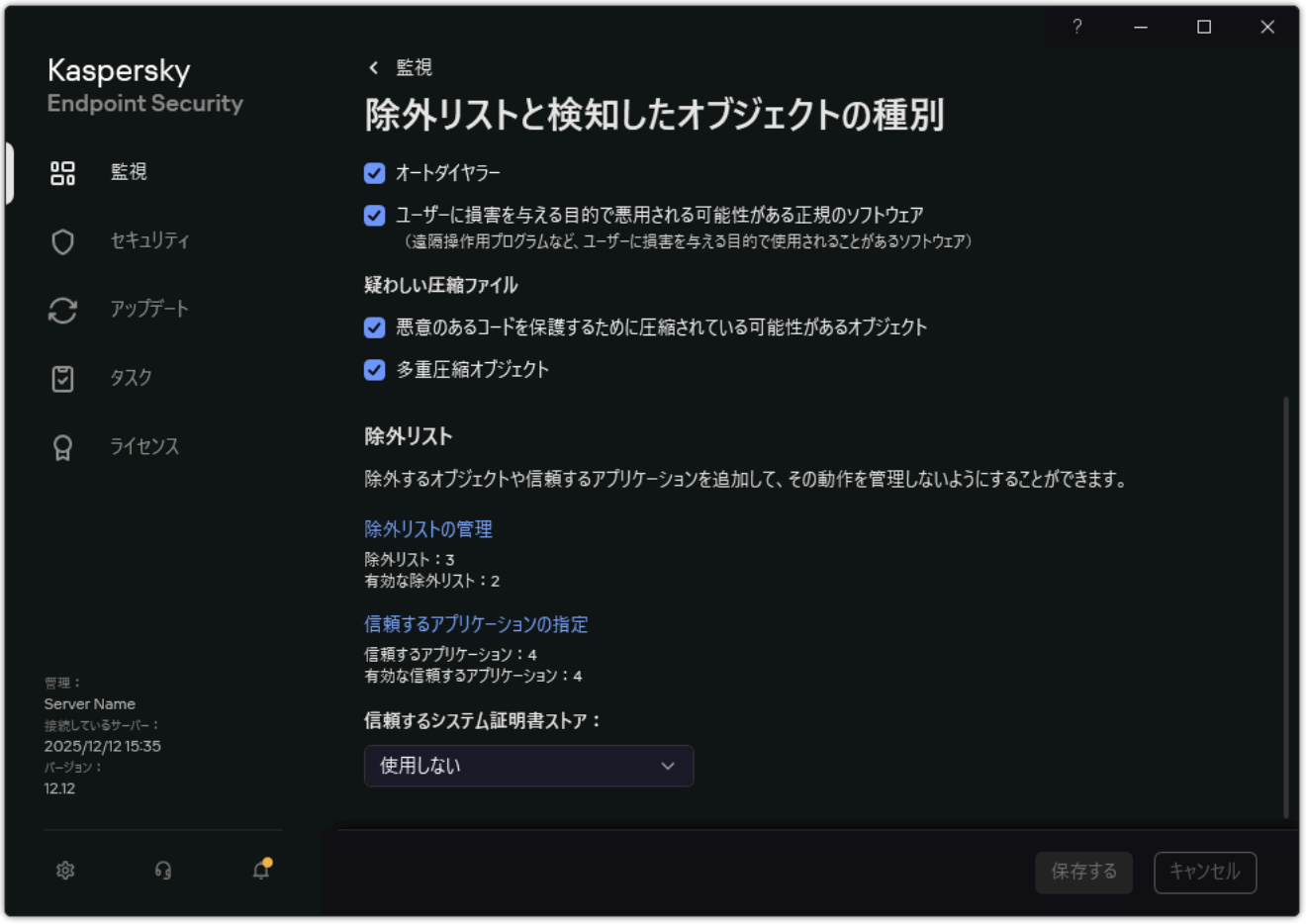
    新しい信頼するアプリケーションがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

12. 変更内容を保存します。

製品インターフェイスから信頼リストにアプリケーションを追加する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。
3. ［**除外リスト**］セクションで、［**信頼するアプリケーションの指定**］をクリックします。

信頼するアプリケーションの設定が管理者によってコンソールでブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するアプリケーションが禁止されている場合（[**ローカルの信頼するアプリケーションの使用を許可する**] チェックボックスがオフ）は、すべての信頼するアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。



除外リストの設定

4. [**追加**] をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも1つカテゴリに追加します。
   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するアプリケーションをリストのルートに追加します。
   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するアプリケーション*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するアプリケーションが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するアプリケーションを選択する必要があります。

   新しい信頼するアプリケーションを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、[**新しい除外**] オプションを選択します。

5. 信頼の基準を選択します。

   - **ディスク上のプロセスの完全パスを使用して信頼済みと判断する**：信頼するアプリケーションの実行ファイルのパスを入力します。

     Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

Kaspersky Endpoint Security は、信頼するアプリケーションのファイル名を、大文字と小文字を区別して扱います。入力したファイル名の大文字と小文字が間違っていると、Kaspersky Endpoint Security は、信頼するアプリケーションを認識しません。

- **プロセスファイルのハッシュを使用して信頼済みと判断する**

Kaspersky Endpoint Security は環境変数をサポートしており、本製品のローカルインターフェイスでパスを変換します。たとえば、ファイルパス「`%userprofile%\Documents\File.exe`」、「`C:\Users\Fred123\Documents\File.exe`」がユーザー「Fred123」の本製品のローカルインターフェイスに追加されたとします。結果、Kaspersky Endpoint Security は信頼するアプリケーション「`File.exe`」を別のユーザーに対して無視します。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

6. 信頼するアプリケーションのプロパティウィンドウで、詳細設定を指定します。

7. ［OK］をクリックします。

新しい信頼するアプリケーションがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

8. 変更内容を保存します。



信頼するアプリケーションのリスト

パラメータ	説明
ファイルを開く前にスキャンしない	アプリケーションが開いたファイルはすべて Kaspersky Endpoint Security のスキャンの対象外になります。例えば、信頼するアプリケーションを使用してファイルのバックアップをしていた場合など、この機能により Kaspersky Endpoint Security のリソースの消費量を減少させることができます。
アプリケーションの動作を監視しない	Kaspersky Endpoint Security はアプリケーションのファイルとオペレーティングシステム内のネットワークアクティビティを監視しません。Kaspersky Endpoint Security の別の機能で、アプリケーション処理の監視を設定できます： • **保護および管理コンポーネントを監視しない**：アプリケーションの動作は、ふるまい検知、脆弱性攻撃ブロック、ホスト侵入防止、修復エンジンおよびファイアウォールにより監視されています。 • **Managed Detection and Response および Endpoint Detection and Response を監視しない**：アプリケーションの動作は、組み込みの MDR エージェントおよび組み込みの EDR (KATA) エージェントによって監視されます。 • **Endpoint Detection and Response 用のコンソールでの対話的入力を読み取らない**：Kaspersky Endpoint Security はコンソール上のアプリケーションの管理に関するテレメトリデータを送信しません。テレメトリデータは Kaspersky Anti Targeted Attack Platform (EDR) で使用されます。
子アプリケーションの動作を監視しない	Kaspersky Endpoint Security はファイルまたはこのアプリケーションによって開始されたアプリケーションのネットワークの動作を監視しません。例外は再帰的に適用できます。そのため、子アプリケーションのチェーン全体の動作は監視されません。
親プロセス（アプリケーション）の制限を継承しない	親プロセスで設定された制限は子プロセスには適用されません。親プロセスは、アプリケーション権限（ホスト侵入防止）およびアプリケーションネットワークルール（ファイアウォール）が設定されたアプリケーションによって開始されます。
子アプリケーションの動作を監視しない	Kaspersky Endpoint Security はファイルまたはこのアプリケーションによって開始されたアプリケーションのネットワークの動作を監視しません。例外は再帰的に適用できます。そのため、子アプリケーションのチェーン全体の動作は監視されません。
アプリケーションインターフェイスの操作を許可する	Kaspersky Endpoint Security のセルフディフェンスは、リモートコンピューターからのアプリケーションサービスを管理しようとする試みをすべてブロックします。このチェックボックスをオンにすると、リモートアクセスアプリケーションで Kaspersky Endpoint Security インターフェイスを経由して Kaspersky Endpoint Security 設定を管理できます。
AMSI 保護機能との相互作用をブロックしない	Kaspersky Endpoint Security は AMSI 保護機能によるアプリケーションのオブジェクトのスキャンの要求を監視しません。
ネットワークトラフィックをスキャンしない	アプリケーションにより開始されたネットワークトラフィックは Kaspersky Endpoint Security のスキャンから除外されます。すべてのトラフィックまたは暗号化されたトラフィックをスキャンから除外することも可能です。個別の IP アドレスおよびポート番号をスキャンから除外することも可能です。
ファイル変更を読み取らない *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Endpoint Security は、システム変更監視の監視範囲のファイルの変更を監視しません。本製品は、すべてのシステム変更監視モード（リアルタイムシステム変更監視とオンデマンドのシステム変更チェック）に除外リストを適用します。
レジストリ変更を読み取らない *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Endpoint Security は、システム変更監視の監視範囲のレジストリキーの変更を監視しません。本製品は、すべてのシステム変更監視モード（リアルタイムシステム変更監視とオンデマンドのシステム変更チェック）に除外リストを適用します。
コメント	必要に応じて、信頼するアプリケーションについて短いコメントを追加することができます。コメントは信頼するアプリケーションの検索や並べ替えに役に立ちます。
ステータス	信頼するアプリケーションのステータス： • ［**有効**］ステータスは、アプリケーションが信頼ゾーンにあることを示します。 • ［**無効**］ステータスは、アプリケーションが信頼ゾーンにあることを示します。

ローカルの信頼ゾーンの作成

ユーザーが特定のコンピューター用に自分のローカル信頼ゾーンを作成できるようになりました。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。管理者はローカルの除外リストまたはローカルの信頼するアプリケーションの使用をポリシー設定で許可またはブロックできます。これを行うには、ポリシーの［**除外リスト**］セクションで［**ローカルの除外リストの使用を許可する**］と［**ローカルの信頼するアプリケーションの使用を許可する**］を使用します。

ローカルの信頼ゾーンの作成を管理者が許可している場合、ユーザーは製品のユーザーインターフェイスで自分の除外リストと信頼するアプリケーションを追加できます。また、ユーザーはポリシーで設定された信頼するゾーンに含まれるオブジェクトを変更または削除する権限がありません。管理者は、個別のコンピューターに除外リストを追加する必要がある場合、Kaspersky Security Center のコンソールでリスト項目の表示、追加、変更、削除も行なうことができます。

信頼ゾーンの設定がコンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトとアプリケーションが禁止されている場合は、信頼するオブジェクトとアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。

管理コンソール（MMC）でローカルの信頼リストにオブジェクトを追加する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**デバイス**］タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。
6. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Endpoint Security for Windows (12.12)**］を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。
7. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］を選択します。
8. ［**信頼するオブジェクトとアプリケーション**］→［**ローカルの信頼するオブジェクト**］ブロックの［**設定**］をクリックします。

ローカルの除外リストを含むウィンドウが表示されます。



信頼ゾーンの設定

9. ローカルの信頼するオブジェクトのリストを作成します。

   ローカルの信頼するオブジェクトのリストを作成するルールは、一般的な除外リストの場合と同じです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

10. ［**信頼するオブジェクトとアプリケーション**］→［**ローカルの信頼するアプリケーション**］ブロックの［**設定**］をクリックします。

    ローカルの信頼するアプリケーションのリストを含むウィンドウが表示されます。

11. ローカルの信頼するアプリケーションのリストを作成します。

    ローカルの信頼するアプリケーションのリストにアプリケーションを追加するルールは、一般的なリストに追加するルールと同じです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

12. 変更内容を保存します。

Web コンソールと Cloud コンソールでローカルの信頼ゾーンにオブジェクトを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ブロックされている操作の実行を許可するユーザーのコンピューターの名前をクリックします。

3. ［**アプリケーション**］タブを選択します。

4. **Kaspersky Endpoint Security for Windows** をクリックします。

   ローカルアプリケーション設定が表示されます。

5. ［**アプリケーション設定**］タブを選択します。

6. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。

7. ［**信頼するオブジェクトとアプリケーション**］セクションで、［**ローカルの信頼するオブジェクト**］をクリックします。

8. ローカルの信頼するオブジェクトのリストを作成します。

   ローカルの除外リストを作成するルールは、一般的な除外リストを作成するルールと同じです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

9. ［**信頼するオブジェクトとアプリケーション**］セクションで、［**ローカルの信頼するアプリケーション**］をクリックします。

10. ローカルの信頼するアプリケーションのリストを作成します。

    ローカルの信頼するアプリケーションのリストにアプリケーションを追加するルールは、一般的なリストに追加するルールと同じです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

11. 変更内容を保存します。

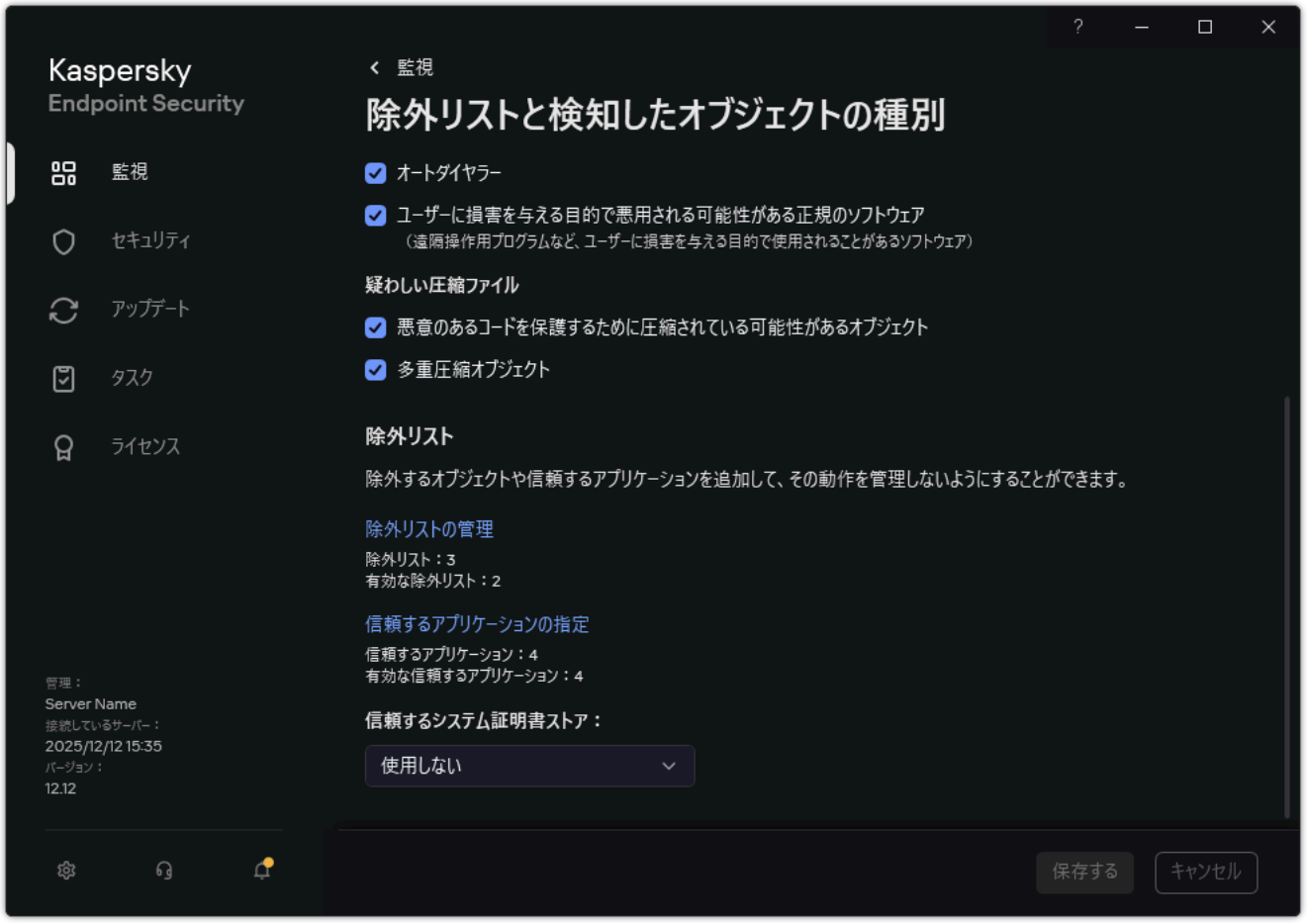
製品インターフェイスでローカルの信頼するオブジェクトを作成する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。

3. ［**除外リスト**］セクションで、［**除外リストの管理**］をクリックします。

信頼するオブジェクトの設定がコンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトが禁止されている場合（[**ローカルの除外リストの使用を許可する**]チェックボックスがオフ）は、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。



除外リストの設定

4. [**追加**]をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも1つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **リストから除外を選択してください**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するオブジェクト*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するオブジェクトが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するオブジェクトを選択する必要があります。

   新しい信頼するオブジェクトを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、[**新しい除外**]オプションを選択します。

5. ファイルまたはフォルダーをスキャンから除外する場合は、[**参照**]をクリックしてファイルまたはフォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

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

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

  ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「?:\Users*\Folder\」と入力できます。

  ネットワークフォルダーを除外できます。これを行うには、ネットワークフォルダーのパスを手動で入力します（例：\\Network Share*）。

6. 特定のオブジェクトをスキャンから除外する場合は、［**検知するオブジェクトの種別**］フィールドで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（例：「Email-Worm」、「Rootkit」、「RemoteAdmin」）。

   任意の 1 文字を置き換える「?」と複数の文字を置き換える「*」を使用してマスクを使用することができます。たとえば、マスク「Client*」を使用すると、「Client-IRC」、「Client-P2P」および「Client-SMTP」がスキャンから除外されます。

7. 個別のファイルをスキャンから除外する場合は、［**オブジェクトハッシュ**］フィールドにファイルのハッシュを入力します。

   ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

8. ［**保護機能**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

9. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

10. 信頼するオブジェクトのステータスに［**有効**］を選択します。

11. ［**追加する**］をクリックします。

    新しい信頼するオブジェクトがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼するオブジェクトを無効にできます。

12. 変更内容を保存します。

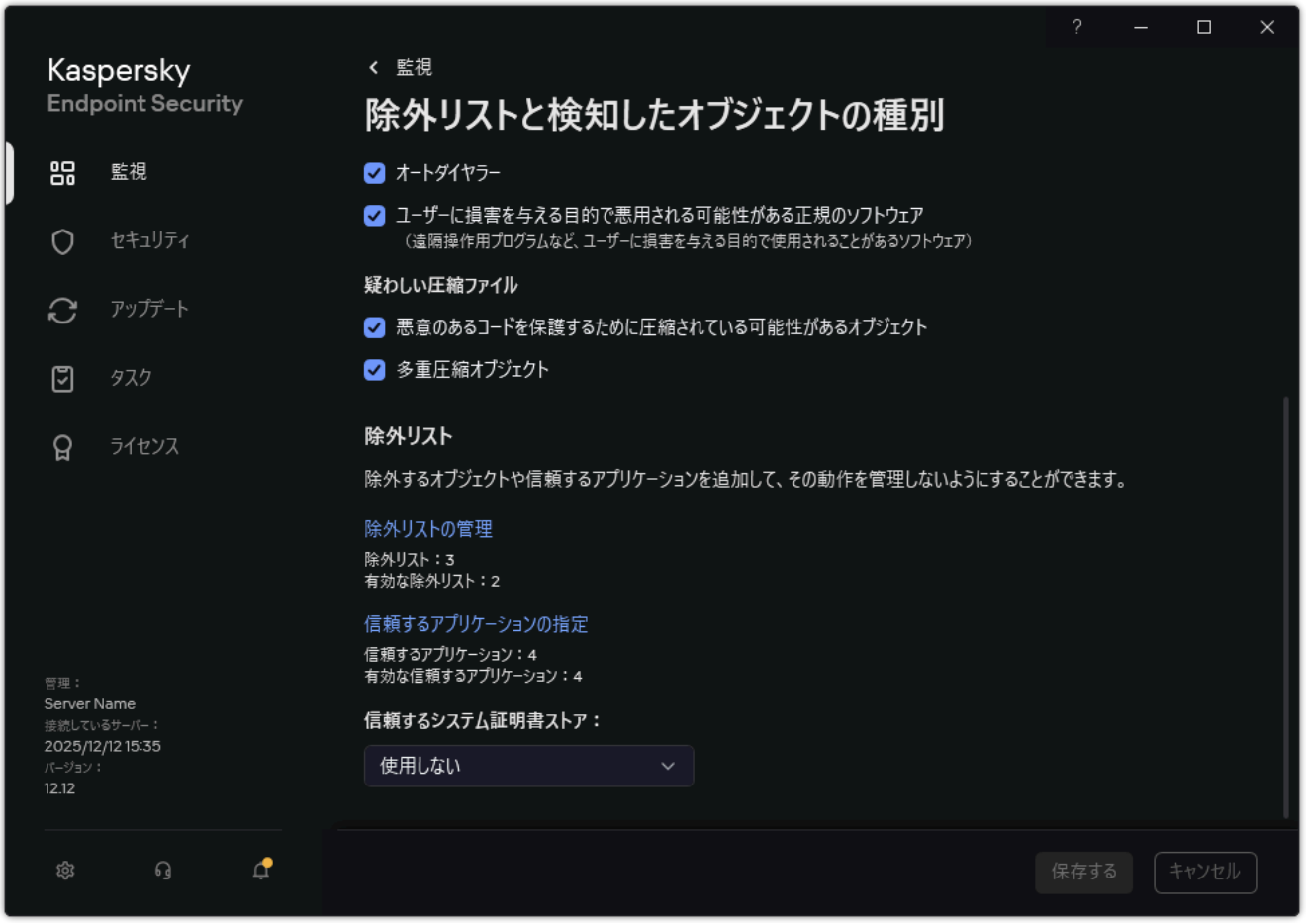


除外リスト

製品インターフェイスでローカルの信頼するアプリケーションにアプリケーションを追加する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。
3. ［**除外リスト**］セクションで、［**信頼するアプリケーションの指定**］をクリックします。

信頼するアプリケーションの設定が管理者によってコンソールでブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するアプリケーションが禁止されている場合（[**ローカルの信頼するアプリケーションの使用を許可する**] チェックボックスがオフ）は、すべての信頼するアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。



除外リストの設定

4. [**追加**] をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも1つカテゴリに追加します。
   - **新しい除外**：Kaspersky Endpoint Security は新しい信頼するアプリケーションをリストのルートに追加します。
   - **リストから除外を選択**：SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager で Kaspersky Endpoint Security を素早く設定するために、本製品には*設定済みの信頼するアプリケーション*が含まれています。また、Citrix や VMware の仮想環境におけるアプリケーションの設定をサポートするために設定済みの信頼するアプリケーションが追加されました。保護対象サーバーの目的に応じて、設定済みの信頼するアプリケーションを選択する必要があります。

   新しい信頼するアプリケーションを特定のカテゴリに追加するには、そのカテゴリの横にあるチェックボックスをオンにして、[**新しい除外**] オプションを選択します。

5. 信頼の基準を選択します。

   - **ディスク上のプロセスの完全パスを使用して信頼済みと判断する**：信頼するアプリケーションの実行ファイルのパスを入力します。

     Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

Kaspersky Endpoint Security は、信頼するアプリケーションのファイル名を、大文字と小文字を区別して扱います。入力したファイル名の大文字と小文字が間違っていると、Kaspersky Endpoint Security は、信頼するアプリケーションを認識しません。

- **プロセスファイルのハッシュを使用して信頼済みと判断する**

Kaspersky Endpoint Security は環境変数をサポートしており、本製品のローカルインターフェイスでパスを変換します。たとえば、ファイルパス「`%userprofile%\Documents\File.exe`」、「`C:\Users\Fred123\Documents\File.exe`」がユーザー「Fred123」の本製品のローカルインターフェイスに追加されたとします。結果、Kaspersky Endpoint Security は信頼するアプリケーション「`File.exe`」を別のユーザーに対して無視します。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

6. 信頼するアプリケーションのプロパティウィンドウで、詳細設定を指定します。

7. ［OK］をクリックします。

新しい信頼するアプリケーションがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

8. 変更内容を保存します。



信頼するアプリケーションのリスト

信頼ゾーンでのエクスポート / インポート

*信頼ゾーン*は Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。信頼ゾーンは、*信頼するオブジェクト*と*信頼するアプリケーション*の 2 つのリストから構成されます。これらのリストは、XML ファイルまたはその他の形式にエクスポートすることができます。これにより、例えば同じ種別の多数の除外リストをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストおよび信頼するアプリケーションのリストのバックアップをとったり、別のサーバーにリストを移行することができます。

本製品は、*除外リスト*のエクスポートおよびインポートに次の形式を使用します：

- XML： 管理コンソール（MMC）、Web コンソール、Cloud コンソールで利用可能です。
- DAT：管理コンソール（MMC）へのインポートにのみ使用できます。本製品の以前のバージョンとの互換性を保つためにこの形式が採用されています。Web コンソールに除外リストを移行する際には、管理コンソール（MMC）で DAT ファイルを XML ファイルに変換することができます。
- CSV は本製品のローカルインターフェイスでのみ使用可能です。

Kaspersky Endpoint Security は*信頼するアプリケーションのリスト*のインポートおよびエクスポートに XML 形式のファイルを使用します。

管理コンソール（MMC）で信頼ゾーンをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
4. ［**信頼するオブジェクトとアプリケーション**］で、エクスポートまたはインポートする信頼ゾーンのコンポーネントを選択します（［**信頼するオブジェクト**］または［**信頼するアプリケーション**］）。
5. ［**設定**］をクリックします。
6. ルールのリストをエクスポートするには：
   a. エクスポートする除外リストを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
      除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。
   b. → ［**エクスポート**］を選択します。
   c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. ファイルを保存します。

Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。Kaspersky Endpoint Security では、除外リストの DAT ファイルへのエクスポートもサポートされています。



信頼するアプリケーションのリスト

7. 除外リストをインポートするには：

a. → [**インポート**] を選択します。

b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

c. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。Kaspersky Endpoint Security では、除外リストの DAT ファイルからのインポートもサポートされています。

8. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで信頼ゾーンをエクスポートまたはインポートする方法

1. Web コンソールのメインウィンドウで、[**アセット（デバイス）**] → [**ポリシーとプロファイル**] の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. [**アプリケーション設定**] タブを選択します。

4. [**信頼ゾーン**] に移動します。

5. ルールのリストをエクスポートするには：

   a. ［**マルウェアスキャンの除外リスト**］リンクをクリックします。

   b. エクスポートする除外リストを選択します。

   c. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーに除外リストを JSON ファイルでエクスポートします。

6. 信頼するアプリケーションのリストをエクスポートするには：

   a. エクスポート対象の信頼するアプリケーションを選択します。

   b. → ［**エクスポート**］を選択します。

      Kaspersky Endpoint Security は既定のダウンロードフォルダーに信頼するアプリケーションのリストを JSON ファイルでエクスポートします。

7. 除外リストをインポートするには：

   a. ［**マルウェアスキャンの除外リスト**］リンクをクリックします。

   b. → ［**インポート**］を選択します。

      表示されたウィンドウで、除外リストをインポートする JSON ファイルを選択します。

   c. ファイルを開きます。

      コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 信頼するアプリケーションのリストをインポートするには：

   a. ［**アプリケーション**］リンクをクリックします。

   b. → ［**インポート**］を選択します。

      表示されたウィンドウで、信頼するアプリケーションのリストをインポートする JSON ファイルを選択します。

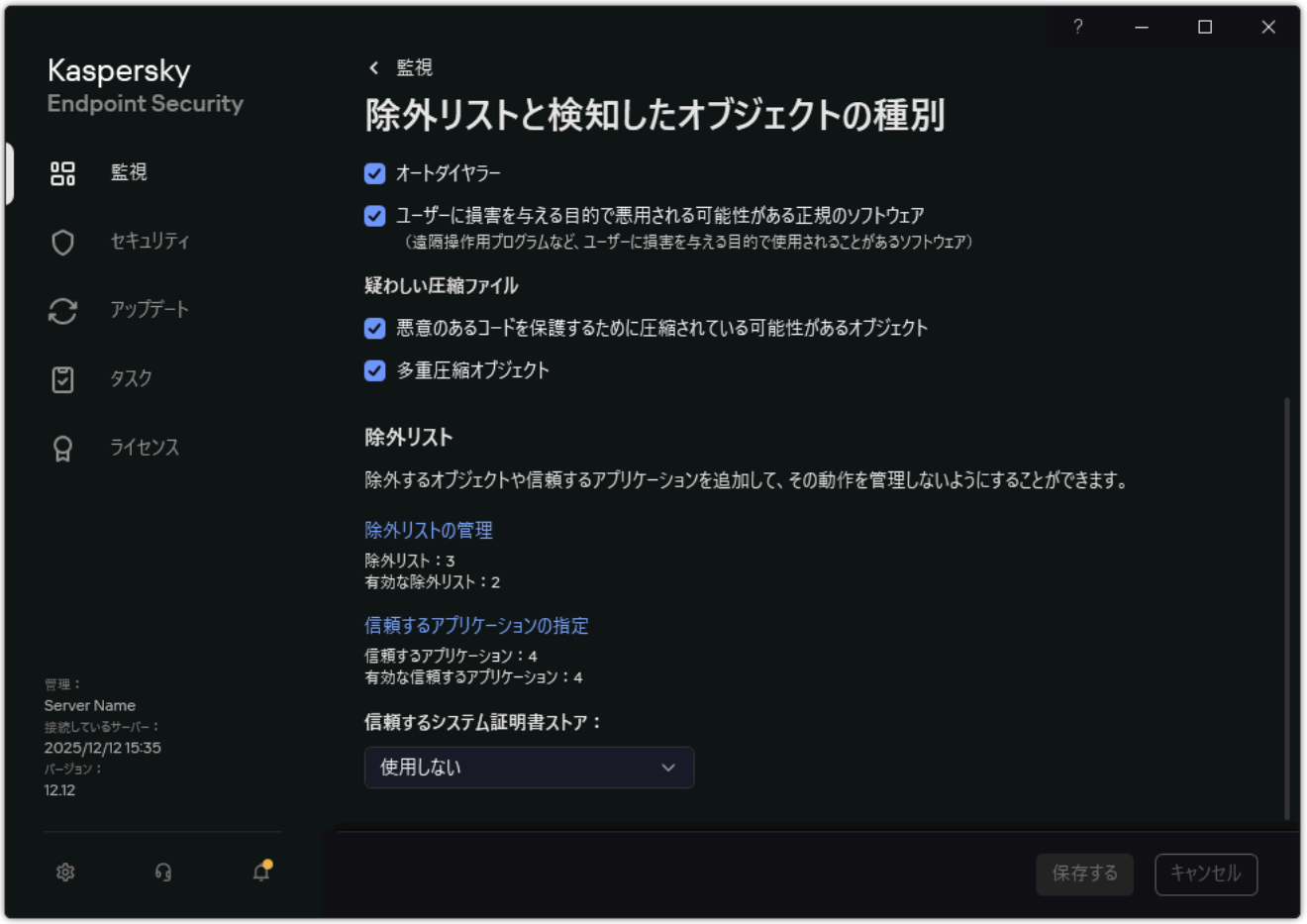
   c. ファイルを開きます。

      コンピューターに信頼するアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

9. 変更内容を保存します。

製品インターフェイスで信頼ゾーンをエクスポートまたはインポートする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。



除外リストの設定

3. ルールのリストをエクスポートするには：
   a. ［**除外リスト**］セクションで、［**除外リストの管理**］をクリックします。
   b. エクスポートする除外リストを選択します。
   c. ［**エクスポート**］をクリックします。
   d. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。
   e. 表示されたウィンドウで、除外リストをエクスポートする CSV ファイルの名前とそのファイルを保存するフォルダーを指定します。

f. ファイルを保存します。

Kaspersky Endpoint Security は、除外リスト全体を CSV ファイルにエクスポートします。



除外リスト

4. 信頼するアプリケーションのリストをエクスポートするには：

a. ［**除外リスト**］セクションで、［**信頼するアプリケーションの指定**］をクリックします。

b. エクスポート対象の信頼するアプリケーションを選択します。

c. ［**エクスポート**］をクリックします。

d. 選択した信頼するアプリケーションのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。

e. 表示されたウィンドウで、信頼するアプリケーションのリストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

f. ファイルを保存します。

Kaspersky Endpoint Security は、信頼するアプリケーションのリスト全体を XML ファイルにエクスポートします。



信頼するアプリケーションのリスト

5. 除外リストをインポートするには：

a. ［**除外リスト**］セクションで、［**除外リストの管理**］をクリックします。

b. ［**インポート**］をクリックします。

c. 表示されたウィンドウで、除外リストをインポートする CSV ファイルを選択します。

d. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、CSV ファイルから新しいエントリを追加するよう要求されます。

6. 信頼するアプリケーションのリストをインポートするには：

a. ［**除外リスト**］セクションで、［**信頼するアプリケーションの指定**］をクリックします。

b. ［**インポート**］をクリックします。

c. 表示されたウィンドウで、信頼するアプリケーションのリストをインポートする XML ファイルを選択します。

d. ファイルを開きます。

コンピューターに信頼するアプリケーションのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

信頼できるデジタル署名によるアプリケーションの処理

システム証明書ストアを使用することで、信頼されるデジタル署名で署名されたアプリケーションをスキャンから除外できます。Kaspersky Endpoint Security はこのようなアプリケーションを*信頼済みグループ*に割り当てます。

管理コンソール（MMC）で信頼するシステム証明書ストアの使用を開始する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
4. ［**信頼するシステム証明書ストア**］ブロックで、［**信頼するシステム証明書ストアを使用**］をオンにします。
5. ドロップダウンリストで、信頼するシステムストアを選択します。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールで信頼するシステム証明書ストアの使用を開始する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。
4. ［**信頼ゾーン**］に移動します。
5. 表示されたウィンドウで、［**信頼済み証明書**］をクリックします。
6. 表示されたウィンドウで、［**信頼するシステム証明書ストアを使用**］をオンにします。
7. 信頼するシステムストアを選択します。
8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

製品インターフェイスで信頼するシステム証明書ストアの使用を開始する方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。
3. ［**信頼するシステム証明書ストア**］で、信頼するシステムストアを選択します。
4. 変更内容を保存します。

補足資料：設定済みの信頼するオブジェクトとアプリケーション

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。

設定済みの信頼するオブジェクトとアプリケーションを次の方法で選択します：

- 本製品のインストール。
  - ウィザードを使用したローカルへの製品のインストール
  - インストールパッケージのプロパティ
- ポリシーの設定。
  - 新規ポリシーウィザード
  - ポリシーのプロパティ：信頼するオブジェクトとアプリケーション

SQL サーバー

Kaspersky Endpoint Security を SQL サーバーにインストールする場合、設定済みの除外リストと信頼するアプリケーションから信頼ゾーンを作成してサーバーの動作が干渉されないようにする必要があります。

設定済みの信頼するオブジェクト

パス	SQL のバージョン
`%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA\*.mdf`	2012 2014 2016 2017 2019 2022
`%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012

パス	SQL のバージョン
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange サーバー

Kaspersky Endpoint Security を Microsoft Exchange サーバーにインストールする場合、設定済みの除外リストと信頼するアプリケーションから信頼ゾーンを作成して、サーバーの動作が妨げられないようにする必要があります。

設定済みの信頼するオブジェクト

パス	Microsoft Exchange のバージョン
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019

パス	Microsoft Exchange のバージョン
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

設定済みの信頼するアプリケーション

パス	Microsoft Exchange のバージョン
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

設定済みの信頼するオブジェクト

パス	System Center Configuration Manager のバージョン
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Kaspersky Endpoint Security を Citrix の仮想環境にインストールする場合、設定済みの除外リストと信頼するアプリケーションから信頼ゾーンを作成して、サーバーの動作が妨げられないようにする必要があります。

設定済みの信頼するオブジェクト

パス
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys

パス
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%UserProfile%\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

設定済みの信頼するアプリケーション

パス	Citrix ソリューション
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops

パス	Citrix ソリューション
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace アプリ

パス	Citrix ソリューション
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace アプリ
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace アプリ
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Kaspersky Endpoint Security を VMware の仮想環境にインストールする場合、設定済みの信頼するアプリケーションから信頼ゾーンを作成して、サーバーの動作が妨げられないようにする必要があります。

パス	VMware ソリューション
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon

パス	VMware ソリューション
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

バックアップの管理

*バックアップ保管領域*には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。*バックアップコピー*は、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルのバックアップコピーは、フォルダー `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。

駆除中にファイルの整合性を維持できない場合があります。駆除後に、駆除されたファイルに含まれている重要な情報の一部または全体にアクセスできなくなった場合、バックアップコピーからファイルを元のフォルダーに復元することを試みることができます。

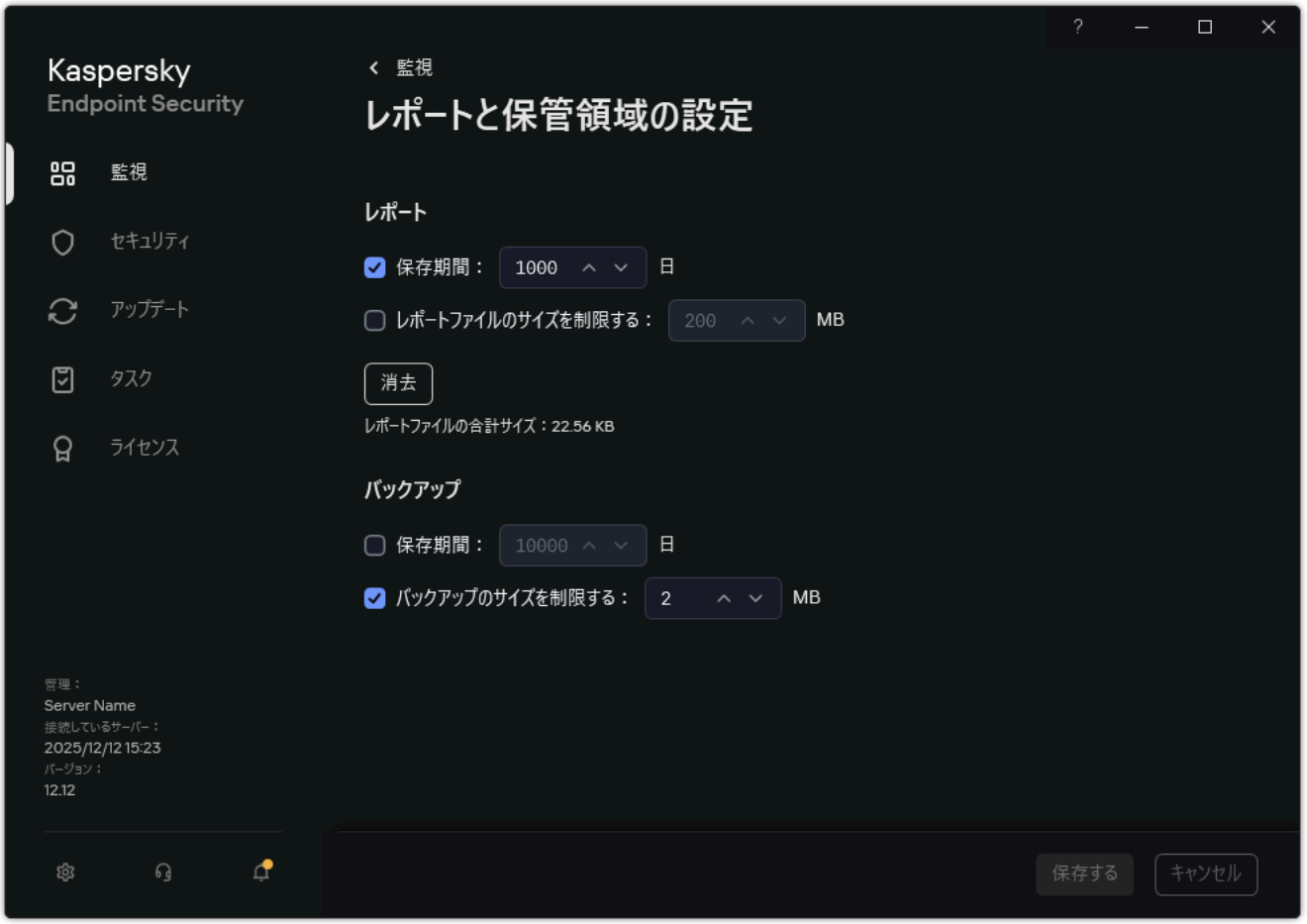
Kaspersky Endpoint Security が Kaspersky Security Center の管理下で動作している場合、ファイルのバックアップコピーが Kaspersky Security Center の管理サーバーに送信される場合があります。Kaspersky Security Center でのファイルのバックアップコピーの管理について詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。

バックアップファイルの最大保管期間の設定

既定では、最大保管期間は 30 日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。

バックアップファイルの最大保管期間を設定するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウの［**全般設定**］で、［**レポートと保管領域**］をクリックします。



バックアップ設定

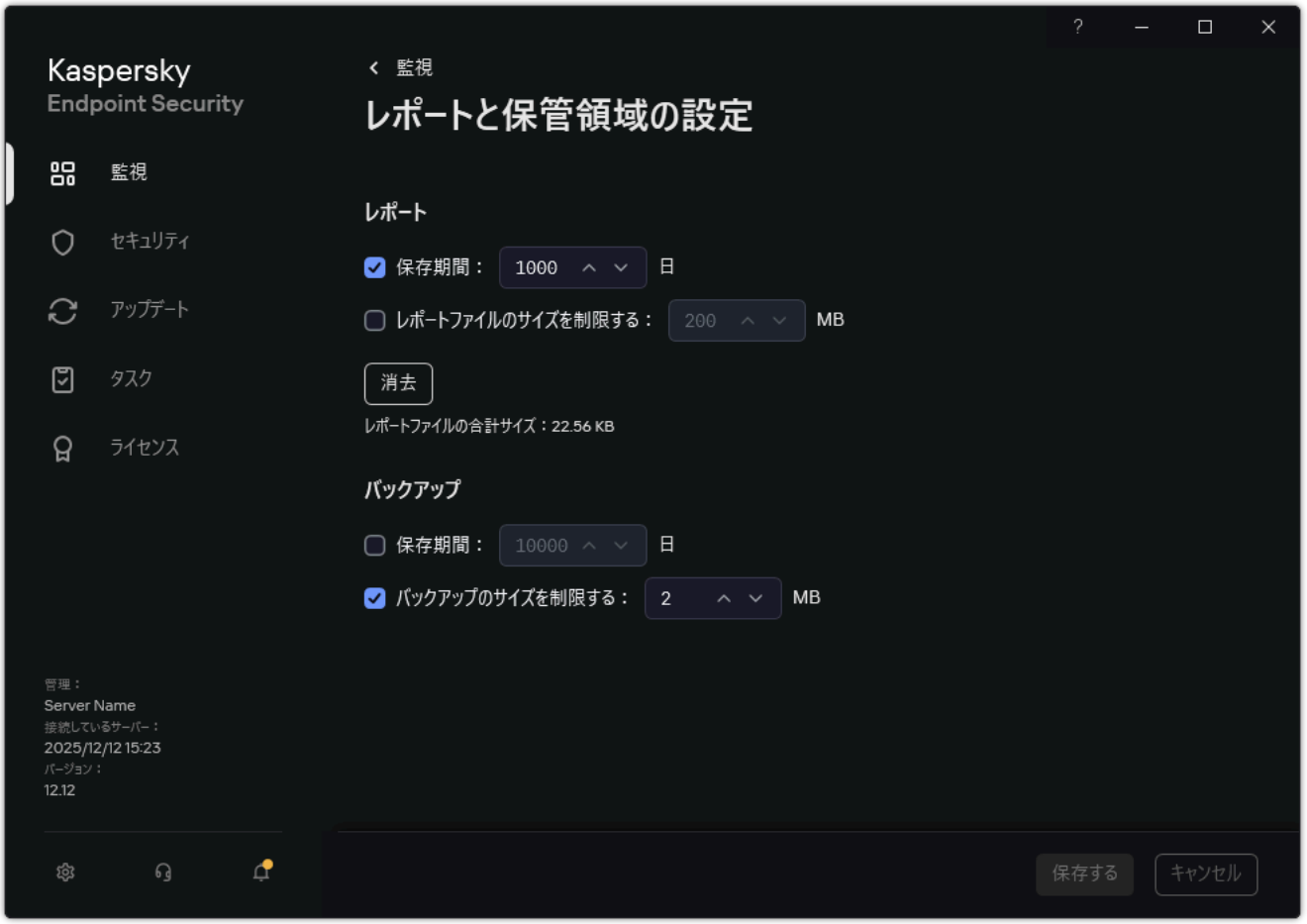
3. バックアップ内のコピーの保管期限を設定する場合は、［**バックアップ**］ブロックで［**保存期間**］チェックボックスをクリックします。バックアップ内コピーのの最大保管期間を入力します。
4. 変更内容を保存します。

バックアップの最大サイズの設定

バックアップの最大サイズを設定できます。既定では、バックアップのサイズは制限されていません。最大サイズに到達すると、最も古いファイルがバックアップから自動的に削除されます。

バックアップの最大サイズを設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウの［**全般設定**］で、［**レポートと保管領域**］をクリックします。



バックアップ設定

3. ［**バックアップ**］ブロックで、［**バックアップのサイズを制限する**］をオンにします。このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。既定では、最大サイズは 1024 MB です。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Endpoint Security は最も古いファイルを保管領域から自動的に削除します。
4. 変更内容を保存します。

バックアップからのファイルの復元

悪意のあるコードがファイル内で検知された場合、Kaspersky Endpoint Security はそのファイルをブロックし、「*未処理*」ステータスを割り当て、コピーをバックアップに保存してから駆除を試みます。ファイルの駆除に成功すると、ファイルのバックアップコピーのステータスが「*駆除済み*」に変わります。ファイルは元のフォルダーで利用可能になります。ファイルを駆除できない場合、元のフォルダーからファイルを削除します。バックアップコピーから元のフォルダーにファイルを復元できます。

［*コンピューターの再起動後に削除*］ステータスのファイルは復元できません。コンピューターを再起動すると、ステータスが「*駆除済み*」または「*削除済み*」に変更されます。バックアップコピーから元のフォルダーにファイルを復元することもできます。

Windows ストアアプリの一部であるファイルに悪意のあるコードが検知されると、Kaspersky Endpoint Security は即座にそのファイルを削除します。ファイルのコピーがバックアップに移動されることはありません。Windows ストアアプリの整合性を復元するには、オペレーティングシステムの適切なツールを使用します（Windows ストアアプリの復元の詳細については、Microsoft Windows のヘルプファイルを参照してください）。

ファイルのバックアップコピーはテーブル形式で表示されます。ファイルのバックアップコピーでは、ファイルの元のフォルダーのパスが表示されます。ファイルの元のフォルダーのパスには個人情報が含まれる場合があります。

同じフォルダーにある名前が同一で内容が異なる複数のファイルがバックアップに移動された場合、最後にバックアップに移動されたファイルのみを復元できます。

バックアップからファイルを復元するには：

1. 製品のメインウィンドウの［**監視**］で、［**バックアップ**］をクリックします。
2. バックアップにあるファイルのリストが表示されます。リストから復元したいファイルを選択して［**復元**］をクリックします。

   選択したバックアップコピーのファイルが元のフォルダーに復元されます。



バックアップ

バックアップからのファイルのバックアップコピーの削除

Kaspersky Endpoint Security は、製品の設定で指定した保管期間を過ぎると、バックアップコピーのステータスに関係なく、ファイルのバックアップコピーをバックアップから自動的に削除します。また、ファイルのコピーは、バックアップから手動で削除することもできます。

バックアップからファイルのバックアップコピーを削除するには：

1. 製品のメインウィンドウの［**監視**］で、［**バックアップ**］をクリックします。
2. バックアップにあるファイルのリストが表示されます。リストから、バックアップから削除するファイルを選択して［**削除**］をクリックします。

選択したバックアップファイルがバックアップから削除されます。



バックアップ

通知サービス

Kaspersky Endpoint Security の動作中には、あらゆる種類のイベントが発生します。イベントの通知には、単にお知らせのものもあれば重要な情報が含まれるものもあります。たとえば、定義データベースと製品機能のアップデートが正常に完了したことを通知したり、修復が必要なコンポーネントエラーを記録したりします。

Kaspersky Endpoint Security では、Microsoft Windows のアプリケーションログや Kaspersky Endpoint Security のイベントログの動作のイベントに関する情報の記録をサポートします。

Kaspersky Endpoint Security は次の方法で通知を配信します：

- Microsoft Windows タスクバーの通知領域でポップアップ通知を表示する
- メールで送信する

イベント通知の配信を設定できます。通知配信の方法はイベントの種類ごとに設定します。

イベントのテーブルを使用して通知サービスを設定する場合は、次のことができます：

- 通知サービスイベントを列の値または絞り込み条件でフィルター処理する。
- 通知サービスイベントの検索機能を使用する。
- 通知サービスイベントを並べ替える。
- 通知サービスイベントのリストに表示される順番と列を変更する。

イベントログ設定の指定

イベントログ設定を指定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
3. ［**通知**］ブロックの［**通知の設定**］をクリックします。

   Kaspersky Endpoint Security のコンポーネントとタスクがウィンドウの左側に表示されます。ウィンドウの右側に、選択したコンポーネントまたはタスクで発生したイベントが表示されます。

   イベントには、以下のユーザーデータが含まれる場合があります：

   - Kaspersky Endpoint Security がスキャンしたファイルのパス
   - Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
   - Microsoft Windows のユーザー名
   - ユーザーが開いた Web ページのアドレス
4. ウィンドウの左側で、イベントログを設定するコンポーネントまたはタスクを選択します。

5. ［**ローカルレポートに保存**］および［**Windows イベントログに保存**］列で、該当するイベントのチェックボックスをオンにします。

   ［**ローカルレポートに保存**］列のチェックボックスがオンになっているイベントは、アプリケーションログに表示されます。［**Windows イベントログに保存**］列のチェックボックスがオンになっているイベントは、`Application` チャネルの Windows ログに表示されます。

6. 変更内容を保存します。

通知の表示と配信の設定

通知の表示と配信を設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
3. ［**通知**］ブロックの［**通知の設定**］をクリックします。

   Kaspersky Endpoint Security のコンポーネントとタスクがウィンドウの左側に表示されます。ウィンドウの右側に、選択したコンポーネントまたはタスクで発生したイベントが表示されます。

   イベントには、以下のユーザーデータが含まれる場合があります：

   - Kaspersky Endpoint Security がスキャンしたファイルのパス
   - Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
   - Microsoft Windows のユーザー名
   - ユーザーが開いた Web ページのアドレス

4. ウィンドウの左側で、通知の配信を設定するコンポーネントまたはタスクを選択します。
5. ［**画面で通知**］列で、該当するイベントの横のチェックボックスをオンにします。

   選択したイベントに関する情報が、Microsoft Windows タスクバーの通知領域にポップアップメッセージとして画面に表示されます。

6. ［**メールで通知**］列で、該当するイベントの横のチェックボックスをオンにします。

   メール通知配信が設定されている場合、選択したイベントに関する情報がメールで配信されます。

7. ［OK］をクリックします。
8. 通知を有効にする場合は、メール配信を設定します：

   a. ［**メール通知の設定**］をクリックします。

   b. ［**イベントを通知する**］をオンにして、［**メールで通知**］列でオンにした Kaspersky Endpoint Security イベントに関する通知の配信を有効にします。

c. メール通知の配信設定を指定してください。

d. ［**OK**］をクリックします。

9. 変更内容を保存します。

製品のステータスに関する通知領域での警告の表示設定

製品のステータスに関する警告の通知領域での表示を設定するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
3. ［**通知領域に製品のステータスを表示する**］ブロックで、Microsoft Windows の通知領域に通知を表示するイベントカテゴリの横にあるチェックボックスをオンにします。
4. 変更内容を保存します。

選択したカテゴリに属するイベントが発生すると、通知領域の製品アイコンが、警告の重要度に応じて または に変わります。

ユーザーと管理者間のメッセージ

アプリケーションコントロール、デバイスコントロール、ウェブコントロール、アダプティブアノマリーコントロールでは、Kaspersky Endpoint Security がインストールされているコンピューターを使用している LAN ユーザーが管理者にメッセージを送信できます。

次の場合に、ユーザーが LAN 管理者にメッセージを送信することがあります：

- デバイスコントロールがデバイスへのアクセスをブロックした。

  ブロックされたデバイスへのアクセスを要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの［デバイスコントロール］セクションにあります。

- アプリケーションコントロールがアプリケーションの起動をブロックした。

  ブロックされたアプリケーションの起動許可を要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの［アプリケーションコントロール］セクションにあります。

- ウェブコントロールが Web リソースへのアクセスをブロックした。

  ブロックされた Web リソースへのアクセスを要求するメッセージのテンプレートは、Kaspersky Endpoint Security のインターフェイスの［ウェブコントロール］セクションにあります。

メッセージの送信方法および使用するテンプレートは、Kaspersky Endpoint Security がインストールされているコンピューター上での Kaspersky Security Center ポリシーの実行状況、および Kaspersky Security Center 管理サーバーとの接続状況によって異なります。可能なシナリオは次のとおりです：

- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center のポリシーが実行中でない場合、ユーザーのメッセージがローカルエリアネットワークの管理者にメールで送信されます。

  本文のフィールドには、Kaspersky Endpoint Security のローカルインターフェイスで定義されたテンプレートのフィールドの値が入力されます。

- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center のポリシーが実行中の場合、標準のメッセージが Kaspersky Security Center 管理サーバーに送信されます。

  この場合、ユーザーメッセージは、Kaspersky Security Center イベント保管領域で確認できます（以下の手順を参照）。本文のフィールドには、Kaspersky Security Center のポリシーで定義されたテンプレートのフィールドの値が入力されます。

- Kaspersky Endpoint Security がインストールされているコンピューターで Kaspersky Security Center モバイルユーザーポリシーが実行中の場合、メッセージの送信方法は Kaspersky Security Center との接続状況によって異なります。

  - Kaspersky Security Center との接続が確立されている場合、標準のメッセージが Kaspersky Security Center 管理サーバーに送信されます。

  - Kaspersky Security Center との接続がない場合、ユーザーのメッセージがローカルエリアネットワークの管理者にメールで送信されます。

  どちらの場合も、本文のフィールドには Kaspersky Security Center のポリシーで定義されたテンプレートのフィールドの値が入力されます。

Kaspersky Security Center イベント保管領域にあるユーザーのメッセージを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**イベント**］タブを選択します。

   Kaspersky Security Center の作業領域に、LAN ユーザーから受信した管理者向けメッセージを含む、Kaspersky Endpoint Security の動作時に発生したすべてのイベントが表示されます。
3. イベントのフィルターを設定するには、［**イベントの抽出**］で［**ユーザー要求**］を選択します。
4. 管理者に送信するメッセージを選択します。
5. 管理コンソールの作業領域の右側にある［**イベントのプロパティウィンドウの表示**］をクリックします。

レポートの管理

レポートには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

レポートは、フォルダー「`C:\ProgramData\Kaspersky Lab\KES.12.12\Report`」に保存されます。

レポートには、以下のユーザーデータが含まれる場合があります：

- Kaspersky Endpoint Security がスキャンしたファイルのパス
- Kaspersky Endpoint Security の動作中に修正されたレジストリキーのパス
- Microsoft Windows のユーザー名
- ユーザーが開いた Web ページのアドレス

レポートのデータはテーブル形式で表示されます。テーブルの各行には、各イベントの情報が含まれます。イベント属性はテーブルの列に表示されます。特定の列は、詳細属性に入れ子にされた列を含んだ複合列です。追加の属性を表示するには、列の名前の横にある⊞ボタンをクリックします。さまざまなコンポーネントの操作中またはさまざまなタスクの実行中にログに記録されるイベントには、異なる属性セットがあります。

次のレポートを使用できます：

- **システム監査**レポート。ユーザーと製品の相互作用および一般的な製品操作で発生し、特定の Kaspersky Endpoint Security コンポーネントまたはタスクとは無関係なイベントに関する情報が含まれます。
- Kaspersky Endpoint Security コンポーネントの操作に関するレポート。
- Kaspersky Endpoint Security のタスクに関するレポート。
- **データ暗号化**レポート。データの暗号化および復号化の処理中に発生したイベントに関する情報が含まれます。

以下は、レポートで使用するイベントの重要度レベルです：

ⓘ **情報イベント**。通常は重要な情報が含まれていない参照イベントです。

⚠ **警告**。Kaspersky Endpoint Security の処理における重要な状況が反映されているので、注意が必要なイベントです。

ⓘ **緊急イベント**。Kaspersky Endpoint Security の処理上の問題やユーザーのコンピューター保護における脆弱性を示す、きわめて重大なイベントです。

レポートを処理しやすくするために、データの表示方法を次のように変更できます：

- イベントリストを各種基準でフィルタリングする。
- 検索機能を使用して、具体的なイベントを検索する。
- 選択したイベントをセクションごとに表示する。

- イベントのリストをレポートの列ごとに分類する。
- ボタンを使用して、イベントのフィルターによってグループ化されたイベントを表示または非表示にする。
- レポートに表示される列の順番と配置を変更する。

必要に応じて、生成されたレポートをテキストファイルに保存できます。Kaspersky Endpoint Security コンポーネントおよびグループに統合されたタスクに関するレポート情報を削除することもできます。

Kaspersky Endpoint Security が Kaspersky Security Center の管理下で実行されている場合、イベントに関する情報が Kaspersky Security Center 管理サーバーに転送される場合があります。詳細については、Kaspersky Security Center ヘルプを参照してください。

レポートの表示

ユーザーがレポートを表示できる場合、そのユーザーはレポートに関連するすべてのイベントを表示することもできます。

レポートを表示するには、次の手順を実行します：

1. 製品のメインウィンドウの［**監視**］で、［**レポート**］をクリックします。



レポート

2. コンポーネントとタスクのリストで、コンポーネントまたはタスクを選択します。

   ウィンドウの右側に、選択したコンポーネントまたは選択したタスクの動作の結果であるイベントのリストを含むレポートが表示されます。レポート内のイベントは、列の値で並べ替えることができます。

3. イベントの詳細な情報を表示するには、レポート内のイベントを選択します。

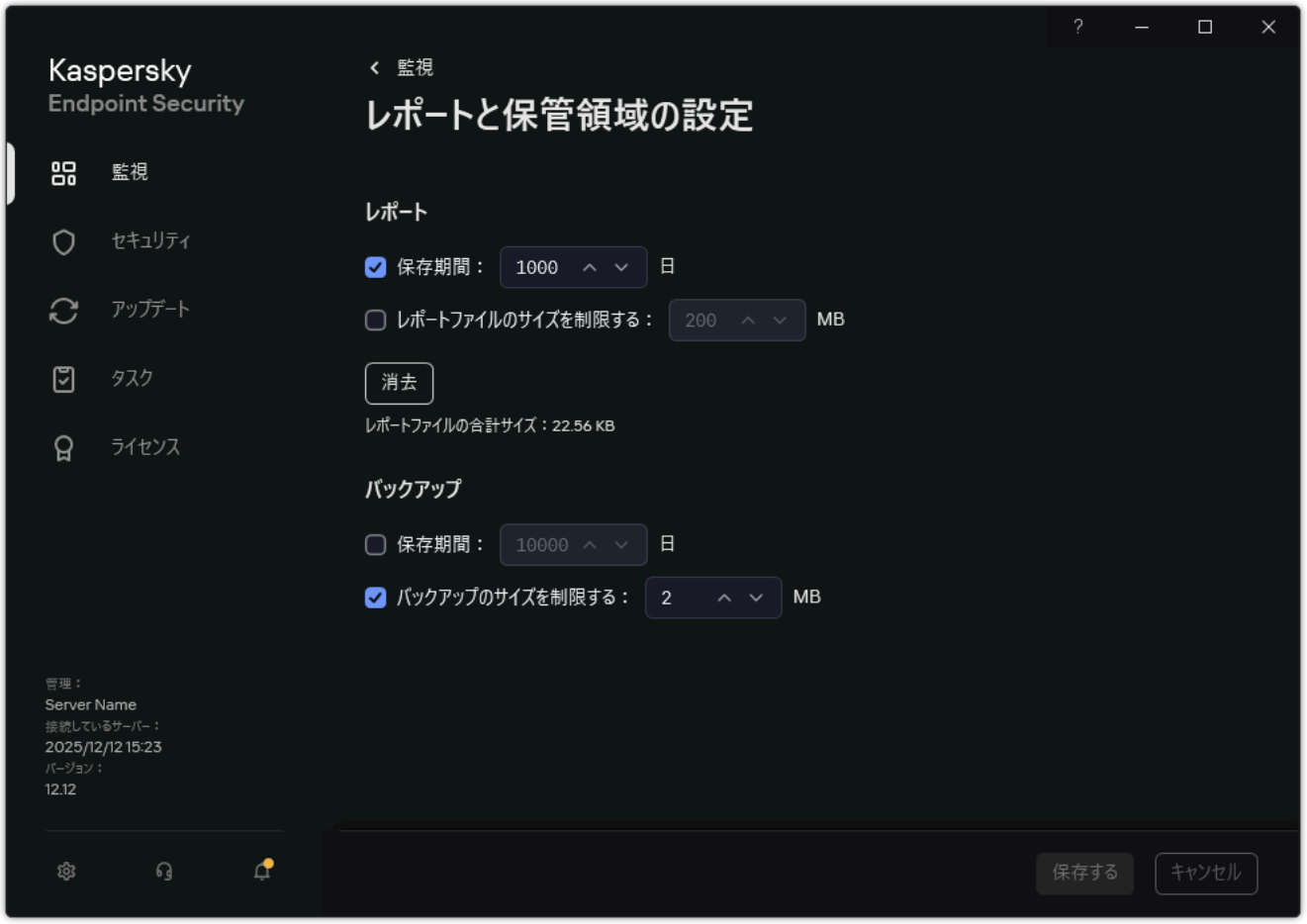
ウィンドウの下部のブロックに、イベントのサマリーが表示されます。

レポート最長保管期間の設定

既定では、Kaspersky Endpoint Security によってログに記録されるイベントに関するレポートの最長保管期間は 30 日間です。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。

レポート最長保管期間を変更するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウの［**全般設定**］で、［**レポートと保管領域**］をクリックします。



レポート設定

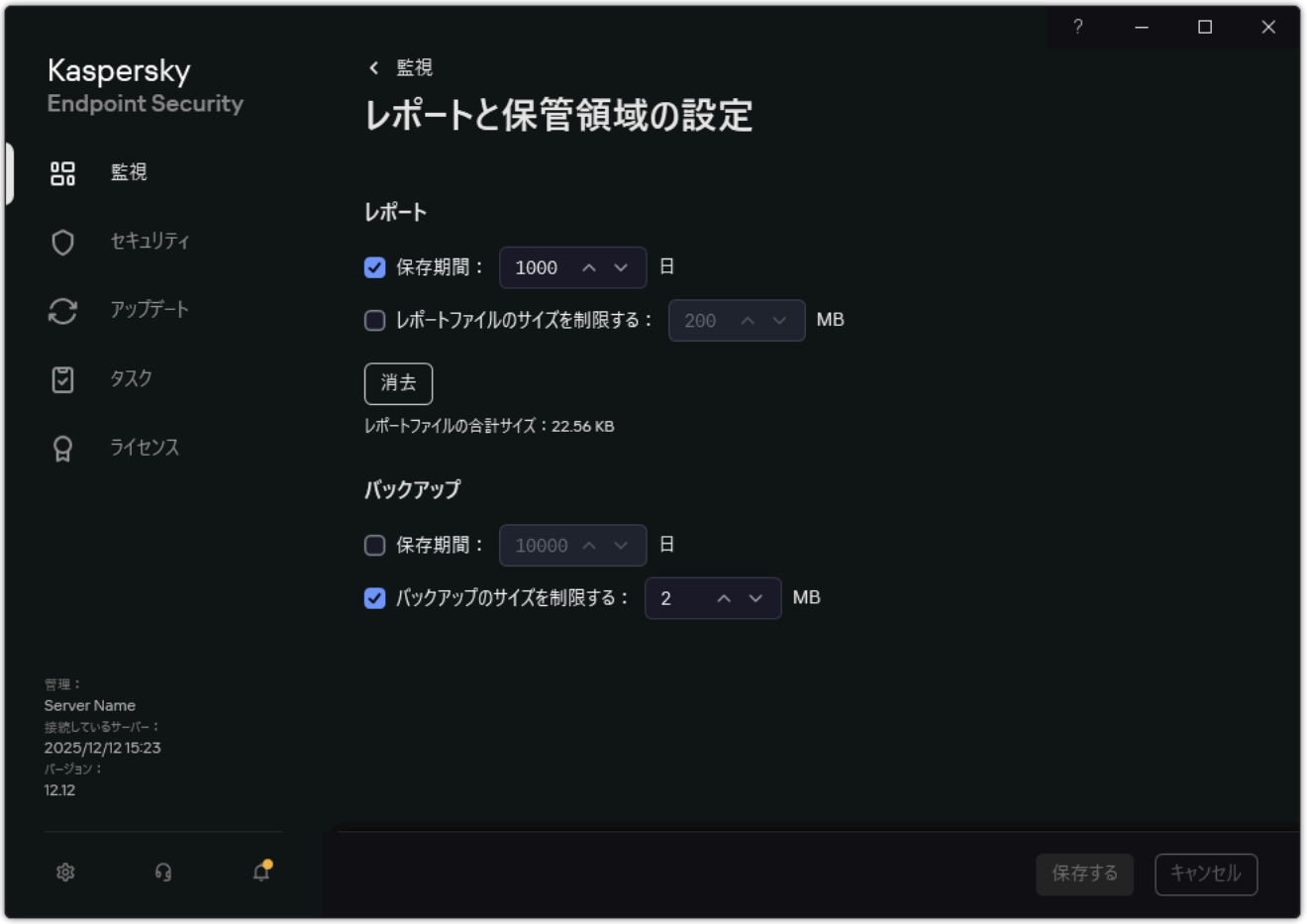
3. レポートの保管期限を設定する場合は、［**レポート**］ブロックで［**保存期間**］チェックボックスをクリックします。レポート最長保管期間を設定します。
4. 変更内容を保存します。

レポートファイルの最大サイズの設定

レポートを含むファイルの最大サイズを指定できます。既定では、レポートの最大ファイルサイズは 1024 MB です。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。

レポートファイルの最大サイズを設定するには：

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウの［**全般設定**］で、［**レポートと保管領域**］をクリックします。



レポート設定

3. レポートファイルのサイズを制限する場合は、［**レポート**］ブロックで、［**レポートファイルのサイズを制限する**］を選択します。レポートファイルの最大サイズを設定します。
4. 変更内容を保存します。

レポートのファイルへの保存

ファイルに保存したレポート内の情報の保護、特にその情報へのアクセスの管理と制限については、ユーザーが責任を負います。

生成したレポートはテキスト形式（txt）ファイルとして、または CSV ファイルとして保存できます。

Kaspersky Endpoint Security では、イベントを画面に表示されるとおり、つまり同一セットおよびシーケンスのイベント属性とともにレポートに記録します。

レポートをファイルに保存するには：

1. 製品のメインウィンドウの［**監視**］で、［**レポート**］をクリックします。



レポート

2. 表示されるウィンドウでコンポーネントまたはタスクを選択します。

   レポートがウィンドウの右側に表示されます。このレポートには、選択した Kaspersky Endpoint Security コンポーネントの操作またはタスクに関するイベントがリスト表示されます。

3. 次の方法で、レポートに表示されるデータを必要に応じて変更できます：

   - イベントをフィルター処理する
   - イベント検索を実行する
   - 列の配置を変更する
   - イベントを並べ替える

4. ウィンドウの右上にある［**レポートを保存する**］をクリックします。

5. 表示されたウィンドウで、レポートファイルの保存先フォルダーを指定します。

6. レポートファイルの名前を入力します。

7. レポートファイルの形式を TXT または CSV から選択します。

8. 変更内容を保存します。

レポートの消去

レポートから情報を削除するには：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウの［**全般設定**］で、［**レポートと保管領域**］をクリックします。



レポート設定

3. ［**レポート**］ブロックの［**消去**］をクリックします。
4. パスワードによる保護が有効な場合は、ユーザーアカウントの認証情報が求められます。ユーザーに十分な権限がなかった場合は、アカウントの認証情報が求められます。

すべてのアプリケーションコンポーネントおよびタスクのレポートがすべて削除されます。

Kaspersky Endpoint Security セルフディフェンス

セルフディフェンスは、他のアプリケーションが Kaspersky Endpoint Security の動作を妨害したり、Kaspersky Endpoint Security をコンピューターから削除したりする操作を実行できないようにします。使用できる Kaspersky Endpoint Security セルフディフェンス技術は、オペレーティングシステムが 32 ビットか 64 ビットかで異なります（下の表を参照してください）。セルフディフェンスには、パスワードによる保護と管理サーバーの接続の保護も含まれます。

*パスワードによる保護*を使用することで、ユーザーに付与された権限（例：アプリケーションの終了権限）に応じて、ユーザーが Kaspersky Endpoint Security で行える操作を制限できます。

*管理サーバーの接続の保護*は、コンピューターが信頼済みでないサーバーに不正に再接続するのを防ぎます。

Kaspersky Endpoint Security セルフディフェンス技術

技術	説明	x86 コンピューター	x64 コンピューター
セルフディフェンス機構	次の製品コンポーネントへのアクセスをブロックします： • Kaspersky Endpoint Security のインストールフォルダーにあるファイルおよび本製品のファイル • 本製品に属する項目を含むレジストリキー • 本製品が実行するプロセス	✓	✓
AM-PPL（Antimalware Protected Process Light）	Kaspersky Endpoint Security のプロセスを悪意のある処理から保護します。AM-PPL 技術について詳しくは、Microsoft の Web サイトの情報 を参照してください。 AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。	✓	✓
外部からの管理に対する防御機構	この技術は、TeamViewer または RemotelyAnywhere などの他のアプリケーションからの Kaspersky Endpoint Security へのアクセスをブロックします。	✓	–（Windows 7 以外）

セルフディフェンスの有効化と無効化

Kaspersky Endpoint Security によってハードディスクのアプリケーションファイル、メモリプロセス、システムレジストリエントリの改竄や削除が防止されます。

次の製品コンポーネントへのアクセスをブロックします：

- Kaspersky Endpoint Security のインストールフォルダーにあるファイルおよび本製品のファイル
- 本製品に属する項目を含むレジストリキー
- 本製品が実行するプロセス

既定では、Kaspersky Endpoint Security のセルフディフェンス機構は有効です。

管理コンソール（MMC）でセルフディフェンスを有効または無効にする方法

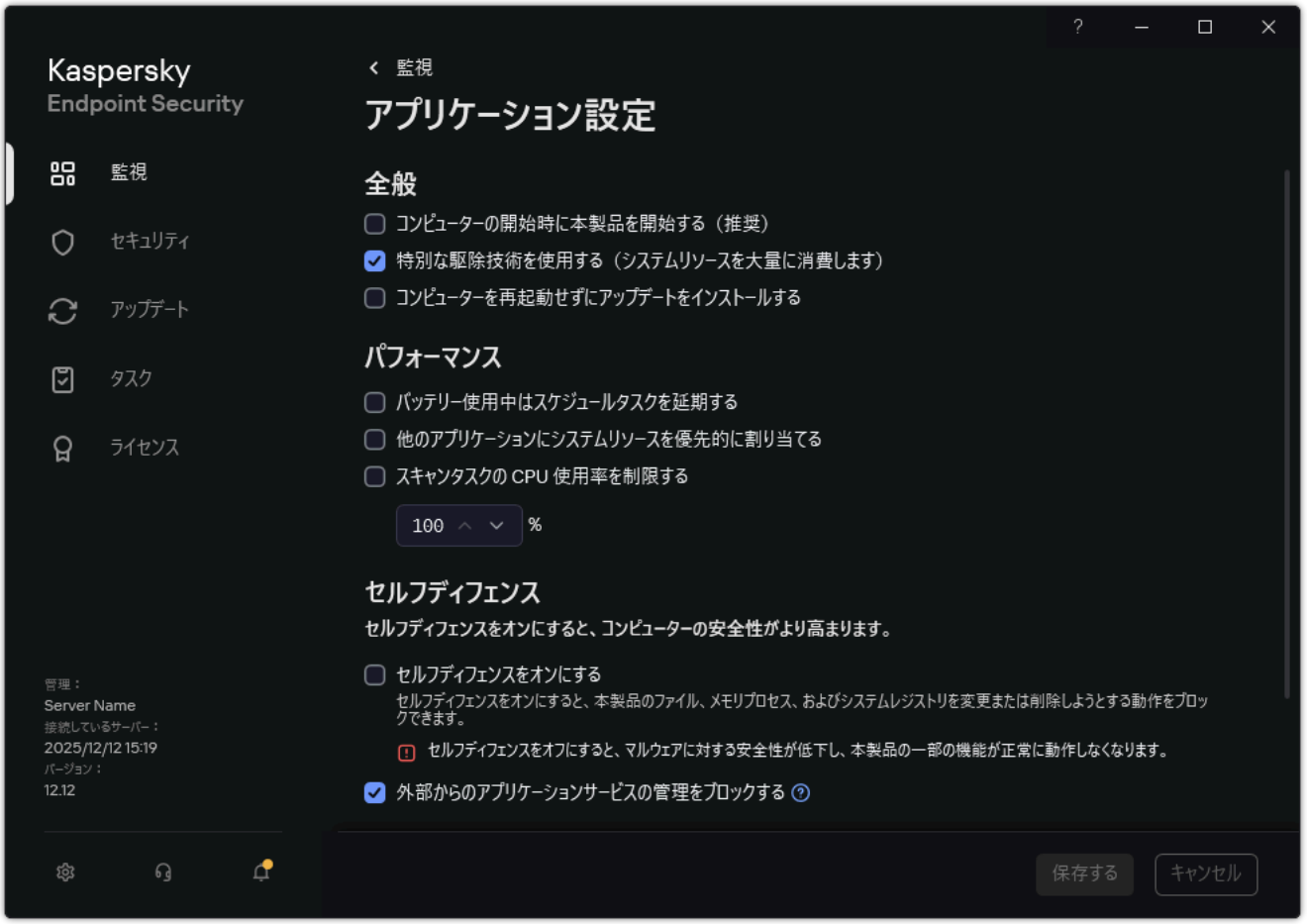
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. ［**セルフディフェンスを有効にする**］を使用してセルフディフェンスを有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールでセルフディフェンスを有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**セルフディフェンス**］に移動します。
5. ［**セルフディフェンスは有効です**］トグルスイッチを使用してセルフディフェンスを有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでセルフディフェンスを有効または無効にする方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**セルフディフェンスをオンにする**］を使用してセルフディフェンスを有効または無効にします。
4. 変更内容を保存します。

AM-PPL のサポートの有効化と無効化

Kaspersky Endpoint Security は Microsoft の Antimalware Protected Process Light 技術（以降、「AM-PPL」）をサポートします。AM-PPL は、Kaspersky Endpoint Security のプロセスを悪意のある処理（アプリケーションの終了など）から保護します。AM-PPL が実行を許可するのは信頼するプロセスのみです。Kaspersky Endpoint Security のプロセスは Windows のセキュリティ要件に従って署名されているため、信頼するプロセスとして扱われます。AM-PPL 技術について詳しくは、Microsoft の Web サイトの情報を参照してください。既定では、AM-PPL 技術が有効です。

また、Kaspersky Endpoint Security には製品のプロセスを保護するための機構が組み込まれています。AM-PPL のサポートにより、プロセスのセキュリティ機能をオペレーティングシステムに委任できます。したがって、本製品の動作速度を向上し、コンピューターリソースの消費量を削減できます。

AM-PPL 技術は、継続的に使用してください。AM-PPL は、オペレーティングシステム保護の重要なコンポーネントです。AM-PPL のサポートを無効にすると、Kaspersky Endpoint Security の一部の機能が動作しなくなる可能性があります（たとえば、本製品と Windows Security Center の連携）。AM-PPL のサポートの無効化は、トラブルシューティングの目的でのみ、個別のテスト環境において許可されます。

AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。

AM-PPL 技術を有効または無効にするには：

1. 製品のセルフディフェンス機構を無効にします。

   セルフディフェンス機構は、AM-PPL の状態の変更を含めて、コンピューターメモリ内で本製品のプロセスが変更されたり削除されたりしないようにします。

2. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。

3. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

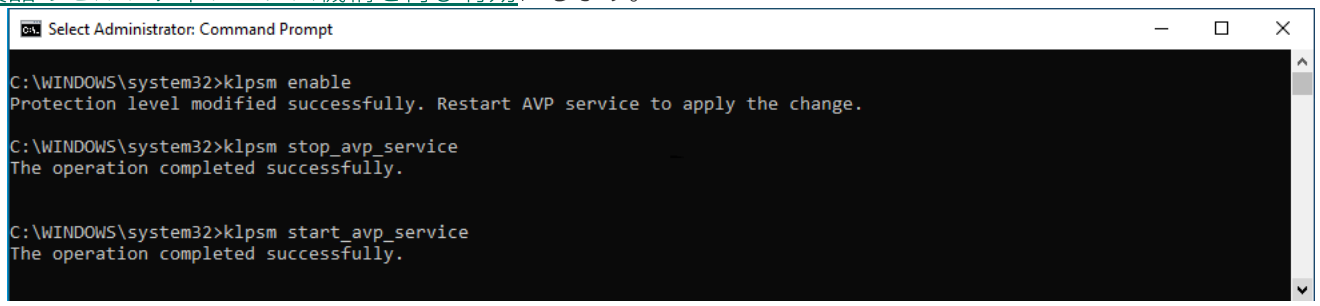
   製品のインストール中に、システム変数 %PATH% を使用して実行ファイルへのパスを追加することができます。

4. コマンドラインに以下のように入力します：

   - `klpsm.exe enable` – AM-PPL 技術のサポートを有効にします（次の図を参照）。
   - `klpsm.exe disable` – AM-PPL 技術のサポートを無効にします。

5. Kaspersky Endpoint Security を再起動します。

6. 製品のセルフディフェンス機構を再び有効にします。



AM-PPL 技術のサポートの有効化

外部からの管理に対するアプリケーションサービスの保護

外部からの管理に対するアプリケーションサービスの保護は、ユーザーや他のアプリケーションが Kaspersky Endpoint Security サービスを停止しようとする試みをブロックします。保護機能により、次のサービスの操作が確保されます：

- Kaspersky Endpoint Security サービス（AVP.KES.12.12）
- Kaspersky Seamless Update Service サービス（AVPSUS.KES.12.12）

コマンドラインから本製品を停止するには、Kaspersky Endpoint Security サービスの外部からの管理に対する保護を無効にします。

外部からのアプリケーションサービスの管理は、AM-PPL 技術をサポートしていないコンピューター、または AM-PPL 技術が無効になっているコンピューターでのみ許可できます。

管理コンソール（MMC）で外部からの管理に対するアプリケーションサービスの保護を有効または無効にする方法

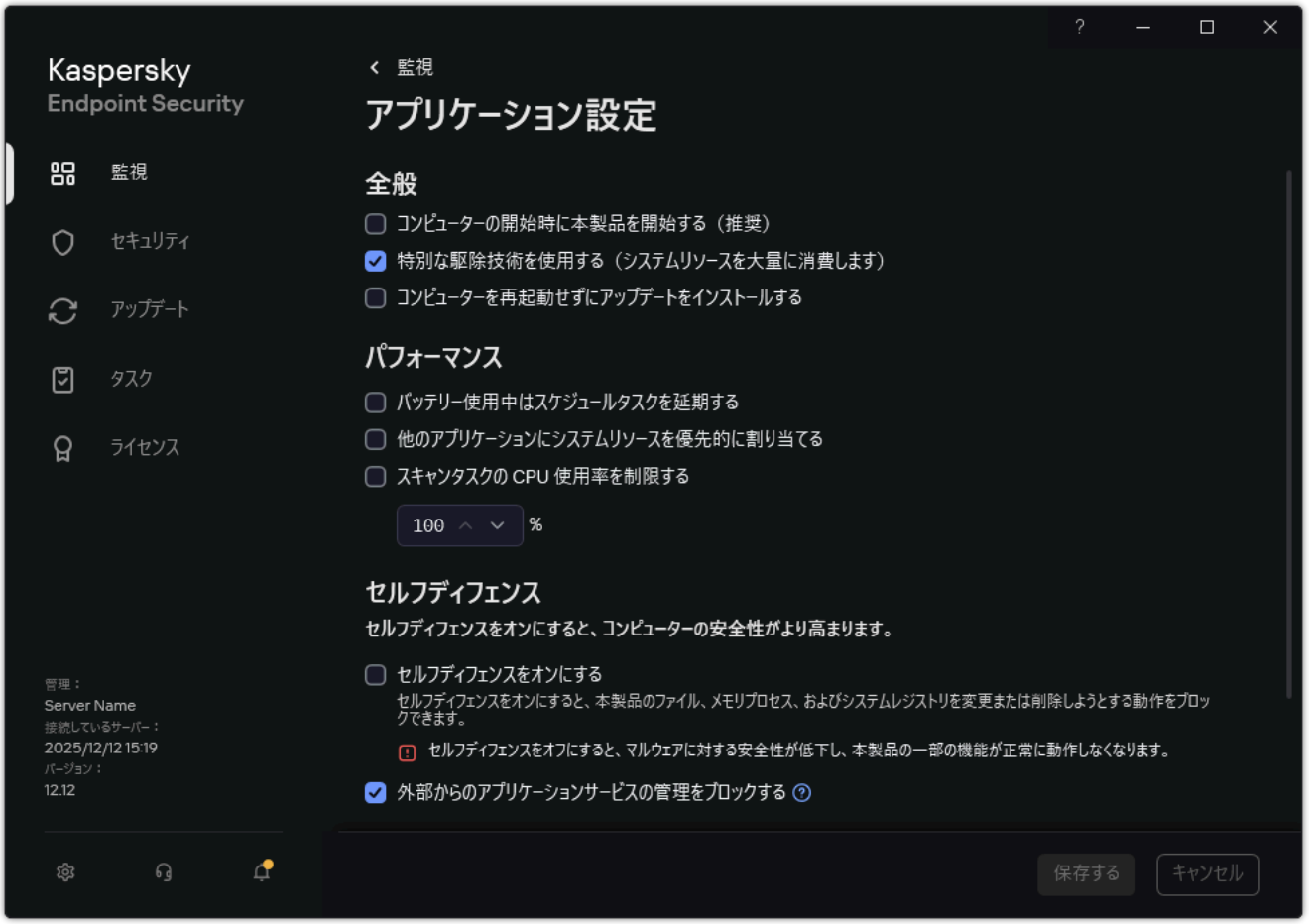
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. ［**外部からのアプリケーションサービスの管理をブロックする**］を使用して Kaspersky Endpoint Security の外部からの管理に対する保護を有効または無効にします。
5. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで外部からの管理に対するアプリケーションサービスの保護を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**セルフディフェンス**］に移動します。
5. ［**外部からのアプリケーションサービスの管理をブロックする**］を使用して Kaspersky Endpoint Security の外部からの管理に対する保護を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスで外部からの管理に対するアプリケーションサービスの保護を有効または無効にする方法

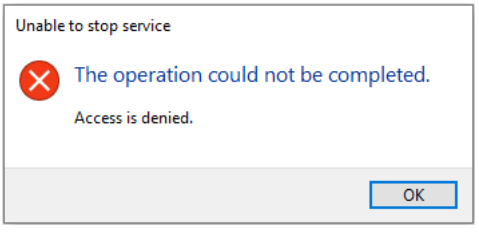
1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**外部からのアプリケーションサービスの管理をブロックする**］を使用して Kaspersky Endpoint Security の外部からの管理に対する保護を有効または無効にします。
4. 変更内容を保存します。

その結果、ユーザーがアプリケーションサービスを停止しようとすると、システムウィンドウにエラーメッセージが表示されます。ユーザーは、Kaspersky Endpoint Security インターフェイスからのみアプリケーションサービスを管理できます。



アプリケーションサービスアクセスエラー

リモート管理アプリケーションのサポート

外部からの管理に対する防御が有効になっているとき、リモート管理アプリケーションの使用が必要になる場合があります。

リモート管理アプリケーションの操作を有効にするには、次の手順を実行します：

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**除外リストと検知したオブジェクトの種別**］を選択します。
3. ［**除外リスト**］セクションで、［**信頼するアプリケーションの指定**］をクリックします。
4. 表示されたウィンドウで、［**追加**］をクリックします。
5. リモート管理アプリケーションの実行ファイルを選択します。

   手動でパスを入力することもできます。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
6. ［**Kaspersky Endpoint Security のインターフェイスの操作を許可する**］チェックボックスをオンにします。
7. 変更内容を保存します。

パスワードによる保護

企業などでは、コンピューターリテラシーのレベルが異なる複数のユーザーで1台の PC を共有することがあります。ユーザーに Kaspersky Endpoint Security およびその設定へのアクセスが制限なく許可されている場合、全体的なコンピューター保護のレベルが低下することがあります。パスワードによる保護を使用することで、ユーザーに付与された権限（例：アプリケーションの終了権限）に応じて、ユーザーが Kaspersky Endpoint Security で行える操作を制限できます。

Windows セッションを開始したユーザー（*セッションユーザー*）に操作を実行する権限が付与されている場合、Kaspersky Endpoint Security はユーザー名とパスワードの入力または一時パスワードの入力を要求しません。付与されている権限に応じて、ユーザーは Kaspersky Endpoint Security の機能にアクセスできます。

セッションユーザーに操作を実行する権限が付与されていない場合、ユーザーは次の方法でアクセスを取得できます：

- ユーザー名とパスワードを入力してください。

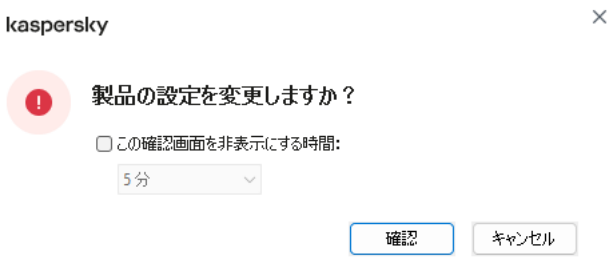
  日常的なコンピューター使用では、この方法が最適です。パスワードによって保護されている操作を実行するには、必要な権限を付与されているユーザーのドメインアカウントの認証情報を入力する必要があります。この場合、コンピューターはドメイン内にある必要があります。コンピューターがドメインにない場合は、KLAdmin アカウントまたは手動で追加されたアカウントを使用できます。

- 一時パスワードを入力する。

  この方法は、組織のネットワーク外のユーザーに、ブロックされている操作（例：本製品の終了）の権限を一時的に付与する場合に最適です。一時パスワードの有効期限が切れたりセッションが終了した場合、Kaspersky Endpoint Security の設定は元に戻ります。

パスワードによって保護されている操作をユーザーが試行した場合、Kaspersky Endpoint Security はユーザー名とパスワードの組み合わせまたは一時パスワードの入力を求めます（以下の図を参照）。

パスワードの入力ウィンドウでは、**ALT+SHIFT**を押すことでのみ言語を切り替えられます。オペレーティングシステムでその他のショートカットが設定されていても、その他のショートカットで言語を切り替えることはできません。



Kaspersky Endpoint Security にアクセスするパスワードの入力

ユーザー名とパスワード

Kaspersky Endpoint Security にアクセスするには、アカウントの認証情報を入力する必要があります。パスワードによる保護では次のアカウントがサポートされます：

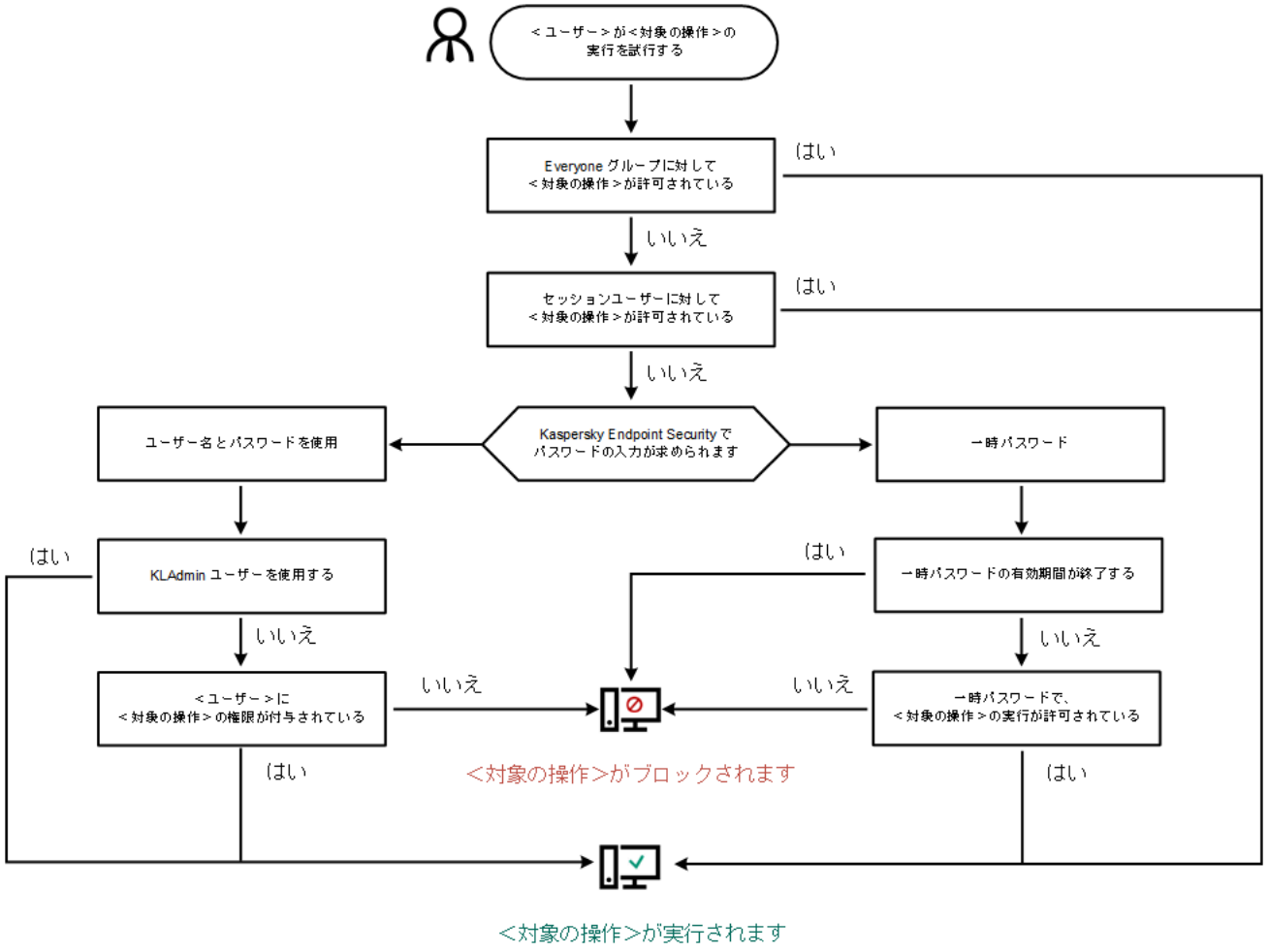
- **KLAdmin**：Kaspersky Endpoint Security に制限なくアクセスできる管理者アカウント。KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。KLAdmin アカウントに対する権限を取り消すことはできません。パスワードによる保護を有効にすると、Kaspersky Endpoint Security では KLAdmin アカウントのパスワードの指定が要求されます。
- **手動で追加されたアカウント**：Active Directory ドメイン外のアカウント。管理者パスワードを共有しない場合は、KLAdmin の代わりにこのサービスアカウントを使用できます。任意のユーザー名とパスワードを設定して、個々の権限を設定できます。
- **Everyone グループ**：Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。Everyone グループに含まれるユーザーは、グループに対して付与されている権限に応じて本製品にアクセスできます。
- **個別のユーザーまたはグループ**：ユーザーアカウントに対して個別に権限を設定できます。たとえば、Everyone グループに対してはブロックされている操作を、個別のユーザーやグループに対して許可することができます。
- **セッションユーザー**：Windows セッションを開始したユーザーのアカウント。パスワードの入力を要求されたときに、別のセッションユーザーに切り替えることができます（[**本製品の終了までパスワードを記憶する**]）。この場合、Kaspersky Endpoint Security は、Windows セッションを開始したユーザーではなく、認証情報を入力したユーザーアカウントをセッションユーザーとして認識します。

一時パスワード

一時パスワードを使用すると、組織ネットワーク外の個別のコンピューターに対して Kaspersky Endpoint Security への一時的なアクセス権を付与できます。管理者は、Kaspersky Security Center で、対象コンピューターのプロパティを使用して個別のコンピューターに対して一時パスワードを生成できます。管理者は、一時パスワードで保護される操作を選択し、一時パスワードの有効期間を指定します。

パスワードによる保護の判定アルゴリズム

Kaspersky Endpoint Security は次のアルゴリズムに従って、パスワードによって保護されている処理の実行を許可するかブロックするかを判定します。



パスワードによる保護の判定アルゴリズム

パスワードによる保護を有効にする

パスワードによる保護を使用することで、ユーザーに付与された権限（例：アプリケーションの終了権限）に応じて、ユーザーが Kaspersky Endpoint Security で行える操作を制限できます。

管理コンソール（MMC）でパスワードによる保護を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**インターフェイス**］の順に選択します。
4. ［**パスワードによる保護**］ブロックの［**設定**］をクリックします。
   パスワードによる保護の設定のウィンドウが開きます。
5. ［**パスワードによる保護を有効にする**］を使用して機能を有効または無効にします。
6. ［**権限**］で、KLAdmin アカウントを選択します。
7. 表示されたウィンドウで、［**パスワード**］をクリックして KLAdmin アカウントのパスワードを設定します。
   KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。

   > KLAdmin アカウントのパスワードを忘れてしまった場合、ポリシーのプロパティでパスワードをリセットできます。

8. アカウント一覧に戻ります。
9. 組織ネットワーク内のすべてのユーザーの権限を設定します。
   a. ［**権限**］で、「Everyone」グループを選択します。
      *Everyone グループ*は Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。
   b. 表示されたウィンドウで、ユーザーがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。
      チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、［**本製品の終了**］権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

      > パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

10. 変更内容を保存します。

Web コンソールと Cloud コンソールでパスワード保護を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**セルフディフェンス**］に移動します。

5. ［**パスワードによる保護**］で、［**パスワードによる保護は有効です**］トグルスイッチを使用してコンポーネントを有効または無効にします。

6. KLAdmin アカウントのパスワードを入力し、確認します。

   KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。

   KLAdmin アカウントのパスワードを忘れてしまった場合、ポリシーのプロパティでパスワードをリセットできます。

7. アカウント一覧に戻ります。

8. 組織ネットワーク内のすべてのユーザーの権限を設定します。

   a. アカウントのテーブルで、「Everyone」グループを選択します。

      *Everyone グループ*は Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。

   b. 表示されたウィンドウで、ユーザーがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。

      チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、［**本製品の終了**］権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

      パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

9. 変更内容を保存します。

製品インターフェイスでパスワードによる保護を有効にする方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。

3. ［**パスワードによる保護**］トグルスイッチを使用して機能を有効または無効にします。

4. KLAdmin アカウントのパスワードを入力し、確認します。

   KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。

   コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、管理者はポリシーのプロパティで KLAdmin アカウントのパスワードをリセットできます。コンピューターが Kaspersky Security Center に接続していない状態で KLAdmin アカウントのパスワードを忘れてしまうと、パスワードを復元することはできません。

5. 組織ネットワーク内のすべてのユーザーの権限を設定します。

   a. アカウントテーブルで、[**編集**]をクリックして Everyone グループの権限のリストを表示します。

      *Everyone グループ*は Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。

   b. ユーザーがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。

      チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、[**本製品の終了**]権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

      パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

6. 変更内容を保存します。

パスワードによる保護をオンにすると、Everyone グループに付与された権限に応じて、ユーザーが Kaspersky Endpoint Security で行える操作が制限されます。Everyone グループに対してブロックされている動作は、KLAdmin アカウントを使用している場合、必要な権限を付与されたその他のアカウントを使用している場合、あるいは一時パスワードを入力した場合にのみ実行できます。

KLAdmin としてログインしている場合にのみ、パスワードによる保護をオフにできます。その他のユーザーアカウントでログインしている場合または一時パスワードを使用してログインしている場合は、パスワードによる保護をオフにできません。

パスワードの確認時に、[**本製品の終了までパスワードを記憶する**]をオンにできます。この場合、セッションの継続中は、その他のパスワードによって保護された操作を実行しようとしてもパスワードの入力を要求されることはありません。

個別のユーザーまたはグループへの権限付与

パスワードによる保護を使用すると、個々の Active Directory ユーザーアカウントと、手動で追加されたユーザーアカウントに、Kaspersky Endpoint Security へのアクセス権を付与できます。

Active Directory ユーザーアカウント

Active Directory ドメイン内の個々のユーザーまたはグループに、Kaspersky Endpoint Security へのアクセス権を付与できます。たとえば、Everyone グループに対して「本製品の終了」操作がブロックされている場合でも、[**本製品の終了**]権限を個別のユーザーに対して付与できます。これにより、権限を付与されたユーザーまたは KLAdmin としてログインしている場合にのみ、本製品を終了できます。

コンピューターがドメイン内にある時のみ、本製品にアクセスするアカウントの認証情報を使用できます。コンピューターがドメインにない場合は、KLAdmin アカウントまたは一時パスワードを使用できます。

手動で追加されたユーザーアカウント

Active Directory 内に存在しないユーザーアカウントを作成し、そのユーザーアカウントに個別の権限を割り当てることができます。つまり、KLAdmin の代わりに *サービスユーザーアカウント*を作成して使用できます。これにより、KLAdmin パスワードを他のユーザーと共有したり、新しい Active Directory ユーザーアカウントを作成したりする必要がなくなります。任意のユーザー名とパスワードを指定できます。たとえば、サービスユーザーアカウントに［**レポートの表示**］権限を付与することができます。これにより、［すべて］グループに対してレポートの表示が禁止された場合は、サービスユーザーアカウントまたは KLAdmin ユーザーアカウントを使用してレポートを開くことができます。

個別のユーザーまたはグループへの権限付与

管理コンソール（MMC）で個々のユーザーまたはグループに権限を付与する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**インターフェイス**］の順に選択します。
4. ［**パスワードによる保護**］ブロックの［**設定**］をクリックします。
   パスワードによる保護の設定のウィンドウが開きます。
5. アカウントテーブルで、［**追加**］をクリックします。
6. 追加するユーザーアカウントの種別を選択します：
   - **Active Directory からユーザーまたはグループを選択する** – Active Directory ユーザーアカウント
     ユーザーアカウントを選択するには、［**選択**］をクリックします。Active Directory のユーザーまたはグループを選択し、選択内容を確認します。
   - **ユーザーまたはユーザーグループを手動で追加する**（手動で追加されたサービスユーザーアカウント）。
     サービスユーザーアカウントを追加するには、ユーザー名とパスワード（例：SecureAdmin）を入力します。

     ポリシー設定でサービスユーザーアカウントのパスワードをリセットできます。サービスユーザーアカウントのパスワードは、KLAdmin パスワードと同じ方法でリセットする必要があります。パスワードによる保護の設定の編集が許可されている（鍵が開いている）場合、またはコンピューターにポリシーが適用されていない場合、製品のインターフェイスでサービスユーザーアカウントのパスワードをリセットできます。そのためには、KLAdmin パスワードを使って、サービスユーザーアカウント情報の変更を確認します。
7. ［**権限**］リストで、選択したユーザーまたはグループがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。
   チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、［**本製品の終了**］権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

8. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで個々のユーザーまたはグループに権限を付与する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**セルフディフェンス**］に移動します。
5. ［**パスワードによる保護**］セクションで、［**ユーザー権限**］をクリックします。
   これにより、パスワードの権限を付与するためのフォームが開きます。
6. ［**追加**］をクリックします。
7. 追加するユーザーアカウントの種別を選択します：
   - **Active Directory から選択** – Active Directory ユーザーアカウント
     ユーザーアカウントを選択するには、［**編集する**］をクリックします。Active Directory のユーザーまたはグループを選択し、選択内容を確認します。
   - **手動で追加**（手動で追加されたサービスユーザーアカウント）。
     サービスユーザーアカウントを追加するには、ユーザー名とパスワード（例：SecureAdmin）を入力します。

     ポリシー設定でサービスユーザーアカウントのパスワードをリセットできます。サービスユーザーアカウントのパスワードは、KLAdmin パスワードと同じ方法でリセットする必要があります。パスワードによる保護の設定の編集が許可されている（鍵が開いている）場合、またはコンピューターにポリシーが適用されていない場合、製品のインターフェイスでサービスユーザーアカウントのパスワードをリセットできます。そのためには、KLAdmin パスワードを使って、サービスユーザーアカウント情報の変更を確認します。
8. ［**権限**］リストで、選択したユーザーまたはグループがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。
   チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、［**本製品の終了**］権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

9. ［**追加**］をクリックします。

10. 変更内容を保存します。

製品のユーザーインターフェイスで個々のユーザーまたはグループに権限を付与する方法

1. メインウィンドウで、⚙をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。

3. アカウントテーブルで、［**追加**］をクリックします。

4. 追加するユーザーアカウントの種別を選択します：

   - **Active Directoryからユーザーまたはグループを選択する** – Active Directory ユーザーアカウント

     ユーザーアカウントを選択するには、［**ユーザーまたはグループを選択**］をクリックします。Active Directory のユーザーまたはグループを選択し、選択内容を確認します。

   - **ユーザーを手動で追加する**（手動で追加されたサービスユーザーアカウント）。

     サービスユーザーアカウントを追加するには、ユーザー名とパスワード（例：SecureAdmin）を入力します。

     > ポリシー設定でサービスユーザーアカウントのパスワードをリセットできます。サービスユーザーアカウントのパスワードは、KLAdmin パスワードと同じ方法でリセットする必要があります。パスワードによる保護の設定の編集が許可されている（鍵が開いている）場合、またはコンピューターにポリシーが適用されていない場合、製品のインターフェイスでサービスユーザーアカウントのパスワードをリセットできます。そのためには、KLAdmin パスワードを使って、サービスユーザーアカウント情報の変更を確認します。

5. ［**権限**］リストで、選択したユーザーまたはグループがパスワードを入力せずに実行できるようにする操作のチェックボックスをオンにします。

   チェックボックスをオフにすると、ユーザーによるその操作の実行がブロックされます。たとえば、［**本製品の終了**］権限のチェックボックスをオフにすると、KLAdmin アカウントでログインしている場合、または必要な権限を付与された個別のユーザーでログインしている場合、あるいは一時パスワードを入力した場合にのみ本製品の終了を実行できます。

   > パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作などいくつかの留意事項があります。Kaspersky Endpoint Security へのアクセスに関するすべての条件が満たされていることを確認してください。

6. 変更内容を保存します。

これにより、Everyone グループに対して Kaspersky Endpoint Security へのアクセスが制限されている場合でも、個別に権限を付与されたユーザーはその権限に応じて Kaspersky Endpoint Security にアクセスできます。

一時パスワードを使用した権限の付与

一時パスワードを使用すると、組織ネットワーク外の個別のコンピューターに対して Kaspersky Endpoint Security への一時的なアクセス権を付与できます。該当するユーザーに KLAdmin アカウントの認証情報を共有せずに、ブロックされている操作の実行を許可するには、この手順が必要です。一時パスワードを使用するには、Kaspersky Security Center の管理対象にコンピューターを追加する必要があります。

管理コンソール（MMC）で一時パスワードを使用して、ブロックされている操作の実行をユーザーに許可する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**デバイス**］タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。
6. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Endpoint Security for Windows (12.12)**］を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。
7. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
8. ［**パスワードによる保護**］ブロックの［**設定**］をクリックします。
9. 表示されたウィンドウで、［**一時パスワード**］ブロックの［**一時パスワードのリスト**］をクリックします。
   一時パスワードの管理ウィンドウが表示されます。
10. ［**追加**］をクリックします。
11. ［**有効期限**］で、一時パスワードの有効期限が切れる日付を指定します。
12. ［**一時パスワードを要求する操作**］リストで、一時パスワードの入力後にユーザーが使用できるようにする操作の横にあるチェックボックスをオンにします。
13. ［**生成**］をクリックします。
    ウィンドウが開き、一時パスワードが表示されます（以下の図を参照）。
14. パスワードをコピーし、ユーザーに共有します。

Web コンソールと Cloud コンソールで一時パスワードを使用して、ブロックされている操作の実行をユーザーに許可する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ブロックされている操作の実行を許可するユーザーのコンピューターの名前をクリックします。
3. ［**アプリケーション**］タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。
5. ［**アプリケーション設定**］タブを選択します。
6. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
7. ［**一時パスワード**］ブロックの［**追加**］をクリックします。

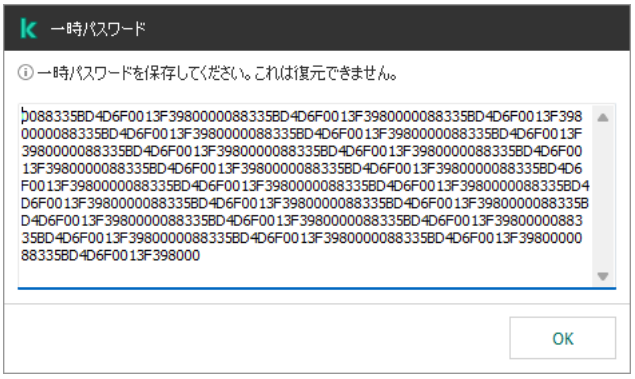
8. ［**有効期限**］で、一時パスワードの有効期限が切れる日付を指定します。

9. ［**一時パスワードを要求する操作**］リストで、一時パスワードの入力後にユーザーが使用できるようにする操作の横にあるチェックボックスをオンにします。

10. ［**生成**］をクリックします。

    一時パスワードが表示されたウィンドウが表示されます。

11. パスワードをコピーし、ユーザーに共有します。



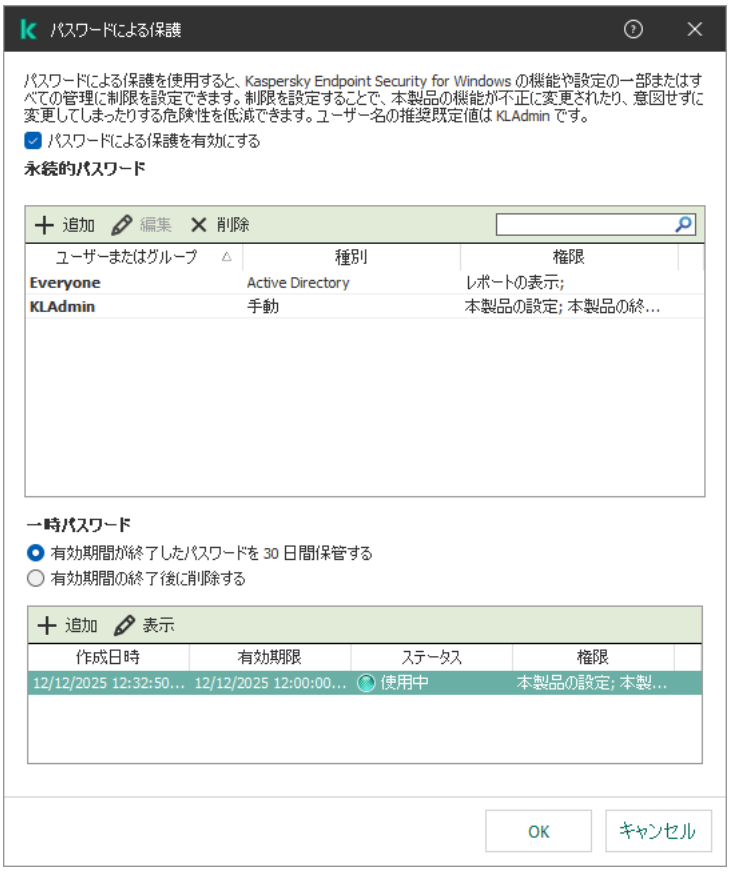
一時パスワード

一時パスワードの取り消し

バージョン 12.9 から、Kaspersky Endpoint Security for Windows には*一時パスワードの管理*機能が含まれるようになりました。一時パスワードの管理では、次の操作を実行できます：

- パスワード履歴の保存（最大 30 日間）
- 一時パスワードのステータス（*使用中*、*有効期間終了*、*失効*）の監視

- 一時パスワードの取り消し



一時パスワードの管理

一時パスワードの管理では、コンピューターを Kaspersky Security Center と同期した後でのみ、パスワードのステータスが更新されて、パスワードが取り消されます。

管理コンソール（MMC）を使用して一時パスワードを取り消す方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**デバイス**］タブを選択します。
4. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
5. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。
6. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Endpoint Security for Windows (12.12)**］を選択し、ダブルクリックしてアプリケーションのプロパティを開きます。
7. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。
8. ［**パスワードによる保護**］ブロックの［**設定**］をクリックします。
9. ウィンドウが表示されるので、そのウィンドウの［**一時パスワード**］で、有効期間が終了したパスワードの保管を設定します。
10. ［**一時パスワードのリスト**］をクリックします。

    一時パスワードの管理ウィンドウが表示されます。一時パスワードの管理では、パスワードの有効期限、パスワードのステータス、権限のリストが表示されます。

11. 取り消す必要があるアクティブな一時パスワードを選択し、パスワードをダブルクリックしてそのプロパティを開きます。

12. 表示されたウィンドウで、［**取消**］をクリックします。

13. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールおよび Cloud コンソールを使用して一時パスワードを取り消す方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ブロックされている操作の実行を許可するユーザーのコンピューターの名前をクリックします。

3. ［**アプリケーション**］タブを選択します。

4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。

5. ［**アプリケーション設定**］タブを選択します。

6. 本製品の設定ウィンドウで、［**全般設定**］→［**インターフェイス**］を選択します。

7. ［**一時パスワード**］で、有効期間が終了したパスワードの保管を設定します。

8. ［**一時パスワード**］リンクをクリックします。
   一時パスワードの管理ウィンドウが表示されます。一時パスワードの管理では、パスワードの有効期限、パスワードのステータス、権限のリストが表示されます。

9. 取り消す必要があるアクティブな一時パスワードを選択します。

10. 表示されたウィンドウで、［**パスワードを取り消す**］をクリックします。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

これにより、一時パスワードの管理で、パスワードのステータスが「*取消中（ホストと同期中）*」に設定されます。コンピューターを Kaspersky Security Center と同期すると、一時パスワードが取り消されて、付与された権限がすぐにブロックされます。

パスワードによる保護で付与する権限に関する留意事項

パスワードによる保護で権限を付与するにあたっては、単独の権限だけでは実行できない操作など、いくつかの留意事項があります。

本製品の設定

コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。

本製品の終了

特別な留意事項はありません。

保護機能の停止

- Everyone グループの保護機能を無効にする権限を付与することはできません。KLAdmin 以外のユーザーに管理機能の無効化を許可する場合は、パスワードによる保護の設定で［**保護機能の停止**］権限を持つユーザーまたはグループを追加してください。
- コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。
- ユーザーが本製品の設定で保護機能を停止するには、［**本製品の設定**］権限も付与されている必要があります。
- コンテキストメニューから保護機能を無効にするには（［**保護機能の一時停止**］メニュー項目を使用して）、ユーザーは［**保護機能の停止**］権限に加えて、［**管理コンポーネントの停止**］権限が必要です。

管理コンポーネントの停止

- Everyone グループの管理コンポーネントを停止する権限を付与することはできません。KLAdmin 以外のユーザーに管理機能の無効化を許可する場合は、パスワードによる保護の設定で［**管理コンポーネントの停止**］権限を持つユーザーまたはグループを追加してください。
- コンピューターが Kaspersky Security Center のポリシーの管理下にある場合、ポリシー内の目的の設定がすべて編集可能であること（「」のロックが開いている）を確認してください。
- ユーザーが本製品の設定で管理コンポーネントを停止するには、［**本製品の設定**］権限も付与されている必要があります。
- コンテキストメニューから管理コンポーネントを無効にするには（［**保護機能の一時停止**］メニュー項目を使用して）、ユーザーは［**管理コンポーネントの停止**］権限に加えて、［**保護機能の停止**］権限が必要です。

Kaspersky Security Center ポリシーを無効にする

Kaspersky Security Center ポリシーを無効にする権限を「Everyone」グループに付与することはできません。KLAdmin 以外のユーザーにポリシーの無効化を許可する場合は、パスワードによる保護の設定でユーザーまたはグループを追加し、このユーザーまたはグループに［**Kaspersky Security Center ポリシーを無効にする**］権限を付与してください。

ライセンスの削除

特別な留意事項はありません。

本製品の削除 / 変更 / 修復

「すべて」のグループに本製品の削除、変更、修復を許可した場合、ユーザーがこれらの操作を実行しようとした場合に Kaspersky Endpoint Security はパスワードを要求しません。そのため、ドメイン外のユーザーを含むすべてのユーザーが本製品をインストール、変更、復元することができます。

暗号化されたドライブ上のデータへのアクセスの復元

暗号化されたドライブ上のデータへのアクセスは、KLAdmin としてログインしている場合にのみ復元できます。この操作を実行する権限は、その他のユーザーには付与できません。

レポートの表示

特別な留意事項はありません。

バックアップから復元

特別な留意事項はありません。

設定のエクスポート

既定では、「すべて」グループに対する本製品の設定のエクスポートは拒否されます。KLAdmin ユーザーアカウントを使用して本製品の設定をエクスポートできます。本製品の設定のエクスポートには、製品インターフェイスでの Kaspersky Endpoint Security の設定を含む設定ファイルの作成のみが含まれます。この権限では、信頼するオブジェクトのリスト、信頼する Web アドレスのリスト、信頼するデバイスのリスト、または製品コンポーネントによって維持されるその他のリストのエクスポートは制限されません。

KLAdmin パスワードのリセット

KLAdmin アカウントのパスワードを忘れてしまった場合、ポリシーのプロパティでパスワードをリセットできます。製品のインターフェイスからはパスワードをリセットすることはできません。

パスワード保護された操作は一時パスワードを使用して実行することができます。この場合、KLAdmin の認証情報を入力する必要はありません。

コンピューターが Kaspersky Security Center に接続していない状態で KLAdmin アカウントのパスワードを忘れてしまうと、パスワードを復元することはできません。

管理コンソール（MMC）を使用して KLAdmin アカウントのパスワードをリセットする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**インターフェイス**］の順に選択します。
4. ［**パスワードによる保護**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、［**パスワードによる保護を有効にする**］をオフにします。
6. 変更内容を保存します。
7. ［**パスワードによる保護を有効にする**］チェックボックスを再度オンにします。
8. ［**OK**］をクリックします。
   管理者パスワードのウィンドウが表示されます。
9. KLAdmin アカウントの新しいパスワードを入力し、確認します。
10. 変更内容を保存します。

Web コンソールおよび Cloud コンソールを使用して KLAdmin アカウントのパスワードをリセットする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。
   コンピューターのプロパティが表示されます。
3. ［**アプリケーション**］タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。
5. ［**アプリケーション設定**］タブを選択します。
6. ［**全般設定**］→［**セルフディフェンス**］に移動します。
7. ［**パスワードによる保護**］で、［**パスワードによる保護**］をオンにします。
8. 変更内容を保存します。
9. ［**パスワードによる保護**］を再度オンにします。

10. KLAdmin アカウントの新しいパスワードを入力し、確認します。

11. 変更内容を保存します。

ポリシーが適用された後、KLAdmin アカウントのパスワードが更新されます。

管理サーバーの接続の保護

コンピューターを管理サーバーに接続するには、Kaspersky Security Center のネットワークエージェントのコンポーネントを使用します。侵入者がサーバーの接続設定を変更する十分な権限を持っている場合、信頼済みでないサーバーにコンピューターが接続される危険性があります。こうすることで、侵入者が独自のグループポリシーを適用したり、アプリケーションのセルフディフェンスを無効にしたりできるようになります。Kaspersky Endpoint Security は、コンピューターの別のサーバーへの不正な再接続を防ぐことができます。サーバー接続を保護するために、パスワードを設定し、パスワードベースのキー導出関数（Password-Based key Derivation Function – PBKDF2）を使用することを推奨します。その結果、パスワードなしでアプリケーションにアクセスすることはできなくなります。

Kaspersky Endpoint Security とネットワークエージェントを不正アクセスから包括的に保護するために、追加の保護を有効にすることを推奨します。Kaspersky Endpoint Security では、パスワードによる保護を有効にすることを推奨します。ネットワークエージェントを保護するために、アンインストール用パスワードを設定することを推奨します。ネットワークエージェントの削除からの保護の詳細については、Kaspersky Security Center ヘルプを参照してください。

コンピューターの管理サーバーへの接続を管理するには、［*管理サーバーの接続の保護*］タスクを使用します。このタスクでは、次の操作を実行できます：

- サーバー接続を保護するためのパスワードの設定
- パスワードの変更
- コンピューターの別のサーバーへの再接続
- サーバー接続の保護の無効化

管理サーバーへの接続時のコンピューターの認証

パスワードを設定すると、パスワードの PBKDF2 変換を使用してデータ配列が作成されます。次に、ネットワークエージェントのキーを使用して、このデータ配列が暗号化されます。その後の接続で管理サーバーの権限を確認するために、この暗号化されたデータ配列が使用されます。

それ以降、コンピューターを管理サーバーに再接続しようとするたびに、ネットワークエージェントのキーでデータ配列が復号化されて、ローカルコピーと比較されます。一致しない場合、アプリケーションへのアクセスは制限されます。

管理サーバーの接続の保護

管理コンソール（MMC）でサーバー接続の保護用のパスワードを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**管理サーバーの接続の保護**］の順に選択します。

ステップ 2：管理サーバーの接続の保護

管理サーバーの接続を保護するためのパスワードを設定します：

1. ［**管理サーバーの接続の保護**］で、［**パスワードで保護する**］を選択します。
2. ［**管理サーバー**］から［**新しいサーバー**］を選択します。
3. ［**管理サーバーへの接続用パスワード**］フィールドで、管理サーバーに接続するためのパスワードを設定し、確認します。
   パスワードを忘れた場合は、タスクを使用してパスワードを変更できます。
4. Kaspersky Endpoint Security 12.7 またはそれ以前のバージョンを導入した場合は、［**製品の以前のバージョン（12.7 以前）とのパスワード暗号化の互換性を有効にする**］チェックボックスをオンにします。
   Kaspersky Endpoint Security 12.8 for Windows 以降では、より強力なパスワード暗号化が使用されています。Kaspersky Endpoint Security 12.8 以降を導入した場合は、このチェックボックスをオフにして、より強力なパスワード暗号化を使用することを推奨します。以前のバージョンでは、強力なパスワード暗号化はサポートされていません。タスクを実行するには、チェックボックスをオンにする必要があります。

ステップ 3：タスクを実行するアカウントの選択

［**既定のアカウント**］を選択します。既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

ステップ 4：タスク開始スケジュールの設定

［**実行予定**］で、［**手動**］を選択します。

ステップ 5：タスク名の定義

タスクの名前を入力します（たとえば、「*メインサーバー接続のパスワード*」など）。

ステップ 6：タスク作成の完了

ウィザードを終了します。［**ウィザードの終了後にタスクを実行**］をオンにするか、タスクを手動で実行します。タスクのプロパティでタスクの進行状況を監視できます。

Web コンソールおよび Cloud コンソールでサーバー接続の保護用のパスワードを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**管理サーバーの接続の保護**］を選択します。
   c. ［**タスク名**］に「*メインサーバー接続のパスワード*」などの簡潔な名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. 既定のユーザーアカウントを選択します。既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。
6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. Kaspersky Endpoint Security の **管理サーバーの接続の保護**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. ［**管理サーバーの接続の保護**］で、［**パスワードで保護する**］を選択します。

10. ［**管理サーバーへの接続**］から［**新しいパスワード**］を選択します。

11. ［**パスワード**］フィールドで、管理サーバーに接続するためのパスワードを設定し、確認します。

    パスワードを忘れた場合は、タスクを使用してパスワードを変更できます。

12. Kaspersky Endpoint Security 12.7 またはそれ以前のバージョンを導入した場合は、［**製品の以前のバージョン（12.7 以前）とのパスワード暗号化の互換性を有効にする**］チェックボックスをオンにします。

    Kaspersky Endpoint Security 12.8 for Windows 以降では、より強力なパスワード暗号化が使用されています。Kaspersky Endpoint Security 12.8 以降を導入した場合は、このチェックボックスをオフにして、より強力なパスワード暗号化を使用することを推奨します。以前のバージョンでは、強力なパスワード暗号化はサポートされていません。タスクを実行するには、チェックボックスをオンにする必要があります。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。

コンピューターの別の管理サーバーへの再接続

コンピューターを別の管理サーバーに再接続するには、次の手順を実行します：

1. 現在の [KSC1] サーバーのコンソールで、ネットワークエージェントに対して*管理サーバーの変更*タスクを実行します。

   タスクの実行後、コンピューターは新しい [KSC2] サーバーに再接続されます。

   コンピューターは [KSC1] サーバーコンソールに*緊急*🖥ステータスで表示されます。ポリシーを使ってアプリケーションを設定したり、コンピューターでタスクをリモート実行したりすることはできません。

2. 新しい [KSC2] サーバーのコンソールで、Kaspersky Endpoint Security 用に新しい*管理サーバーの接続の保護*タスクを作成します。タスクのプロパティで、以前のサーバーのパスワードを入力し、新しいサーバーのパスワードを設定します。

   管理コンソール（MMC）で新しいサーバーに再接続するための新しいパスワードを設定する方法

   1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。

      タスクのリストが表示されます。

   2. ［**新規タスク**］をクリックします。

   タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**管理サーバーの接続の保護**］の順に選択します。

ステップ 2：管理サーバーの接続の保護

新しい管理サーバーへの接続を保護するためのパスワードを設定します：

1. ［**管理サーバーの接続の保護**］で、［**パスワードで保護する**］を選択します。
2. ［**管理サーバー**］から［**別のサーバーから再接続**］を選択します。
3. ［**現在のパスワード**］に、以前に使用していた信頼済みサーバーへの接続用に設定したパスワードを入力します。
4. ［**新しいパスワード**］フィールドで、新しい管理サーバーに接続するためのパスワードを設定し、入力して確認します。

   パスワードを忘れた場合は、タスクを使用してパスワードを変更できます。
5. Kaspersky Endpoint Security 12.7 またはそれ以前のバージョンを導入した場合は、［**製品の以前のバージョン（12.7 以前）とのパスワード暗号化の互換性を有効にする**］チェックボックスをオンにします。

   Kaspersky Endpoint Security 12.8 for Windows 以降では、より強力なパスワード暗号化が使用されています。Kaspersky Endpoint Security 12.8 以降を導入した場合は、このチェックボックスをオフにして、より強力なパスワード暗号化を使用することを推奨します。以前のバージョンでは、強力なパスワード暗号化はサポートされていません。タスクを実行するには、チェックボックスをオンにする必要があります。

ステップ 3：タスクを実行するアカウントの選択

［**既定のアカウント**］を選択します。既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

ステップ 4：タスク開始スケジュールの設定

［**実行予定**］で、［**手動**］を選択します。

ステップ 5：タスク名の定義

タスクの名前を入力します（たとえば、「*メインサーバー接続のパスワード*」など）。

ステップ 6：タスク作成の完了

ウィザードを終了します。［**ウィザードの終了後にタスクを実行**］をオンにするか、タスクを手動で実行します。タスクのプロパティでタスクの進行状況を監視できます。

Web コンソールおよび Cloud コンソールで新しいサーバーに再接続するための新しいパスワードを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**管理サーバーの接続の保護**］を選択します。
   c. ［**タスク名**］に「*メインサーバー接続のパスワード*」などの簡潔な名前を付けます。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. 既定のユーザーアカウントを選択します。既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。
6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. Kaspersky Endpoint Security の **管理サーバーの接続の保護**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. ［**管理サーバーの接続の保護**］で、［**パスワードで保護する**］を選択します。
10. ［**管理サーバーへの接続**］から［**別のサーバーから再接続**］を選択します。
11. ［**現在のパスワード**］に、以前に使用していた信頼済みサーバーへの接続用に設定したパスワードを入力します。
12. ［**新しいパスワード**］フィールドで、新しい管理サーバーに接続するためのパスワードを設定し、入力して確認します。
    パスワードを忘れた場合は、タスクを使用してパスワードを変更できます。
13. Kaspersky Endpoint Security 12.7 またはそれ以前のバージョンを導入した場合は、［**製品の以前のバージョン（12.7 以前）とのパスワード暗号化の互換性を有効にする**］チェックボックスをオンにします。
    Kaspersky Endpoint Security 12.8 for Windows 以降では、より強力なパスワード暗号化が使用されています。Kaspersky Endpoint Security 12.8 以降を導入した場合は、このチェックボックスをオフにして、より強力なパスワード暗号化を使用することを推奨します。以前のバージョンでは、強力なパスワード暗号化はサポートされていません。タスクを実行するには、チェックボックスをオンにする必要があります。
14. 変更内容を保存します。
15. タスクの横にあるチェックボックスをオンにします。

16. ［**開始**］をクリックします。

    タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。

タスクが完了したら、新しい [KSC2] サーバーのコンソールで、コンピューターのステータスが *OK* になっていることを確認してください。テストを行い、タスクをリモート実行できること、およびポリシーを使用してアプリケーションを設定できることを確認します。

管理サーバーへの接続用パスワードのリセット

管理サーバーへの接続用パスワードを忘れた場合や、パスワードが漏洩した場合は、タスクのプロパティでパスワードをリセットできます。また、管理サーバーの接続の保護のステータスが異なる複数のコンピューターのグループを対象にパスワードをリセットし、新しいパスワードを設定することもできます。つまり、保護が有効になっているコンピューターと無効になっているコンピューターがある場合、すべてのコンピューターにパスワードが設定されます。

管理サーバーへの接続用パスワードは、コンピューターが接続されている信頼済みサーバーのコンソールでのみリセットできます。

管理コンソール（MMC）を使用して管理サーバーへの接続用パスワードをリセットする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. **管理サーバーの接続の保護**タスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。
5. ［**管理サーバーの接続の保護**］で、［**パスワードで保護し、パスワードを変更する**］を選択します。
6. ［**管理サーバーへの接続用パスワード**］フィールドで、現在の信頼済みサーバーに接続するための新しいパスワードを設定し、パスワードを確認します。
7. 変更内容を保存します。
8. タスクを実行します。

Web コンソールおよび Cloud コンソールを使用して管理サーバーの接続のパスワードをリセットする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **管理サーバーの接続の保護**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**管理サーバーの接続の保護**］で、［**パスワードで保護し、パスワードを変更する**］を選択します。

5. ［**パスワード**］フィールドで、現在の信頼済みサーバーに接続するための新しいパスワードを設定し、パスワードを確認します。
6. 変更内容を保存します。
7. タスクの横にあるチェックボックスをオンにします。
8. ［**開始**］をクリックします。

その結果、タスクの終了後に管理サーバーへの接続用パスワードがリセットされます。

管理サーバーの接続の保護を無効にする

管理サーバーの接続の保護は、コンピューターが接続されている信頼済みサーバーのコンソールでのみ、リモートで無効にできます。ローカルでコマンドラインを使用して製品を無効にすることもできます。

管理コンソール（MMC）でサーバー接続の保護を無効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. **管理サーバーの接続の保護**タスクを選択し、ダブルクリックしてタスクのプロパティを表示します。
4. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。
5. ［**管理サーバーの接続の保護**］で、［**保護しない**］を選択します。
6. 変更内容を保存します。
7. タスクを実行します。
   タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。

Web コンソールおよび Cloud コンソールでサーバー接続の保護を無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **管理サーバーの接続の保護**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**管理サーバーの接続の保護**］で、［**保護しない**］を選択します。
5. 変更内容を保存します。
6. タスクの横にあるチェックボックスをオンにします。

7. ［**開始**］をクリックします。

   タスクのステータス、タスクが正常に完了したデバイスの数、タスクの実行中にエラーが発生したデバイスの数を監視できます。

コマンドラインでサーバー接続の保護を無効にする方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   <password> には KLAdmin ユーザーアカウントのパスワードまたは*管理サーバーの接続の保護*タスクからのパスワードを入力します。パラメータが指定されていない場合、次の行でパスワードを入力するよう求められます。

   > このコマンドを実行するには、パスワードによる保護を有効にする必要があります。

   例：

   ```
   avp.com SERVERBINDINGDISABLE /password=samplePassword
   ```

データ暗号化

Kaspersky Endpoint Security では、ローカルドライブおよびリムーバブルドライブに保存されているファイルやフォルダー、またはリムーバブルドライブおよびハードディスク全体を暗号化できます。データを暗号化すると、ノートパソコン、リムーバブルドライブ、ハードディスクの消失や盗難、承認されていないユーザーやアプリケーションによるデータへのアクセスなどに伴って発生する情報漏洩のリスクを最小限に抑えることができます。Kaspersky Endpoint Security では、Advanced Encryption Standard（AES）暗号アルゴリズムが使用されます。

ライセンスの有効期間が終了すると、新しいデータの暗号化は行いませんが、暗号化された既存のデータは暗号化されたままで、使用可能です。この場合、新たにデータを暗号化するには、暗号化の使用が許可された新しいライセンスで製品をアクティベートする必要があります。

ライセンスの有効期間が終了した場合や、使用許諾契約書の違反が発生した場合、ライセンスや Kaspersky Endpoint Security、暗号化のコンポーネントが削除された場合、以前に暗号化されたファイルの暗号化状態は保証されなくなります。これは、Microsoft Office Word など一部のアプリケーションが、編集中にファイルの一時的なコピーを作成するためです。元のファイルが保存されるとき、一時コピーが元のファイルと入れ替わります。その結果、暗号化機能がないコンピューターや暗号化機能にアクセスできないコンピューターでは、ファイルは暗号化されていない状態になります。

Kaspersky Endpoint Security は、次に示すようにデータを多面的に保護します：

- **ローカルコンピュータードライブでのファイルレベルの暗号化**：拡張子や拡張子グループ、ローカルコンピューターのドライブに保存されているフォルダーのリストに基づいて、ファイルのリストを作成できます。また、特定のアプリケーションで作成されたファイルを暗号化するルールを作成できます。ポリシーが適用されると、Kaspersky Endpoint Security は以下のファイルを暗号化および復号化します：
  - 暗号化および復号化のリストに追加されたファイル
  - 暗号化および復号化のリストに追加されたフォルダーにあるファイル
  - 別々のアプリケーションによって作成されたファイル
- **リムーバブルドライブの暗号化**：既定の暗号化ルールを指定すると、そのルールに基づいてすべてのリムーバブルドライブに同じ処理を適用できます。また、個々のリムーバブルドライブの暗号化ルールを指定することもできます。

  既定の暗号化ルールの優先度は、個々のリムーバブルドライブに対して作成された暗号化ルールよりも低くなります。指定されたデバイスモデルのリムーバブルドライブについて作成された暗号化ルールの優先度は、指定されたデバイス ID のリムーバブルドライブについて作成された暗号化ルールよりも低くなります。

  Kaspersky Endpoint Security は、リムーバブルドライブ上のファイルの暗号化ルールを選択するために、デバイスモデルと ID が既知かどうかをチェックします。チェック後、次のいずれかの操作が行われます：
  - デバイスモデルのみが既知の場合は、特定のデバイスモデルのリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。
  - デバイス ID のみが既知の場合は、特定のデバイス ID のリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。

- デバイスモデルもデバイス ID も既知の場合は、特定のデバイス ID のリムーバブルドライブを対象に作成された暗号化ルール（存在する場合）が適用されます。そのようなルールが存在せず、特定のデバイスモデルのリムーバブルドライブを対象に作成された暗号化ルールが存在する場合、そのルールが適用されます。特定のデバイス ID についても特定のデバイスモデルについても暗号化ルールが設定されていない場合は、既定の暗号化ルールが適用されます。

- デバイスモデルもデバイス ID も未知の場合は、既定の暗号化ルールが適用されます。

ユーザーは、リムーバブルドライブに保存されている暗号化データをポータブルモードで使用できるようリムーバブルドライブを準備できます。ポータブルモード有効にすると、暗号化機能を持たないコンピューターに接続されているリムーバブルドライブ上の暗号化ファイルにアクセスできます。

- **アプリケーションの暗号化ファイルアクセスルールの管理**：任意のアプリケーションについて、暗号化ファイルへのアクセスをブロックしたり暗号化ファイルへのアクセスを暗号文（暗号化が適用された状態の文字列）としてのみ許可したりする暗号化ファイルアクセスルールを作成できます。

- **暗号化されたパッケージへの追加**：暗号化されたアーカイブを作成して、そのアーカイブに対するアクセスをパスワードで保護できます。暗号化されたアーカイブの内容には、アーカイブへのアクセスの保護に使用したパスワードを入力しないとアクセスできません。このアーカイブは、ネットワーク経由またはリムーバブルドライブを使用して安全に転送できます。

- **ディスク全体の暗号化**次の暗号化技術を選択できます：Kaspersky Disk Encryption、BitLocker ドライブ暗号化（単に BitLocker とも）。

  BitLocker は、Windows オペレーティングシステムの一部です。コンピューターに Trusted Platform Module（TPM）が搭載されている場合、BitLocker は、暗号化されたハードディスクにアクセスするための回復キーを TPM に保管します。コンピューターの起動時、BitLocker は Trusted Platform Module からハードディスク回復キーを要求し、ドライブのロックを解除します。回復キーにアクセスするためにパスワードや暗証番号を使用するよう設定できます。

  既定のディスク暗号化のルールを指定して、暗号化から除外するハードディスクのリストを作成できます。Kaspersky Endpoint Security は、Kaspersky Security Center ポリシーが適用されると、ディスク全体をセクター単位で暗号化します。本製品は、ハードディスクのすべての論理パーティションを同時に暗号化します。

  システムハードディスクが暗号化されると、次回のコンピューターの起動時、ユーザーはハードディスクにアクセスしてオペレーティングシステムを読み込む前に認証エージェントによる認証を完了する必要があります。それには、コンピューターに接続されているトークンまたはスマートカードのパスワードを入力するか、*認証エージェントアカウントの管理*タスクを使用して LAN 管理者により作成される認証エージェントアカウントのユーザー名とパスワードを入力します。これらのアカウントは、ユーザーがオペレーティングシステムにログインする際にログインアカウントとして使用する Microsoft Windows アカウントに基づいています。また、認証エージェントアカウントのユーザー名とパスワードを使用してオペレーティングシステムに自動的にログインできるSingle Sign-On（シングルサインオン、SSO）技術を使用することもできます。

  > コンピューターをバックアップしてから、そのコンピューターのデータを暗号化した場合、その後、コンピューターのバックアップコピーを復元し、コンピューターのデータをもう一度暗号化すると、Kaspersky Endpoint Security により、認証エージェントアカウントの複製が作成されます。この複製されたアカウントを削除するには、klmover ユーティリティを `dupfix` キーを指定して使用します。klmover ユーティリティは、Kaspersky Security Center のビルドに含まれています。この操作の詳細については、Kaspersky Security Center のオンラインヘルプを参照してください。

暗号化されたハードディスクにアクセスできるコンピューターは、ディスク全体の暗号化機能を含む Kaspersky Endpoint Security がインストールされたコンピューターに限定されています。この予防策により、企業のローカルエリアネットワークの外からアクセスが試みられ、暗号化されたハードディスクからデータが漏出するリスクが最小限に抑えられます。

ハードディスクとリムーバブルドライブを暗号化する際、［使用されているディスク領域のみを暗号化］機能を使用できます。この機能は、まだ使用されていない新しいデバイスでのみ使用するようにしてください。すでに使用されているデバイスに暗号化を適用する場合、デバイス全体を暗号化するようにしてください。それにより、削除されているが取り出すことのできる情報を含む可能性があるデータを含め、すべてのデータが保護されます。

Kaspersky Endpoint Security は、暗号化を開始する前に、ファイルシステムセクターのマッピングを取得します。暗号化の第1段階では、暗号化を開始した時点でファイルによって占められているセクターが対象になります。暗号化の第2段階で、暗号化が開始された後に書き込まれたセクターが対象になります。暗号化が完了すると、データを含んでいるすべてのセクターが暗号化されます。

暗号化が完了した後にユーザーがファイルを削除すると、削除されたファイルが格納されていたセクターはファイルシステムレベルで新しい情報を格納するために使用可能になりますが、引き続き暗号化されます。このように、ファイルが新しいデバイスに書き込まれ、そのデバイスが［**使用されているディスク領域のみを暗号化**］機能が有効な状態で定期的に暗号化されていくことで、しばらくするとすべてのセクターが暗号化されます。

ファイルの復号化に必要なデータは、暗号化時にこのコンピューターをコントロールしていた Kaspersky Security Center 管理サーバーから提供されます。暗号化されたオブジェクトを持つコンピューターが何らかの理由で別の管理サーバーによって管理されていた場合、次のいずれかの方法で暗号化されたデータへのアクセスを取得できます：

- 同じ階層の管理サーバー：
  - 追加の操作は必要ありません。ユーザーは暗号化されたオブジェクトに引き続きアクセスできる。すべての管理サーバーに暗号鍵が配布される。
- 独立した管理サーバー：
  - LAN 管理者に暗号化されたオブジェクトへのアクセスを要求します。
  - 暗号化されたデバイスのデータの復元ツールを使用して復元する。
  - 暗号化時にこのコンピューターを管理していた Kaspersky Security Center 管理サーバーの構成をバックアップコピーから復元し、暗号化されたオブジェクトを持つコンピューターを現在管理している管理サーバーでこの構成を使用する。

暗号化されたデータへのアクセスがない場合は、暗号化されたデータを操作するための特別な指示に従ってください（暗号化されたファイルへのアクセスの復元処理、暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用）。

暗号化機能の制限

データ暗号化には次の制限があります：

- 暗号化時にサービスファイルが作成されます。これらのファイルを保存するために、ハードディスク上でフラグメント化していない約 0.5% の空き容量が必要です。ハードディスク上のフラグメント化していない空き容量が足りない場合は、十分な空き容量が用意されるまで暗号化が開始されません。
- Kaspersky Security Center の管理コンソール および Kaspersky Security Center の Web コンソールですべてのデータ暗号化を管理できます。Kaspersky Security Center Cloud コンソールでは、Bitlocker のみ管理できます。

- Kaspersky Security Center 管理システムまたは Kaspersky Security Center Cloud コンソール（BitLocker のみ）とともに Kaspersky Endpoint Security を使用する場合のみ、データ暗号化を利用できます。Kaspersky Endpoint Security は暗号鍵を Kaspersky Security Center に保存するため、Kaspersky Endpoint Security をオフラインモードで使用している場合、データ暗号化は不可能です。

- サーバー用の Microsoft Windows を実行するコンピューターに Kaspersky Endpoint Security がインストールされている場合、BitLocker ドライブ暗号化技術を使用したディスク全体の暗号化のみ使用できます。ワークステーション用の Windows を実行するコンピューターに Kaspersky Endpoint Security がインストールされている場合、データ暗号化機能が完全に利用できます。

Kaspersky Disk Encryption 技術を使用したディスク全体の暗号化は、ハードウェアおよびソフトウェア要件を満たさないハードディスクでは使用できません。

Kaspersky Endpoint Security と Kaspersky Anti-Virus for UEFI のディスク全体の暗号化機能との互換性はサポートされていません。Kaspersky Anti-Virus for UEFI はオペレーティングシステムの読み込み前に起動します。ディスク全体の暗号化を使用している場合、コンピューターにオペレーティングシステムがインストールされていないという検知を行います。これにより、Kaspersky Anti-Virus for UEFI でエラーが発生して動作が終了します。ファイルレベルの暗号化（FLE）は、Kaspersky Anti-Virus for UEFI の動作に影響しません。

Kaspersky Endpoint Security は、以下の設定をサポートします：

- HDD、SSD および USB ドライブ。

  Kaspersky Disk Encryption（FDE）技術は SSD ドライブのパフォーマンスおよびサービス残存期間が保持されている間は SSD をサポートします。

- バス経由で接続されているドライブ：SCSI、ATA、IEEE1934、USB、RAID、SAS、SATA、NVME。

- SD または MMC バス経由で接続されている非リムーバブルドライブ。

- 512 バイトセクタのドライブ。

- 512 バイトをエミュレートする 4096 バイトセクタのドライブ。

- 次の種別のパーティションを持つドライブ：GPT、MBR、および VBR（リムーバブルドライブ）。

- UEFI 64 およびレガシー BIOS 標準の埋め込みソフトウェア。

- UEFI 標準で Secure Boot がサポートされる埋め込みソフトウェア。

  *Secure Boot*は UEFI ローダーアプリケーションおよびドライバー向けにデジタル署名を検証するために設計された技術です。Secure Boot は未署名または不明な発行元により署名された UEFI アプリケーションおよびドライバーの開始をブロックします。Kaspersky Disk Encryption（FDE）は Secure Boot をサポートしています。認証エージェントは Microsoft Windows UEFI Driver Publisher 証明書により署名されています。

  一部のデバイスでは（例えば Microsoft Surface Pro および Microsoft Surface Pro 2 など）、デジタル署名検証証明書の日付の古いリストが既定でインストールされていることがあります。ドライブを暗号化する前に、これらの証明書のリストをアップデートする必要があります。

- UEFI 標準で Fast Boot がサポートされる埋め込みソフトウェア。

  Fast Boot は、コンピューターの起動速度向上に役立つ技術です。Fast Boot 技術が有効になっていると、通常コンピューターはオペレーティングシステムの開始に必要な最低限の UEFI ドライバー設定のみ読み込みます。Fast Boot 技術が有効になっていると、認証エージェントが実行している最中に USB キーボード、マウス、USB トークン、タッチパッドおよびタッチスクリーンが正常に動作しないことがあります。

Kaspersky Disk Encryption（FDE）を使用するには、Fast Boot 技術を無効にすることを推奨します。FDE テストユーティリティを使用して、Kaspersky Disk Encryption（FDE）の動作をテストすることもできます。

Kaspersky Endpoint Security は、以下の構成をサポートしません：

- ブートローダーが配置されているドライブとオペレーティングシステムが配置されているドライブが異なる。
- システムに UEFI 32 標準の組み込みソフトウェアが含まれている。
- システムが Intel® Rapid Start Technology を持ち、ハイバネーション用パーティションがあるドライブ（Intel® Rapid Start Technology を無効にしている場合も含む）。
- 10 以上の拡張パーティションを含む MBR 形式のドライブ。
- スワップファイルがシステムドライブ以外のドライブに配置されている。
- 複数のオペレーティングシステムがインストールされているマルチブートシステム。
- 動的パーティション（最初のパーティションのみがサポートされます）。
- 断片化していない空き容量が 0.5% 未満のドライブ。
- セクターサイズが 512 バイト（または 512 バイトをエミュレートする 4096 バイト）以外であるドライブ。
- ハイブリッドドライブ。
- システムにサードパーティローダーがある。
- 圧縮 NTFS ディレクトリのドライブ。
- Kaspersky Disk Encryption（FDE）技術はほかのディスク全体の暗号化技術（BitLocker、McAfee Drive Encryption、および WinMagic SecureDoc など）とは互換性がありません。
- Kaspersky Disk Encryption（FDE）技術は ExpressCache 技術とは互換性がありません。
- 暗号化されたドライブ上のパーティションの作成、削除、変更はサポートされていません。データ損失の可能性があります。
- ファイルシステムのフォーマットはサポートされていません。データ損失の可能性があります。

  Kaspersky Disk Encryption（FDE）技術で暗号化されたドライブをフォーマットする必要がある場合、Kaspersky Endpoint Security for Windows がインストールされていないコンピューター上で、ディスク全体の暗号化のみ使用してドライブをフォーマットしてください。

  クイックフォーマットオプションでフォーマットされた暗号化されたドライブは、次に Kaspersky Endpoint Security for Windows がインストールされたコンピューターに接続した際に暗号化されたものと誤認される可能性があります。ユーザーデータは利用できなくなります。
- 認証エージェントは 100 アカウント以上はサポートしません。
- シングルサインオン技術はサードパーティ開発元によるその他の技術とは互換性がありません。

- Kaspersky Disk Encryption（FDE）技術は次のデバイスのモデルではサポートされていません：
  - Dell Latitude E6410（UEFI モード）
  - HP Compaq nc8430（レガシー BIOS モード）
  - Lenovo ThinkCentre 8811（レガシー BIOS モード）
- 認証エージェントはレガシー USB サポートが有効になっている場合は USB トークンの動作はサポートしません。コンピューター上ではパスワードによる認証のみ可能です。
- レガシー BIOS モードでドライブを暗号化する場合は、次のモデルのデバイスではレガシー USB サポートを有効にすることをお勧めします：
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530

- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s（74665YG）
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51（マザーボード）

暗号鍵（AES56 / AES256）の鍵長の変更

Kaspersky Endpoint Security では、Advanced Encryption Standard（AES）暗号アルゴリズムが使用されます。Kaspersky Endpoint Security では、鍵長が 256 ビットまたは 56 ビットの AES 暗号アルゴリズムがサポートされます。データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（*強度の高い暗号化（AES256）*または*相対的に強度の低い暗号化（AES56）*）。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。

暗号鍵の鍵長の変更は Kaspersky Endpoint Security 11.2.0 以降でのみ利用できます。

暗号鍵長の変更は、次の手順で行います：

1. 暗号鍵長を変更する前に Kaspersky Endpoint Security によって暗号化されているオブジェクトを復号します。
   a. ハードディスクを復号します。
   b. ローカルドライブでファイルを復号します。
   c. リムーバブルドライブを復号します。

   暗号鍵長を変更すると、それ以前に暗号化されたオブジェクトは使用できなくなります。
2. Kaspersky Endpoint Security をアンインストールします。
3. 鍵長が異なる暗号化ライブラリを含む配布パッケージから Kaspersky Endpoint Security をインストールします。

あるいは、本製品をアップグレードすることで暗号鍵長を変更することもできます。次の条件を満たす場合にのみ、本製品のアップグレードによって鍵長を変更できます：

- Kaspersky Endpoint Security 10 Service Pack 2 以降がコンピューターにインストールされている。
- データ暗号化コンポーネント（ファイルレベルの暗号化、ディスク全体の暗号化）がコンピューターにインストールされていない。

  既定では、データ暗号化コンポーネントは Kaspersky Endpoint Security のインストールに含まれていません。BitLocker の管理コンポーネントは暗号鍵長の変更に影響しません。

暗号鍵長を変更するには、目的の暗号化ライブラリを含む配布パッケージから kes_win.msi または setup_kes.exe ファイルを実行します。インストールパッケージを使用してリモートで本製品をアップグレードすることもできます。

コンピューターにインストールされている製品をアンインストールせずに、この製品と同じバージョンの配布パッケージを使用して暗号鍵の鍵長を変更することはできません。

Kaspersky Disk Encryption

Kaspersky Disk Encryption は、ワークステーション用の Windows オペレーティングシステム上でのみ使用できます。サーバー用の Windows オペレーティングシステムを実行しているコンピューターには、BitLocker ドライブ暗号化技術を使用してください。

Kaspersky Endpoint Security は、FAT32 、NTFS および exFat ファイルシステムの暗号化に対応しています。

ディスク全体の暗号化を開始する前に、多数のチェックが実行され、暗号化をデバイスに適用できるかどうかが判断されます。このチェックには、システムのハードディスクと認証エージェントまたは BitLocker 暗号化との互換性チェックも含まれます。互換性をチェックするため、コンピューターを再起動する必要があります。コンピューターの再起動後、必要なチェックがすべて自動的に行われます。互換性チェックが正常に終了すると、オペレーティングシステムが起動し本製品が読み込まれます。その後、ディスク全体の暗号化が実行されます。システムのハードディスクに認証エージェントおよび BitLocker 暗号化との互換性がないことがわかった場合は、ハードウェアリセットボタンを押して、コンピューターを再起動する必要があります。互換性がないという情報は、Kaspersky Endpoint Security によりレポートに記録されます。この情報に基づき、オペレーティングシステムの起動時に、ディスク全体の暗号化は開始されません。このイベントに関する情報は、Kaspersky Security Center レポートに記録されます。

コンピューターのハードウェア構成の変更後、システムのハードディスクと認証エージェントおよび BitLocker 暗号化との互換性をチェックするには、前述のチェック中に記録された非互換性情報を削除する必要があります。そのためには、ディスク全体を暗号化する前に、コマンドラインに `avp pbatestreset` と入力します。システムのハードディスクで認証エージェントとの互換性がチェックされた後にオペレーティングシステムを読み込めない場合は、復元ツールを使用して認証エージェントのテスト操作後に残ったオブジェクトとデータを削除する必要があります。その後 Kaspersky Endpoint Security を起動し、`avp pbatestreset` コマンドを再度実行します。

ディスク全体の暗号化の開始後、Kaspersky Endpoint Security は、ハードディスクに書き込まれているデータをすべて暗号化します。

ディスク全体の暗号化の実行中にユーザーがコンピューターをシャットダウンまたは再起動した場合、次回のオペレーティングシステムの起動前に、認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ディスク全体の暗号化を再開します。

ディスク全体の暗号化の進行中にオペレーティングシステムがハイバネーションモードに切り替わった場合は、オペレーティングシステムがハイバネーションモードから通常のモードに復帰した時点で認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ディスク全体の暗号化を再開します。

ディスク全体の暗号化の進行中にオペレーティングシステムがスリープモードに入った場合、オペレーティングシステムがスリープモードから復帰したときにディスク全体の暗号化が再開されます。認証エージェントは読み込まれません。

認証エージェントでのユーザー認証は 2 通りの方法で実行できます：

- LAN 管理者が Kaspersky Security Center ツールを使用して作成した認証エージェントアカウントの名前とパスワードを入力する。
- コンピューターに接続されたトークンまたはスマートカードのパスワードを入力する。

  トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合にのみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

認証エージェントは、以下の言語のキーボード配列をサポートします：

- 英語（英国）
- 英語（米国）
- アラビア語（アルジェリア、モロッコ、チュニジア、AZERTY 配列）
- スペイン語（ラテンアメリカ）
- イタリア語
- ドイツ語（ドイツ、オーストリア）
- ドイツ語（スイス）
- ポルトガル語（ブラジル、ABNT2 配列）
- ロシア語（IBM / Windows 105 キーボード、QWERTY 配列）
- トルコ語（QWERTY 配列）
- フランス語（フランス）
- フランス語（スイス）

- フランス語（ベルギー、AZERTY 配列）
- 日本語（106 キーボード、QWERTY 配列）

キーボードの配列がオペレーティングシステムの言語と地域の規格の設定に追加されており、Microsoft Windows のログオン画面で使用可能である場合に、認証エージェントでその配列が使用できるようになります。

認証エージェントのアカウント名に、認証エージェントで使用できるキーボード配列で入力できない記号が含まれている場合、暗号化されたハードディスクは、復元ユーティリティを使用して復元してから、または認証エージェントのアカウント名とパスワードを復元してからでないと、アクセスできません。

SSD ドライブ暗号化の特別な機能

本製品は SSD ドライブ、ハイブリッド SSHD ドライブ、Intel Smart Response を持つドライブをサポートします。本製品は Intel Rapid Start を持つドライブの暗号化はサポートしません。このようなドライブを暗号化する前に Intel Rapid Start を無効にしてください。

SSD ドライブの暗号化には、次の特別な機能があります：

- SSD ドライブが新しい、または SSD に重要なデータがない場合は、使用済みのスペースのみの暗号化を有効にしてください。関連するドライブセクターを上書きできます。
- SSD ドライブが使用中で、重要なデータがある場合は、次のオプションから 1 つ選択します：
  - SSD ドライブを完全に消去し、オペレーティングシステムをインストールしてから 使用済みのスペースのみの暗号化を有効するオプションを使用して SSD ドライブの暗号化を実行する
  - 使用済みのスペースのみの暗号化を有効するオプションを無効にして SSD ドライブの暗号化を実行する

SSD ドライブの暗号化には 5〜10 GB の空き容量が必要です。暗号化した管理データの保存に必要な空き容量は下の表に記載されています。

暗号化した管理データの保存に必要な空き容量

SSD ドライブのサイズ（GB）	SSD ドライブのプライマリパーティションの空き容量（MB）	SSD ドライブのセカンダリパーティションの空き容量（MB）
128	250	64
256	250	640
512	300	128

Kaspersky Disk Encryption の開始

ディスク全体の暗号化を行う前に、コンピューターが感染していないことを確認してください。確認するには、完全スキャンか簡易スキャンを開始します。ルートキットによって感染したコンピューターでディスク全体の暗号化を行うと、ハードディスクが動作しなくなる可能性があります。

ディスクの暗号化を開始する前に、認証エージェントアカウントの設定を確認してください。Kaspersky Disk Encryption（FDE）技術を使用して保護されているドライブを操作するには、認証エージェントが必要です。オペレーティングシステムを読み込む前に、ユーザーはエージェントで認証を完了する必要があります。Kaspersky Endpoint Security では、ドライブを暗号化する前に認証エージェントアカウントを自動的に作成できます。ディスク全体の暗号化ポリシー設定で認証エージェントアカウントの自動作成を有効にできます（下の説明を参照してください）。シングルサインオン（SSO）技術の使用もできます。

Kaspersky Endpoint Security では、次のユーザーグループ向けの認証エージェントアカウントを自動的に作成できます。

- **コンピューター上のすべてのアカウント**：常時有効なコンピューター上のすべてのアカウント。
- **コンピューター上のすべてのドメインアカウント**：いずれかのドメインに属しており、常時有効なコンピューター上のすべてのアカウント。
- **コンピューター上のすべてのローカルアカウント**：常時有効なコンピューター上のすべてのローカルアカウント。
- **ワンタイムパスワードが設定されたサービスアカウント**：サービスアカウントは、ユーザーがパスワードを忘れたときなどにコンピューターへのアクセス権を取得するために必要です。このサービスアカウントは予備のアカウントとして使用することもできます。アカウントの名前を入力する必要があります（既定では `ServiceAccount` です）。Kaspersky Endpoint Security はパスワードを自動で作成します。Kaspersky Security Center コンソールでパスワードを確認できます。
- **ローカル管理者**：Kaspersky Endpoint Security は、コンピューターのローカル管理者に認証エージェントのユーザーアカウントを作成します。
- **コンピューター管理者**：Kaspersky Endpoint Security は、コンピューター管理者に認証エージェントのユーザーアカウントを作成します。Active Directory のコンピューターのプロパティで、どのアカウントがコンピューター管理者ロールを持っているか確認できます。既定では、コンピューター管理者ロールは定義されておらず、どのアカウントにも紐づけられていません。
- **アクティブなアカウント**：Kaspersky Endpoint Security は、ディスクの暗号化時に有効になっているアカウントに対して自動的に認証エージェントアカウントを作成します。

*認証エージェントアカウントの管理*タスクは、ユーザー認証設定を設定するために構成されています。このタスクを使用して、新しいアカウントの追加、現在のアカウントの設定の編集、または必要に応じてアカウントを削除することができます。個別のコンピューターにローカルタスクを使用できるだけでなく、個別の管理グループまたは選択されたコンピューターにグループタスクを使用できます。

管理コンソール（MMC）を使用して Kaspersky Disk Encryption を実行する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。
4. ［**暗号化技術**］から［**Kaspersky Disk Encryption**］を選択します。

   Kaspersky Disk Encryption 技術は、コンピューターに BitLocker で暗号化されたハードディスクがある場合は使用できません。

5. ［**暗号化モード**］から［**すべてのハードディスクを暗号化する**］を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、すべてのディスクの暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。

いくつかのハードディスクを暗号化から除外する必要がある場合は、除外するハードディスクのリストを作成します。

6. Kaspersky Disk Encryption の詳細なオプションを設定します（下記の表を参照）。
7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールを使用して Kaspersky Disk Encryption を実行する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**ディスク全体の暗号化**］に移動します。
5. ［**Kaspersky Disk Encryption**］技術を選択します。

Kaspersky Disk Encryption 技術は、コンピューターに BitLocker で暗号化されたハードディスクがある場合は使用できません。

6. ［**デバイスの操作**］ブロックで、［**すべてのハードディスクを暗号化する**］を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化すると、暗号化を実行したオペレーティングシステムのみを読み込めます。

いくつかのハードディスクを暗号化から除外する必要がある場合は、除外するハードディスクのリストを作成します。

7. Kaspersky Disk Encryption の詳細なオプションを設定します（下記の表を参照）。
8. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品のメインウィンドウから実行できます。



暗号化モニター

システムのハードディスクが暗号化されている場合、オペレーティングシステムの起動前に認証エージェントが読み込まれます。認証エージェントを使用して認証を完了し、暗号化されたハードディスクへのアクセス権を得てオペレーティングシステムを読み込みます。認証手順が問題なく完了したら、オペレーティングシステムが読み込まれます。認証プロセスは、オペレーティングシステムが再起動するたびに繰り返されます。

Kaspersky Disk Encryption の設定

パラメータ	説明
暗号化中にユーザーの認証エージェントアカウントを自動で作成する	このチェックボックスをオンにすると、コンピューター上の Windows ユーザーアカウントのリストに基づいて認証エージェントアカウントを作成します。既定では、Kaspersky Endpoint Security は、過去 30 日間にユーザーがオペレーティングシステムにログインしたすべてのローカルアカウントとドメインアカウントを使用します。
このコンピューターのすべてのユーザーの初回ログイン時に認証エージェントアカウントを自動で作成する	このチェックボックスをオンにすると、認証エージェントの開始前にコンピューター上の Windows ユーザーアカウントに関する情報をチェックします。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。認証エージェントアカウントには次の既定の設定（パスワードで保護されているログインのみ、初回認証時のパスワード変更を要求）が適用されています。そのため、すでに暗号化されたドライブを持つコンピューター用に*認証エージェントアカウントの管理*タスクを使用して認証エージェントを手動で追加する必要はありません。
認証エージェントに入力したユーザー名を保存する	チェックボックスをオンにすると、認証エージェントアカウントの名前が保存されます。次回、認証エージェントで同じアカウントを使用して認証を完了しようとした場合、アカウント名の入力は要求されません。

パラメータ	説明
使用されているディスク領域のみを暗号化（暗号化時間を短縮）	このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。 暗号化の開始後に［**使用されているディスク領域のみを暗号化（暗号化時間を短縮）**］を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。 このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。 チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。 データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。既に使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。 既定では、このチェックボックスはオフです。
レガシー USB サポートを使用する（推奨されません）	このチェックボックスでは、Legacy USB Support 機能を有効または無効にします。*レガシー USB サポート* **は** BIOS / UEFI 機能であり、オペレーティングシステム（BIOS モード）を起動する前のコンピューターのブートフェーズ中に USB デバイス（セキュリティトークンなど）を使用することができます。レガシー USB サポートは、オペレーティングシステムが起動した後の USB デバイスのサポートには影響しません。 このチェックボックスをオンにすると、コンピューター起動中の USB デバイスのサポートが有効になります。 レガシー USB サポート（Legacy USB Support）が有効になっている場合、BIOS モードの認証エージェントでは USB を介してトークンを操作することはできません。ハードウェアの互換性の問題が発生しているコンピューターでのみ、このオプションをオンにしてください。

暗号化から除外するハードディスクのリスト作成

暗号化から除外するリストは、Kaspersky Disk Encryption 技術でのみ作成できます。

暗号化から除外するハードディスクのリストを作成するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。
4. ［**暗号化技術**］から［**Kaspersky Disk Encryption**］を選択します。
   ［**次のハードディスクを暗号化しない**］テーブルに、暗号化から除外するハードディスクに対応するエントリが表示されます。暗号化から除外するハードディスクのリストを以前に作成していない場合、このテーブルは空白です。
5. 暗号化から除外するハードディスクのリストにハードディスクを追加するには：
   a. ［**追加**］をクリックします。
   b. 表示されるウィンドウで、［**デバイス名**］、［**コンピューター**］、［**ディスク種別**］、［**Kaspersky Disk Encryption**］の値を指定します。

c. ［**更新**］をクリックします。

d. ［**名前**］列で、暗号化から除外するハードディスクのリストに追加するハードディスクのテーブル列のチェックボックスをオンにします。

e. ［**OK**］をクリックします。

［**次のハードディスクを暗号化しない**］テーブルに、選択したハードディスクが表示されます。

6. 変更内容を保存します。

暗号化から除外するハードディスクのリストのエクスポートおよびインポート

暗号化から除外するハードディスクのリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別の多数の除外リストをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、除外リストのバックアップをとったり、別のサーバーに除外リストを移行することができます。

管理コンソール（MMC）で暗号化から除外するハードディスクのリストをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。

4. ［**暗号化技術**］から［**Kaspersky Disk Encryption**］を選択します。

［**次のハードディスクを暗号化しない**］テーブルに、暗号化から除外するハードディスクに対応するエントリが表示されます。

5. 除外リストをエクスポートするには：

a. エクスポートする除外リストを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。

除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。

b. → ［**エクスポート**］を選択します。

c. 表示されたウィンドウで、除外リストをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. ファイルを保存します。

Kaspersky Endpoint Security は、除外リスト全体を XML ファイルにエクスポートします。

6. ルールのリストをインポートするには：

a. → ［**インポート**］を選択します。

b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

c. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

Web コンソールで暗号化から除外するハードディスクのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**ディスク全体の暗号化**］に移動します。

［**Kaspersky Disk Encryption**］技術を選択します。

5. ［**除外リスト**］リンクをクリックします。

除外リストが表示されます。

6. ルールのリストをエクスポートするには：

a. エクスポートする除外リストを選択します。

b. → ［**エクスポート**］を選択します。

Kaspersky Endpoint Security は既定のダウンロードフォルダーに除外リストを JSON ファイルでエクスポートします。

7. 除外リストをインポートするには：

a. → ［**インポート**］を選択します。

表示されたウィンドウで、除外リストをインポートする JSON ファイルを選択します。

b. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、JSON ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

シングルサインオン（SSO）技術の有効化

シングルサインオン（Single Sign-On、SSO）技術を使用すると、認証エージェントの認証情報を使用してオペレーティングシステムに自動的にログインできます。つまり、ユーザーがパスワード（認証エージェントアカウントのパスワード）を入力する必要があるのは、Windows にログインするときの 1 度のみということです。シングルサインオン技術を使用すると、Windows アカウントのパスワードが変更された際にも、認証エージェントアカウントのパスワードを自動的に更新することができます。

シングルサインオン技術を使用する場合、認証エージェントは Kaspersky Security Center で指定されたパスワードの強度の要件を無視します。パスワードの強度の要件は、オペレーティングシステムの設定で設定できます。

シングルサインオン（SSO）技術の有効化

管理コンソール（MMC）でシングルサインオン技術の使用を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**暗号化の共通設定**］の順に選択します。
4. ［**パスワードの設定**］ブロックの［**設定**］をクリックします。
5. 開いたウィンドウの［**認証エージェント**］タブで、［**シングルサインオン（SSO）技術を使用する**］をオンにします。
6. サードパーティの資格情報プロバイダーを使用している場合は、［**サードパーティの資格情報プロバイダーをラップする**］をオンにします。
7. 変更内容を保存します。

その結果、ユーザーは、エージェントで一度だけ認証手順を完了する必要があります。認証手順は、オペレーティングシステムの読み込みには必要ありません。オペレーティングシステムが自動的にロードされます。

Web コンソールでシングルサインオンの使用を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**ディスク全体の暗号化**］に移動します。
5. ［**Kaspersky Disk Encryption**］技術を選択します。
6. ［**パスワードの設定**］ブロックで、［**シングルサインオン（SSO）技術を使用する**］をオンにします。
7. サードパーティの資格情報プロバイダーを使用している場合は、［**サードパーティの資格情報プロバイダーをラップする**］をオンにします。
8. 変更内容を保存します。

その結果、ユーザーは、エージェントで一度だけ認証手順を完了する必要があります。認証手順は、オペレーティングシステムの読み込みには必要ありません。オペレーティングシステムが自動的にロードされます。

シングルサインオンが機能するには、Windows アカウントのパスワードと認証エージェントアカウントのパスワードが一致する必要があります。パスワードが一致しない場合、ユーザーは認証手順を 2 回実行する必要があります。認証エージェントのインターフェイス上および、オペレーティングシステムをロードする前です。パスワードを同期するため、これらの操作を 1 度だけ実行する必要があります。その後、Kaspersky Endpoint Security は、認証エージェントアカウントのパスワードを Windows アカウントのパスワードに置き換えます。Windows アカウントのパスワードが変更された場合、本製品は自動的に認証エージェントアカウントのパスワードを更新します。

サードパーティの資格情報プロバイダー

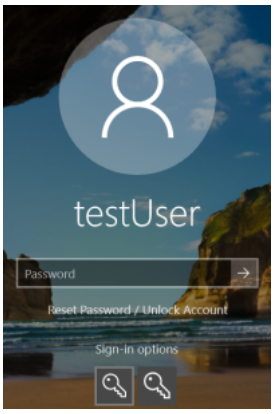
Kaspersky Endpoint Security では、サードパーティの資格情報プロバイダー ADSelfService Plus がサポートされます。

サードパーティの資格情報プロバイダーと連携する際には、認証エージェントはオペレーティングシステムが読み込まれる前にパスワードを読み取ります。つまり、ユーザーがパスワードを入力する必要があるのは、Windows にログインするときの 1 度のみということです。Windows にログインした後、ユーザーは企業のサービスの認証などにサードパーティの資格情報プロバイダーを使用することができます。サードパーティの資格情報プロバイダーを使用して、ユーザーは個別に自身のパスワードをリセットすることが可能です。この場合、Kaspersky Endpoint Security は認証エージェントのパスワードを自動的に更新します。

本製品がサポートしていないサードパーティの資格情報プロバイダーを使用している場合は、シングルサインオン技術の操作に制限がある可能性があります。Windows にログインする際、ユーザーは、システム内の資格情報プロバイダーとサードパーティの資格情報プロバイダーの 2 つのプロファイルを使用できます。これらのプロファイルのアイコンは同一になります（以下の図を参照）。ユーザーが続行するには次の 2 つのオプションがあります：

- ユーザーが *サードパーティの資格情報プロバイダー*を選択した場合は、認証エージェントは Windows アカウントのパスワードを同期することができません。このため、ユーザーが Windows アカウントのパスワードを変更すると、Kaspersky Endpoint Security は認証エージェントアカウントのパスワードを更新することができません。結果、ユーザーは認証手順を 2 回実行する必要があります。認証エージェントのインターフェイス上および、オペレーティングシステムを読み込む前です。この場合、ユーザーは企業のサービスの認証などにサードパーティの資格情報プロバイダーを使用することができます。

- ユーザーが *システム内の資格情報プロバイダー*を選択した場合は、認証エージェントは Windows アカウントのパスワードを同期します。この場合、ユーザーは企業のサービスの認証などにはサードパーティの資格情報プロバイダーを使用することができません。



システム認証プロファイルと Windows ログオン用サードパーティの認証プロファイル

認証エージェントアカウントの管理

Kaspersky Disk Encryption（FDE）技術を使用して保護されているドライブを操作するには、認証エージェントが必要です。オペレーティングシステムを読み込む前に、ユーザーはエージェントで認証を完了する必要があります。*認証エージェントアカウントの管理*タスクは、ユーザー認証設定を設定するために構成されています。個別のコンピューターにローカルタスクを使用できるだけでなく、個別の管理グループまたは選択されたコンピューターにグループタスクを使用できます。

*認証エージェントアカウントの管理*タスクを開始するスケジュールを構成することはできません。タスクを強制的に停止することもできません。

管理コンソール（MMC）で認証エージェントアカウントの管理タスクを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**認証エージェントアカウントの管理**］の順に選択します。

ステップ 2：認証エージェントアカウント管理コマンドの選択

認証エージェントアカウント管理コマンドのリストを生成します。管理コマンドを使用すると、認証エージェントアカウントを追加、変更、および削除できます。認証エージェントアカウントを持つユーザーのみが認証手順を完了し、オペレーティングシステムをロードし、暗号化されたドライブにアクセスできます。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスク名の定義

タスクの名前を入力します。たとえば、「*管理者アカウント*」など。

ステップ 5：タスク作成の完了

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

その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

Web コンソールで認証エージェントアカウントの管理タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］ドロップダウンリストで、**Kaspersky Endpoint Security for Windows (12.12)** を選択します。
2. ［**タスク種別**］から［**認証エージェントアカウントの管理**］を選択します。

3. ［**タスク名**］に「*管理者アカウント*」などの簡潔な名前を付けます。

4. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

ステップ 2：認証エージェントアカウントの管理

認証エージェントアカウント管理コマンドのリストを生成します。管理コマンドを使用すると、認証エージェントアカウントを追加、変更、および削除できます。認証エージェントアカウントを持つユーザーのみが認証手順を完了し、オペレーティングシステムをロードし、暗号化されたドライブにアクセスできます。

ステップ 3：タスク作成の完了

ウィザードを終了します。タスクのリストに新しいタスクが表示されます。

タスクを実行するには、タスクのチェックボックスをオンにし、［**開始**］をクリックします。

その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

認証エージェントアカウントを追加するには、*認証エージェントアカウントの管理*タスクに特別なコマンドを追加する必要があります。たとえば、すべてのコンピューターに管理者アカウントを追加するには、グループタスクを使用すると便利です。

Kaspersky Endpoint Security では、ドライブを暗号化する前に認証エージェントアカウントを自動的に作成できます。ディスク全体の暗号化ポリシー設定で認証エージェントアカウントの自動作成を有効にできます。シングルサインオン（SSO）技術の使用もできます。

管理コンソール（MMC）を使用して認証エージェントアカウントを追加する方法

1. *認証エージェントアカウントの管理*タスクのプロパティを開きます。

2. タスクのプロパティで、［**設定**］セクションを選択します。

3. ［**追加**］→［**アカウント追加コマンド**］をクリックします。

4. 開いたウィンドウの［**Windows アカウント**］フィールドで、認証エージェントアカウントの作成に使用される Microsoft Windows アカウントの名前を指定します。

5. Windows アカウント名を手動で入力した場合は、［**許可**］をクリックして、アカウントのセキュリティ識別子（SID）を定義します。

   ［**許可**］をクリックしてセキュリティ識別子（SID）を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

   > Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、*認証エージェントアカウントの管理*タスクはエラーで終了します。

6. 認証エージェントのために以前に作成されたアカウントを、作成されるアカウントで置き換える場合、［**既存のアカウントの置き換え**］をオンにします。

   このステップは、認証エージェントアカウントの管理用のグループタスクのプロパティに認証エージェントアカウント作成コマンドを追加する場合に使用できます。このステップは、ローカルタスクの［*認証エージェントアカウントの管理*］のプロパティに認証エージェントアカウント作成コマンドを追加する場合には使用できません。

7. ［**ユーザー名**］に、暗号化されたハードディスクへのアクセスのための認証時に入力する必要がある認証エージェントアカウントの名前を入力します。

8. 暗号化されたハードディスクへのアクセスのための認証時に、認証エージェントアカウントのパスワードの入力を求めるメッセージをユーザーに表示する場合は、［**パスワードベースの認証を有効にする**］をオンにします。認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。

9. 暗号化されたハードディスクへのアクセスのための認証時に、トークンまたはスマートカードをコンピューターに接続することを求める場合は、［**証明書ベースの認証を有効にする**］をオンにします。スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。

10. 必要に応じて、［**コマンドの説明**］に、コマンド管理に必要な認証エージェントアカウントの詳細情報を入力します。

11. ［**認証エージェントでの認証へのアクセス**］ブロックで、コマンド内で指定されたアカウントを使用するユーザーの認証エージェントでの認証へのアクセスを設定します。

12. 変更内容を保存します。

Web コンソールを使用して認証エージェントアカウントを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. Kaspersky Endpoint Security の **認証エージェントアカウントの管理**タスクを選択します。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. 認証エージェントアカウントのリストで、［**追加**］をクリックします。

   これにより、認証エージェントアカウント管理ウィザードが起動します。

5. **追加**コマンドタイプを選択します。

6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。次の手順に進みます。

   Kaspersky Endpoint Security は、アカウントセキュリティ識別子（SID）を決定します。これは、アカウントを確認するために必要です。ユーザー名を誤って入力した場合、Kaspersky Endpoint Security はエラーでタスクを終了します。

7. 認証エージェントのアカウント設定を設定します。

   - **認証エージェントアカウントを新規に作成して既存のアカウントを置き換える**：Kaspersky Endpoint Security は、コンピューター上の既存のアカウントをスキャンします。コンピューターとタスクのユーザーセキュリティ識別子が一致する場合、Kaspersky Endpoint Security はタスクに従ってアカウント設定を変更します。

   - **ユーザー名**：認証エージェントアカウントの既定のユーザー名は、ユーザーのドメイン名に対応しています。

   - **パスワードベースの認証を有効にする**：認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。このようにして、各ユーザーは独自のパスワードを持ちます。ポリシーで、認証エージェントアカウントのパスワードの強度要件を設定することもできます。

   - **証明書ベースの認証を有効にする**：スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。この方法では、ユーザーはスマートカードまたはトークンのパスワードを入力する必要があります。

   - **暗号化されたデータへのアカウントのアクセス**：暗号化されたドライブへのユーザーアクセスを設定します。たとえば、認証エージェントアカウントを削除する代わりに、ユーザー認証を一時的に無効にすることができます。

   - **コメント**：必要に応じて、アカウントの説明を入力します。

8. 変更内容を保存します。

9. タスクの横のチェックボックスをオンにし、［**開始**］をクリックします。

   その結果、コンピューターの次回起動時にタスクが完了した後、新規ユーザーは認証手順を完了し、オペレーティングシステムを読み込み、暗号化されたドライブにアクセスできます。

認証エージェントアカウントのパスワードおよびその他の設定を変更するには、*認証エージェントアカウントの管理*タスクに特別なコマンドを追加する必要があります。たとえば、すべてのコンピューターの管理者トークン証明書を置き換えるには、グループタスクを使用すると便利です。

管理コンソール（MMC）を使用して認証エージェントアカウントを変更する方法

1. *認証エージェントアカウントの管理*タスクのプロパティを開きます。

2. タスクのプロパティで、［**設定**］セクションを選択します。

3. ［**追加**］→［**アカウント編集コマンド**］をクリックします。

4. 開いたウィンドウの［**Windows アカウント**］フィールドで、変更する Microsoft Windows ユーザーアカウントの名前を指定します。

5. Windows アカウント名を手動で入力した場合は、［**許可**］をクリックして、アカウントのセキュリティ識別子（SID）を定義します。

   ［**許可**］をクリックしてセキュリティ識別子（SID）を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

   > Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、*認証エージェントアカウントの管理*タスクはエラーで終了します。

6. ［**ユーザー名の変更**］で示される名前を持つ Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントのユーザー名をその下にあるフィールドに入力した名前に変更する場合は、［**Windows アカウント**］をオンにして、認証エージェントユーザーアカウントの新しい名前を入力します。

7. パスワードベースの認証設定を編集できるようにするには、［**パスワードベースの認証設定を変更する**］をオンにします。

8. 暗号化されたハードディスクへのアクセスのための認証時に、認証エージェントアカウントのパスワードの入力を求めるメッセージをユーザーに表示する場合は、［**パスワードベースの認証を有効にする**］をオンにします。認証エージェントアカウントのパスワードを設定します。

9. ［**認証エージェントでの認証時のパスワード変更ルールの編集**］に表示された名前を持つ Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントについて、パスワード変更設定の値をその下で指定する設定値に変更する場合は、［**Windows アカウント**］をオンにします。

10. 認証エージェントでの認証時のパスワード変更設定の値を指定します。

11. トークンまたはスマートカードの電子証明書に基づく認証の設定を編集できるようにするには、［**証明書ベースの認証設定を変更する**］をオンにします。

12. 暗号化されたハードディスクへのアクセスのための認証プロセスで、コンピューターに接続されたトークンまたはスマートカードに対するパスワードの入力を求めるメッセージをユーザーに表示する場合は、［**証明書ベースの認証を有効にする**］をオンにします。スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。

13. ［**コマンドの説明の編集**］に表示されている名前の Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントのコマンド説明を変更する場合は、［**Windows アカウント**］をオンにして、コマンド説明を編集します。

14. ［**認証エージェントでの認証アクセスルールの編集**］に表示されている名前の Microsoft Windows アカウントを使用して作成されたすべての認証エージェントアカウントについて、認証エージェントでの認証ダイアログへのユーザーアクセスのルールを、その下で指定する値に変更する場合は、［**Windows アカウント**］をオンにします。

15. 認証エージェントでの認証ダイアログへのアクセスのルールを指定します。

16. 変更内容を保存します。

Web コンソールを使用して認証エージェントアカウントを変更する方法

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

2. Kaspersky Endpoint Security の **認証エージェントアカウントの管理**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. 認証エージェントアカウントのリストで、［**追加**］をクリックします。
   これにより、認証エージェントアカウント管理ウィザードが起動します。

5. **変更**コマンドタイプを選択します。

6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。次の手順に進みます。

   Kaspersky Endpoint Security は、アカウントセキュリティ識別子（SID）を決定します。これは、アカウントを確認するために必要です。ユーザー名を誤って入力した場合、Kaspersky Endpoint Security はエラーでタスクを終了します。

7. 編集する設定の横にあるチェックボックスをオンにします。

8. 認証エージェントのアカウント設定を設定します。

   - **認証エージェントアカウントを新規に作成して既存のアカウントを置き換える**：Kaspersky Endpoint Security は、コンピューター上の既存のアカウントをスキャンします。コンピューターとタスクのユーザーセキュリティ識別子が一致する場合、Kaspersky Endpoint Security はタスクに従ってアカウント設定を変更します。

   - **ユーザー名**：認証エージェントアカウントの既定のユーザー名は、ユーザーのドメイン名に対応しています。

   - **パスワードベースの認証を有効にする**：認証エージェントアカウントのパスワードを設定します。必要に応じて、最初の認証後にユーザーに新しいパスワードを要求できます。このようにして、各ユーザーは独自のパスワードを持ちます。ポリシーで、認証エージェントアカウントのパスワードの強度要件を設定することもできます。

   - **証明書ベースの認証を有効にする**：スマートカードまたはトークンを使用した認証用の証明書ファイルを選択します。この方法では、ユーザーはスマートカードまたはトークンのパスワードを入力する必要があります。

   - **暗号化されたデータへのアカウントのアクセス**：暗号化されたドライブへのユーザーアクセスを設定します。たとえば、認証エージェントアカウントを削除する代わりに、ユーザー認証を一時的に無効にすることができます。

   - **コメント**：必要に応じて、アカウントの説明を入力します。

9. 変更内容を保存します。

10. タスクの横のチェックボックスをオンにし、［**開始**］をクリックします。

認証エージェントアカウントを削除するには、*認証エージェントアカウントの管理*タスクに特別なコマンドを追加する必要があります。たとえば、解雇された従業員のアカウントを削除するには、グループタスクを使用すると便利です。

管理コンソール（MMC）を使用して認証エージェントアカウントを削除する方法

1. *認証エージェントアカウントの管理*タスクのプロパティを開きます。

2. タスクのプロパティで、［**設定**］セクションを選択します。

3. ［**追加**］→［**アカウント削除コマンド**］をクリックします。

4. 開いたウィンドウの［**Windows アカウント**］フィールドで、削除する認証エージェントアカウントの作成に使用された Windows ユーザーアカウントの名前を指定します。

5. Windows アカウント名を手動で入力した場合は、［**許可**］をクリックして、アカウントのセキュリティ識別子（SID）を定義します。

   ［**許可**］をクリックしてセキュリティ識別子（SID）を特定しない場合は、コンピューター上でタスクが実行される際に SID が決定されます。

Windows アカウント名が正しく入力されたことを確認するには、Windows アカウントのセキュリティ識別子を定義する必要があります。Windows アカウントがコンピューターまたは信頼するドメインに存在しない場合、*認証エージェントアカウントの管理*タスクはエラーで終了します。

6. 変更内容を保存します。

Web コンソールを使用して認証エージェントアカウントを削除する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **認証エージェントアカウントの管理**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. 認証エージェントアカウントのリストで、［**追加**］をクリックします。
   これにより、認証エージェントアカウント管理ウィザードが起動します。
5. **削除**コマンドタイプを選択します。
6. ユーザーアカウントを選択します。ドメインアカウントのリストからアカウントを選択するか、アカウント名を手動で入力できます。
7. 変更内容を保存します。
8. タスクの横のチェックボックスをオンにし、［**開始**］をクリックします。

その結果、コンピューターの次回起動時にタスクが完了した後、ユーザーは認証手順を完了してオペレーティングシステムを読み込むことができなくなります。Kaspersky Endpoint Security は、暗号化されたデータへのアクセスを拒否します。

エージェントで認証を完了し、オペレーティングシステムの読み込みができるユーザーのリストを表示するには、管理されたコンピューターのプロパティに移動する必要があります。

管理コンソール（MMC）を使用して認証エージェントアカウントのリストを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。
3. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
4. コンピューターのプロパティウィンドウで、［**タスク**］セクションを選択します。
5. タスクリストで、［**認証エージェントアカウントの管理**］を選択してダブルクリックでタスクのプロパティを開きます。
6. タスクのプロパティで、［**設定**］セクションを選択します。

その結果、このコンピューター上の認証エージェントアカウントのリストにアクセスできるようになります。リストのユーザーのみが、エージェントで認証を完了し、オペレーティングシステムの読み込みができます。

Web コンソールを使用して認証エージェントアカウントのリストを表示する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. 認証エージェントアカウントのリストを表示するコンピューターの名前をクリックします。
3. コンピューターのプロパティで、［**タスク**］タブを選択します。
4. タスクリストで、［**認証エージェントアカウントの管理**］を選択します。
5. タスクのプロパティで、［**アプリケーション設定**］セクションを選択します。

その結果、このコンピューター上の認証エージェントアカウントのリストにアクセスできるようになります。リストのユーザーのみが、エージェントで認証を完了し、オペレーティングシステムの読み込みができます。

認証エージェントでのトークンまたはスマートカードの使用

暗号化されたハードディスクにアクセスする際、認証にトークンまたはスマートカードを使用できます。これを行うには、トークンまたはスマートカードの電子証明書ファイルを*認証エージェントアカウントの管理*タスクに追加する必要があります。

トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合にのみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

Kaspersky Endpoint Security は、以下のトークン、スマートカードリーダー、およびスマートカードをサポートします：

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K Java
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511
- Rutoken ECP
- Rutoken ECP Flash

- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI

トークンまたはスマートカードの電子証明書ファイルを認証エージェントアカウント作成コマンドに追加するには、まず、証明書を管理するサードパーティソフトウェアを使用してファイルを保存する必要があります。

トークンまたはスマートカードの証明書は、次の属性を満たす必要があります：

- 証明書が X.509 標準に準拠し、証明書ファイルが DER で符号化されている。
- 証明書が、長さ 1024 ビット以上の RSA キーを含む。

トークンまたはスマートカードの電子証明書がこれらの要件を満たしていない場合、認証エージェントアカウントを作成するためのコマンドに証明書ファイルを読み込むことはできません。

証明書の `KeyUsage` パラメーターには、値 `keyEncipherment` または `dataEncipherment` が必要です。`KeyUsage` パラメーターは、証明書の目的を決定します。パラメーターの値が異なる場合、Kaspersky Security Center は証明書ファイルをダウンロードしますが、警告を表示します。

ユーザーがトークンまたはスマートカードを紛失してしまった場合、管理者は、トークンまたはスマートカードの電子署名ファイルを、認証エージェントアカウントの作成コマンドに追加する必要があります。その後、暗号化されたデバイスへのアクセス権を取得するか暗号化されたデバイスのデータを復元するための手順をユーザー側で完了させます。

ハードディスクの復号化

現在のライセンスでデータの暗号化が許可されていない場合でも、ハードディスクの復号化は可能です。

ハードディスクを復号化するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。
4. ［**暗号化技術**］で、ハードディスクを暗号化する技術を選択します。
5. 次のいずれかの手順を実行します：
   - 暗号化されているすべてのハードディスクを復号化するには、［**暗号化モード**］で［**すべてのハードディスクを復号化する**］を選択します。
   - 復号化する暗号化されたハードディスクを［**次のハードディスクを暗号化しない**］表に追加します。

     このオプションは、Kaspersky Disk Encryption 技術でのみ使用できます。
6. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品のメインウィンドウから実行できます。



暗号化モニター

Kaspersky Disk Encryption 技術で暗号化されたハードディスクの復号化中にユーザーがコンピューターをシャットダウンまたは再起動した場合、次回のオペレーティングシステムの起動前に、認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ハードディスクの復号化を再開します。

Kaspersky Disk Encryption 技術で暗号化されたハードディスクの復号化中にオペレーティングシステムがハイバネーションモードに切り替わった場合は、オペレーティングシステムがハイバネーションモードから復帰した時点で認証エージェントが読み込まれます。Kaspersky Endpoint Security は、認証エージェントでの認証が成功しオペレーティングシステムが起動した後で、ハードディスクの復号化を再開します。ハードディスクの復号化後、オペレーティングシステムを再起動するまで、ハイバネーションモードは使用できません。

ハードディスクの復号化中にオペレーティングシステムがスリープモードに入った場合、オペレーティングシステムがスリープモードから復帰したときにハードディスクの復号化が再開されます。認証エージェントは読み込まれません。

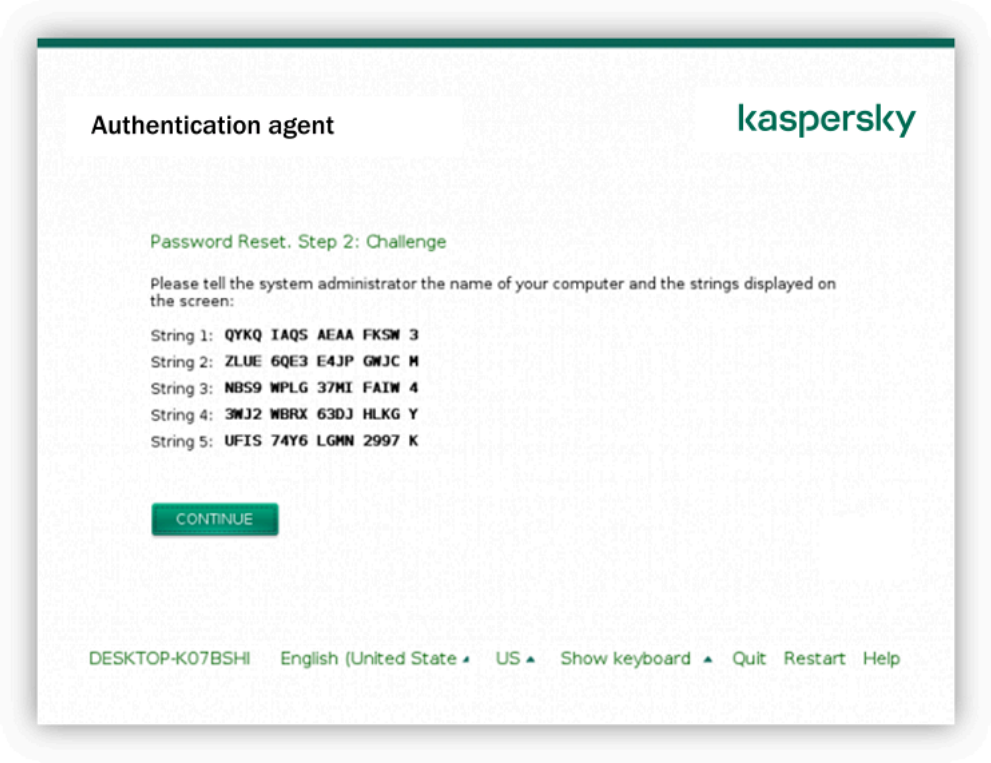
Kaspersky Disk Encryption 技術で保護されたドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたハードドライブにアクセスするためのパスワードをユーザーが忘れた場合、復元手順（要求と応答）を開始する必要があります。この機能がディスクの暗号化設定で有効になっている場合はサービスアカウントを使用してハードディスクへのアクセス権を取得することができます。

システムのハードドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたシステムハードドライブへのアクセスを復元するには、次の手順を実行します：

1. ユーザーは、要求ブロックを管理者に報告します（以下の図を参照）。
2. 管理者は要求ブロックを Kaspersky Security Center に入力し、応答ブロックを受け取り、応答ブロックをユーザーに報告します。
3. ユーザーは、認証エージェントのインターフェイスに応答ブロックを入力し、ハードドライブへのアクセスを取得します。



Kaspersky Disk Encryption 技術で保護されたシステムハードドライブへのアクセスの復元

復元手順を開始するには、ユーザーは、認証エージェントのインターフェイスの［**Forgot your password**］をクリックする必要があります。

管理コンソール（MMC）で Kaspersky Disk Encryption 技術で保護されたシステムハードドライブの応答ブロックを取得する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。
3. ［**デバイス**］タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
4. コンテキストメニューから［**オフラインモードでのアクセスを許可する**］を選択します。
5. 表示されたウィンドウで、**認証エージェント**タブを選択します。

6. ［**使用されている暗号化アルゴリズム**］ブロックで、［**AES56**］または［**AES256**］の暗号化アルゴリズムを選択します。

   データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（*高度な暗号化（AES256）*または*中程度の暗号化（AES56）*）。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。

7. ［**アカウント**］で、認証エージェントのアカウント名とパスワードの復元を要求しているユーザーの認証エージェントアカウント名を選択します。

8. ［**ハードディスク**］で、アクセスを復元する暗号化されたハードディスクを選択します。

9. ［**ユーザーの要求**］ブロックに、ユーザーが提示した要求ブロックを入力します。

その結果、認証エージェントアカウントのユーザー名とパスワードの復元を求めるユーザー要求に対する応答ブロックの内容が、**アクセスキー**フィールドに表示されます。応答ブロックの内容をユーザーに伝えます。



オフラインモードでのアクセスを許可する

Web コンソールで Kaspersky Disk Encryption 技術で保護されたシステムハードドライブの応答ブロックを取得する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。

3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

4. 表示されたウィンドウで、［**認証エージェント**］セクションを選択します。

5. ［**アカウント**］で、認証エージェントのアカウント名とパスワードの復元を要求しているユーザーのために作成された認証エージェントアカウントの名前を選択します。

6. ユーザーから伝えられた要求ブロックを入力します。

認証エージェントのアカウントのユーザー名とパスワードの復元に関するユーザー要求に対する応答ブロックの内容は、ウィンドウの下部に表示されます。応答ブロックの内容をユーザーに伝えます。

復元手順が完了すると、認証エージェントはユーザーにパスワードの変更を求めます。

システム以外のハードドライブへのアクセスの復元

Kaspersky Disk Encryption 技術で保護されたシステム以外のハードドライブへのアクセスを復元するには、次の手順を実行します：

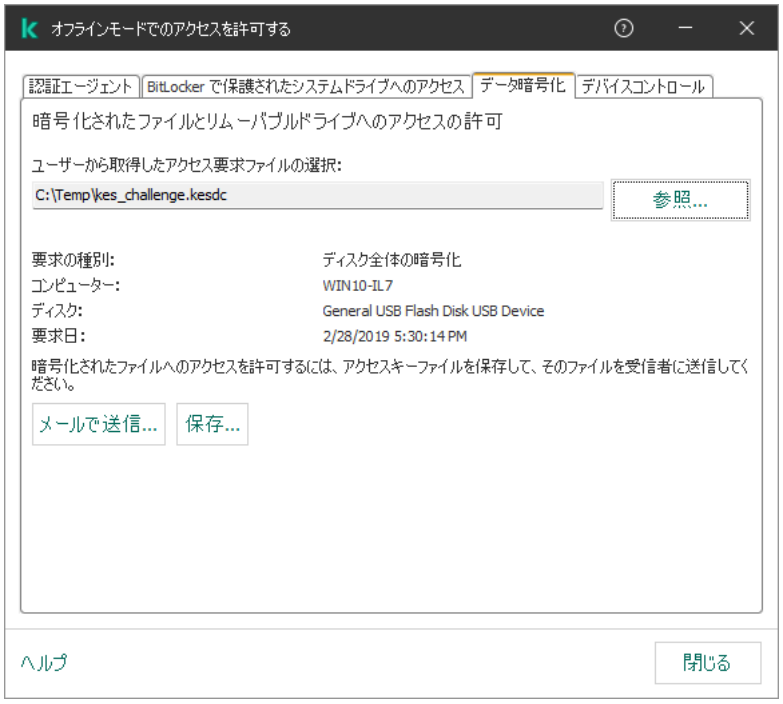
1. ユーザーがアクセス要求ファイルを管理者に送信します。
2. 管理者はアクセス要求ファイルを Kaspersky Security Center に追加し、アクセスキーファイルを作成してユーザーに送信します。
3. ユーザーはアクセスキーファイルを Kaspersky Endpoint Security に追加し、ハードドライブへのアクセスを取得します。

復元手順を開始するには、ユーザーはハードドライブにアクセスする必要があります。その結果、Kaspersky Endpoint Security はアクセス要求ファイル（拡張子が KESDC のファイル）を作成します。ユーザーは、このファイルを管理者に電子メールなどで送信する必要があります。

管理コンソール（MMC）で暗号化されたシステム以外のハードドライブのアクセスキーファイルを取得する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。
3. ［**デバイス**］タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
4. コンテキストメニューから［**オフラインモードでのアクセスを許可する**］を選択します。
5. 表示されたウィンドウで、**データ暗号化**タブを選択します。
6. ［**データ暗号化**］タブで［**参照**］をクリックします。
7. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。



オフラインモードでのアクセスを許可する

Web コンソールで暗号化されたシステム以外のハードドライブのアクセスキーファイルを取得する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
4. ［**データ暗号化**］を選択します。
5. ［**ファイルの選択**］をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。

   Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。
6. ［**ライセンスを保存**］をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

認証エージェントのサービスアカウントを使用したログイン

Kaspersky Endpoint Security では、ドライブを暗号化する際に認証エージェントのサービスアカウントを追加できます。サービスアカウントは、ユーザーがパスワードを忘れたときなどにコンピューターへのアクセス権を取得するために必要です。このサービスアカウントは予備のアカウントとして使用することもできます。アカウントを追加するには、サービスアカウントをディスクの暗号化設定で選択してユーザーアカウントの名前を入力します（既定では `ServiceAccount` です）。エージェントを使用して認証するには、ワンタイムパスワードが必要です。

管理コンソール（MMC）でワンタイムパスワードを確認する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。
3. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
4. コンピューターのプロパティウィンドウで、［**タスク**］セクションを選択します。
5. タスクリストで、［**認証エージェントアカウントの管理**］を選択してダブルクリックでタスクのプロパティを開きます。
6. コンピューターのプロパティウィンドウで、［**設定**］セクションを選択します。
7. アカウントのリストで、認証エージェントのサービスアカウント（例：`WIN10-USER\ServiceAccount`）を選択します。
8. ［**処理**］から［**アカウントの表示**］を選択します。
9. アカウントのプロパティで、［**元のパスワードの表示**］をオンにします。
10. サービスアカウントでログインするためのワンタイムパスワードをコピーします。

Web コンソールでワンタイムパスワードを確認する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. 認証エージェントアカウントのリストを表示するコンピューターの名前をクリックします。
   コンピューターのプロパティが表示されます。
3. コンピューターのプロパティで、［**タスク**］タブを選択します。
4. タスクリストで、［**認証エージェントアカウントの管理**］を選択します。
5. タスクのプロパティで、［**アプリケーション設定**］セクションを選択します。
6. アカウントのリストで、認証エージェントのサービスアカウント（例：`WIN10-USER\ServiceAccount`）を選択します。
7. アカウントのプロパティで、［**パスワードを表示**］をオンにします。
8. サービスアカウントでログインするためのワンタイムパスワードをコピーします。

Kaspersky Endpoint Security はサービスアカウントでユーザーが認証を実行するたびにパスワードを更新します。エージェントを使用して認証した後に、Windows アカウントのパスワードを入力する必要があります。サービスアカウントでログインする際、SSO を使用することはできません。

オペレーティングシステムのアップデート

ディスク全体の暗号化（FDE）を使用して保護しているコンピューターのオペレーティングシステムのアップデートでは、いくつか特別に留意すべき事項が存在します。次の順序でオペレーティングシステムをアップデートします：1 台のコンピューターで最初に OS をアップデートします。次に、数台のコンピューターで OS をアップデートします。その後、ネットワーク内のすべての OS をアップデートします。

Kaspersky Disk Encryption 技術を使用している場合、オペレーティングシステムの起動前に認証エージェントが読み込まれます。認証エージェントを使用することで、ユーザーはシステムにサインインして暗号化されたディスクにアクセスできます。これに続いて、オペレーティングシステムが読み込まれます。Kaspersky Disk Encryption 技術を使用して保護されているコンピューター上のオペレーティングシステムのアップデートを開始すると、OS のアップデートウィザードによって認証エージェントが削除されます。その結果、OS ローダーは暗号化されたドライブにアクセスできないため、コンピューターをロックできます。

オペレーティングシステムのアップデートの機能：

- **WSUS 経由で OS をアップデート**：通常の方法でオペレーティングシステムをアップデートできます。
- **ISO から OS をアップデート**：オペレーティングシステムをアップデートするには、Kaspersky Disk Encryption ドライバーが含まれるフォルダーを指定する必要があります。本製品はドライバーを個別のフォルダーに自動的にコピーします。次の手順に従います：

  1. ISO イメージをマウントします。
  2. 次のキーを指定してシステムアップデートのインストールを開始します：

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky
     Lab\KES.12.12\reflect_drivers
     ```

自動 OS アップデートは、コンピューターで Windows 10 1607（RS1）以降が稼働している場合にのみ使用可能です。以前のバージョンのオペレーティングシステムをアップグレードするには、最初にディスクを復号化し、OS のアップグレードを実行してから、ディスクを暗号化することを推奨します。

BitLocker ディスク暗号化技術を使用している場合、Windows 10 をアップデートするためにハードドライブを復号化する必要はありません。BitLocker について詳しくは、Microsoft の Web サイトの情報を参照してください。

暗号化機能のアップデートのエラーの解決

以前のバージョンの製品が Kaspersky Endpoint Security for Windows 12.12 にアップグレードされると、ディスク全体の暗号化がアップデートされます。

ディスク全体の暗号化機能のアップデートの開始時に、次のエラーが発生する場合があります：

- アップグレードを開始できませんでした
- デバイスと認証エージェントとの互換性がありません

ディスク全体の暗号化機能のアップデートを新しいバージョンの製品で開始したときに発生するエラーを解決するには：

1. ハードディスクを復号します。
2. もう一度ハードディスクを暗号化します。

ディスク全体の暗号化機能のアップデートを実行中に、次のエラーが発生する場合があります：

- アップグレードを完了できませんでした。
- ディスク全体の暗号化のアップグレードのロールバックがエラーで終了した。

ディスク全体の暗号化機能のアップデートを実行中に発生するエラーを解決するには：

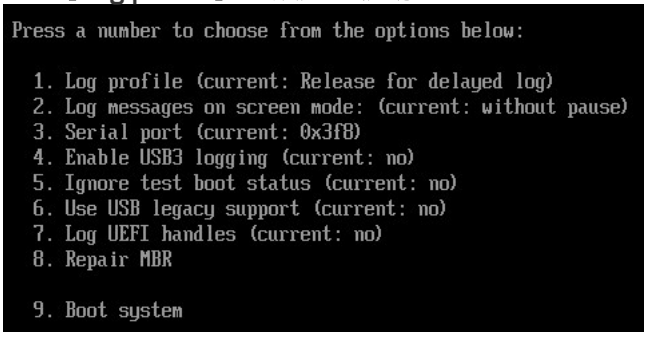
復元ツールを使用して、暗号化されたデバイスへのアクセスを回復します。

認証エージェントのトレース

本製品は、認証エージェントが行う操作のサービス情報と、ユーザーが認証エージェントに対して行う操作の情報をトレースファイルに記録します。

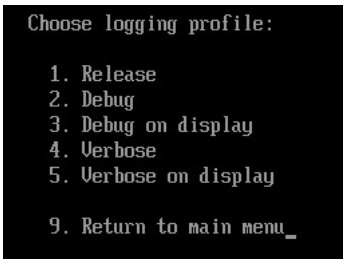
認証エージェントのトレースを有効にするには：

1. Kaspersky Endpoint Security のトレースを有効にします。
2. コンピューターを再起動します。
3. 暗号化されたハードディスクでコンピューターが起動したら、すぐに **F3** キーを押して認証エージェントを設定するウィンドウを表示します。
4. FDE ブートローダーが起動したら、［**KES (FDE <version>)**］ブートマネージャーを選択します。
5. ブートマネージャーメニューで、［**Log profile**］の設定に移動します。



ブートマネージャーメニュー

6. ログプロファイルの設定ウィンドウで、トレースレベルを選択します：



認証エージェントのトレースレベル

- **Release**：このオプションを選択すると、認証エージェントのイベントに関する情報がトレースファイルに記録されません。
- **Debug**：このオプションを選択すると、認証エージェントの動作と、認証エージェントに対してユーザーが実行する操作に関する情報がトレースファイルに記録されます。
- **Debug on display**：このオプションを選択すると、認証エージェントが行う操作と、認証エージェントに対してユーザーが実行する操作に関する情報がトレースファイルに記録され、COM ポート経由で送信されます。

  暗号化されたハードディスクのあるコンピューターが COM ポート経由で別のコンピューターに接続されている場合、この別のコンピューターから認証エージェントのイベントを確認できます。
- **Verbose**：このオプションを選択すると、認証エージェントの動作と、認証エージェントに対してユーザーが実行する操作に関する詳細な情報がトレースファイルに記録されます。

  > このオプションは、［**Debug**］と比較して、項目の詳細レベルが高くなります。項目の詳細レベルを高くすると、認証エージェントとオペレーティングシステムの起動が遅くなることがあります。
- **Verbose on display**：このオプションを選択すると、認証エージェントが行う操作と、認証エージェントに対してユーザーが実行する操作に関する詳細な情報がトレースファイルに記録され、COM ポート経由で送信されます。

  > このオプションは、［**Debug on display**］と比較して、項目の詳細レベルが高くなります。項目の詳細レベルを高くすると、認証エージェントとオペレーティングシステムの起動が遅くなることがあります。

トレースレベルを選択すると、ブートマネージャーによってメニューが再度表示されます。

7. ブートマネージャーメニューで、［**Boot system**］を選択します。

FDE ブートローダーによって認証エージェントが起動されます。

問題を再現します。

コンピューターに暗号化されたハードディスクがある場合、またはディスク全体の暗号化を実行中の場合、データは認証エージェントのトレースファイルに記録されます。

8. トレースのプロセスを停止するには、［サポートツール］ウィンドウに戻ってトレースを無効にします。

認証エージェントの KES.SRV 動作のトレースファイルがフォルダー「`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`」に作成されます。認証エージェントのトレースファイルは、本製品の他のトレースファイルと異なり、カスペルスキーに送信されません。必要に応じて、認証エージェントのトレースファイルを分析するため、手動でカスペルスキーに送信できます。

認証エージェントのヘルプテキストの編集

認証エージェントのヘルプメッセージを編集する前に、起動前環境でサポートされる文字のリストを参照してください（以下を参照）。

認証エージェントのヘルプメッセージを編集するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**暗号化の共通設定**］の順に選択します。
4. ［**テンプレート**］ブロックの［**ヘルプ**］をクリックします。
5. 表示されたウィンドウで、次の操作を実行します：
   - ［**認証**］タブを選択して、アカウント情報を入力するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。
   - ［**パスワードの変更**］タブを選択して、認証エージェントアカウントのパスワードを変更するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。
   - ［**パスワードの復元**］タブを選択して、認証エージェントアカウントのパスワードを復元するときに認証エージェントのウィンドウに表示されるヘルプテキストを編集します。
6. ヘルプメッセージを編集します。
   元のテキストを復元する場合は、［**既定**］をクリックします。

   ヘルプのテキストは 16 行以内で入力してください。1 行に入力できる最大文字数は 64 です。
7. 変更内容を保存します。

認証エージェントのヘルプメッセージでサポートされる文字

起動前環境では、以下のユニコード文字がサポートされます：

- 基本ラテン文字（0000 ～ 007F）
- ラテン 1 補助（0080 ～ 00FF）
- ラテン文字拡張 A（0100 ～ 017F）
- ラテン文字拡張 B（0180 ～ 024F）
- 前進を伴う修飾文字（02B0 ～ 02FF）

- ダイアクリティカルマーク（0300 ～ 036F）
- ギリシア文字およびコプト文字（0370 ～ 03FF）
- キリル文字（0400 ～ 04FF）
- ヘブライ文字（0590 ～ 05FF）
- アラビア文字（0600 ～ 06FF）
- ラテン文字拡張追加（1E00 ～ 1EFF）
- 一般句読点（2000 ～ 206F）
- 通貨記号（20A0 ～ 20CF）
- 文字様記号（2100 ～ 214F）
- 幾何学模様（25A0 ～ 25FF）
- アラビア表示形 B（FE70 ～ FEFF）

このリストに示されていない文字は、起動前環境ではサポートされません。それらの文字は認証エージェントのヘルプメッセージに使用しないでください。

認証エージェントの動作テスト後に残存するオブジェクトとデータの削除

製品のアンインストール時に、認証エージェントのテスト操作後のオブジェクトとデータがシステムのハードディスクに残っていることを製品が検出した場合、製品のアンインストールは中断され、そのようなオブジェクトとデータが削除されるまで再開できません。

認証エージェントのテスト操作後のオブジェクトとデータは、例外的な場合のみ、システムのハードディスクに残ることがあります。たとえば、暗号化設定を含む Kaspersky Security Center ポリシーを適用した後にコンピューターを再起動していない場合や、認証エージェントのテスト操作の後、本製品の起動に失敗した場合などです。

認証エージェントのテスト操作後に、システムのハードディスクに残っているオブジェクトやデータを削除するには次の方法があります：

- Kaspersky Security Center のポリシーを使用する。
- 復元ツールを使用する。

Kaspersky Security Center のポリシーを使用して認証エージェントのテスト操作後に残っているオブジェクトとデータを削除するには：

1. コンピューターのすべてのハードディスクを復号化するよう設定した Kaspersky Security Center ポリシーを、コンピューターに適用します。
2. Kaspersky Endpoint Security を起動します。

認証エージェントとアプリケーションとの非互換性に関する情報を削除するには：

コマンドラインに「`avp pbatestreset`」コマンドを入力します。

BitLocker の管理

BitLocker は、Windows オペレーティングシステムに組み込まれた暗号化技術です。Kaspersky Endpoint Security では、Kaspersky Next のインフラストラクチャを使用して BitLocker を制御および管理できます。BitLocker は論理ボリュームを暗号化します。BitLocker はリムーバブルドライブの暗号化には使用できません。BitLocker について詳しくは、Microsoft 社の資料を参照してください。

BitLocker は、ディスクを暗号化する際に、ブートローダーとその他の補助ファイルを system partition に配置します。このパーティションは暗号化されません。Windows のインストール中に、オペレーティングシステムによって、システムパーティションが自動的に作成されます。Windows をインストールする前にディスクが完全にパーティション分割されている場合、オペレーティングシステムはシステムパーティションを作成できません。この場合、BitLocker のディスク暗号化を開始すると、オペレーティングシステムは、ディスクを再パーティション化してシステムパーティションを作成するよう要求します。システムパーティションが作成されると、オペレーティングシステムによって BitLocker 暗号化が開始されます。

BitLocker 信頼済みプラットフォームモジュールを使用して、安全なアクセスキーの保管領域を提供します。*Trusted Platform Module*（TPM）は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。TPM は起動前のシステム整合性検証を行うため、TPM を使用すると最も安全に BitLocker アクセスキーを保管できます。TPM なしでもコンピューター上のドライブを暗号化することは可能です。この場合は、アクセスキーはパスワードで暗号化されます。BitLocker は次の暗号化の方法を使用します：

- TPM。
- TPM と PIN。
- パスワード。

システムの暗号化後、ユーザーはオペレーティングシステムを起動するために BitLocker 認証の手順を完了する必要があります。認証後、 BitLocker はユーザーのログインを許可します。BitLocker はシングルサインオン（SSO）をサポートしていません。

ドライブを暗号化した後、BitLocker はマスター鍵を作成します。Kaspersky Endpoint Security はこのマスター鍵を Kaspersky Security Center に送るため、ユーザーがパスワードを忘れた場合などにディスクへのアクセスを復元することができます。

ユーザーが BitLocker を使用してディスクを暗号化すると、Kaspersky Endpoint Security は Kaspersky Security Center にディスク暗号化に関する情報 を送ります。一方、Kaspersky Endpoint Security はマスター鍵を Kaspersky Security Center に送らないため、Kaspersky Security Center を使用してディスクへのアクセスを復元することはできません。Kaspersky Security Center と BitLocker が正しく動作するために、ドライブの復号化および再暗号化にはポリシーを使用してください。ローカルで、またはポリシーを使用してドライブを復号化できます。

Windows のグループポリシーを使用している場合、ポリシーで BitLocker の管理をオフにしてください。Windows のポリシー設定は Kaspersky Endpoint Security のポリシー設定と競合する可能性があります。ドライブの暗号化の際にエラーが発生する可能性があります。

BitLocker ドライブ暗号化の開始

ディスク全体の暗号化を行う前に、コンピューターが感染していないことを確認してください。確認するには、完全スキャンか簡易スキャンを開始します。ルートキットによって感染したコンピューターでディスク全体の暗号化を行うと、ハードディスクが動作しなくなる可能性があります。

Windows サーバーのオペレーティングシステムが搭載されたコンピューターで BitLocker ドライブ暗号化を使用するには、BitLocker ドライブ暗号化機能をインストールする必要がある場合があります。オペレーティングシステムツール（ロールとコンポーネントを追加するウィザード）を使用して機能をインストールしてください。BitLocker ドライブ暗号化のインストールについて詳しくは、Microsoft 社の資料を参照してください。

管理コンソール（MMC）を使用した BitLocker ドライブ暗号化を実行する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。
4. ［**暗号化技術**］から［**BitLocker ドライブ暗号化**］を選択します。
5. ［**暗号化モード**］から［**すべてのハードディスクを暗号化する**］を選択します。

   コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化すると、暗号化を実行したオペレーティングシステムのみを読み込めます。

6. BitLocker ドライブ暗号化の詳細なオプションを設定します（下記の表を参照）。
7. 変更内容を保存します。

Web コンソールおよび Cloud コンソールを使用した BitLocker ドライブ暗号化を実行する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**ディスク全体の暗号化**］に移動します。
5. ［**BitLocker ディスク暗号化**］技術を選択します。

6. ［**デバイスの操作**］ブロックで、［**すべてのハードディスクを暗号化する**］を選択します。

コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化すると、暗号化を実行したオペレーティングシステムのみを読み込めます。

7. BitLocker ドライブ暗号化の詳細なオプションを設定します（下記の表を参照）。

8. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品のメインウィンドウから実行できます。



暗号化モニター

ポリシーの適用後、認証の設定によって次の内容が表示されます：

- TPM のみ：ユーザーの入力は必要ありません。ディスクはコンピューターの再起動時に暗号化されます。
- TPM および PIN / パスワード：TPM モジュールが利用可能な場合、PIN コードの入力ウィンドウが表示されます。TPM モジュールが利用できない場合、起動前認証用のパスワードの入力ウィンドウが表示されます。
- パスワードのみ：起動認証用のパスワードを求めるウィンドウが表示されます。

コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、Windows 8 以前のオペレーティングシステムでは、回復キーのファイルを保存するのに USB デバイスなどのストレージデバイスの接続を求めるウィンドウが表示されます。複数の回復キーのファイルを、単一のストレージデバイスに保存できます。

パスワードまたは PIN を設定したあと、暗号化を完了するために BitLocker は再起動を求めます。次に、BitLocker の認証の手順を完了します。認証手順の後に、システムにログオンする必要があります。オペレーティングシステムが読み込まれると、BitLocker は暗号化を完了します。

暗号鍵にアクセスできない場合、回復キーを付与してもらうよう、ユーザーからローカルネットワークの管理者にリクエストできます（回復キーが事前にストレージデバイスに保存されていない場合、または回復キーを紛失した場合）。

BitLocker ドライブ暗号化の設定

パラメータ	説明
タブレットでプリブート キーボード入力が必要な BitLocker 認証を使用できるようにする	起動前の環境でデータ入力を必要とする認証を使用します。この設定は、起動前に入力できる機能がないプラットフォームに対しても適用されます（例：タブレットのタッチスクリーンキーボード）。 タブレットコンピューターのタッチスクリーンは起動前環境では利用できません。タブレットコンピューターで BitLocker 認証を完了するには、ユーザーは USB キーボードなどを接続する必要があります。 このチェックボックスをオンにすると、起動前の入力を必要とする認証の使用が許可されます。この設定は、起動前の環境でデータ入力ができるツールがあるデバイスに対してのみ使用してください（例：タッチスクリーンキーボードだけでなく USB キーボードも付いているデバイスなど）。 チェックボックスをオフにすると、タブレットコンピューターで BitLocker ドライブ暗号化が使用できなくなります。
ハードウェア暗号化を使用（Windows 8 以降）	このチェックボックスをオンにすると、ハードウェア暗号化が適用されます。ハードウェア暗号化を使用すると、より少ないコンピューターリソースで、より速く暗号化することができます。
使用されているディスク領域のみを暗号化（Windows 8 以降）	このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。 暗号化の開始後に［**使用されているディスク領域のみを暗号化（暗号化時間を短縮）**］を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。 このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。 チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。 データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。既に使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。 既定では、このチェックボックスはオフです。

パラメータ	説明
認証方法	**パスワードのみ（OS が Windows 8 以降のバージョンの場合）** このオプションを選択すると、暗号化されたドライブにアクセスしようとした際に、パスワードの入力が要求されます。 このオプションは、Trusted Platform Module（TPM）が使用されていない場合に選択できます。 **トラステッド プラットフォーム モジュール（TPM）** このオプションを選択すると、BitLocker は Trusted Platform Module（TPM）を使用します。 *Trusted Platform Module*（TPM）は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。 Windows 7 と Windows 2008 R2 では、TPM モジュールを使用した暗号化のみを利用できます。TPM モジュールがインストールされていない場合、BitLocker 暗号化は実行できません。これらのオペレーティングシステムを使用しているコンピューターでは、パスワードを使用した暗号化はサポートされません。 Trusted Platform Module を搭載したデバイスで作成された暗号鍵は、そのデバイスでしか復号化できません。Trusted Platform Module は、各 TPM が保持するストレージルートキーを使って暗号鍵を暗号化します。ストレージルートキーは Trusted Platform Module 内部に格納されています。そのため、暗号鍵を盗もうとする試みに対して、より強固な保護を提供することができます。 既定では、この処理が選択されています。 暗号化鍵およびパスワードまたは PIN で保護された暗号化鍵へのアクセスに、より強固な保護を提供することが可能です。 • **TPM の PIN を使用する**：このチェックボックスをオンにすると、Trusted Platform Module（TPM）内に格納されている暗号鍵にアクセスする際に暗証番号を使用できます。このチェックボックスをオフにすると、PIN コードの使用が禁止されます。暗号鍵へのアクセスには、パスワードの入力が必要となります。 • **トラステッド プラットフォーム モジュール（TPM）、TPM が使用できない場合はパスワード**：このオプションをオンにすると、Trusted Platform Module（TPM）が使用できない場合、パスワードを使用して暗号鍵にアクセスできます。チェックボックスがオフの場合は TPM は使用できず、ディスク全体の暗号化は開始されません。 パスワードまたは PIN の要件を指定して、選択した認証方法を設定する必要があります： • **PIN の最小文字数** • **パスワードの最小文字数** • **TPM のパスワード / PIN の有効期間を設定する（日）** • **拡張 PIN を使用する（文字と数字）**：*拡張 PIN* を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります
回復キーを自動的に再生成する（日）	パスワードを自動的に更新して、BitLocker で保護されたハードドライブへのアクセスを復元します。このチェックボックスをオンにしたら、回復キーのパスワードの有効期間を指定します。これは、回復キーのパスワードの再使用を防ぐのに役立ちます。

BitLocker で保護されたハードドライブの復号化

ユーザーはオペレーティングシステムを使用してディスクを復号化することができます（*BitLocker 機能をオフにしてください*）。その後、Kaspersky Endpoint Security はディスクを再度暗号化するよう求められます。Kaspersky Endpoint Security は、ポリシー内でディスク暗号化を有効にするまでディスクを暗号化するよう求めます。

管理コンソール（MMC）で BitLocker で保護されたハードドライブを復号化する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ディスク全体の暗号化**］の順に選択します。
4. ［**暗号化技術**］から［**BitLocker ドライブ暗号化**］を選択します。

5. ［**暗号化モード**］から［**すべてのハードディスクを復号化する**］を選択します。

6. 変更内容を保存します。

BitLocker で暗号化されたハードドライブを Web コンソールおよび Cloud コンソールで復号化するには

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**データ暗号化**］→［**ディスク全体の暗号化**］に移動します。

5. ［**BitLocker ディスク暗号化**］技術を選択します。

6. ［**デバイスの操作**］ブロックで、［**すべてのハードディスクを復号化する**］を選択します。

7. 変更内容を保存します。

暗号化モニターツールを使用して、ディスクの暗号化またはユーザーのコンピューター上でのディスクの復号化を制御します。暗号化モニターツールは製品のメインウィンドウから実行できます。



暗号化モニター

BitLocker で保護されたハードドライブへのアクセスの復元

ユーザーが BitLocker で暗号化されたハードドライブにアクセスするためのパスワードを忘れた場合は、復元手順（要求と応答）を開始する必要があります。

コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、Windows 8 以前のオペレーティングシステムでは、暗号化の前に回復キーのファイルがリムーバブルドライブに保存されます。ドライブへのアクセスを復旧するには、リムーバブルドライブを接続し、画面上の指示に従います。

BitLocker によって暗号化されたハードドライブへのアクセスは、次の復元手順で構成されます：

1. ユーザーは、管理者に回復キーの ID を伝えます（下の図を参照）。
2. 管理者は、Kaspersky Security Center のコンピューターのプロパティで回復キーの ID を確認します。ユーザーが提供した ID は、コンピューターのプロパティに表示される ID と一致する必要があります。
3. 回復キーの ID が一致する場合、管理者はユーザーに回復キーを提供するか、回復キーのファイルを送信します。

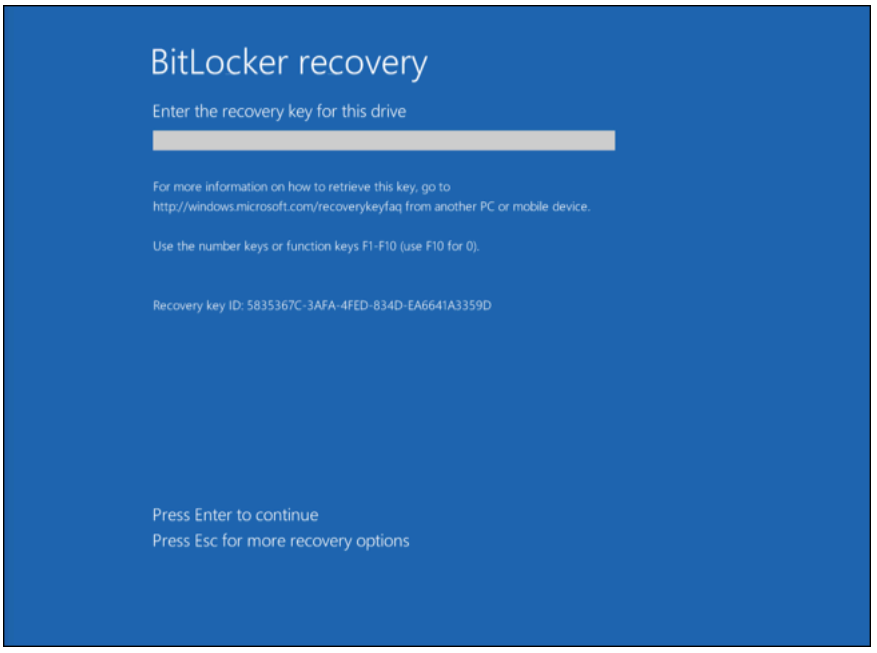
   回復キーのファイルは、次のオペレーティングシステムを実行しているコンピューターに使用されます：

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   他のすべてのオペレーティングシステムでは、回復キーが使用されます。

   回復キーのパスワードの再使用を防ぐために、ポリシー設定でパスワードの自動更新を設定できます。

4. ユーザーは回復キーを入力し、ハードドライブにアクセスします。



BitLocker で暗号化されたハードドライブへのアクセスの復元

システムドライブへのアクセスの復元

復元手順を開始するには、ユーザーはプリブート認証段階で **Esc** キーを押す必要があります。

管理コンソール（MMC）で BitLocker によって暗号化されたシステムドライブの回復キーを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**管理対象デバイス**］を選択します。
3. ［**デバイス**］タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
4. コンテキストメニューから［**オフラインモードでのアクセスを許可する**］を選択します。
5. 表示されたウィンドウで、**BitLocker で保護されたシステムドライブへのアクセス**タブを選択します。
6. BitLocker パスワード入力ウィンドウに示されている回復キーの ID をユーザーに尋ね、［**回復キーの ID**］の値と比較します。

ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。



BitLocker で暗号化されたドライブへのアクセスの復元

Web コンソールまたは Cloud コンソールで BitLocker で暗号化されたシステムドライブの回復キーを表示する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。
3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
4. 表示されたウィンドウで、［**BitLocker**］セクションを選択します。
5. 回復キーの ID を確認します。ユーザーが提供する ID は、コンピューターの設定に表示される ID と一致する必要があります。

   ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

6. ［**予備のライセンス**］をクリックします。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。

オペレーティングシステムが読み込まれた後、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促します。新しいパスワードまたは PIN コードを設定した後、BitLocker は新しいマスター鍵を作成し、その鍵を Kaspersky Security Center に送ります。回復キーおよび回復キーファイルが更新されます。ユーザーがパスワードを変更していない場合は、オペレーティングシステムが次に読み込まれるときに古い回復キーを使用できます。

Windows 7 搭載のコンピューターでは、パスワードまたは PIN コードの変更が許可されません。回復キーが入力され、オペレーティングシステムが読み込まれた後は、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促しません。このため、新しいパスワードまたは PIN コードを設定することはできません。この問題はオペレーティングシステムの特性によるものです。続行するには、ハードドライブを再度暗号化する必要があります。

システムドライブ以外のドライブへのアクセスの復元

復元手順を開始するには、ユーザーがドライブへのアクセスを提供するウィンドウで［**パスワードをお忘れの方**］のリンクをクリックする必要があります。暗号化されたドライブにアクセスした後、ユーザーは BitLocker の設定で Windows 認証中にドライブの自動ロック解除を有効にできます。

管理コンソール（MMC）で BitLocker によって暗号化されたシステムドライブ以外のドライブの回復キーを表示する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］フォルダーの順に選択します。
3. 作業領域で、アクセスキーファイルを作成する暗号化されたデバイスを選択し、デバイスのコンテキストメニューで［**Kaspersky Endpoint Security のデバイスへのアクセス**］をクリックします。
4. BitLocker パスワード入力ウィンドウに示されている回復キーの ID をユーザーに尋ね、［**回復キーの ID**］の値と比較します。

   ID が一致しない場合、キーは無効であり、指定されたドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

5. ［**回復キー**］に表示されているキーをユーザーに送信します。



BitLocker で暗号化されたドライブへのアクセスの復元

Web コンソールおよび Cloud コンソールで BitLocker で暗号化されたシステムドライブ以外のドライブの回復キーを表示する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］をクリックします。

2. ドライブのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。

3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
   これにより、デバイスへのアクセスを許可するためのウィザードが開始されます。

4. ウィザードの指示に従って、デバイスへのアクセスを許可します。

   a. **Kaspersky Endpoint Security for Windows** のプラグインを選択します。

   b. 回復キーの ID を確認します。ユーザーが提供する ID は、コンピューターの設定に表示される ID と一致する必要があります。

      > ID が一致しない場合、キーは無効であり、指定されたシステムドライブへのアクセスを復元できません。選択したコンピューターの名前がユーザーのコンピューターの名前と一致していることを確認してください。

   c. ［**予備のライセンス**］をクリックします。

その結果、回復キーまたは回復キーのファイルにアクセスできるようになり、これをユーザーに転送する必要があります。

ソフトウェアアップデート時の BitLocker 保護の一時停止

BitLocker 保護が有効な状態でのオペレーティングシステムのアップデート、オペレーティングシステムへのアップデートパッケージのインストール、またはその他のソフトウェアのアップデート時には留意事項が少なくありません。アップデートのインストールには、コンピューターの再起動が複数回必要になることがあります。再起動ごとにユーザーは BitLocker 認証を完了する必要があります。アップデートを正常にインストールするために、一時的に BitLocker 認証をオフにすることができます。この場合ディスクは暗号化されたままで、ユーザーはシステムにサインインした後にデータにアクセスすることができます。BitLocker 認証を管理するには、*BitLocker 保護の管理*タスクを使用できます。このタスクを使用して、BitLocker 認証を必要としないコンピューターの再起動の回数を指定することができます。アップデートがインストールされて*BitLocker 保護の管理*タスクが完了すると、BitLocker 認証は自動的にオンになります。いつでも BitLocker 認証をオンにできます。

管理コンソール（MMC）を使用して BitLocker 保護を一時停止する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。

2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

［**Kaspersky Endpoint Security for Windows (12.12)**］→［**BitLocker 保護の管理**］の順に選択します。

ステップ 2：BitLocker 保護の管理

BitLocker 認証を設定します。BitLocker 保護を一時停止するには、［**一時的に BitLocker 認証のスキップを許可する**］を選択して BitLocker 認証をスキップする再起動の回数を入力します（1 ～ 15 回）。必要に応じて、タスクの有効期限の日時を入力します。指定した回数でタスクは自動的にオフになり、ユーザーはその後コンピューターが再起動した際に BitLocker 認証を完了する必要があります。

ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 4：タスク名の定義

「*Windows 10 のアップデート*」などのタスクの名前を入力します。

ステップ 5：タスク作成の完了

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

Web コンソールを使用して BitLocker 保護を一時停止する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］から［**Kaspersky Endpoint Security**］を選択します。
2. ［**タスク種別**］から［**BitLocker 保護の管理**］を選択します。
3. ［**タスク名**］に「*Windows 10 のアップデート*」などの簡潔な名前を付けます。
4. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

ステップ 2：BitLocker 保護の管理

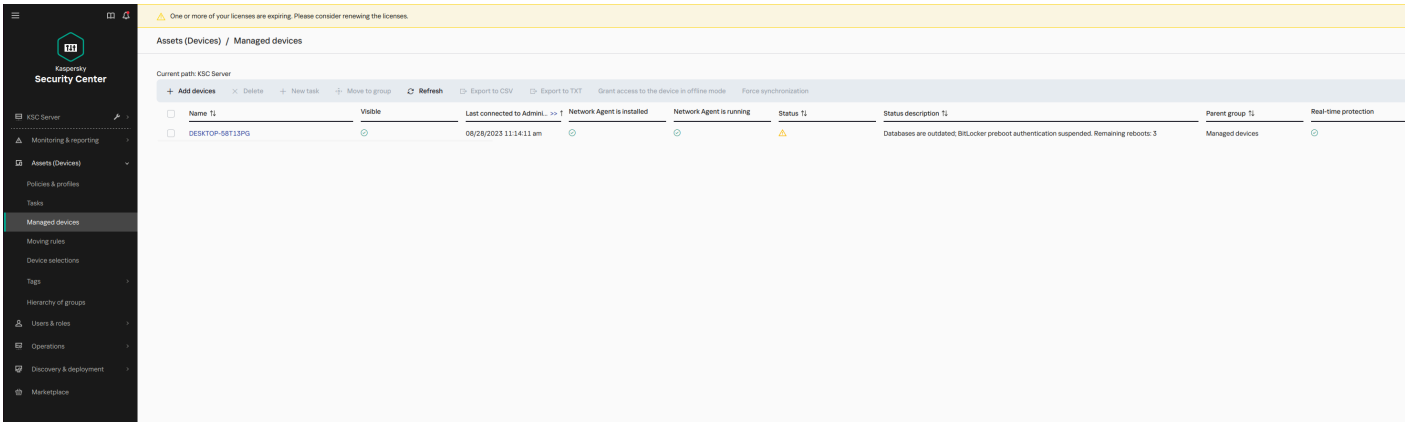
BitLocker 認証を設定します。BitLocker 保護を一時停止するには、［**一時的に BitLocker 認証のスキップを許可する**］を選択して BitLocker 認証をスキップする再起動の回数を入力します（1～15 回）。必要に応じて、タスクの有効期限の日時を入力します。指定した回数でタスクは自動的にオフになり、ユーザーはその後コンピューターが再起動した際に BitLocker 認証を完了する必要があります。

ステップ 3：タスク作成の完了

ウィザードを終了します。タスクのリストに新しいタスクが表示されます。

タスクを実行するには、タスクのチェックボックスをオンにし、［**開始**］をクリックします。

その結果、タスクの実行中は次のコンピューターの再起動以降 BitLocker がユーザー認証を求めることはありません。BitLocker 認証を省略してコンピューターを再起動するたびに、Kaspersky Endpoint Security は対応するイベントを作成し、残りの再起動回数を記録します。Kaspersky Endpoint Security は次にそのイベントを Kaspersky Security Center に送り、管理者が監視できるようにします。また、Kaspersky Security Center コンソールの［**管理対象デバイス**］フォルダーのデバイスステータスの説明で、残りの再起動回数を確認できます。



管理対象デバイスのリスト

指定した再起動の回数に到達する、もしくはタスクの有効期間が終了すると、BitLocker 認証は自動的に有効になります。データにアクセスするためには、ユーザーは BitLocker 認証を完了する必要があります。

Windows 7 を実行しているコンピューターでは、BitLocker はコンピューターの再起動の回数を記録できません。Windows 7 のコンピューターの再起動回数は、Kaspersky Endpoint Security 側で記録します。このため、再起動ごとに自動的に BitLocker 認証をオンにするには、Kaspersky Endpoint Security が開始されている必要があります。

事前に BitLocker 認証をオンにするには、*BitLocker 保護の管理*タスクのプロパティを開いて、［**常に起動前認証を要求する**］を選択してください。

ローカルコンピュータードライブでのファイルレベルの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ファイル暗号化には、次の特別な機能があります：

- Kaspersky Endpoint Security は、オペレーティングシステムのローカルユーザープロファイルについてのみ定義済みフォルダーのファイルの暗号化や復号化を行います。Kaspersky Endpoint Security は、移動ユーザープロファイル、固定ユーザープロファイル、一時ユーザープロファイル、またはリダイレクトされたフォルダーの、定義済みフォルダー内のファイルを暗号化または復号化しません。

- Kaspersky Endpoint Security は、暗号化が原因でオペレーティングシステムやインストールされたアプリケーションに損害を与える可能性がある場合は、ファイルを暗号化しません。たとえば、次のファイルおよびフォルダーは、入れ子になっているすべてのフォルダーとともに、暗号化しないファイルまたはフォルダーのリストに含まれます：

  - %WINDIR%
  - %PROGRAMFILES% および %PROGRAMFILES(X86)%
  - Windows のレジストリファイル

  暗号化しないファイルまたはフォルダーのリストは、表示することも編集することもできません。暗号化除外リストにあるファイルとフォルダーは暗号化リストに追加できますが、ファイルの暗号化中は暗号化されません。

ローカルコンピュータードライブのファイルの暗号化

Kaspersky Endpoint Security は OneDrive クラウドストレージまたは OneDrive を名前にしているその他のフォルダーを暗号化しません。ファイルが暗号化ルールに追加されていない場合、暗号化されたファイルの OneDrive フォルダーへのコピーはブロックされます。

ローカルドライブでファイルを暗号化するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ファイルレベルの暗号化**］の順に選択します。
4. ［**暗号化モード**］から［**ルールに従う**］を選択します。
5. ［**暗号化**］タブで［**追加**］をクリックし、ドロップダウンリストから次のいずれかを選択します：

   a. カスペルスキーが推奨するローカルユーザープロファイルフォルダーのファイルを暗号化ルールに追加するには、［**定義済みフォルダー**］を選択します。

   - **ドキュメント**：オペレーティングシステムの標準の［*ドキュメント*］フォルダー内のファイルとそのサブフォルダー。
   - **お気に入り**：オペレーティングシステムの標準の［*お気に入り*］フォルダー内のファイルとそのサブフォルダー。
   - **デスクトップ**：オペレーティングシステムの標準の［*デスクトップ*］フォルダー内のファイルとそのサブフォルダー。
   - **一時ファイル**：コンピューターにインストールされたアプリケーションの動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。

     データが消失する可能性があるため、一時ファイルの暗号化は推奨されません。たとえば、Microsoft Word は文書の処理中に一時ファイルを作成します。一時ファイルが暗号化されて、元のファイルが暗号化されていない場合、文書を保存する際に「*アクセスが拒否されました*」というエラーが表示される可能性があります。さらに、Microsoft Word がファイルを保存することはできても、データが消失して次回文書を開くことができなくなる問題が発生する可能性があります。

   - **Outlook ファイル**：Outlook メールクライアントの動作に関連するファイル (データファイル (PST)、オフラインデータファイル (OST)、オフラインアドレス帳ファイル (OAB)、および個人のアドレス帳ファイル (PAB))。

   b. 暗号化ルールに追加するフォルダーのパスを手動で入力するには、［**カスタムフォルダー**］を選択します。

フォルダーのパスを追加するときは、次のルールに従います：

- 環境変数を使用します（たとえば、`%FOLDER%\UserFolder\`）。環境変数は、パスの先頭で一度だけ使用できます。
- 相対パスは使用しないでください。
- `*` および `?` の文字は使用しないでください。
- UNC パスは使用しないでください。
- 区切り文字として、`;` または `,` を使用してください。

c. ［**ファイルの拡張子による指定**］を選択して、暗号化ルールに個々のファイルの拡張子を追加します。Kaspersky Endpoint Security は、コンピューターのすべてのローカルドライブ上の指定された拡張子を持つファイルを暗号化します。

d. ［**ファイルの拡張子のグループによる指定**］を選択して、ファイルの拡張子のグループを暗号化ルールに追加します（たとえば、*Microsoft Office* ドキュメントなど）。拡張子のグループに含まれるファイル拡張子を持つ、コンピューターのローカルドライブにあるすべてのファイルが暗号化されます。

6. 変更内容を保存します。

ポリシーを適用すると、Kaspersky Endpoint Security は、暗号化ルールに含まれ復号化ルールに含まれていないファイルをただちに暗号化します。

ファイル暗号化には、次の特別な機能があります：

- 同じファイルが暗号化ルールと復号化ルールの両方に追加されている場合、Kaspersky Endpoint Security は次の処理を実行します：
  - ファイルが暗号化されていない場合、Kaspersky Endpoint Security はファイルを暗号化しません。
  - ファイルが暗号化されている場合は、Kaspersky Endpoint Security はファイルを復号化します。
- 暗号化ルールの条件に一致する新しいファイルがある場合、Kaspersky Endpoint Security は続けて暗号化します。例えば、暗号化されていないファイルのパスや拡張子などの属性を変更した場合、暗号化ルールの条件に一致することになります。Kaspersky Endpoint Security はこのファイルを暗号化します。
- 新しいファイルが作成され、そのファイルのプロパティが暗号化ルールの条件と一致する場合、Kaspersky Endpoint Security はそのファイルが開かれると同時に暗号化します。
- Kaspersky Endpoint Security は、開かれているファイルについては、閉じられるまで暗号化を延期します。
- 暗号化されているファイルを同じローカルドライブ上の別のフォルダーに移動する場合、移動先のフォルダーが暗号化ルールに含まれるかどうかとは関係なく、ファイルの暗号化は維持されます。
- ファイルを復号化して、復号化ルールに含まれていない別のローカルのフォルダーにコピーした場合、このファイルのコピーは暗号化される可能性があります。コピーしたファイルが暗号化されないようにするには、対象のフォルダーに復号化ルールを作成します。

アプリケーションを対象にした暗号化ファイルへのアクセスルールの策定

既定では、すべてのアプリケーションは、暗号化ファイルを復号化された状態で処理します。特定のアプリケーション（ブラウザーやテキストエディターなど）を頻繁に使用する場合は、情報を保護するために暗号化ファイルのアクセスルールを作成できます。

Microsoft Internet Explorer および Microsoft Edge のブラウザーに対して暗号化ファイルのアクセスルールを作成することを推奨します。これらのブラウザーの仕組みにより、暗号化ファイルを Web サイト（クラウド保管領域など）にアップロードすると、ファイルは自動的に復号化されます。これによりデータ流出が発生する可能性があります。これらのブラウザーを使用して暗号化ファイルをアップロードすることはできません。［**暗号化されたファイルへのアクセスを暗号化された状態でのみ許可する**］のルールを設定することを推奨します。その他のブラウザー（Google Chrome など）に対してルールを作成する必要はありません。

アプリケーションを対象に暗号化ファイルへのアクセスルールを策定するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ファイルレベルの暗号化**］の順に選択します。
4. ［**暗号化モード**］から［**ルールに従う**］を選択します。

   アクセスルールは、［**ルールに従う**］が選択されている場合のみ適用されます。［**ルールに従う**］を選択した後、［**変更しない**］に変更すると、すべてのアクセスルールが無視されます。すべてのアプリケーションがすべての暗号化されたファイルへアクセスできるようになります。

5. ウィンドウの右側で、［**アプリケーションのルール**］タブを選択します。
6. Kaspersky Security Center のリストからのみアプリケーションを選択するには、［**追加**］をクリックして、ドロップダウンリストで［**Kaspersky Security Center のリストからのアプリケーションの追加**］を選択します。

   a. テーブルのアプリケーションリストの項目を絞るためのフィルターを指定します。そのためには、［**アプリケーション**］、［**製造元**］、［**追加された期間**］の各パラメータと［**グループ**］ブロックのすべてチェックボックスの値を指定します。

   b. ［**更新**］をクリックします。

   c. テーブルに適用されたフィルターの基準を満たすアプリケーションが表示されます。

   d. ［**アプリケーション**］列で、暗号化ファイルアクセスルールの策定の対象にするアプリケーションの横にあるチェックボックスをオンにします。

e. ［**アプリケーションのルール**］で、暗号化ファイルへのアプリケーションのアクセスを決定するルールを選択します。

f. ［**以前に選択したアプリケーションの処理**］で、アプリケーションに対して以前に作成された暗号化ファイルアクセスルールに対する処理を選択します。

アプリケーションの暗号化ファイルアクセスルールの詳細が［**アプリケーションのルール**］タブのテーブルに表示されます。

7. 手動でアプリケーションを選択するには、［**追加**］をクリックして、ドロップダウンリストで［**カスタムアプリケーション**］を選択します。

a. エントリフィールドに、アプリケーションの実行ファイルの名前または名前のリストを拡張子を含めて入力します。

［**Kaspersky Security Center のリストからの追加**］をクリックすることで、Kaspersky Security Center のリストからアプリケーションの実行ファイルの名前を追加することもできます。

b. 必要に応じて、［**説明**］にアプリケーションリストの説明を入力します。

c. ［**アプリケーションのルール**］で、暗号化ファイルへのアプリケーションのアクセスを決定するルールを選択します。

アプリケーションの暗号化ファイルアクセスルールの詳細が［**アプリケーションのルール**］タブのテーブルに表示されます。

8. 変更内容を保存します。

特定のアプリケーションによって作成または変更されたファイルの暗号化

ルールで指定されたアプリケーションによって作成または変更されたすべてのファイルを暗号化するようなルールを作成できます。

その暗号化ルールが適用される前に、指定されたアプリケーションで作成または変更されたファイルは、暗号化されません。

特定のアプリケーションによって作成または変更されたファイルを暗号化するよう設定するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**データ暗号化**］→［**ファイルレベルの暗号化**］の順に選択します。

4. ［**暗号化モード**］から［**ルールに従う**］を選択します。

暗号化ルールは、［**ルールに従う**］が選択されている場合のみ適用されます。［**ルールに従う**］を選択した後、［**変更しない**］に変更すると、すべての暗号化ルールが無視されます。すでに暗号化されたファイルは暗号化されたままになります。

5. ウィンドウの右側で、［**アプリケーションのルール**］タブを選択します。

6. Kaspersky Security Center のリストからのみアプリケーションを選択するには、［**追加**］をクリックして、ドロップダウンリストで［**Kaspersky Security Center のリストからのアプリケーションの追加**］を選択します。

   a. テーブルのアプリケーションリストの項目を絞るためのフィルターを指定します。そのためには、［**アプリケーション**］、［**製造元**］、［**追加された期間**］の各パラメータと［**グループ**］ブロックのすべてチェックボックスの値を指定します。

   b. ［**更新**］をクリックします。

      テーブルに適用されたフィルターの基準を満たすアプリケーションが表示されます。

   c. ［**アプリケーション**］列で、作成したファイルを暗号化するアプリケーションの横にあるチェックボックスを選択します。

   d. ［**アプリケーションのルール**］から［**作成されたすべてのファイルを暗号化する**］を選択します。

   e. ［**以前に選択したアプリケーションの処理**］で、アプリケーションに対して以前に作成されたファイル暗号化ルールに対する処理を選択します。

   選択されたアプリケーションによって作成または変更されたファイルの暗号化ルールの情報が［**アプリケーションのルール**］タブのテーブルに表示されます。

7. 手動でアプリケーションを選択するには、［**追加**］をクリックして、ドロップダウンリストで［**カスタムアプリケーション**］を選択します。

   a. エントリフィールドに、アプリケーションの実行ファイルの名前または名前のリストを拡張子を含めて入力します。

      ［**Kaspersky Security Center のリストからの追加**］をクリックすることで、Kaspersky Security Center のリストからアプリケーションの実行ファイルの名前を追加することもできます。

   b. 必要に応じて、［**説明**］にアプリケーションリストの説明を入力します。

   c. ［**アプリケーションのルール**］から［**作成されたすべてのファイルを暗号化する**］を選択します。

   選択されたアプリケーションによって作成または変更されたファイルの暗号化ルールの情報が［**アプリケーションのルール**］タブのテーブルに表示されます。

8. 変更内容を保存します。

復号化ルールの作成

復号化ルールを作成するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**データ暗号化**］→［**ファイルレベルの暗号化**］の順に選択します。

4. ［**暗号化モード**］から［**ルールに従う**］を選択します。

5. ［**復号化**］タブで［**追加**］をクリックし、ドロップダウンリストから次のいずれかを選択します：

   a. カスペルスキーが推奨するローカルユーザープロファイルフォルダーのファイルを復号化ルールに追加するには、［**定義済みフォルダー**］を選択します。

   b. 復号化ルールに追加するフォルダーのパスを手動で入力するには、［**カスタムフォルダー**］を選択します。

   c. ［**ファイルの拡張子による指定**］を選択して、暗号化ルールに個々のファイルの拡張子を追加します。Kaspersky Endpoint Security は、コンピューターのすべてのローカルドライブ上のファイルのうち指定された拡張子を持つものについては暗号化を行いません。

   d. ［**ファイルの拡張子のグループによる指定**］を選択して、ファイルの拡張子のグループを暗号化ルールに追加します（たとえば、*Microsoft Office* ドキュメントなど）。拡張子のグループに含まれるファイル拡張子を持つ、コンピューターのローカルドライブにあるすべてのファイルが暗号化されません。

6. 変更内容を保存します。

同じファイルが暗号化ルールと復号化ルールの両方に追加されると、そのファイルが暗号化されていない場合は暗号化されず、暗号化されている場合は復号化されます。

ローカルコンピュータードライブでのファイルの復号化

ローカルドライブでファイルを復号化するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**ファイルレベルの暗号化**］の順に選択します。
4. ウィンドウの右側で、［**暗号化**］タブを選択します。
5. 復号化するファイルとフォルダーを暗号化リストから削除します。リストからの削除には、ファイルを選択して、［**ルールの削除とファイルの復号化**］のコンテキストメニューから［**削除**］を選択します。

   暗号化リストから削除されたファイルやフォルダーは、自動的に復号化リストに追加されます。
6. ファイル復号化リストを作成します。
7. 変更内容を保存します。

Kaspersky Endpoint Security は、ポリシーが適用されると、復号化リストに追加された暗号化ファイルをすぐに復号化します。

Kaspersky Endpoint Security は、暗号化されているファイルのパラメータ（ファイルパス / ファイル名 / ファイル拡張子）が変更され、復号化リストに追加されているオブジェクトのパラメータと一致すると、そのファイルを復号化します。

Kaspersky Endpoint Security は、開かれているファイルについては、閉じられるまで復号化を延期します。

暗号化されたパッケージへの追加

企業ネットワーク外のユーザーへのファイル送付時にデータを保護する目的で、暗号化されたパッケージを使用できます。メールクライアントには添付ファイルのサイズ制限があるため、暗号化されたパッケージは、リムーバブルドライブ上にあるサイズが大きなファイルを送付するのに便利です。

暗号化されたパッケージの作成前に、パスワードの設定が要求されます。データ保護の信頼性を高めるため、パスワードの強度チェックと、パスワードの強度の指定の有効化が可能です。有効にすると、「1234」のような短く単純なパスワードが使用できなくなります。

暗号化されたアーカイブを管理コンソール（MMC）で作成するときにパスワードの強度チェックを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**暗号化の共通設定**］の順に選択します。
4. ［**パスワードの設定**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、**暗号化されたパッケージ**タブを選択します。
6. 暗号化されたパッケージの作成時のパスワードの複雑さを設定します。

暗号化されたアーカイブを Web コンソールで作成するときにパスワードの強度チェックを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**ファイルレベルの暗号化**］に移動します。
5. ［**暗号化されたパッケージのパスワード設定**］ブロックで、暗号化されたパッケージの作成時に必要なパスワードの強度の条件を設定します。

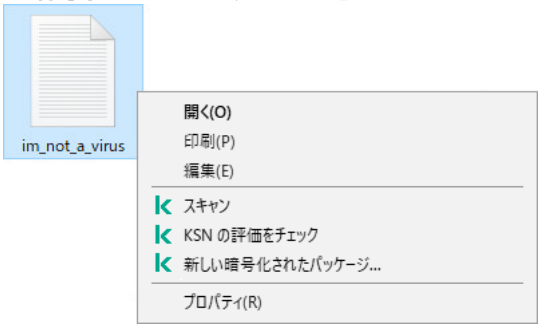
暗号化されたパッケージは、ファイルレベルの暗号化機能とともに Kaspersky Endpoint Security がインストールされたコンピューターで作成できます。

OneDrive クラウドストレージ上にある暗号化されたパッケージにファイルを追加すると、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードして暗号化を実行します。

暗号化されたパッケージを作成するには：

1. 任意のファイル管理アプリケーションで、暗号化されたパッケージに追加するファイルまたはフォルダーを選択します。右クリックして、ファイルまたはフォルダーのコンテキストメニューを開きます。

2. コンテキストメニューで、［**新しい暗号化されたパッケージ**］を選択します（下の図を参照）。



暗号化されたパッケージの作成

3. 表示されたウィンドウで、パスワードを指定し、入力して確認します。

   パスワードは、ポリシーで指定したパスワードの複雑さの基準を満たす必要があります。

4. ［**作成**］をクリックします。

   暗号化されたパッケージの作成プロセスが開始されます。Kaspersky Endpoint Security は、暗号化されたパッケージの作成時に、ファイルの圧縮は行いません。プロセスが終了すると、パスワードで保護されており暗号化された自己解凍形式パッケージ（  ）が、選択した保存先フォルダーに作成されます。

暗号化されたパッケージ内のファイルにアクセスするには、ダブルクリックして解凍ウィザードを開始し、パスワードを入力します。忘れたり紛失したりしたパスワードは復旧できず、暗号化されたパッケージ内のファイルへのアクセスもできなくなります。暗号化されたパッケージを再作成してください。

暗号化されたファイルへのアクセスの復元処理

ファイルが暗号化されると、Kaspersky Endpoint Security は、暗号化されたファイルに直接アクセスするために必要な暗号化鍵を受け取ります。この暗号化鍵を使用すると、ファイルの暗号化中にアクティブだった Windows アカウントで作業しているユーザーは、暗号化ファイルに直接アクセスできます。ファイルの暗号化中、アクティブではなかった Windows アカウントで作業しているユーザーは、暗号化ファイルにアクセスするには、Kaspersky Security Center に接続する必要があります。

次の状況では、暗号化されたファイルにアクセスできないことがあります：

- ユーザーのコンピューターに暗号鍵が保存されているが、Kaspersky Security Center と接続されていないため鍵の管理ができない。この場合、ユーザーは LAN 管理者に暗号化ファイルへのアクセスを要求する必要があります。

  Kaspersky Security Center にアクセスする手段がない場合は、次を行ってください：

  - コンピューターのハードディスクにある暗号化されたファイルにアクセスするためのアクセスキーを要求する。

  - リムーバブルドライブに保存されている暗号化ファイルにアクセスするには、各リムーバブルドライブの暗号化ファイルに対してそれぞれアクセスキーを要求する。

- 暗号化機能がユーザーのコンピューターから削除されている。この場合、ローカルドライブおよびリムーバブルドライブ上の暗号化されたファイルを開くことはできますが、ファイルの内容は暗号化された状態で表示されます。

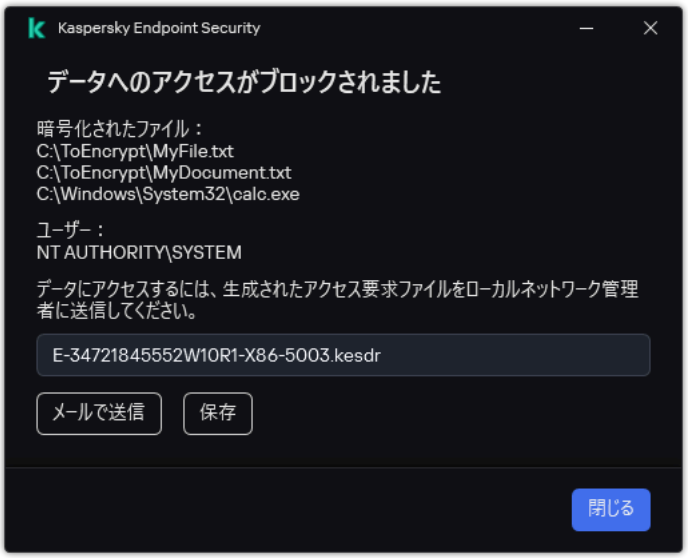
  ユーザーは次の場合に、暗号化されたファイルにアクセスできます：

  - Kaspersky Endpoint Security がインストールされているコンピューターで作成された暗号化パッケージの中にファイルが保存されている。
  - ポータブルモードが許可されたリムーバブルドライブにファイルが保存されている。

暗号化されたファイルにアクセスするには、ユーザーは復元手順（要求と応答）を開始する必要があります。

暗号化されたファイルへのアクセスを復元するには、次の手順を実行します：

1. ユーザーがアクセス要求ファイルを管理者に送信します（以下の図を参照）。
2. 管理者はアクセス要求ファイルを Kaspersky Security Center に追加し、アクセスキーファイルを作成してユーザーに送信します。
3. ユーザーはアクセスキーファイルを Kaspersky Endpoint Security に追加し、ファイルへのアクセスを取得します。



暗号化されたファイルへのアクセスの復元処理

復元手順を開始するには、ユーザーはファイルにアクセスを試みる必要があります。その結果、Kaspersky Endpoint Security はアクセス要求ファイル（拡張子が KESDC のファイル）を作成します。ユーザーは、このファイルを管理者に電子メールなどで送信する必要があります。

Kaspersky Endpoint Security は、コンピューターのドライブ（ローカルドライブまたはリムーバブルドライブ）に保存されているすべての暗号化されたファイルにアクセスするためのアクセス要求ファイルを生成します。

管理コンソール（MMC）で暗号化されたデータアクセスキーファイルを取得する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。

3. ［**デバイス**］タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。

4. コンテキストメニューから［**オフラインモードでのアクセスを許可する**］を選択します。

5. 表示されたウィンドウで、**データ暗号化**タブを選択します。

6. ［**データ暗号化**］タブで［**参照**］をクリックします。

7. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。



オフラインモードでのアクセスを許可する

Web コンソールで暗号化されたデータアクセスキーファイルを取得する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。

3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

4. ［**データ暗号化**］を選択します。

5. ［**ファイルの選択**］をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。

   Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。

6. ［**ライセンスを保存**］をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

暗号化されたデータアクセスキーファイルを受信した後、ユーザーはファイルをダブルクリックして実行する必要があります。その結果、Kaspersky Endpoint Security はドライブに保存されているすべての暗号化されたファイルへのアクセスを許可します。他のドライブに保存されている暗号化ファイルにアクセスするには、ドライブごとに別々のアクセスキーファイルを入手する必要があります。

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

オペレーティングシステム障害が発生した場合は、ファイルレベルの暗号化（FLE）を使用していた場合のみ、データへのアクセスを復元できます。ディスク全体の暗号化（FDE）を使用していた場合は、データへのアクセスは復元できません。

オペレーティングシステム障害が発生した後に、暗号化されたデータへのアクセスを復元するには：

1. ハードディスクをフォーマットせずにオペレーティングシステムを再インストールします。
2. Kaspersky Endpoint Security をインストールします。
3. コンピューターと、データの暗号化時にコンピューターを管理していた Kaspersky Security Center の管理サーバーとの接続を確立します。

   オペレーティングシステム障害が発生する前と同じ条件で、暗号化されたデータへのアクセスが許可されます。

暗号化ファイルアクセスメッセージのテンプレートの編集

暗号化ファイルアクセスメッセージのテンプレートを編集するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**暗号化の共通設定**］の順に選択します。
4. ［**テンプレート**］ブロックの［**テンプレート**］をクリックします。
5. 表示されたウィンドウで、次の操作を実行します：

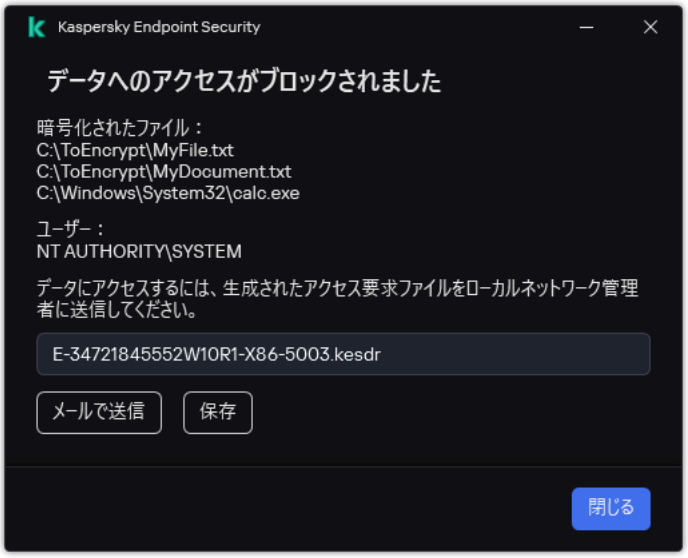
   - ユーザーメッセージテンプレートを編集するには、［**ユーザーのメッセージ**］タブを選択します。コンピューター上に暗号化ファイルへのアクセスに使用できるキーがない場合、ユーザーが暗号化されたファイルにアクセスを試みると、次のウィンドウが表示されます。［**メールで送信**］をクリックすると、ユーザーメッセージが自動で作成されます。このメッセージが、暗号化ファイルへのアクセスを要求するファイルとともに企業の LAN 管理者に送信されます。
   - 管理者メッセージテンプレートを編集するには、［**管理者のメッセージ**］タブを選択します。ユーザーは暗号化されたファイルへのアクセスが許可された後にこのメッセージを受け取ります。

6. メッセージテンプレートを編集します。

   テンプレートテキストに変数を追加するには、カーソルを目的の位置に置き、［**変数**］をクリックして、使用可能なオプションのリストから必要な変数を選択します。

   ［**既定**］を使用して既定のテンプレートテキストを復元することもできます。

7. 変更内容を保存します。



暗号化されたファイルへのアクセスの復元処理

リムーバブルドライブの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムのファイルの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、このリムーバブルドライブの暗号化タスクはエラーにより失敗し、リムーバブルドライブが読み取り専用になります。

リムーバブルドライブ上のデータを保護するには、次の暗号化種別を使用できます：

- Full Disk Encryption（FDE）：

  ファイルシステムを含むリムーバブルドライブ全体の暗号化。

  企業ネットワークの外部で暗号化されたデータにアクセスすることはできません。Kaspersky Security Center へ接続されていないコンピューターの場合（ゲストコンピューターなど）も、企業ネットワーク内の暗号化されたデータへアクセスできません。

- File Level Encryption（FLE）：

  リムーバブルドライブ上のファイルのみの暗号化。ファイルシステムは変更されません。

リムーバブルドライブ上のファイルの暗号化は、*ポータブルモード*と呼ばれる特別なモードを使用して、企業ネットワークの外部のデータにアクセスする機能を提供します。

暗号化中に、Kaspersky Endpoint Security はマスター鍵を作成します。Kaspersky Endpoint Security は、マスター鍵を次のリポジトリに保存します：

- Kaspersky Security Center
- ユーザーのコンピューター

  マスター鍵はユーザーの秘密鍵で暗号化されます。
- リムーバブルドライブ

  マスター鍵は、Kaspersky Security Center の公開鍵で暗号化されています。

暗号化が完了すると、従来のリムーバブルドライブを暗号化せずに使用しているかのように、企業ネットワーク内でリムーバブルドライブ上のデータにアクセスできます。

暗号化されたデータへのアクセス

暗号化されたデータのリムーバブルドライブが接続されると、Kaspersky Endpoint Security は次の処理を実行します：

1. ユーザーのコンピューターのローカル保管領域でマスター鍵を確認します。

   マスター鍵が見つかった場合、ユーザーはリムーバブルドライブ上のデータにアクセスできます。

   マスター鍵が見つからない場合、Kaspersky Endpoint Security は次の処理を実行します：

   a. Kaspersky Security Center に要求を送信します。

      要求を受け取った後、Kaspersky Security Center はマスター鍵を含む応答を送信します。

   b. Kaspersky Endpoint Security は、暗号化されたリムーバブルドライブを使用した、それ以降の操作のために、ユーザーのコンピューターのローカル保管領域にマスター鍵を保存します。
2. データを復号化します。

リムーバブルドライブ暗号化の特別な機能

リムーバブルドライブの暗号化には、次の特別な機能があります：

- リムーバブルドライブの暗号化に関する事前設定はポリシーに含まれます。このポリシーは、管理対象コンピューターの特定のグループに対して作成されています。このため、リムーバブルドライブの暗号化または復号化の設定を含む Kaspersky Security Center ポリシーの適用結果は、そのリムーバブルドライブがどのコンピューターに接続しているかによって異なります。
- Kaspersky Endpoint Security は、リムーバブルドライブに保存されている読み取り専用ステータスのファイルの暗号化や復号化は行いません。

- リムーバブルドライブとして、次のデバイス種別がサポートされています：
  - USB バス経由で接続されているリムーバブルドライブ
  - USB および FireWire バス経由で接続されているハードディスク
  - USB および FireWire バス経由で接続されている SSD ドライブ

リムーバブルドライブの暗号化の開始

ポリシーを使用して、リムーバブルドライブを復号化できます。リムーバブルドライブの暗号化の設定が定義されたポリシーが、特定の管理グループに対して生成されます。このため、リムーバブルドライブに対するデータ復号化の結果は、リムーバブルドライブが接続されているコンピューターによって異なります。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムのファイルの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、このリムーバブルドライブの暗号化タスクはエラーにより失敗し、リムーバブルドライブが読み取り専用になります。

リムーバブルドライブ上のファイルを暗号化する前に、フォーマットされていること、隠しパーティション（EFI システムパーティションなど）がないことを確認します。ドライブに未フォーマットや隠しパーティションがある場合、ファイルの暗号化がエラーにより失敗することがあります。

リムーバブルドライブを暗号化するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**リムーバブルドライブの暗号化**］の順に選択します。
4. ［**暗号化モード**］ドロップダウンリストで、リムーバブルドライブに対して実行する既定の処理を選択します。
   - **リムーバブルドライブ全体の暗号化**（FDE）：Kaspersky Endpoint Security によって、リムーバブルドライブのすべてのセクションが暗号化されます。その結果、リムーバブルドライブに保存されているファイルだけでなく、ファイル名やフォルダー構造を含むファイルシステムも暗号化されます。
   - **すべてのファイルの暗号化**（FLE）：Kaspersky Endpoint Security によって、リムーバブルドライブ上のすべてのファイルが暗号化されます。ファイルの名前やフォルダー構造を含めて、リムーバブルドライブのファイルシステムは暗号化されません。
   - **新しいファイルのみ暗号化**（FLE）：Kaspersky Security Center ポリシーが前回適用された後でリムーバブルドライブに追加されたファイルと、以前からリムーバブルドライブに保存されていたがポリシーの前回の適用後に変更されたファイルだけを暗号化します。

   Kaspersky Endpoint Security は、既に暗号化されているリムーバブルドライブは暗号化しません。

5. リムーバブルドライブの暗号化でポータブルモードを使用する場合は、［**ポータブルモード**］をオンにします。

   ［*ポータブルモード*］は、リムーバブルドライブ上のファイル暗号化（FLE）のモードであり、このモードを使用すると社内ネットワーク外にあるデータにアクセスできます。また、ポータブルモードでは、Kaspersky Endpoint Security をインストールしていないコンピューターで暗号化データを操作することもできます。

6. 未使用の新しいリムーバブルドライブを暗号化するときは、［**使用されているディスク領域のみを暗号化**］をオンにすることを推奨します。このチェックボックスがオフの場合、過去に削除されたファイルや変更が加えられたファイルの残存している断片も含めたすべてのファイルが Kaspersky Endpoint Security によって暗号化されます。

7. それぞれのリムーバブルドライブに対して個別に暗号化の設定を指定する場合は、暗号化ルールを設定します。

8. オフラインモードでリムーバブルドライブ全体の暗号化を使用する場合は、［**オフラインモードでのリムーバブルドライブの暗号化を許可する**］をオンにします。

   *オフラインモードでの暗号化*は、Kaspersky Security Center との接続がない状態でのリムーバブルドライブの暗号化（FDE）です。暗号化を実行中、Kaspersky Endpoint Security はクライアントコンピューター上にのみマスター鍵を保存します。Kaspersky Security Center と次に同期したときに、Kaspersky Endpoint Security は Kaspersky Security Center にマスター鍵を送信します。

   > マスター鍵が保存されているコンピューターでマスター鍵のデータが破損し、なおかつマスター鍵が Kaspersky Security Center に送信されていなかった場合、リムーバブルドライブのデータへのアクセスを復元することはできません。

   ［**オフラインモードでのリムーバブルドライブの暗号化を許可する**］がオフの場合、Kaspersky Security Center への接続が確立されていない状況ではリムーバブルドライブの暗号化は実行できません。

9. 変更内容を保存します。

ポリシーの適用後、ユーザーがリムーバブルドライブを接続したタイミングで（あるいは既にリムーバブルドライブが接続されている場合はただちに）、暗号化を実行するかどうかの確認メッセージがユーザーに表示されます（以下の図を参照）。

ユーザーは次の操作を実行できます：

- 暗号化を実行することをユーザーが承認した場合、Kaspersky Endpoint Security によってデータが暗号化されます。
- 暗号化の実行をユーザーが拒否した場合、データは変更されませんが、リムーバブルドライブは読み取り専用になります。
- 暗号化を実行するかどうかの確認メッセージにユーザーが応答しない場合、データは変更されませんが、リムーバブルドライブは読み取り専用になります。ポリシーが次に更新されて適用されたとき、あるいはこのリムーバブルドライブが次に接続されたときに、暗号化を実行するかどうかの確認メッセージが再表示されます。

データの暗号化中にユーザーがリムーバブルドライブを安全な手順で取り出そうとすると、Kaspersky Endpoint Security はデータの暗号化プロセスを中断して、暗号化プロセスの完了前にリムーバブルドライブを取り出せるようにします。同じリムーバブルドライブがこのコンピューターに次に接続されたときに、データの暗号化が引き続き実行されます。

リムーバブルドライブの暗号化が失敗した場合、**データ暗号化**レポートを本製品のインターフェイスで参照してください。他のアプリケーションによってファイルアクセスがブロックされている可能性があります。その場合、リムーバブルドライブをコンピューターから取り外してから再度接続してみてください。



リムーバブルドライブの暗号化要求

リムーバブルドライブの暗号化ルールの追加

リムーバブルドライブの暗号化ルールを追加するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**リムーバブルドライブの暗号化**］の順に選択します。
4. ［**追加**］をクリックし、ドロップダウンリストから次のいずれかを選択します：
   - デバイスコントロールの信頼するデバイスのリストにあるリムーバブルドライブの暗号化ルールを追加するには、［**このポリシーの信頼するデバイスのリストから指定する**］を選択します。
   - Kaspersky Security Center のリストにあるリムーバブルドライブの暗号化ルールを追加するには、［**Kaspersky Security Center のデバイスリストから指定する**］を選択します。
5. ［**選択したデバイスの暗号化モード**］で、選択したリムーバブルドライブに保存されているファイルに対して Kaspersky Endpoint Security が行う処理を選択します。

6. 暗号化の前に Kaspersky Endpoint Security にリムーバブルドライブの準備をさせて、リムーバブルドライブに保存される暗号化ファイルをポータブルモードで使用できるようにする場合は、［**ポータブルモード**］をオンにします。

   ポータブルモードでは、暗号化機能を持たないコンピューターに接続されたリムーバブルドライブに保存された暗号化ファイルを使用できます。

7. ファイルによって占められているディスクセクターのみを暗号化する場合、［**使用されているディスク領域のみを暗号化**］をオンにします。

   既に使用されているドライブに暗号化を適用する場合、ドライブ全体を暗号化してください。それにより、削除されているが取り出すことのできる情報を含む可能性があるデータを含め、すべてのデータが保護されます。［**使用されているディスク領域のみを暗号化**］は、まだ使用されていない新しいドライブに推奨します。

   デバイスがすでに［**使用されているディスク領域のみを暗号化**］をオンにして暗号化されている場合、［**リムーバブルドライブ全体の暗号化**］をオンにしたポリシーを適用しても、ファイルによって占められていないセクターは暗号化されません。

8. ［**以前に選択したデバイスの処理**］で、リムーバブルドライブに対して以前に定義された暗号化ルールについて Kaspersky Endpoint Security が行う処理を選択します：

   - リムーバブルドライブに対して以前に作成された暗号化ルールを変更しない場合、［**スキップ**］を選択します。
   - リムーバブルドライブに対して以前に作成された暗号化ルールを新しいルールで置き換える場合、［**更新**］を選択します。

9. 変更内容を保存します。

リムーバブルドライブに追加された暗号化ルールは、組織内の任意のコンピューターに接続されたリムーバブルドライブに適用されます。

リムーバブルドライブの暗号化ルールのリストのエクスポートまたはインポート

リムーバブルドライブの暗号化ルールのリストを XML ファイルにエクスポートすることができます。これにより、例えば同じ種別のリムーバブルドライブのルールをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、ルールのリストのバックアップをとったり、別のサーバーにルールを移行することができます。

管理コンソール（MMC）でリムーバブルドライブの暗号化ルールのリストをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**データ暗号化**］→［**リムーバブルドライブの暗号化**］に移動します。

5. ［**選択したデバイスの暗号化ルール**］セクションで、［**<N> 個のルール**］をクリックします。
リムーバブルドライブの暗号化ルールのリストが開きます。

6. リムーバブルドライブの暗号化ルールのリストをエクスポートするには：

   a. エクスポートするルールを選択します。

   b. ［**エクスポート**］をクリックします。

   c. 選択したルールのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。

   d. ファイルを保存します。
   Kaspersky Endpoint Security は既定のダウンロードフォルダーにルールのリストを XML ファイルでエクスポートします。

7. ルールのリストをインポートするには：

   a. ［**インポート**］リンクをクリックします。
   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

   b. ファイルを開きます。
   コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**データ暗号化**］→［**リムーバブルドライブの暗号化**］の順に選択します。

4. リムーバブルドライブの暗号化ルールのリストをエクスポートするには：

   a. エクスポートするルールを選択します。複数のポートを選択するには、**CTRL** または **SHIFT** キーを使用します。
   ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

   b. ［**エクスポート**］リンクをクリックします。

   c. 表示されたウィンドウで、ルールをエクスポートする XML ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。
   Kaspersky Endpoint Security は、ルールのリスト全体を XML ファイルにエクスポートします。

5. リムーバブルドライブの暗号化ルールのリストをインポートするには：

   a. ［**インポート**］リンクをクリックします。
   表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

b. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Endpoint Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

6. 変更内容を保存します。

リムーバブルドライブ上の暗号化ファイルにアクセスするためのポータブルモード

［*ポータブルモード*］は、リムーバブルドライブ上のファイル暗号化（FLE）のモードであり、このモードを使用すると社内ネットワーク外にあるデータにアクセスできます。また、ポータブルモードでは、Kaspersky Endpoint Security をインストールしていないコンピューターで暗号化データを操作することもできます。

ポータブルモードは、次の場合に使用すると便利です：

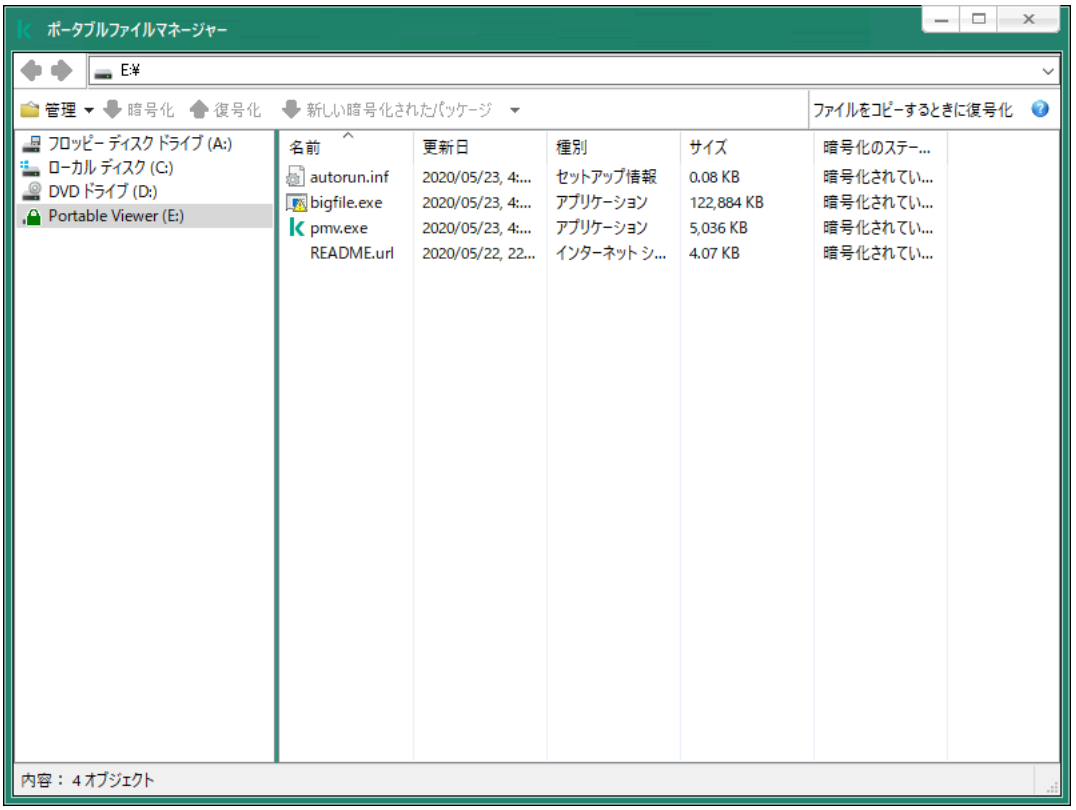
- コンピューターと Kaspersky Security Center 管理サーバーとの間に接続がない。
- Kaspersky Security Center 管理サーバーの変更により、インフラストラクチャが変更された。
- Kaspersky Endpoint Security がコンピューターにインストールされていない。

ポータブルファイルマネージャー

ポータブルモードで作業するために、Kaspersky Endpoint Security は、*ポータブルファイルマネージャー*という特別な暗号化モジュールをリムーバブルドライブにインストールします。ポータブルファイルマネージャーは、Kaspersky Endpoint Security がコンピューターにインストールされていない場合に暗号化データを操作するためのインターフェイスを提供します（以下の図を参照）。コンピューターに Kaspersky Endpoint Security がインストールされている場合は、通常のファイルマネージャー（エクスプローラーなど）を使用して、暗号化されたリムーバブルドライブを操作できます。

ポータブルファイルマネージャーは、リムーバブルドライブ上のファイルを暗号化するためのキーを保存します。キーは、ユーザーパスワードで暗号化されます。ユーザーは、リムーバブルドライブ上のファイルを暗号化する前に、パスワードを設定します。

Kaspersky Endpoint Security がインストールされていないコンピューターにリムーバブルドライブが接続されると、ポータブルファイルマネージャーが自動的に起動します。コンピューターでアプリケーションの自動起動が無効になっている場合は、ポータブルファイルマネージャーを手動で起動します。これを行うには、リムーバブルドライブに保存されている pmv.exe という名前のファイルを実行します。



ポータブルファイルマネージャー

暗号化ファイルを操作するためのポータブルモードのサポート

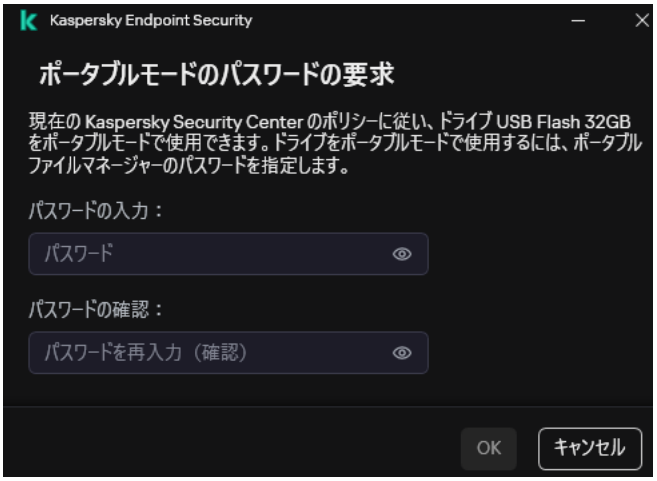
管理コンソール（MMC）でリムーバブルドライブ上の暗号化ファイルを操作するためのポータブルモードのサポートを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**データ暗号化**］→［**リムーバブルドライブの暗号化**］の順に選択します。
4. ［**選択したデバイスの暗号化モード**］で、［**すべてのファイルの暗号化**］または［**新しいファイルのみ暗号化**］を選択します。

   ポータブルモードは、ファイルレベルの暗号化（FLE）でのみ使用できます。ディスク全体の暗号化（FDE）のポータブルモードのサポートを有効にすることはできません。

5. ［**ポータブルモード**］チェックボックスをオンにします。
6. 必要に応じて、個々のリムーバブルドライブの暗号化ルールを追加します。
7. 変更内容を保存します。
8. ポリシーを適用後、リムーバブルドライブをコンピューターに接続します。
9. リムーバブルドライブの暗号化操作を確認します。

ポータブルファイルマネージャーのパスワードを作成するウィンドウが表示されます。



ポータブルモードのパスワードの要求

10. 強度の要件を満たすパスワードを指定し、再度入力します。

11. 変更内容を保存します。

Web コンソールでリムーバブルドライブ上の暗号化ファイルを操作するためのポータブルモードのサポートを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**データ暗号化**］→［**リムーバブルドライブの暗号化**］に移動します。

5. ［**既定の動作**］ブロックで［**すべてのファイルの暗号化**］または［**新しいファイルのみ暗号化**］をオンにします。

   ポータブルモードは、ファイルレベルの暗号化（FLE）でのみ使用できます。ディスク全体の暗号化（FDE）のポータブルモードのサポートを有効にすることはできません。

6. ［**ポータブルモード**］チェックボックスをオンにします。

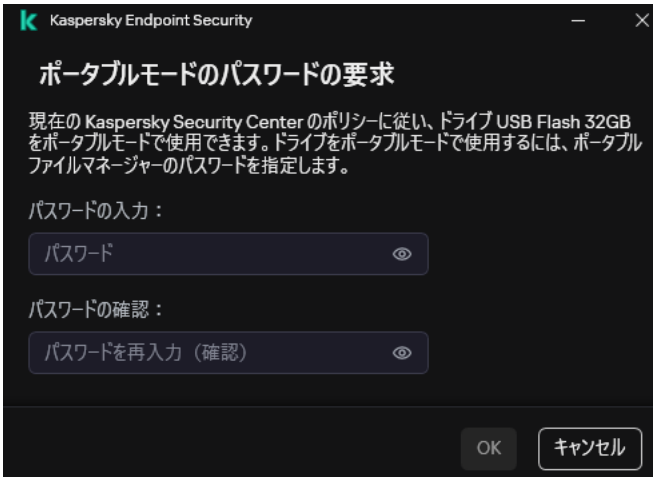
7. 必要に応じて、個々のリムーバブルドライブの暗号化ルールを追加します。

8. 変更内容を保存します。

9. ポリシーを適用後、リムーバブルドライブをコンピューターに接続します。

10. リムーバブルドライブの暗号化操作を確認します。

ポータブルファイルマネージャーのパスワードを作成するウィンドウが表示されます。



ポータブルモードのパスワードの要求

11. 強度の要件を満たすパスワードを指定し、再度入力します。

12. 変更内容を保存します。

Kaspersky Endpoint Security は、リムーバブルドライブ上のファイルを暗号化します。暗号化ファイルの操作に使用されるポータブルファイルマネージャーも、リムーバブルドライブに追加されます。リムーバブルドライブに既に暗号化されたファイルがある場合は、Kaspersky Endpoint Security は独自のキーを使用してそれらを再度暗号化します。これによりユーザーは、ポータブルモードでリムーバブルドライブ上のすべてのファイルにアクセスできます。

リムーバブルドライブ上の暗号化ファイルにアクセスする

ポータブルモードをサポートするリムーバブルドライブ上のファイルを暗号化した後、次のファイルアクセス方法を使用できます：

- Kaspersky Endpoint Security がコンピューターにインストールされていない場合、ポータブルファイルマネージャーにパスワードの入力を要求されます。コンピューターを再起動するたび、またはリムーバブルドライブを再接続するたびに、パスワードを入力する必要があります。

- コンピューターが企業ネットワークの外部にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合は、パスワードの入力を要求されるか、管理者にファイルへのアクセス要求が送信されます。リムーバブルドライブ上のファイルにアクセスすると、Kaspersky Endpoint Security は秘密の鍵をコンピューターの保管領域に保存します。これにより今後は、パスワードを入力したり、管理者に依頼したりすることなく、ファイルにアクセスできるようになります（以下の図を参照）。

- コンピューターが企業ネットワーク内にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合、パスワードを入力せずにデバイスにアクセスできます。Kaspersky Endpoint Security は、コンピューターが接続されている Kaspersky Security Center 管理サーバーから秘密鍵を受信します。



リムーバブルドライブ上の暗号化ファイルにアクセスする

ポータブルモードで作業するためのパスワードの復元

ポータブルモードで作業するためのパスワードを忘れた場合は、企業ネットワーク内の Kaspersky Endpoint Security がインストールされているコンピューターに、リムーバブルドライブを接続する必要があります。秘密の鍵はコンピューターの保管領域または管理サーバーに保存されているため、ファイルにアクセスできます。新しいパスワードでファイルを復号化および再暗号化します。

リムーバブルドライブを別のネットワークからコンピューターに接続するときのポータブルモードの機能

コンピューターが企業ネットワークの外部にあり、Kaspersky Endpoint Security がコンピューターにインストールされている場合は、次の方法でファイルにアクセスできます：

- **パスワードベースでアクセスする**

  パスワードを入力すると、リムーバブルドライブ上のファイルを表示、変更、保存できるようになります（*透過的アクセス権*）。リムーバブルドライブの暗号化に関するポリシー設定で、次のパラメータが設定されている場合は、Kaspersky Endpoint Security はリムーバブルドライブの読み取り専用アクセス権を設定できます：

  - ポータブルモードのサポートが無効になっている
  - ［**すべてのファイルの暗号化**］または［**新しいファイルのみ暗号化**］モードが選択されている

  それ以外の場合は、リムーバブルドライブへのフルアクセス権（読み取り／書き込み権限）が付与されます。ファイルの追加と削除ができるようになります。

  リムーバブルドライブがコンピューターに接続中であっても、リムーバブルドライブへのアクセス権限を変更できます。リムーバブルドライブへのアクセス権限が変更されると、ファイルへのアクセスがブロックされ、パスワードを再度入力するよう要求されます。

  パスワードの入力後は、リムーバブルドライブの暗号化ポリシー設定を適用できません。この場合、リムーバブルドライブ上のファイルを復号化または再暗号化することはできません。

- **管理者にファイルへのアクセス権を依頼する**

ポータブルモードで作業するためのパスワードを忘れた場合は、管理者にファイルへのアクセス権を依頼します。ファイルにアクセスするには、ユーザーは管理者にアクセス要求ファイル（拡張子が KESDC のファイル）を送信する必要があります。ユーザーは、メールなどでアクセス要求ファイルを送信できます。管理者は、暗号化されたデータアクセスファイル（拡張子が KESDR のファイル）を送信します。

要求と応答のパスワード復元手順を完了すると、リムーバブルドライブ上のファイルへの透過的アクセス権とリムーバブルドライブへのフルアクセス権（読み取り／書き込み権限）が付与されます。

たとえば、リムーバブルドライブの暗号化ポリシーの適用やファイルの復号化を行えます。パスワードの復元を完了するか、ポリシーが更新されると、変更を確認するよう要求されます。

管理コンソール（MMC）で暗号化されたデータアクセスファイルを取得する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**デバイス**］を選択します。
3. ［**デバイス**］タブで、暗号化データへのアクセスを要求しているユーザーのコンピューターを選択して、右クリックしコンテキストメニューを表示します。
4. コンテキストメニューから［**オフラインモードでのアクセスを許可する**］を選択します。
5. 表示されたウィンドウで、**データ暗号化**タブを選択します。
6. ［**データ暗号化**］タブで［**参照**］をクリックします。
7. アクセス要求ファイルを選択するウィンドウで、ユーザーから受け取ったファイルへのパスを指定します。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。



オフラインモードでのアクセスを許可する

Web コンソールで暗号化されたデータのアクセスファイルを取得する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. データへのアクセスを復元するコンピューターの名前の横にあるチェックボックスをオンにします。

3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

4. ［**データ暗号化**］を選択します。

5. ［**ファイルの選択**］をクリックして、ユーザーから受け取ったアクセス要求ファイル（拡張子が KESDC のファイル）を選択します。

   Web コンソールには、リクエストに関する情報が表示されます。これには、ユーザーがファイルへのアクセスを要求しているコンピューターの名前が含まれます。

6. ［**ライセンスを保存**］をクリックして、暗号化されたデータのアクセスキーファイル（拡張子が KESDR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

リムーバブルドライブの復号化

ポリシーを使用して、リムーバブルドライブを復号化できます。リムーバブルドライブの暗号化の設定が定義されたポリシーが、特定の管理グループに対して生成されます。このため、リムーバブルドライブに対するデータ復号化の結果は、リムーバブルドライブが接続されているコンピューターによって異なります。

リムーバブルドライブを復号化するには：

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**データ暗号化**］→［**リムーバブルドライブの暗号化**］の順に選択します。

4. リムーバブルドライブに保存されている暗号化ファイルをすべて復号化するには、［**暗号化モード**］で［**リムーバブルドライブ全体の復号化**］を選択します。

5. 個々のリムーバブルドライブに保存されているデータを復号化するには、復号化の対象にするデータを保存しているリムーバブルドライブの暗号化ルールを編集します。次の手順に従います：

   a. 暗号化ルールの設定対象にしたリムーバブルドライブのリストで、必要なリムーバブルドライブに対応するエントリを選択します。

   b. ［**ルールの設定**］をクリックして、選択したリムーバブルドライブの暗号化ルールを編集します。

   c. ［**ルールの設定**］のコンテキストメニューで、［**リムーバブルドライブ全体の復号化**］を選択します。

6. 変更内容を保存します。

その結果、ユーザーがリムーバブルドライブを接続する場合、または既に接続されている場合は、Kaspersky Endpoint Security はリムーバブルドライブを復号化します。復号化プロセスには一定の時間がかかることについての警告も表示されます。データの復号化中にユーザーがリムーバブルドライブを安全な手順で取り出そうとすると、Kaspersky Endpoint Security はデータの復号化プロセスを中断して、復号化操作の完了前にリムーバブルドライブを取り出せるようにします。同じリムーバブルドライブがコンピューターに次に接続されたときに、データの復号化が引き続き実行されます。

リムーバブルドライブの復号化が失敗した場合、**データ暗号化**レポートを本製品のインターフェイスで参照してください。他のアプリケーションによってファイルアクセスがブロックされている可能性があります。その場合、リムーバブルドライブをコンピューターから取り外してから再度接続してみてください。

データ暗号化の詳細の表示

Kaspersky Endpoint Security は、暗号化または復号化の進行中に、クライアントコンピューターに適用される暗号化パラメータのステータスに関する情報を Kaspersky Security Center にリレーします。

暗号化ステータスの表示

データの暗号化を監視するためのステータスを確認できます。Kaspersky Endpoint Security では、次の暗号化ステータスが割り当てられます：

- **ポリシー不適合。ユーザーがキャンセル**：ユーザーがデータ暗号化をキャンセルしました。
- **エラーによりポリシーに適合しません**：ライセンスがないなどの暗号化エラーです。
- **ポリシーの適用中。再起動が必要です**：このコンピューターで、データの暗号化が進行中です。データ暗号化を完了するには、コンピューターを再起動してください。
- **暗号化ポリシーが指定されていません**：データ暗号化がポリシーでオフになっています。
- **サポートされていません**：このコンピューターにデータ暗号化コンポーネントがインストールされていません。
- **ポリシーの適用中**：このコンピューターで、データの暗号化または復号化あるいはその両方が進行中です。

コンピューターデータの暗号化ステータスを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**管理対象デバイス**］を選択します。
3. ［**デバイス**］タブの作業領域で、スクロールバーを右端までスライドさせます。［**暗号化ステータス**］列が表示されていない場合、Kaspersky Security Center コンソールの設定でこの列を追加してください。

   ［**暗号化ステータス**］列に、選択された管理グループに属するコンピューター上のデータの暗号化ステータスが表示されます。このステータスは、コンピューターのローカルドライブでのファイル暗号化とディスク全体の暗号化に関する情報をもとに作成されます。
4. コンピューターのデータ暗号化のステータスが［**ポリシーの適用中**］の場合は、暗号化の進捗パネルで監視できます：
   a. ［**ポリシーの適用中**］ステータスをダブルクリックしてコンピューターのプロパティを開きます。
   b. コンピューターのプロパティウィンドウで、［**アプリケーション**］セクションを選択します。
   c. コンピューターにインストールされているカスペルスキー製品のリストで、［**Kaspersky Endpoint Security for Windows**］を選択します。
   d. ［**統計**］をクリックします。
   e. ［**デバイスの暗号化**］で、現在のデータ暗号化の進行状況（%）を確認することができます。

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

Kaspersky Security Center ダッシュボードで暗号化の統計情報を表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
3. コンソールツリーの右側の作業領域で、［**統計**］タブを選択します。
4. データ暗号化の統計情報を含む情報ペインを備えた新しいページを作成します。次の手順に従います：
   a. ［**統計**］タブで［**表示のカスタマイズ**］をクリックします。
   b. 表示されたウィンドウで、［**追加**］をクリックします。
   c. ウィンドウが表示されます。表示されたウィンドウの［**全般**］セクションで、ページの名前を入力します。
   d. ［**情報パネル**］セクションで、［**追加**］をクリックします。
   e. 表示されたウィンドウの［**保護ステータス**］グループで、［**デバイスの暗号化**］を選択します。
   f. ［**OK**］をクリックします。

g. 必要に応じて、詳細ペインの設定を編集します。ペインを編集するには、［**表示**］および［**デバイス**］セクションを使用します。

h. ［OK］をクリックします。

i. 手順のステップ d ～ h を繰り返します。［**保護ステータス**］セクションでは、［**リムーバブルドライブの暗号化**］項目を選択します。

追加された詳細ペインが、［**情報パネル**］リストに表示されます。

j. ［OK］をクリックします。

ここまでのステップで作成された情報ペインを含むページの名前が、［**ページ**］リストに表示されます。

k. ［**閉じる**］をクリックします。

5. ［**統計**］タブで、手順のここまでのステップで作成したページを開きます。

情報ペインが表示され、コンピューターとリムーバブルドライブの暗号化ステータスが示されます。

ローカルコンピュータードライブでのファイル暗号化エラーの表示

ローカルコンピュータードライブでのファイル暗号化エラーを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーで、［**管理対象デバイス**］を選択します。

3. ［**デバイス**］タブで、リスト内のコンピューター名を選択して右クリックしコンテキストメニューを表示します。

4. コンピューターのコンテキストメニューから［**プロパティ**］項目を選択します。表示されたウィンドウで、［**プロテクション**］セクションを選択します。

5. ［**データ暗号化エラーの表示**］をクリックして［**データ暗号化エラー**］ウィンドウを開きます。

このウィンドウには、ローカルコンピューターのドライブ上でのファイル暗号化エラーの詳細が表示されます。エラーが訂正されると、この詳細情報は［**データ暗号化エラー**］ウィンドウから削除されます。

データ暗号化レポートの表示

Kaspersky Security Center を使用して、データ暗号化のレポートを作成することができます。

- **管理対象デバイスの暗号化ステータスレポート**：レポートには、コンピューターの暗号化ステータスが暗号化ポリシーに従っているかどうかの情報が含まれます。

- **大容量ストレージデバイスの暗号化ステータスレポート**：レポートには、外部デバイスとストレージ機器の暗号化ステータスに関する情報が含まれます。

- **暗号化されたドライブへのアクセス権に関するレポート**：レポートには、暗号化されたドライブにアクセスできるアカウントのステータスに関する情報が含まれます。

- **ファイル暗号化のエラーに関するレポート**：レポートには、コンピューターのデータ暗号化もしくは復号化タスクの実行中に発生したエラーに関する情報が含まれます。
- **暗号化されたファイルへのアクセスのブロックに関するレポート**：レポートには、暗号化されたファイルへのアクセス権を取得する際にブロックされているアプリケーションに関する情報が含まれます。

データ暗号化レポートを表示するには：

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理サーバー**］フォルダーで、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ウィンドウの［**その他**］セクションで、データ暗号化レポートのうち1つを選択します。
   新規レポートテンプレートウィザードが完了すると、［**レポート**］タブのテーブルに新しいレポートテンプレートが表示されます。
5. 手順のここまでのステップで作成したレポートテンプレートを選択します。
6. テンプレートのコンテキストメニューから［**レポートの表示**］を選択します。

   レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

暗号化されたデバイスにアクセスできない状況での暗号化デバイスの使用

暗号化されたデバイスへのアクセスの取得

次の場合、暗号化されたデバイスにアクセスできるようユーザーから要求しなければならないことがあります：

- ハードディスクの暗号化が別のコンピューターで行われたとき。
- デバイスの暗号鍵がコンピューター上になく（コンピューター上の暗号化されたリムーバブルドライブに最初にアクセスしようとしたとき、など）、さらにコンピューターが Kaspersky Security Center に接続していないとき。
  ユーザーが暗号化されたデバイスへのアクセスキーを適用すると、ユーザーのコンピューターに暗号鍵が保存され、Kaspersky Security Center に接続されていない場合でもこのコンピューターで以降にアクセスを試みるたびにこのデバイスへのアクセスが許可されます。

暗号化されたデバイスには、次の方法でアクセスできます：

1. ユーザー側で Kaspersky Endpoint Security のインターフェイスを使用して拡張子が kesdc のアクセス要求ファイルを作成し、企業 LAN の管理者に送信します。
2. 管理者は Kaspersky Security Center の管理コンソールを使用して拡張子が kesdr のアクセスキーファイルを作成し、ユーザーに送信します。
3. ユーザーはアクセスキーを適用します。

暗号化されたデバイス上のデータの復元

ユーザーは、暗号化されたデバイスの復元ツール（以下、「復元ツール」）を使用して、暗号化されたデバイスにアクセスできます。この操作は次の場合に必要になります：

- アクセスキーを使用してアクセスを取得する方法に失敗した。
- デバイスが暗号化されているコンピューターに暗号化機能がインストールされていない。

復元ツールによる暗号化デバイスへのアクセスの復元に必要なデータは、ユーザーのコンピューターのメモリに暗号化されていない形式で一定期間保存されます。そのようなデータに対する不正アクセスのリスクを減らすために、暗号化されたデバイスへのアクセスの復元は信頼できるコンピューター上で行ってください。

暗号化されたデバイス上のデータは次の方法で復元できます：

1. ユーザー側で 復元ツールを使用して拡張子が fdertc のアクセス要求ファイルを作成し、企業 LAN の管理者に送信します。
2. 管理者は Kaspersky Security Center の管理コンソールを使用して拡張子が fdertr のアクセスキーファイルを作成し、ユーザーに送信します。
3. ユーザーはアクセスキーを適用します。

ユーザーは、復元ツールで認証エージェントアカウントの認証情報を指定して、暗号化されたシステムハードディスクのデータを復元することもできます。認証エージェントのメタデータが破損している場合、アクセス要求ファイルによる復元方法を完了させてください。

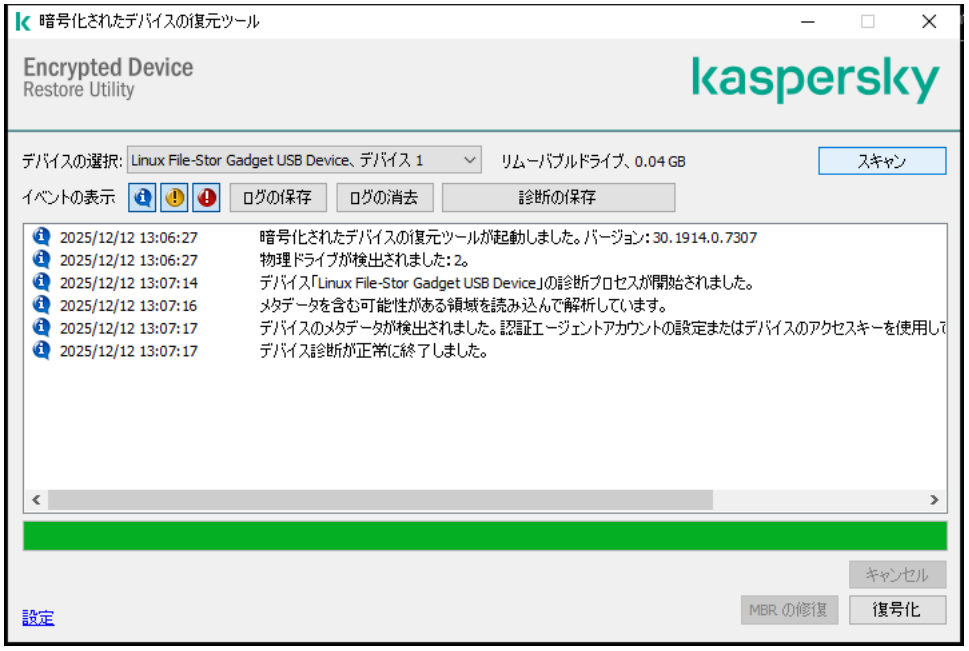
暗号化されたデバイスのデータを復元する前に、この操作を実行するコンピューターで Kaspersky Security Center ポリシーをキャンセルするか、Kaspersky Security Center ポリシー内の暗号化を無効にしてください。これにより、デバイスの再暗号化を防ぐことができます。

FDERT 復元ツールを使用してデータを復元する

ハードドライブに障害が発生した場合、ファイルシステムが破損している可能性があります。この場合、Kaspersky Disk Encryption 技術で保護されたデータは利用できません。データを復号化し、新しいドライブにデータをコピーできます。

Kaspersky Disk Encryption 技術で保護されたドライブでのデータの復元は、次の手順で構成されます：

1. スタンドアロン復元ツールの作成（下の図を参照）。
2. Kaspersky Endpoint Security 暗号化コンポーネントがインストールされていないコンピューターにドライブを接続します。
3. 復元ツールを実行して、ハードドライブを診断します。
4. ドライブ上のデータにアクセスします。これを行うには、認証エージェントの認証情報を入力するか、復元手順（要求と応答）を開始します。



FDERT 復元ツール

スタンドアロン復元ツールの作成

復元ツールの実行ファイルを作成するには：

1. メインウィンドウで、 をクリックします。
2. 表示されたウィンドウで、［**暗号化されたデバイスの復元**］をクリックします。
   暗号化されたデバイスの復元ツールが起動します。

3. 復元ツールのウィンドウで［**スタンドアロン復元ツールの作成**］をクリックします。

4. スタンドアロン復元ツールをコンピューターのメモリに保存します。

その結果、復元ツールの実行ファイル（fdert.exe）が、指定したフォルダーに保存されます。Kaspersky Endpoint Security 暗号化コンポーネントを持たないコンピューターに復元ツールをコピーします。これにより、ドライブの再暗号化を防ぐことができます。

復元ツールによる暗号化デバイスへのアクセスの復元に必要なデータは、ユーザーのコンピューターのメモリに暗号化されていない形式で一定期間保存されます。そのようなデータに対する不正アクセスのリスクを減らすために、暗号化されたデバイスへのアクセスの復元は信頼できるコンピューター上で行ってください。

ハードドライブ上のデータを回復する

復元ツールを使用して、暗号化されたデバイスへのアクセスを復元するには：

1. 復元ツールの実行ファイルである fdert.exe という名前のファイルを実行します。このファイルは、Kaspersky Endpoint Security によって作成されます。

2. 復元ツールのウィンドウで、アクセスを復元する暗号化されたデバイスを選択します。

3. ［**スキャン**］をクリックして、デバイスに対して行う処理（ロック解除するか復号化するか）をユーティリティが定義できるようにします。

   Kaspersky Endpoint Security の暗号化機能へのアクセス権がコンピューターにある場合、デバイスロックの解除が要求されます。デバイスのロックを解除しても復号化されませんが、ロック解除の結果、このデバイスに直接アクセスできるようになります。Kaspersky Endpoint Security の暗号化機能へのアクセス権がコンピューターにない場合、デバイスの復号化が要求されます。

4. 診断情報をインポートする場合は、［**診断の保存**］をクリックします。

   ユーティリティは、診断情報を含むファイルとともにアーカイブを保存します。

5. 暗号化されたシステムハードディスクの診断からのメッセージで、デバイスのマスターブートレコード（MBR）に関する問題が報告された場合は、［**MBR の修復**］をクリックします。

   デバイスのマスターブートレコードを修正すると、デバイスのロック解除や復号化に必要な情報の取得速度が速くなります。

6. 診断結果に応じて、［**ロック解除**］または［**復号化**］をクリックします。

7. 認証エージェントアカウントを使用してデータを復元する場合は、［**認証エージェントアカウント設定の使用**］オプションを選択し、認証エージェントの認証情報を入力します。

   この方法は、システムハードディスク上のデータを復元する場合でのみ可能です。システムハードディスクが破損して認証エージェントのアカウントデータを失ってしまった場合、企業 LAN の管理者からアクセスキーを取得して暗号化されたデバイスにあるデータを復元してください。

8. 復元手順を開始する場合は、次の手順を実行します：

   a. ［**デバイスアクセスキーを手動で指定する**］を選択します。

   b. ［**アクセスキーの取得**］をクリックし、アクセス要求ファイルをコンピューターのメモリ（拡張子が FDERTC のファイル）に保存します。

   c. アクセス要求ファイルを企業 LAN の管理者に送信します。

   > アクセスキーを取得するまで［**デバイスアクセスキーの取得**］ウィンドウは閉じないでください。再度このウィンドウを表示しても、管理者が以前に作成したアクセスキーは適用できません。

   d. 企業の LAN 管理者によって作成および送信されたアクセスファイル（拡張子が FDERTR のファイル）を受信して保存します（以下の手順を参照）。

   e. ［**デバイスアクセスキーの取得**］ウィンドウでアクセスファイルをダウンロードします。

9. デバイスを復号化する場合は、追加の復号化設定を行う必要があります：

   - 復号化の範囲を指定します。
     - デバイス全体を復号化する場合は、［**デバイス全体の復号化**］を選択します。
     - デバイスのデータの一部を復号化する場合は、［**特定のデバイス範囲の復号化**］を選択し、復号化の範囲を指定します。
   - 復号化データを書き込む場所を選択します：
     - 元のデバイスにあるデータを復号化されたデータに書き換える場合、［**ディスクイメージのファイルに復号化**］をオフにします。
     - 復号化されたデータと元の暗号化データを別に保存する場合、［**ディスクイメージのファイルに復号化**］をオンにし、VHD ファイルの保存先のパスを［**参照**］から指定します。

10. ［**OK**］をクリックします。

デバイスのロック解除 / 復号化プロセスが開始されます。

管理コンソール（MMC）で暗号化されたデータアクセスファイルを作成する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］フォルダーの順に選択します。
3. 作業領域で、アクセスキーファイルを作成する暗号化されたデバイスを選択し、デバイスのコンテキストメニューで［**Kaspersky Endpoint Security のデバイスへのアクセス**］をクリックします。

> アクセス要求ファイルが生成されたコンピューターが不明な場合は、コンソールツリーで、［**詳細**］→［**データ暗号化と保護機能**］フォルダーの順に選択し、作業領域で［**デバイスの暗号化鍵を取得**］をクリックします。

4. 表示されたウィンドウで、使用する暗号化アルゴリズムを選択します：AES256 または AES56。

   データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（*高度な暗号化（AES256）*または*中程度の暗号化（AES56）*）。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。

5. ［**参照**］をクリックしてウィンドウを開き、 ユーザーから受け取った、拡張子が fdertc の要求ファイルへのパスを指定します。

6. ［**ロックを解除する**］をクリックします。

ユーザーのリクエストに関する情報が表示されます。Kaspersky Security Center はキーファイルを生成します。生成された暗号化データのアクセスキーファイルをユーザーにメールで送信します。または、アクセスファイルを保存し、任意の受け渡し方法でファイルを転送します。

Web コンソールで暗号化されたデータアクセスファイルを作成する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］をクリックします。

2. データを回復するコンピューターの名前の横にあるチェックボックスをオンにします。

3. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

   これにより、デバイスへのアクセスを許可するためのウィザードが開始されます。

4. ウィザードの指示に従って、デバイスへのアクセスを許可します。

   a. Kaspersky Endpoint Security for Windows のプラグインを選択します。

   b. 使用する暗号化アルゴリズムを選択します：AES256 または AES56。

      データ暗号化アルゴリズムは配布パッケージに含まれる AES 暗号化ライブラリによって異なります（*高度な暗号化（AES256）*または*中程度の暗号化（AES56）*）。AES 暗号化ライブラリは本製品と合わせてインストールされます（※日本では 256 ビットのインストーラーのみ提供しています。56 ビットについては日本国内で提供していません）。

   c. ユーザーから受け取ったアクセス要求ファイル（拡張子が FDERTC のファイル）を選択します。

   d. 暗号化されたデータのアクセスキーファイル（拡張子が FDERTR のファイル）を保存するフォルダーを選択します。

その結果、暗号化されたデータのアクセスキーを取得できます。そのアクセスキーは、ユーザーに転送する必要があります。

オペレーティングシステムのレスキューディスクの作成

暗号化されたハードディスクに何らかの理由でアクセスできなくなり、オペレーティングシステムを読み込めなくなったときには、オペレーティングシステムのレスキューディスクが便利です。

レスキューディスクを使用して、Windows オペレーティングシステムのイメージを読み込み、オペレーティングシステムのイメージに用意されている復元ツールを使用して、暗号化されたハードディスクへのアクセスを復元することができます。

オペレーティングシステムのレスキューディスクを作成するには：

1. 暗号化されたデバイスの復元ツールの実行ファイルを作成します。

2. Windows プリブート環境のカスタムイメージを作成します。Windows プリブート環境のカスタムイメージの作成中に、復元ツールの実行ファイルをこのイメージに追加します。

3. Windows プリブート環境のカスタムイメージを、CD やリムーバブルドライブなどのブート可能なドライブに保存します。

   Windows プリブート環境のカスタムイメージを作成するための手順については、Microsoft のヘルプファイル（Microsoft TechNet リソースなどにあるもの）を参照してください。

Detection and Response ソリューション

Kaspersky Detection and Response ソリューションは、組織インフラの様々なレベルで高度な脅威や攻撃の兆候を検出するためのセキュリティシステムです。Detection and Response ソリューションは、検知された脅威に関する情報を提供し、脅威対応処理の管理を可能にします。

そのため、Detection and Response ソリューションは以下を行います。

- コンピューター、サーバー、その他の機器の動作に関する情報（テレメトリ）を受信します。
- 情報を自動的に解析し、脅威を検知します。
- 脅威の分析およびその対応処理の選択のために、脅威の活動連鎖の列としてアラートの詳細を生成します。
- 脅威の対応処理を実行します（たとえば、コンピューターのネットワーク隔離など）。

Kaspersky Endpoint Security は組み込みエージェントを使用して Detection and Response ソリューションをサポートします。組み込みエージェントは、ソリューションのサーバーにテレメトリを送信し、脅威の対応処理を実行します。組み込みエージェントは以下をサポートします：

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform：
  - Endpoint Detection and Response (EDR) バージョン 7.1 以降
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）
- Kaspersky Sandbox 2.0

Kaspersky Endpoint Security と Detection and Response ソリューションの組み合わせは、[EDR Optimum+MDR] などさまざまな構成で使用できます。

MDR および EDR Optimum のライセンス管理

Kaspersky Endpoint Security は、Kaspersky Managed Detection and Response (MDR) および Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) ソリューションの機能をサポートします。Kaspersky Endpoint Security をこれらのソリューションと併せて様々な構成で使用することができるため、お客様の組織のニーズに合わせてカスタマイズした保護システムを構築することができます。そのためには、各ソリューションのライセンスを購入する必要があります。ライセンスは、MDR アドオンのみのように単一のソリューションを使用できるライセンスと、EDR Optimum + MDR のように、複数のソリューションを使用できるものがあります。

MDR と EDR Optimum は次のライセンス方式をサポートします：

- MDR と EDR Optimum は Kaspersky Endpoint Security for Windows のライセンスの適用対象となっている。

  機能は Kaspersky Endpoint Security for Windows のアクティベーション後すぐに使用できます。追加するライセンスは1つのみです。

- MDR または EDR Optimum の別のライセンス（MDR Add-on、EDR Optimum Add-on、[EDR Optimum+MDR] Add-on）。

  機能は、MDR アドオン、EDR Optimum アドオン、または [EDR Optimum+MDR] アドオン用の個別のライセンスの追加後、使用できるようになります。結果として、Kaspersky Endpoint Security のライセンスおよび MDR または EDR Optimum のライセンスの 2 種類のライセンスがコンピューターに追加されることになります。最初に Kaspersky Endpoint Security のライセンスを追加する必要があります。

Kaspersky Endpoint Security では、MDR と EDR Optimum の*現在のライセンス*は 1 つのみ追加できます。このため、これらのソリューションの両方をアクティベートする必要がある場合は、MDR と EDR Optimum のライセンスを個別に追加するのではなく、[EDR Optimum+MDR] Add-onのライセンスを 1 つ追加する必要があります。また、*予備のライセンス*を 1 つ追加することができます。

MDR の導入時に BLOB ファイルを使用した場合は、MDR をアクティベートするために別のライセンスを追加する必要はありません。BLOB ファイルにはライセンス情報が含まれています。

ソリューションの初期ライセンス方式

MDR と EDR Optimum の初回導入時には、ソリューションは Kaspersky Endpoint Security アプリケーションと同様の方法でアクティベートされます。［*ライセンスの追加*］タスクを使用するか、自動ライセンス配布機能を使用することができます。ライセンスは、お客様の選択したチェックボックスの内容に合わせて、2 つ目の現在のライセンスか、予備のライセンスとして追加されます。

別のライセンスへの切り替え

お客様の組織がすでにこれらのソリューションを導入済みの場合で、対応するライセンスがアプリケーションに追加されていた場合は、新しい構成のライセンス管理に関して特別な考慮事項があります。別のライセンスに切り替える際、アプリケーションは新しいライセンスを追加せず、現在のライセンスを新しいライセンスで置き換えます。これは MDR と EDR Optimum をアクティベートするために追加できるライセンスは 1 つのみという制限があるためです。

例えば、組織で既に [EDR Optimum+MDR] ソリューションが導入されており、MDR アドオン構成に切り替えようとした場合を想定します。新しい構成に切り替えるには、[EDR Optimum+MDR] Add-on アドオンのライセンスを MDR アドオンのライセンスで置き換える必要があります。

EDR Optimum と MDR （[EDR Optimum+MDR] アドオン）の個別のライセンスは使用できなくなります。これらのソリューションの両方を使用したい場合は、BLOB ファイルを使用して MDR をアクティベートして、EDR Optimum をライセンスでアクティベートしてください。

ライセンスの自動配布機能を使用すると、アプリケーションは同じ数のソリューションを対象とするライセンスを拒否します。つまり、EDR Optimum アドオンのライセンスを追加した場合は、このライセンスを MDR アドオンのライセンスで置き換えることはできません。ですが、EDR Optimum アドオンのライセンスを [EDR Optimum+MDR] アドオンのライセンスで置き換えることは可能です。MDR アドオンのライセンスを EDR アドオンのライセンスで置き換えようとすると拒否されます。［*ライセンスの追加*］タスクを実行してライセンスを置き換えることができます。［*ライセンスの追加*］タスクは、ソリューションの数に関係なくライセンスを置き換えることができます。

[EDR Optimum+MDR] Add-onの予備のライセンスが追加されている場合、EDR Optimum アドオンまたは MDR アドオンの現在のライセンスを正しく追加するため、最初に予備のライセンスを EDR Optimum アドオンまたは MDR アドオンのライセンスで置き換えるか、予備のライセンスを削除してから現在のライセンスを置き換えてください。

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent は、本製品とその他のカスペルスキーのソリューション（Kaspersky Sandbox など）を連携して高度な脅威を検知します。カスペルスキーのソリューションは特定のバージョンの Kaspersky Endpoint Agent と互換性を持ちます。

Kaspersky Endpoint Agent をカスペルスキーソリューションの一部として使用する場合は、対応するライセンスでカスペルスキーソリューションをアクティベートしておく必要があります。

ご利用中のソフトウェアソリューションに含まれる Kaspersky Endpoint Agent およびスタンドアロンのソリューションに関する詳細な情報については、関連製品のヘルプを参照してください：

- Kaspersky Anti Targeted Attack Platform のヘルプ
- Kaspersky Sandbox のヘルプ
- Kaspersky Endpoint Detection and Response Optimum のヘルプ
- Kaspersky Managed Detection and Response のヘルプ

Kaspersky Endpoint Security のバージョン 11.2.0 ～ 11.8.0 の配信キットには Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Agent は Kaspersky Endpoint Security for Windows のインストール時に選択することができます。結果、KEA と KES の 2 つのアプリケーションがお客様のコンピューターにインストールされることになります。Kaspersky Endpoint Security 11.9.0 では、Kaspersky Endpoint Agent 配布パッケージは Kaspersky Endpoint Security 配信キットには含まれません。

KEA のバージョン（KES の一部）と KES のバージョンの対応

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

カスペルスキーは、すべての Detection and Response が Kaspersky Endpoint Agent ではなく、Kaspersky Endpoint Security の組み込みエージェントと連携するよう切り替えています。カスペルスキーは、これらのソリューション向けのサポートを順に追加していき、Kaspersky Endpoint Agent を段階的に廃止していく方針です（以下の表を参照）。バージョン 12.1 から、本製品はすべての Detection and Response ソリューションがサポートされるようになりました。さらに、バージョン 12.1 から、本製品と Kaspersky Endpoint Agent は互換性がなくなり、同じコンピューターに両方のアプリケーションを並行してインストールすることはできなくなります。

Detection and Response ソリューションを管理する組み込みエージェントの導入

Kaspersky Endpoint Security のバージョン	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform（Endpoint Detection and Response コンポーネント）	Kaspersky Anti Targeted Attack Platform（Network Detection and Response コンポーネント）
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	Kaspersky Endpoint Agent
12.6	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**	**組み込みエージェント**

［KES + KEA］構成からの［KES + 組み込みエージェント］構成への移行

Kaspersky Endpoint Security には、Managed Detection and Response ソリューションと動作する組み込みエージェントが含まれています。これらのソリューションと連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security を導入する場合は、Detection and Response ソリューションと Kaspersky Endpoint Security は継続して連携します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。

Kaspersky Endpoint Security のバージョン 11.2.0 ～ 11.8.0 の配信キットには Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Agent は Kaspersky Endpoint Security for Windows のインストール時に選択することができます。結果、KEA と KES の 2 つのアプリケーションがお客様のコンピューターにインストールされることになります。Kaspersky Endpoint Security 11.9.0 では、Kaspersky Endpoint Agent 配布パッケージは Kaspersky Endpoint Security 配信キットには含まれません。

[KES + KEA] 設定から [KES + 組み込みエージェント] への移行には次の手順が含まれます：

1. **Kaspersky Security Center のアップグレード**

   ユーザーのコンピューター上にあるネットワークエージェントと Web コンソールを含むすべての Kaspersky Security Center コンポーネントをバージョン 13.2 以降にアップグレードします。

2. **Kaspersky Endpoint Security Web プラグインのアップグレード**

   Kaspersky Security Center Web コンソールで、Kaspersky Endpoint Security Web プラグインをバージョン 11.7.0 以降にアップグレードします。EDR Optimum および Kaspersky Sandbox コンポーネントを管理するには、Web コンソールを使用する必要があります。

   Kaspersky Anti Targeted Attack Platform (EDR) を使用するには、Kaspersky Endpoint Security バージョン 12.1 以降向けの Web プラグインが必要になります。

   Kaspersky Anti Targeted Attack Platform (NDR) を使用するには、Kaspersky Endpoint Security バージョン 12.7 以降向けの Web プラグインが必要になります。

3. **ポリシーおよびタスクの移行**

   Kaspersky Endpoint Agent のポリシーおよびタスクの移行ウィザードを使用して Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。

   これにより、新規の Kaspersky Endpoint Security のポリシーが作成されます。新しいポリシーのステータスは*非アクティブ*になっています。ポリシーを適用するには、ポリシーのプロパティを開いて Kaspersky Security Network に関する声明に同意して状態を*アクティブ*にします。

4. **ライセンス機能**

   共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Security for Windows および Kaspersky Endpoint Agent をアクティベートした場合は、本製品をバージョン 11.7.0 にアップグレードした後に EDR Optimum 機能は自動的にアクティベートされます。追加で操作する必要はありません。

   スタンドアロンの Kaspersky Endpoint Detection and Response Optimum アドオンのライセンスを使用して EDR Optimum 機能をアクティベートした場合は、EDR Optimum アドオンのライセンスが Kaspersky Security Center リポジトリに追加されていて、ライセンスの自動配信機能が有効になっていることを確認してください。本製品をバージョン 11.7.0 にアップグレードした後に、EDR Optimum 機能が自動的にアクティベートされます。

   Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Agent をアクティベートしており、別のライセンスを使用して Kaspersky Endpoint Security for Windows をアクティベートしていた場合、Kaspersky Endpoint Security for Windows のライセンスを共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security のライセンスで置き換える必要があります。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。

   Kaspersky Sandbox 機能をアクティベートする必要はありません。Kaspersky Sandbox 機能は Kaspersky Endpoint Security for Windows をアップグレードおよびアクティベートした後すぐに利用可能になります。

   Kaspersky Anti Targeted Attack Platform のライセンスは、Kaspersky Anti Targeted Attack Platform ソリューションの一部として Kaspersky Endpoint Security のアクティベートに使用することができます。本製品をバージョン 12.1 にアップグレードした後に、EDR (KATA) 機能が自動的にアクティベートされます。追加で操作する必要はありません。

5. **Kaspersky Endpoint Security のアップグレード**

   本製品のアップグレードと、EDR Optimum および Kaspersky Sandbox 機能を移行するには、リモートインストールタスクの使用を推奨します。

本製品をリモートインストールタスクを使用してアップグレードするには、次の設定を変更する必要があります：

- インストールパッケージの設定で Detection and Response ソリューションを選択する。
- インストールパッケージの設定で Kaspersky Endpoint Agent コンポーネントを除外する（Kaspersky Endpoint Security for Windows バージョン 11.2.0～11.8.0）。
- Kaspersky Endpoint Agent へのアクセスを制限するために、パスワードによる保護が有効になっている場合、*アプリケーションのリモートインストール*タスクの設定にアプリケーションのアンインストール用パスワードを入力します。アンインストール用パスワードを入力できるのは、Kaspersky Security Center Linux 15.1 以降です。

次の方法で本製品をアップグレードすることもできます：

- カスペルスキーのアップデートサービスを使用する（シームレスアップデート – SMU）。
- クライアントデバイスのローカルで、インストールウィザードを使用する。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security をインストールする場合、コンポーネントの自動選択がサポートされます。自動選択されるコンポーネントは、本製品のアップグレードを実行するユーザーアカウントの権限により異なります。

Kaspersky Endpoint Security をシステムアカウント（SYSTEM）で EXE または MSI ファイルを使用してアップグレードする場合は、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されます。そのため、たとえばコンピューターに Kaspersky Endpoint Agent がインストールされており、EDR Optimum ソリューションがアクティベートされていた場合、Kaspersky Endpoint Security のインストーラーは自動的にコンポーネントのセットを構成して EDR Optimum コンポーネントを選択します。これにより、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。通常、システムアカウント（SYSTEM）を使用した MSI インストーラーの実行は、カスペルスキーのアップデートサービス（SMU）経由または Kaspersky Security Center 経由でのインストールパッケージの配信時などに行われます。

権限のないユーザーアカウントで MSI ファイルを使用して Kaspersky Endpoint Security をアップグレードすると、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されません。この場合、Kaspersky Endpoint Security は Kaspersky Endpoint Agent 構成に基づいて、コンポーネントを選択します。それから、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

6. **コンピューターの再起動**

   組み込みエージェントを含む製品へのアップグレードを完了するためにコンピューターを再起動します。本製品のアップグレード中、インストーラーはコンピューターの再起動前に Kaspersky Endpoint Agent を削除します。コンピューターの再起動後、組み込みエージェントが追加されます。つまり、コンピューターが再起動されるまで、Kaspersky Endpoint Security は EDR および Kaspersky Sandbox の機能を実行しません。

7. **Kaspersky Endpoint Detection and Response Optimum および Kaspersky Sandbox の状態を確認する。**

アップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

- *製品コンポーネントのステータスレポート*を使用して EDR Optimum 機能がアクティベートされているかどうかを確認してください。コンポーネントの状態が「*ライセンスに含まれていません*」と表示されている場合は、EDR Optimum の自動ライセンス配信機能がオンになっていることを確認してください。

Kaspersky Endpoint Agent のポリシーとタスクの移行

Kaspersky Endpoint Security for Windows に Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザードが含まれるようになりました。次のソリューション用のポリシーおよびタスクの設定を移行することができます：

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザードは、Web コンソールと Cloud コンソールでのみ動作します。管理コンソール（MMC）では、標準の Kaspersky Security Center のポリシーとタスクの一括変換ウィザードを使用して Kaspersky Anti Targeted Attack Platform (EDR) ソリューションの設定を移行することのみ可能です。

最初に単一のコンピューターで Kaspersky Endpoint Agent から Kaspersky Endpoint Security に移行し、次にコンピューターのグループで移行してから組織のすべてのコンピューターへの移行を完了させてください。

Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行するには、

Web コンソールのメインウィンドウで、［**操作**］→［**Kaspersky Endpoint Agent からの移行**］をクリックします。

ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

ステップ1：ポリシーの移行

移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Agent のポリシーをクリックして、設定を統合する Kaspersky Endpoint Security のポリシーを選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

ステップ 2：タスクの移行

移行ウィザードが Kaspersky Endpoint Security 向けの新しいタスクを作成します。タスクのリストで、Kaspersky Endpoint Security のポリシー向けに作成する Kaspersky Endpoint Agent のタスクを選択します。このウィザードでは Kaspersky Endpoint Detection and Response および Kaspersky Sandbox 向けのタスクがサポートされます。次の手順に進みます。

ステップ 3：ウィザードの完了

ウィザードを終了します。ウィザードは以下の処理を実行します：

- 新規の Kaspersky Endpoint Security のポリシーを作成する

  ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには *<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>* という名前が付けられます。新しいポリシーのステータスは*非アクティブ*になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ*非アクティブ*にして、新しく統合されたポリシーを有効にします。

  > Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行後、新しいポリシーに管理サーバーへのデータ転送機能（隔離されたファイルのデータと脅威の活動連鎖のデータ）が設定されていることを確認してください。データ転送のパラメータ値は Kaspersky Endpoint Agent ポリシーからは移行されません。

  Kaspersky Endpoint Agent から Kaspersky Anti Targeted Attack Platform (EDR) ソリューションの Kaspersky Endpoint Security に移行する際、Central Node サーバーにコンピューターを接続するときにエラーが発生することがあります。これは、Web コンソールの移行ウィザードが次のポリシー設定をスキップして移行しないために発生します。

  - 設定の変更の禁止（[**KATA サーバーへの接続**] が鍵のかかったアイコンの状態）。

    既定では、設定は編集可能です（鍵が開いたアイコン）。このため、コンピューターに設定が適用されません。設定の変更を禁止して、アイコンは鍵がかかった状態にする必要があります。

  - 暗号化コンテナー。

    Central Node サーバーとの接続に相互認証を使用している場合は、暗号化コンテナーを再度追加する必要があります。移行ウィザードはサーバーの TLS 証明書を正常に移行します。

  管理コンソール（MMC）のポリシーとタスクの移行ウィザードは Kaspersky Anti Targeted Attack Platform (EDR) ソリューションのすべての設定を移行します。

- 新規の Kaspersky Endpoint Security のタスクを作成する

  新規タスクは Kaspersky Endpoint Detection and Response および Kaspersky Sandbox 向けの Kaspersky Endpoint Agent タスクのコピーです。同時に、ウィザードは Kaspersky Endpoint Agent タスクには変更を加えません。

管理コンソール（MMC）で Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行する方法（KATA (EDR) のみ）

1. 管理コンソールで、管理サーバーを選択して右クリックしてコンテキストメニューを開きます。
2. ［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

ポリシーとタスクの一括変換ウィザードが開始されます。ウィザードの指示に従います。

ステップ 1：ポリシーとタスクを変換するアプリケーションの選択

ここでは、Kaspersky Endpoint Security for Windows を選択します。次の手順に進みます。

ステップ 2：ポリシーの変換

移行ウィザードでは、最初に Kaspersky Endpoint Agent の設定を移行するための新規の Kaspersky Endpoint Security ポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーに移動する Kaspersky Endpoint Agent のポリシーを選択します。次の手順に進みます。

移行ウィザードはポリシーの返還を開始します。ポリシーの変換中、移行ウィザードで Kaspersky Security Network に関する声明への同意が求められます。新しいポリシーは「*<ポリシー名>（変換済み）*」という名前になります。

ステップ 3：タスクの変換

この手順をスキップします。このウィザードでは Kaspersky Endpoint Detection and Response Optimum および Kaspersky Sandbox 向けのタスクのみがサポートされます。これらのコンポーネントは、Web コンソールでのみ管理できます。次の手順に進みます。

ステップ 4：ウィザードの完了

ウィザードを終了します。ウィザードを実行した結果、新規の Kaspersky Endpoint Security ポリシーが作成されます。

Endpoint Detection and Response Agent (EDR Agent)

Kaspersky Endpoint Security 12.3 for Windows から、EDR Agent (Endpoint Detection and Response Agent) の設定が追加されました。*Endpoint Detection and Response Agent* は、カスペルスキーの次の Detection and Response ソリューションをサポートするために、組織の IT インフラストラクチャ内の個々のワークステーションやサーバーにインストールされるアプリケーションです：

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA)（バージョン 12.6 以降）
- Kaspersky Anti Targeted Attack Platform (NDR)（バージョン 12.7 以降）
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）（バージョン 12.11 以降）

EDR Agent は、これらのコンピューターで実行されているプロセス、オープンネットワーク接続、および変更されたファイルを継続的に監視します。EDR Agent では本製品の保護および管理コンポーネントは使用できません。

EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。これにより、カスペルスキーの Detection and Response と同時にサードパーティのインフラストラクチャセキュリティツールを使用できるようになります。

EDR Agent を導入するには、コンピューターにネットワークエージェントがインストールされており、Kaspersky Security Center のコンソールにコンピューターが追加されている必要があります。EDR Agent と Kaspersky Security Center との連携を有効にするには、Kaspersky Endpoint Security for Windows 管理プラグインをインストールする必要があります。グループポリシーを使用して EDR Agent の設定を指定できます。EDR Agent を統合するには、適切なポリシーセクションで統合を設定する必要があります。

Kaspersky Detection and Response ソリューションをサポートするために、以下のカスペルスキー製品をインフラストラクチャにインストールする必要があります：

	• ネットワークエージェント • EDR Agent
Endpoint	
	Kaspersky Endpoint Security for Windows 管理プラグイン
Kaspersky Security Center	
	
Detection and Response ソリューション：MDR、KATA (EDR)、KATA (NDR)、KUMA、EDR Expert（オンプレミス）	

EDR Agent のインストール

Kaspersky Detection and Response ソリューション用の Endpoint Detection and Response Agent (EDR Agent) 設定の Kaspersky Endpoint Security も、同様にインストールします。

EDR Agent は、以下のいずれかの方法でコンピューターにインストールできます：

- Kaspersky Security Center を使用してリモートで実行。
- インストールウィザードを使用してローカルで実行。
- コマンドラインを使用してローカルで実行（KATA (EDR) と EDR Expert（オンプレミス）のみ）。

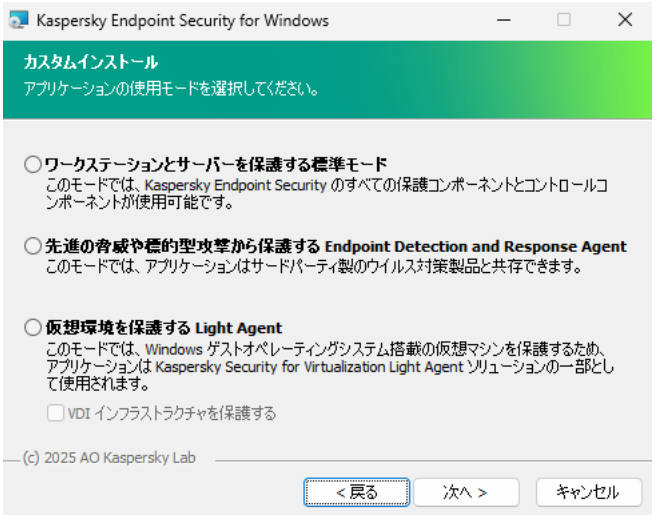
EDR Agent をインストールするには、インストールパッケージの設定またはインストールウィザードで適切な設定を選択する必要があります。

インストールウィザードを使用して EDR Agent をインストールする方法

1. ユーザーのコンピューターに配信キットフォルダーをコピーします。
2. Setup_kes.exe を実行します。

   インストールウィザードが起動します。

Kaspersky Endpoint Security の設定



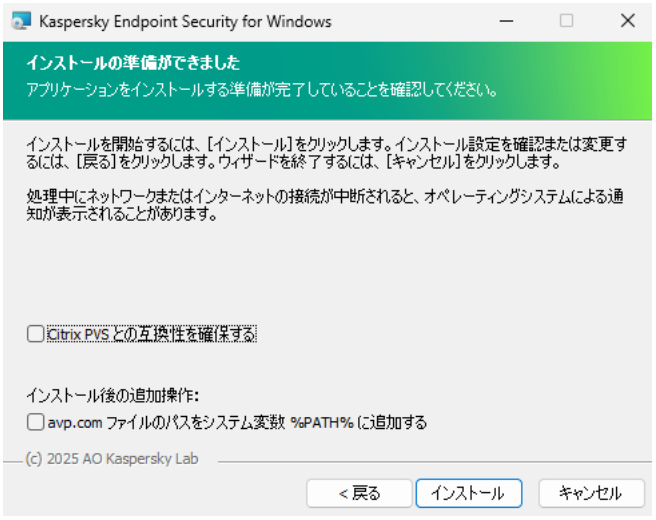
アプリケーションの設定の選択

Endpoint Detection and Response Agent 設定を選択します。この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。

Kaspersky Endpoint Security の各コンポーネント

インストールするコンポーネントを選択します。アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。これを行うには、インストールウィザードを再度実行し、使用可能なコンポーネントの変更を選択する必要があります。

詳細設定



詳細な製品のインストール設定

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

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

avp.com ファイルのパスをシステム変数 %PATH% に追加するコマンドラインインターフェイスの使用で便利なように、%PATH% 変数にインストール先のパスを追加できます。

コマンドラインで EDR Agent をインストールする方法（KATA (EDR) と EDR Expert（オンプレミス）のみ）

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
   ```

   または

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   その結果、Kaspersky Anti Targeted Attack Platform (EDR) または Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携用に EDR Agent がコンピューターにインストールされます。本製品がインストールされたこと、また本製品の設定は `status` コマンドを実行することで確認できます。

管理コンソール（MMC）を使用して EDR Agent をインストールする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

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

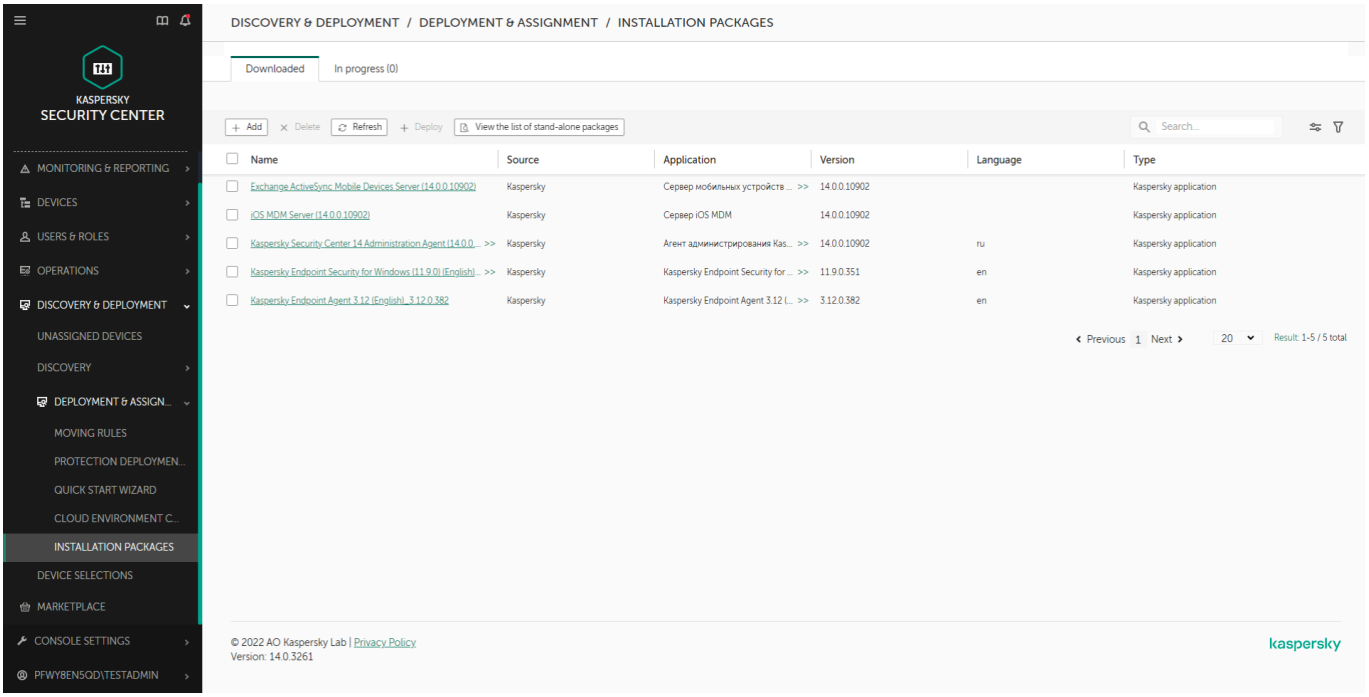
   必要に応じて、新しいインストールパッケージを作成します。
4. ［**保護コンポーネント**］に移動します。
5. **先進の脅威や標的型攻撃から保護する Endpoint Detection and Response Agent** 設定を選択します。この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。
6. インストールするコンポーネントを選択します。

   アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。
7. 変更内容を保存します。
8. リモートインストールタスクを作成します。タスクのプロパティで、作成したインストールパッケージを選択します。

Web コンソールを使用して EDR Agent をインストールする方法

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

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

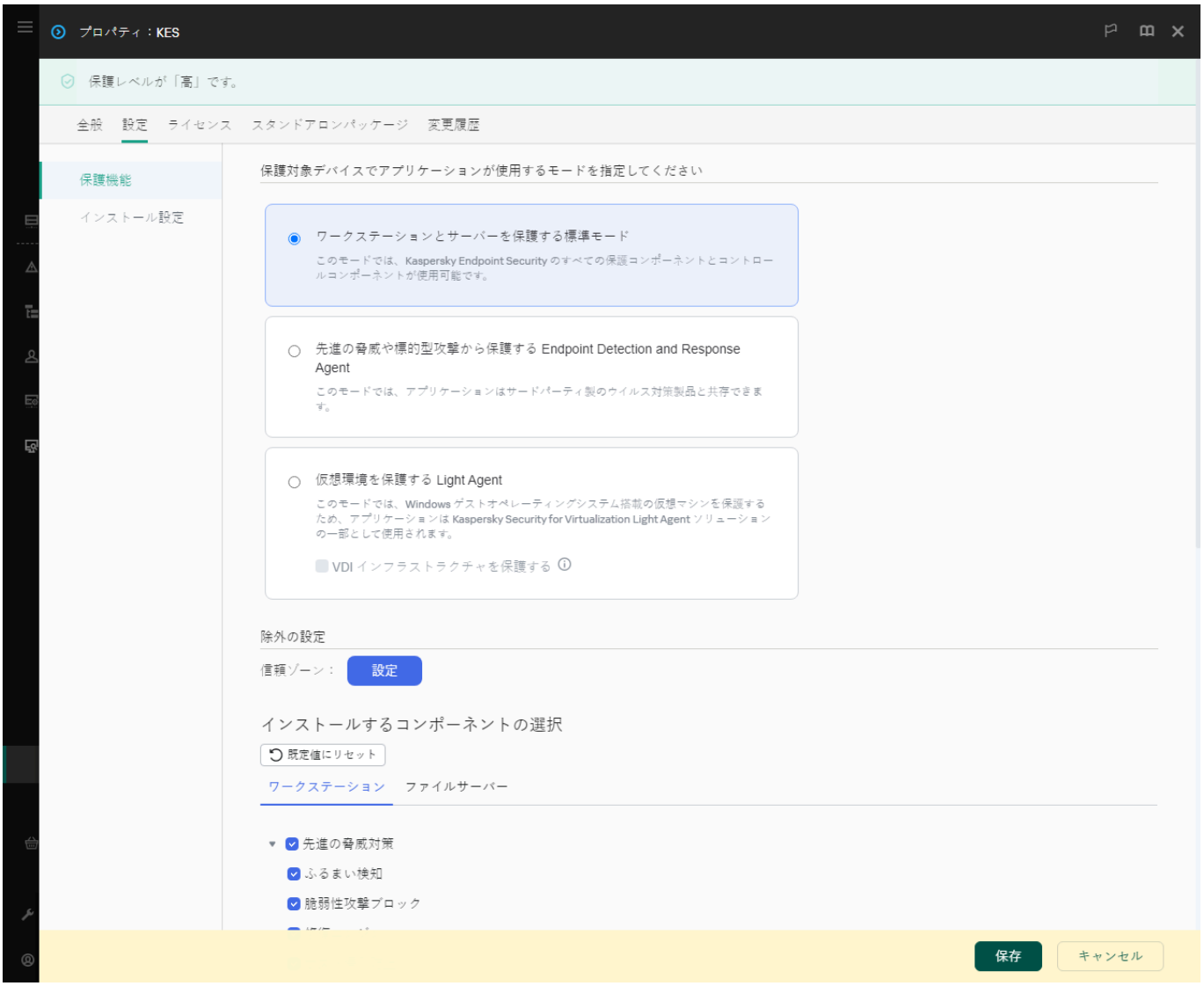


インストールパッケージのリスト

2. インストールパッケージのプロパティを開きます。
   必要に応じて、新しいインストールパッケージを作成します。

3. ［**設定**］タブを選択します。

4. ［**保護コンポーネント**］に移動します。



インストールパッケージに含まれるコンポーネント

5. **先進の脅威や標的型攻撃から保護する Endpoint Detection and Response Agent** 設定を選択します。この設定では、Detection and Response ソリューションのサポートを提供する次のコンポーネントのみをインストールできます：MDR、EDR (KATA)、NDR (KATA)、EDR Expert（オンプレミス）、および KUMA。この設定は、組織の環境に Kaspersky Detection and Response ソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。

6. インストールするコンポーネントを選択します。

   アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。

7. 変更内容を保存します。

8. リモートインストールタスクを作成します。タスクのプロパティで、作成したインストールパッケージを選択します。

この結果、EDR Agent がユーザーのコンピューターにインストールされます。アプリケーションのインターフェイスを使用することができます。また、アプリケーションのアイコンが通知領域に表示されます。

Kaspersky Security Center では、EDR Agent の設定にあるアプリケーションがインストールされたコンピューターのステータスが緊急になります。ファイル脅威対策機能がないため、このコンピューターはこのステータスになっています。追加の対応は必要ありません。

インストーラーがコンピューターで共存できないソフトウェアを検出したことにより、サードパーティ製の EPP 製品を使用しているコンピューターに EDR Agent をインストールできなかった場合は、共存できないソフトウェアのチェックをスキップできます。



EDR Agent のメインウィンドウ

次に、Kaspersky Managed Detection and Response、Kaspersky Anti Targeted Attack (EDR) または Kaspersky Anti Targeted Attack (NDR) ソリューションとの連携を設定する必要があります。また、信頼ゾーンを作成したり、アプリケーションのインターフェイスを非表示にしたり、アプリケーションの高度な設定を指定することもできます。以下のセクションの設定が可能です：

- Kaspersky Security Network
- 製品設定
- ネットワークの設定
- 除外リスト
- レポート

- インターフェイス
- 設定の管理

EDR Agent と MDR の統合

組織の IT インフラストラクチャ内のワークステーションとサーバーに EDR Agent がインストールされます。EDR Agent はデータを処理し、Kaspersky Security Network のストリームを通じてそのデータを Kaspersky Managed Detection and Response に送信します。

Kaspersky Security Center 13 Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド接続を確立する必要があります。Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド接続を確立する必要があります。ソリューションを配備する際に Kaspersky Managed Detection and Response はバックグラウンド接続を確立するよう求めます。バックグラウンド接続が確立されていることを確認してください。

Web コンソールとのバックグラウンド接続を確立する

1. Web コンソールのメインウィンドウで、［**設定**］→［**連携**］の順に選択します。
2. ［**連携**］に移動します。
3. ［**連携用のバックグラウンド接続が［有効］です**］をオンにします。
4. 変更内容を保存します。

Kaspersky Managed Detection and Response とは次の手順で連携されます：

1. **Managed Detection and Response コンポーネントのインストール**

   MDR コンポーネントは、インストール中またはアップグレード中、またはコンポーネントの変更タスクを使用して選択できます。

   > 新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2. **Kaspersky Private Security Network の設定**

   > Kaspersky Security Center Cloud コンソールを使用している場合、この手順は省略してください。Kaspersky Security Center Cloud コンソールは、MDR プラグインのインストール中に自動的に Kaspersky Private Security Network を設定します。

   Kaspersky Private Security Network (KPSN) は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。

   Kaspersky Security Network 設定ファイルを管理サーバーのプロパティ内でアップロードします。Kaspersky Security Network 設定ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。Kaspersky Private Security Network の設定の詳細に関しては、Kaspersky Security Center ヘルプ を参照してください。コマンドラインから Kaspersky Security Network 設定ファイルをコンピューターにアップロードすることも可能です（下記の説明を参照してください）。

コマンドラインから Kaspersky Private Security Network を設定する方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com KSN /private <file name>
   ```

   `<file name>` には Kaspersky Private Security Network の設定を含む設定ファイルの名前を入力します（PKCS7 または PEM ファイル形式）。

   例：
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Kaspersky Endpoint Security は Kaspersky Private Security Network を使用してファイル、アプリケーション、Web サイトの評価を決定します。ポリシー設定の［**Kaspersky Security Network**］セクションに、次の動作ステータスが表示されます：［インフラストラクチャ：*Kaspersky Private Security Network*］。

Managed Detection and Response が動作するためには、拡張 KSN モードを有効にする必要があります。

3 Kaspersky Managed Detection and Response をアクティベートする

Kaspersky Endpoint Security for Windows 12.10 以降では、Managed Detection and Response 機能をアクティベートするために、アクティベーションコードの代わりに、ライセンス情報ファイルを使用することもできます。

MDR（Kaspersky Managed Detection and Response アドオン）の個別ライセンスを購入する必要があります。

この機能は、Kaspersky Managed Detection and Response のアドオン向けの別のライセンスを追加すると使用できるようになります。スタンドアロンの Managed Detection and Response のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

MDR がライセンスでサポートされており、本製品のローカルインターフェイスで稼働していることを確認してください。

4 Managed Detection and Response コンポーネントの有効化

Kaspersky Endpoint Security のポリシーで BLOB 設定ファイルを読み込みます（下の手順を参照してください）。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

Kaspersky Endpoint Security 12.6 for Windows から、現在のライセンスがある場合、テナントのない Kaspersky Managed Detection and Response では BLOB ファイルの追加はオプションになりました。

管理コンソール（MMC）で Managed Detection and Response を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Detection and Response**］→［**Managed Detection and Response (Industrial CyberSecurity)**］の順に選択します。
4. ［**Managed Detection and Response (Industrial CyberSecurity)**］チェックボックスをオンにします。

5. ［**設定**］ブロックで、［**アップロード**］をクリックし、Kaspersky Managed Detection and Response コンソールで受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。

   既定では、ユーザーはアプリケーション設定を管理することができます（「南京錠」が開いています）。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで Managed Detection and Response を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Managed Detection and Response**］に移動します。
5. ［**Managed Detection and Response は有効です**］をオンにします。
6. ［**アップロード**］をクリックし、Kaspersky Managed Detection and Response Console で受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。

   既定では、ユーザーはポリシーの設定を管理することができます（「南京錠」が開いています）。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

7. 変更内容を保存します。

コマンドラインから Managed Detection and Response コンポーネントを有効にする方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**本製品の設定**」操作を実行する権限が付与されている必要があります。

BLOB ファイルが検証されます。BLOB の検証には、デジタル署名およびライセンス期間の確認も含まれます。BLOB ファイルの検証が正常に完了すると、Kaspersky Endpoint Security はファイルをダウンロードして、次回の Kaspersky Security Center との同期の際にファイルをコンピューターに送信します。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Managed Detection and Response**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

5 テレメトリを受信するためのアプリケーションの他のコンポーネントの構成

Managed Detection and Response が動作するためには、次の機能を有効にする必要があります：

- Kaspersky Security Network（拡張モード）

  > Kerberos 認証を使用するプロキシサーバーを利用する場合、HTTPS 伝送プロトコルを備えた KSN プロキシを使用することを推奨します。詳細については、Kaspersky Security Center のヘルプを参照してください。

- ふるまい検知

これらの機能は必ず有効にしてください。有効になっていないと、遠隔測定したデータを受け取ることができないため、Kaspersky Managed Detection and Response は機能できません。

また、Kaspersky Managed Detection and Response は別の製品機能から受け取ったデータを使用します。これらの機能は有効にしなくても Kaspersky Managed Detection and Response を使用できます。追加のデータを提供する機能は次の通りです：

- ウェブ脅威対策
- メール脅威対策
- ファイアウォール

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Managed Detection and Response**］に移動します。
5. ［**Managed Detection and Response は有効です**］をオンにします。
6. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Detection and Response**］→［**Managed Detection and Response (Industrial CyberSecurity)**］の順に選択します。
4. ［**Managed Detection and Response (Industrial CyberSecurity)**］チェックボックスをオンにします。
5. 変更内容を保存します。

EDR Agent と EDR (KATA) の統合

組織の IT インフラストラクチャ内のワークステーションとサーバーに EDR Agent がインストールされます。これらのコンピューター上で、EDR Agent はプロセス、開かれているネットワーク接続、および変更されたファイルを継続的に監視し、Central Node コンポーネントがインストールされたサーバーに監視データを送信します。

EDR (KATA) と連携するには、Endpoint Detection and Response (KATA) コンポーネントを有効にして、EDR Agent を設定する必要があります。

Endpoint Detection and Response (KATA) が動作するには次の条件を満たしている必要があります。

- Kaspersky Anti Targeted Attack Platform のバージョンが 5.0 ～ 7.1 である。
- Kaspersky Security Center のバージョンが 14.2 以降である。以前のバージョンの Kaspersky Security Center では、Endpoint Detection and Response (KATA) をアクティベートすることはできません。

Endpoint Detection and Response (KATA) とは次の手順で連携されます：

1. **Endpoint Detection and Response (KATA) のアクティベート**

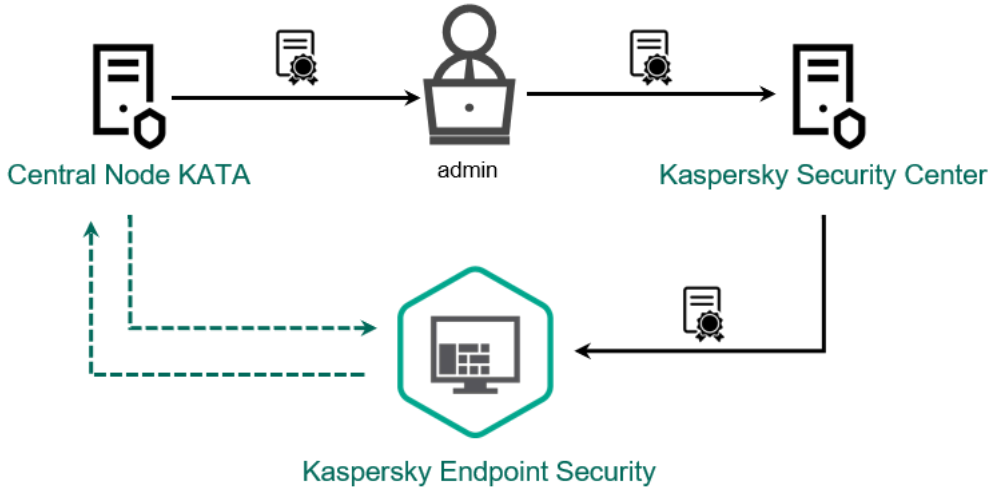
   EDR（KATA）（Kaspersky Endpoint Detection and Response（KATA）アドオン）の個別ライセンスを購入する必要があります。

   この機能は、Kaspersky Endpoint Detection and Response (KATA) 向けの別のライセンスを追加すると使用できるようになります。スタンドアロンの Endpoint Detection and Response (KATA) 機能のライセンス認証は、Kaspersky Endpoint Security のライセンス認証と同じです。

   EDR (KATA) がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

2. **Central Node への接続**

   Kaspersky Anti Targeted Attack Platform では、Kaspersky Endpoint Security と Central Node コンポーネント間に信頼済みの接続を確立する必要があります。信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。



TLS 証明書の Kaspersky Endpoint Security への追加

既定では、Kaspersky Endpoint Security は Central Node の TLS 証明書のみを確認します。接続の安全性をより高めるには、追加で Central Node のコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、Central Node および Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

管理コンソール（MMC）を使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**Detection and Response**］→［**Endpoint Detection and Response Expert（オンプレミス）**］の順に選択します。
5. ［**Endpoint Detection and Response Expert（オンプレミス）**］チェックボックスをオンにします。
6. ［**サーバーの接続設定**］をクリックします。
7. サーバー接続を設定します：
   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。
   - **サーバー TLS 証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。
   - **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

     暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。
8. ［**OK**］をクリックします。
9. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

   複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

10. 必要に応じて、テレメトリを設定してください。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールを使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（オンプレミス）**］に移動します。

5. ［**Endpoint Detection and Response Expert（オンプレミス）が有効です**］をオンにします。

6. EDR (KATA) を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 7.1 以前）**］を選択します。

7. ［**接続設定**］をクリックします。

8. サーバー接続を設定します：

   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。

   - **サーバー証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

   - **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

     暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

9. ［**OK**］をクリックします。

10. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

    複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

11. 必要に応じて、テレメトリを設定してください。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

コンピューターが Kaspersky Anti Targeted Attack Platform コンソールに追加されます。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Endpoint Detection and Response Expert（オンプレミス）**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

EDR Agent と NDR (KATA) の統合

組織の IT インフラストラクチャ内のワークステーションとサーバーに EDR Agent がインストールされます。これらのコンピューター上で、EDR Agent はプロセス、開かれているネットワーク接続、および変更されたファイルを継続的に監視し、Central Node コンポーネントがインストールされたサーバーに監視データを送信します。

NDR (KATA) と連携するには、Network Detection and Response (KATA) コンポーネントを有効にして、EDR Agent を設定する必要があります。

Network Detection and Response (KATA) が動作するには次の条件を満たしている必要があります。

- Kaspersky Anti Targeted Attack Platform のバージョンが 7.0 以降である。
- Kaspersky Security Center のバージョンが 14.2 以降である。以前のバージョンの Kaspersky Security Center では、Network Detection and Response (KATA) をアクティベートすることはできません。



https://www.youtube.com/watch?v=gd-rySv0ThQ

Network Detection and Response (KATA) とは次の手順で連携されます：

1. **Network Detection and Response (KATA) のアクティベート**

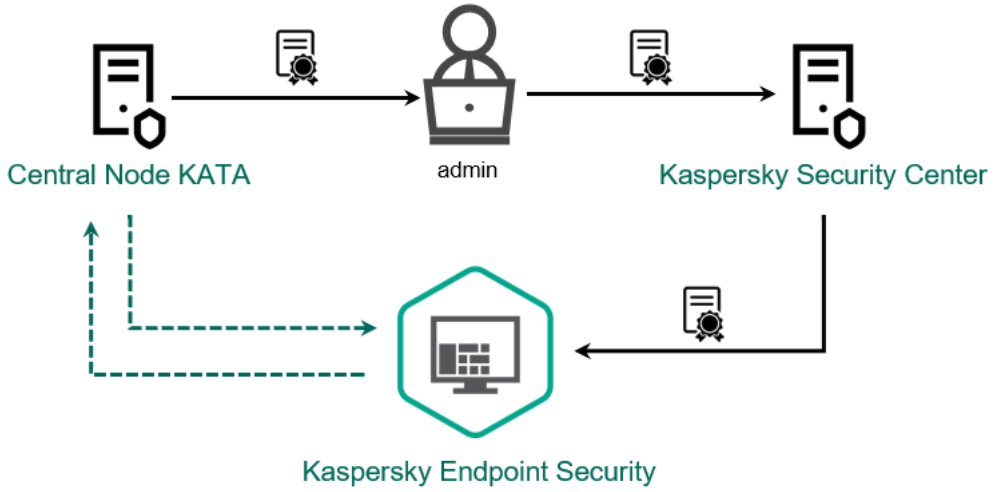
   NDR（KATA）（Kaspersky Network Detection and Response（KATA）アドオン）の個別ライセンスを購入する必要があります。

   この機能は、Kaspersky Network Detection and Response (KATA) 向けの別のライセンスを追加すると使用できるようになります。スタンドアロンの Network Detection and Response (KATA) 機能のライセンス認証は、Kaspersky Endpoint Security のライセンス認証と同じです。

   NDR (KATA) がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

2. **Central Node への接続**

Kaspersky Anti Targeted Attack Platform では、Kaspersky Endpoint Security と Central Node コンポーネント間に信頼済みの接続を確立する必要があります。信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。



TLS 証明書の Kaspersky Endpoint Security への追加

既定では、Kaspersky Endpoint Security は Central Node の TLS 証明書のみを確認します。接続の安全性をより高めるには、追加で Central Node のコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、Central Node および Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

管理コンソール（MMC）を使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Detection and Response**］→［**Network Detection and Response (KATA)**］の順に選択します。
4. ［**Network Detection and Response (KATA)**］チェックボックスをオンにします。
5. ［**接続設定**］をクリックします。
6. サーバー接続を設定します：

   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。
   - **サーバー証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

- **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

7. ［**OK**］をクリックします。
8. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。
9. 複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
10. 必要に応じて、テレメトリを設定してください。
11. 変更内容を保存します。

Web コンソールを使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Network Detection and Response (KATA)**］に移動します。
5. ［**Network Detection and Response (KATA) は有効です**］をオンにします。
6. ［**接続設定**］をクリックします。
7. サーバー接続を設定します：

   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。
   - **サーバー証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

- **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

8. ［**OK**］をクリックします。
9. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。
10. 複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
11. 必要に応じて、テレメトリを設定してください。
12. 変更内容を保存します。

コンピューターが Kaspersky Anti Targeted Attack Platform コンソールに追加されます。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Network Detection and Response (KATA)**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

EDR Agent と EDR Expert（オンプレミス）の連携

組織の IT インフラストラクチャ内のワークステーションとサーバーに EDR Agent がインストールされます。これらのコンピューター上で、EDR Agent はプロセス、開かれているネットワーク接続、および変更されたファイルを継続的に監視し、EDR Expert（オンプレミス）のサーバーに監視データを送信します。

EDR Expert（オンプレミス）と連携するには、Endpoint Detection and Response Expert（オンプレミス）コンポーネントを有効にして、EDR Agent を設定する必要があります。

Endpoint Detection and Response Expert（オンプレミス）とは次の手順で連携されます：

1. **Kaspersky Endpoint Detection and Response Expert（オンプレミス）のアクティベーション**

   EDR Expert（オンプレミス）（Kaspersky Endpoint Detection and Response Expert（オンプレミス）アドオン）の個別ライセンスを購入する必要があります。

   この機能は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）向けの別のライセンスを追加すると使用できるようになります。スタンドアロンの Endpoint Detection and Response (KATA) のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

   EDR Expert（オンプレミス）がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

2 テレメトリ収集サーバーと応答サーバーへの接続

Kaspersky Endpoint Detection and Response Expert（オンプレミス）では、Kaspersky Endpoint Security と次の 2 つのサーバーとの信頼済みの接続が必要です：

- *テレメトリの収集サーバー*は、コンピューター上で発生するイベントに関する情報を収集、正規化、関連付け、分析、保存する SIEM ソリューションの一部であるサーバーです。
- *応答サーバー*は、データを受信してスキャンし、オブジェクトのふるまいを調査し、そのような調査結果を公開するためのサーバーです。

信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。

既定では、Kaspersky Endpoint Security はサーバーの TLS 証明書のみを確認します。接続の安全性をより高めるには、追加でサーバーのコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、サーバーおよび Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。

Web コンソールを使用して Kaspersky Endpoint Security 端末を EDR Expert（オンプレミス）に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（オンプレミス）**］に移動します。
5. ［**Endpoint Detection and Response Expert（オンプレミス）が有効です**］をオンにします。
6. EDR Expert（オンプレミス）を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 8.0 以降）**］を選択します。
7. *テレメトリ収集サーバー*の接続を設定します：
   a. ［**テレメトリ収集サーバーへの接続**］セクションで、［**接続設定**］をクリックします。
   b. テレメトリ収集サーバーの接続を設定します：
      - **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。
      - **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。

- **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

c. ［**OK**］をクリックします。

d. テレメトリ収集サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

   複数のテレメトリ収集サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

e. 必要に応じて、テレメトリを設定してください。

8. *応答サーバー*の接続を設定します：

a. ［**応答サーバーへの接続**］ブロックで、［**サーバーに同期リクエストを送信する間隔（分）**］を設定します：サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は脅威対応タスクを受信し、タスクの結果を送信します。

b. ［**接続設定**］リンクをクリックします。

c. 応答サーバーの接続を設定します：

- **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。
- **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。
- **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

d. ［**OK**］をクリックします。

e. 応答サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

複数の応答サーバーアのドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

その結果、コンピューターが Open Single Management Platform (OSMP) に追加されます。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Endpoint Detection and Response Expert（オンプレミス）**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

サードパーティ製の EPP 製品との互換性

EDR Agent は、Kaspersky Detection and Response ソリューションの機能をサポートします。EDR Agent では保護および管理コンポーネントは使用できません。この設定では、サードパーティ製の EPP 製品をインストールし、組織のインフラストラクチャに Kaspersky Detection and Response ソリューションを導入することができます。EDR Agent は、Kaspersky Managed Detection and Response、Kaspersky Anti Targeted Attack Platform (EDR)、および Kaspersky Anti Targeted Attack Platform (NDR) との連携をサポートします。

EDR Agent は、以下の製造元の EPP 製品と互換性があります：

- **Dr.Web**

  EDR Agent は、Dr.Web Agent for Windows バージョン 13.0.1 以降および Dr.Web Server (x64) 13.0.0.10200 と互換性があります。

- **Dallas Lock**

  EDR Agent は、Dallas Lock 8.0-C バージョン 11.4.2.843 以降と互換性があります。

  > Dallas Lock ソフトウェアがインストールされているコンピューターで EDR エージェントを実行するには、ファイアウォールモジュールの設定でカスペルスキーの外部サービスへの接続を許可する必要があります。

- **Secret Net Studio**

  EDR Agent は、Secret Net Studio バージョン 8.11 以降と互換性があります。

  > ウイルス対策機能を備えた Secret Net Studio が導入されたコンピューターには本製品をインストールすることはできません。連携を可能にするには、Secret Net Studio からウイルス対策機能を削除する必要があります。

- **Trend Micro**

  EDR Agent は、Trend Micro Apex One バージョン 14.0.12994 以降（Security Agent を含む）と互換性があります。

  EDR Agent は、Trend Micro Deep Security バージョン 20.0.2-4960 以降（Security Agent を含む）と互換性があります。

- **Windows Defender**

- **Sophos**

  EDR Agent は、Sophos Intercept X バージョン 2024.1.2 以降（Endpoint Agent を含む）および Sophos Core Agent バージョン 2024.3.2.3 と互換性があります。

- **Bitdefender**

  EDR Agent は、Bitdefender Endpoint Security Tools バージョン 7.9.21.523 以降と互換性があります。

- **ESET**

  EDR Agent は、ESET Endpoint Security バージョン 12.0.2049.0 以降および ESET Management Agent バージョン 12.0 以降と互換性があります。

これらの製品は次の順でインストールする必要があります。まず、EPP 製品をインストールし、次に Kaspersky Security Center Network Agent、そして EDR Agent をインストールします。これは、EPP 製品のインストーラーによって EDR Agent とネットワークエージェントが共存できないソフトウェアとして検出され、削除される可能性があるためです。また、EDR Agent とネットワークエージェントの操作を、サードパーティ製 EPP 製品のアップデート後に確認する必要があります。これは、サードパーティ製 EPP 製品のインストーラーがコンピューターを再スキャンして共存できないソフトウェアを検出し、製品を削除する可能性があるためです。

インストーラーがコンピューターで共存できないソフトウェアを検出したことにより、サードパーティ製の EPP 製品を使用しているコンピューターに EDR Agent をインストールできなかった場合は、共存できないソフトウェアのチェックをスキップできます。

Managed Detection and Response

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

MDR との連携のための Kaspersky Endpoint Security の設定

MDR を使用するには、以下の設定を使用できます：

- **[KES + 組み込みエージェント]**：この設定において、Kaspersky Endpoint Security は、コンピューターのセキュリティを確保するアプリケーションと MDR を操作するアプリケーションの両方の役割を果たします。組み込みエージェントは、Kaspersky Endpoint Security 11.6.0 for Windows 以降で使用できます。

- **[サードパーティ製 EPP+EDR エージェント]**.この設定において、IT インフラストラクチャのセキュリティはサードパーティエンドポイント保護プラットフォーム（EPP）によって確保されます。MDR との連携は、Kaspersky Endpoint Security の Endpoint Detection and Response Agent (EDR Agent) の設定で提供されます。この設定において、EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。EDR Agent は、Kaspersky Endpoint Security 12.3 for Windows 以降で使用できます。

Kaspersky Endpoint Security の旧バージョン向けサポート

MDR ソリューションは Kaspersky Endpoint Security バージョン 11 以降でサポートされます。Kaspersky Endpoint Security のバージョン 11 ～ 11.5.0 は、脅威検知を有効にするために Kaspersky Managed Detection and Response に遠隔測定したデータを送信するだけです。Kaspersky Endpoint Security のバージョン 11.6.0 には、組み込みエージェント（Kaspersky Endpoint Agent）のすべての機能が含まれています。

お客様が Kaspersky Endpoint Security 11 ～ 11.5.0 を使用している場合、MDR ソリューションとの連携のためにデータベースを最新版にアップデートする必要があります。また、Kaspersky Endpoint Agent をインストールする必要があります。

Kaspersky Endpoint Security 11.6.0 以降のバージョンを使用している場合は、MDR ソリューションを使用するために Kaspersky Endpoint Agent をインストールする必要はありません。

Kaspersky Endpoint Security 11 ～ 11.5.0 をインストールしていないコンピューターに Kaspersky Endpoint Security のポリシーが適用されている場合、まずこれらのコンピューターに対して別の Kaspersky Endpoint Agent のポリシーを作成する必要があります。新しいポリシーで、Kaspersky Managed Detection and Response との連携を設定してください。

組み込みエージェントと MDR の連携

Kaspersky Managed Detection and Response との連携を設定するには、Managed Detection and Response コンポーネントを有効にして、Kaspersky Endpoint Security を設定する必要があります。

Kaspersky Security Center 13 Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド*接続*を確立する必要があります。Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド接続を確立する必要があります。ソリューションを配備する際に Kaspersky Managed Detection and Response はバックグラウンド接続を確立するよう求めます。バックグラウンド接続が確立されていることを確認してください。

Web コンソールとのバックグラウンド接続を確立する

1. Web コンソールのメインウィンドウで、［**設定**］→［**連携**］の順に選択します。
2. ［**連携**］に移動します。
3. ［**連携用のバックグラウンド接続が［有効］です**］をオンにします。
4. 変更内容を保存します。

Kaspersky Managed Detection and Response とは次の手順で連携されます：

1. **Managed Detection and Response コンポーネントのインストール**

   MDR コンポーネントは、インストール中またはアップグレード中、またはコンポーネントの変更タスクを使用して選択できます。

   新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2 Kaspersky Private Security Network の設定

Kaspersky Security Center Cloud コンソールを使用している場合、この手順は省略してください。Kaspersky Security Center Cloud コンソールは、MDR プラグインのインストール中に自動的に Kaspersky Private Security Network を設定します。

Kaspersky Private Security Network (KPSN) は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。

Kaspersky Security Network 設定ファイルを管理サーバーのプロパティ内でアップロードします。Kaspersky Security Network 設定ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。Kaspersky Private Security Network の設定の詳細に関しては、Kaspersky Security Center ヘルプを参照してください。コマンドラインから Kaspersky Security Network 設定ファイルをコンピューターにアップロードすることも可能です（下記の説明を参照してください）。

コマンドラインから Kaspersky Private Security Network を設定する方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com KSN /private <file name>
   ```

   `<file name>` には Kaspersky Private Security Network の設定を含む設定ファイルの名前を入力します（PKCS7 または PEM ファイル形式）。

   例：
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Kaspersky Endpoint Security は Kaspersky Private Security Network を使用してファイル、アプリケーション、Web サイトの評価を決定します。ポリシー設定の［**Kaspersky Security Network**］セクションに、次の動作ステータスが表示されます：［*インフラストラクチャ：Kaspersky Private Security Network*］。

Managed Detection and Response が動作するためには、拡張 KSN モードを有効にする必要があります。

3 Kaspersky Managed Detection and Response をアクティベートする

Kaspersky Endpoint Security for Windows 12.10 以降では、Managed Detection and Response 機能をアクティベートするために、アクティベーションコードの代わりに、ライセンス情報ファイルを使用することもできます。

Kaspersky Managed Detection and Response は次のライセンス方法をサポートしています：

- Managed Detection and Response が Kaspersky Endpoint Security for Windows のライセンスの適用対象となっている。

  機能は Kaspersky Endpoint Security for Windows のアクティベーション後すぐに使用できます。

- MDR（Kaspersky Managed Detection and Response のアドオン）用の個別のライセンスが使用されている。

  この機能は、Kaspersky Managed Detection and Response のアドオン向けの別のライセンスを追加すると使用できるようになります。結果として、Kaspersky Endpoint Security のライセンスおよび Kaspersky Managed Detection and Response のライセンスの 2 種類のライセンスがコンピューターに追加されることになります。

  スタンドアロンの Managed Detection and Response のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

MDR がライセンスでサポートされており、本製品のローカルインターフェイスで稼働していることを確認してください。

4. **Managed Detection and Response コンポーネントの有効化**

Kaspersky Endpoint Security のポリシーで BLOB 設定ファイルを読み込みます（下の手順を参照してください）。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

Kaspersky Endpoint Security 12.6 for Windows から、現在のライセンスがある場合、テナントのない Kaspersky Managed Detection and Response では BLOB ファイルの追加はオプションになりました。

管理コンソール（MMC）で Managed Detection and Response を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Detection and Response**］→［**Managed Detection and Response (Industrial CyberSecurity)**］の順に選択します。
4. ［**Managed Detection and Response (Industrial CyberSecurity)**］チェックボックスをオンにします。
5. ［**設定**］ブロックで、［**アップロード**］をクリックし、Kaspersky Managed Detection and Response コンソールで受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。

   既定では、ユーザーはアプリケーション設定を管理することができます（「南京錠」が開いています）。コンピューターにポリシーを適用するには、南京錠を閉じます（）。
6. 変更内容を保存します。

Web コンソールおよび Cloud コンソールで Managed Detection and Response を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Managed Detection and Response**］に移動します。
5. ［**Managed Detection and Response は有効です**］をオンにします。

6. ［**アップロード**］をクリックし、Kaspersky Managed Detection and Response Console で受け取った BLOB ファイルを選択します。ファイルの拡張子は P7 です。

   既定では、ユーザーはポリシーの設定を管理することができます（「南京錠」が開いています）。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

7. 変更内容を保存します。

コマンドラインから Managed Detection and Response コンポーネントを有効にする方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**本製品の設定**」操作を実行する権限が付与されている必要があります。

BLOB ファイルが検証されます。BLOB の検証には、デジタル署名およびライセンス期間の確認も含まれます。BLOB ファイルの検証が正常に完了すると、Kaspersky Endpoint Security はファイルをダウンロードして、次回の Kaspersky Security Center との同期の際にファイルをコンピューターに送信します。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Managed Detection and Response**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

5 テレメトリを受信するためのアプリケーションの他のコンポーネントの構成

Managed Detection and Response が動作するためには、次の機能を有効にする必要があります：

- Kaspersky Security Network（拡張モード）

  Kerberos 認証を使用するプロキシサーバーを利用する場合、HTTPS 伝送プロトコルを備えた KSN プロキシを使用することを推奨します。詳細については、Kaspersky Security Center のヘルプを参照してください。

- ふるまい検知

これらの機能は必ず有効にしてください。有効になっていないと、遠隔測定したデータを受け取ることができないため、Kaspersky Managed Detection and Response は機能できません。

また、Kaspersky Managed Detection and Response は別の製品機能から受け取ったデータを使用します。これらの機能は有効にしなくても Kaspersky Managed Detection and Response を使用できます。追加のデータを提供する機能は次の通りです：

- ウェブ脅威対策
- メール脅威対策

- ファイアウォール

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Managed Detection and Response**］に移動します。
5. ［**Managed Detection and Response は有効です**］をオンにします。
6. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Detection and Response**］→［**Managed Detection and Response (Industrial CyberSecurity)**］の順に選択します。
4. ［**Managed Detection and Response (Industrial CyberSecurity)**］チェックボックスをオンにします。
5. 変更内容を保存します。

MDR の KEA から KES への移行ガイド

Kaspersky Endpoint Security for Windows には Kaspersky Managed Detection and Response ソリューション向けの組み込みエージェントが含まれるようになりました。MDR と連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security を導入する場合は、Kaspersky Managed Detection and Response ソリューションと Kaspersky Endpoint Security は継続して連携します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Security をバージョン 11.6.0 以降にアップデートすると、システムで同じ動作が発生します。

Kaspersky Endpoint Security は Kaspersky Endpoint Agent と互換性はありません。同じコンピューターにこれらの製品の両方をインストールすることはできません。

Kaspersky Endpoint Security が Kaspersky Managed Detection and Response の一部として機能するには、次の条件を満たしている必要があります。

- Kaspersky Security Center のバージョンが 13.2 以降である (ネットワークエージェントを含む)。以前のバージョンの Kaspersky Security Center では、Managed Detection and Response をアクティベートすることはできません。
- Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されている。Kaspersky Security Center Web コンソールを経由した管理サーバーと MDR が連携するためには、新しい保護された接続であるバックグラウンド*接続*を確立する必要があります。

MDR で［KES + KEA］設定から［KES + 組み込みエージェント］に移行する手順

1. **Kaspersky Endpoint Security の管理プラグインのアップグレード**

   MDR コンポーネントは、Kaspersky Endpoint Security の管理プラグインのバージョン 11.6 以降を使用して管理できます。使用している Kaspersky Security Center コンソールの種類に応じて、管理コンソール (MMC) で管理プラグインをアップデートするか、Web コンソールで Web プラグインをアップデートします。

2. **ポリシーおよびタスクの移行**

   Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。次の設定方法があります：

   - Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザード。Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザードは、Web コンソールでのみ動作します。

     Web コンソールで Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行する方法

     Web コンソールのメインウィンドウで、［**操作**］→［**Kaspersky Endpoint Agent からの移行**］の順に選択します。

     ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

ステップ 1：ポリシーの移行

移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Agent のポリシーをクリックして、設定を統合する Kaspersky Endpoint Security のポリシーを選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

ステップ 2：タスクの移行

移行ウィザードは、MDR タスクをサポートしていません。この手順をスキップします。

ステップ 3：ウィザードの完了

ウィザードを終了します。ウィザードを実行した結果、新規の Kaspersky Endpoint Security ポリシーが作成されます。ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには *<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>* という名前が付けられます。新しいポリシーのステータスは*非アクティブ*になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ*非アクティブ*にして、新しく統合されたポリシーを有効にします。

- 標準ポリシーとタスクの一括置換ウィザード。ポリシーとタスクの一括変換ウィザードは、管理コンソール (MMC) でのみ使用可能です。ポリシーとタスクの一括変換ウィザードについて詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。

3 MDR 機能のライセンス

Kaspersky Managed Detection and Response ソリューションの一部として Kaspersky Endpoint Security をアクティベートするには、Kaspersky Managed Detection and Response のアドオンの個別のライセンスが必要です。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。結果として、*Kaspersky Endpoint Security* および *Kaspersky Managed Detection and Response* の 2 種類のライセンスが本製品に追加されることになります。

4 Kaspersky Endpoint Security のインストールまたはアップグレード

製品のインストールまたはアップグレード中に MDR 機能を移行するには、リモートインストールタスクの使用を推奨します。リモートインストールタスクを作成する場合、インストールパッケージの設定で MDR コンポーネントを選択する必要があります。

次の方法で本製品をアップグレードすることもできます：

- Kaspersky Update サービスを使用する。
- クライアントデバイスのローカルで、インストールウィザードを使用する。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security をインストールする場合、コンポーネントの自動選択がサポートされます。自動選択されるコンポーネントは、本製品のアップグレードを実行するユーザーアカウントの権限により異なります。

Kaspersky Endpoint Security をシステムアカウント（SYSTEM）で EXE または MSI ファイルを使用してアップグレードする場合は、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されます。そのため、コンピューターに Kaspersky Endpoint Agent がインストールされており、MDR ソリューションがアクティベートされている場合、Kaspersky Endpoint Security のインストーラーは自動的にコンポーネントのセットを構成して MDR コンポーネントを選択します。これにより、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。通常、システムアカウント (SYSTEM) を使用した MSI インストーラーの実行は、カスペルスキーのアップデートサービス経由または Kaspersky Security Center 経由でのインストールパッケージの配信時などに行われます。

権限のないユーザーアカウントで MSI ファイルを使用して Kaspersky Endpoint Security をアップグレードすると、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されません。この場合、Kaspersky Endpoint Security は、Kaspersky Endpoint Agent のコンポーネントの組み合わせに基づいて、自動的にコンポーネントを選択します。それから、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

Kaspersky Endpoint Security は、コンピューターを再起動することなくアップグレードをサポートします。ポリシーのプロパティで製品のアップグレードモードを選択できます。

5 本製品の動作の確認

製品のインストール後またはアップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。コンポーネントのステータスが「*ライセンスに含まれていません*」となっている場合は、組み込みエージェント機能をアクティベートしていることを確認してください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

Endpoint Detection and Response



Kaspersky Endpoint Security for Windows には Kaspersky Endpoint Detection and Response Optimum ソリューション（以降、「EDR Optimum」とも表記）向けの組み込みエージェントが含まれるようになりました。バージョン 11.8.0 から、Kaspersky Endpoint Security for Windows には Kaspersky Endpoint Detection and Response Expert ソリューション（以降、「EDR Expert」とも表記）向けの組み込みエージェントが含まれるようになりました。*Kaspersky Endpoint Detection and Response* は、高度なサイバー脅威から企業の IT インフラストラクチャを保護する幅広いソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。EDR Expert は EDR Optimum に比べ、より多くの脅威監視および応答機能を備えています。ソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプ および Kaspersky Endpoint Detection and Response Expert のヘルプ を参照してください。

脅威インテリジェンスツール

Kaspersky Endpoint Detection and Response は次の脅威インテリジェンスツールを使用します。

- Kaspersky Threat Intelligence Portal との連携。ファイルや Web アドレスの評価に関する情報を蓄積し、表示できます。
- Kaspersky Threats データベース。
- Kaspersky Security Network（以下、「KSN」とも表記）。クラウドサービスのインフラストラクチャで、カスペルスキーの情報基盤に基づいたリアルタイムのファイル、Web サイト、ソフトウェアの評価情報を提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。
- Cloud Sandbox 技術。検知したファイルを隔離された環境で実行し、ファイルの評価を確認します。

ソリューションの動作原理

Kaspersky Endpoint Detection and Response Optimum は脅威の活動を確認して分析し、迅速な対応に必要となる攻撃の可能性に関する情報を*セキュリティの担当者*または*管理者*に提供します。Kaspersky Endpoint Detection and Response は別のウィンドウでアラートの詳細を表示します。*アラート*とは、本製品によって異常または疑わしいと識別され、企業の IT インフラストラクチャにセキュリティ上の脅威をもたらす可能性がある、企業の IT インフラストラクチャ内のイベントです。*アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプ および Kaspersky Endpoint Detection and Response Expert のヘルプ を参照してください。

Kaspersky Endpoint Security の旧バージョン向けサポート

Kaspersky Endpoint Security 11.2.0〜11.6.0 を Kaspersky Endpoint Detection and Response Optimum との連携に使用している場合は、製品には Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Security のインストール中に並行して Kaspersky Endpoint Agent をインストールできます。Kaspersky Endpoint Security 11.9.0 では、Kaspersky Endpoint Agent 配布パッケージは Kaspersky Endpoint Security 配信キットには含まれません。

Kaspersky Endpoint Detection and Response Expert ソリューションでは、Kaspersky Endpoint Agent との連携はサポートされません。Kaspersky Endpoint Detection and Response Expert ソリューションでは、Kaspersky Endpoint Security の組み込みエージェント（バージョン 11.8.0 以降）を使用します。

組み込みエージェントと EDR Optimum / EDR Expert の連携

Kaspersky Endpoint Detection and Response と連携するには、Endpoint Detection and Response Optimum (EDR Optimum) コンポーネントまたは Endpoint Detection and Response Expert (EDR Expert) コンポーネントを追加し、Kaspersky Endpoint Security で設定する必要があります。

EDR Optimum、EDR Expert および EDR (KATA) コンポーネント間には互換性はありません。

Endpoint Detection and Response が動作するには次の条件を満たしている必要があります。

- Kaspersky Security Center のバージョンが 13.2 以降である。以前のバージョンの Kaspersky Security Center では、Endpoint Detection and Response をアクティベートすることはできません。
- Kaspersky Endpoint Detection and Response プラグイン。

  Kaspersky Endpoint Security バージョン 12.6 以降では、警告の詳細の表示が Kaspersky Endpoint Security 管理プラグインから EDR 管理プラグインに移動されました。EDR 管理プラグインは、Windows、Mac、Linux オペレーティングシステム上のエージェントを操作するための単一のプラグインです。今後、EDR Optimum を使用する場合は、脅威の対応タスクの作成には Kaspersky Endpoint Security 管理プラグインが、アラートの詳細の表示には EDR 管理プラグインが必要になります。
- Kaspersky Endpoint Security の一部としての EDR Optimum コンポーネントは Kaspersky Endpoint Detection and Response Optimum 2.0 ソリューションとの連携をサポートします。Kaspersky Endpoint Detection and Response Optimum バージョン 1.0 との連携はサポートされていません。

- EDR Optimum は Kaspersky Security Center Web コンソール および Kaspersky Security Center Cloud コンソールで管理することができます。

  EDR Expert の機能は、Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。

- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- Endpoint Detection and Response コンポーネントがオンになっている。
- Endpoint Detection and Response が連携する製品機能が有効になっており、動作している。Endpoint Detection and Response は次の機能と連携します：
  - ファイル脅威対策
  - ウェブ脅威対策
  - メール脅威対策
  - 脆弱性攻撃ブロック
  - ふるまい検知
  - ホスト侵入防止
  - 修復エンジン
  - アダプティブアノマリーコントロール

Kaspersky Endpoint Detection and Response とは次の手順で連携されます：

1. **Endpoint Detection and Response コンポーネントのインストール**

   EDR Optimum または EDR Expert コンポーネントは、インストール中またはアップグレード中、または*コンポーネントの変更*タスクを使用して選択できます。

   > 新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2. **Kaspersky Endpoint Detection and Response をアクティベートする**

   次の方法で Kaspersky Endpoint Detection and Response を使用するライセンスを入手できます：

   - Endpoint Detection and Response が Kaspersky Endpoint Security for Windows のライセンスに含まれている。

     機能は Kaspersky Endpoint Security for Windows のアクティベーション後すぐに使用できます。

   - EDR Optimum または EDR Expert の個別のライセンスを購入する（Kaspersky Endpoint Detection and Response のアドオン）。

     この機能は、Kaspersky Endpoint Detection and Response 向けの別のライセンスを追加すると使用できるようになります。結果として、Kaspersky Endpoint Security のライセンスおよび Kaspersky Endpoint Detection and Response のライセンスの 2 種類のライセンスがコンピューターに追加されることになります。

     スタンドアロンの Endpoint Detection and Response のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

EDR Optimum または EDR Expert がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

EDR Optimum の使用許諾契約書について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。

3 Endpoint Detection and Response Optimum コンポーネントの有効化

Kaspersky Endpoint Security for Windows のポリシー設定でこの機能を有効または無効にできます。

Web コンソールおよび Cloud コンソールで Endpoint Detection and Response を有効または無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**Endpoint Detection and Response は有効です**］をオンにします。
6. 変更内容を保存します。

Kaspersky Endpoint Detection and Response コンポーネントが有効になりました。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Endpoint Detection and Response Optimum**］または［**Endpoint Detection and Response Expert**］が Kaspersky Endpoint Security のコンポーネントのリストに追加されました。

4 管理サーバーへのデータ転送を有効にする

すべての Endpoint Detection and Response の機能を有効するには、次の種別のデータの転送を有効にする必要があります。

- 隔離されたファイルのデータ。

  このデータは Web コンソールおよび Cloud コンソールを使用して、コンピューター上で隔離されたファイルに関する情報を取得するために必要となります。たとえば、Web コンソールおよび Cloud コンソールで分析用に隔離からファイルをダウンロードすることができます。

- 脅威の活動連鎖のデータ。

  このデータは Web コンソールおよび Cloud コンソールで、コンピューター上で検知されたファイルに関する情報を取得するために必要となります。Web コンソールおよび Cloud コンソールでアラートの詳細を表示して必要な応答操作を行うことができます。

Web コンソールおよび Cloud コンソールで管理サーバーへのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**レポートと保管領域**］に移動します。

5. ［**管理サーバーへのデータ転送**］で、次のチェックボックスをオンにします：

   - **隔離ファイルの情報**
   - **脅威の活動連鎖の情報**

6. 変更内容を保存します。

セキュリティ侵害インジケーター（IOC）のスキャン

*セキュリティ侵害インジケーター（IOC）*とは、コンピューターへの認証されないアクセス（コンピューターの侵害）の痕跡を示すオブジェクトまたは活動に関する一連のデータです。たとえば、システムへのログインを複数回失敗すると、セキュリティ侵害インジケーターの構成要素となります。*IOC スキャンタスク*は、コンピューターのセキュリティ侵害インジケーターを検索し、脅威への対応方法を確立するのに役立ちます。

Kaspersky Endpoint Security は IOC ファイルを使用して侵害インジケーターを検索します。*IOC ファイル*は、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。IOC ファイルは OpenIOC 標準に準拠している必要があります。

IOC スキャンタスクの実行モード

Kaspersky Endpoint Detection and Response を使用して、侵害されたデータを検知する標準の IOC スキャンタスクを作成できます。*標準の IOC スキャンタスク*は Web コンソールで手動で作成および設定されたタスクまたはタスクのグループを意味します。タスクは、ユーザーが準備した IOC ファイルを使用して実行されます。手動で侵害インジケーターを追加する場合は、IOC ファイルの要件を参照してください。

以下のリンクをクリックしてダウンロードできるファイルには、すべての OpenIOC 標準の IOC タームの一覧が含まれています。

こちらのリンクから IOC_TERMS.XLSX ファイルをダウンロードできます

Kaspersky Endpoint Security は、本製品が Kaspersky Sandbox ソリューションの一部として使用されている場合はスタンドアロンの IOC スキャンタスクをサポートします。

IOC ファイルの作成

Kaspersky Endpoint Security 12.10 for Windows から、タスク設定で直接 IOC ファイルを作成できるようになりました。IOC ファイルを作成するには、侵害インジケーターのリストを含む TXT ファイルを準備する必要があります。侵害インジケーターとして次のオブジェクトのリストを追加できます：

- ファイルハッシュ（MD5 / SHA256）。

  本製品は、FileItem/Md5sum または FileItem/Sha256sum のスキャン範囲で IOC ファイルを準備します。

- IP アドレス（IPv4、IPv6）。

  本製品は、PortItem/RemoteIP のスキャン範囲で IOC ファイルを準備します。

- DNS 名。

  本製品は、DnsEntryItem/RecordName のスキャン範囲で IOC ファイルを準備します。

Web コンソールで IOC ファイルを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

   タスクのリストが表示されます。

2. ［**IOC スキャン**］タスクを選択します。

   タスクのプロパティウィンドウが表示されます。必要に応じて、**IOC スキャン**タスクを作成します。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**IOC スキャン設定**］に移動します。

5. ［**IOC ファイルを再定義する**］をクリックします。

6. これにより、IOC ファイルを作成するためのフォームが表示されます：

   a. ［**IOC ファイルのソース**］で、［**ファイルから生成する**］を選択します。

   b. IOC ファイルの名前を入力します。

   c. 侵害インジケーターのリストを含む TXT ファイルを選択します。

   d. IOC ファイルの種別（［**DNS 名**］、［**ファイルハッシュ**］、［**IP アドレス**］）を選択します。

   e. ［**生成**］をクリックします。

   IOC コレクションに IOC ファイルが追加されます。必要に応じて、IOC ファイルをタスク範囲から一時的に除外できます。

7. 変更内容を保存します。

IOC スキャンタスクの作成

*IOC スキャンタスク*は、手動で作成することができます：

- アラートの詳細（EDR Optimum のみ）で作成する。

  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

- タスクウィザードを使用する。

EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

［IOC スキャン］タスクを作成するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**IOC スキャン**］を選択します。
   c. ［**タスク名**］に簡潔な内容を入力します。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。次の手順に進みます。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。次の手順に進みます。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

   システムアカウント（SYSTEM）にはネットワークドライブの *IOC スキャンタスクを実行する権限がありません。ネットワークドライブに対してタスクを実行する場合に、そのドライブにアクセス権のあるユーザーアカウントを選択してください。

   ネットワークドライブのスタンドアロンの IOC スキャンタスクには、タスクのプロパティで、そのドライブにアクセス権のあるユーザーアカウントを手動で選択する必要があります。

6. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. ［**IOC スキャン設定**］に移動します。
10. 侵害インジケーターを検索するために IOC ファイルをアップロードします。
    IOC ファイルをアップロードすると、チェックに通過しなかったインジケーターのリストなど、ファイルに関する概要情報が本製品に表示されます。IOC ファイルをアップロードしたら、タスクのプロパティで直接、組み込みエディターを使用してファイルを手動で編集できます。Kaspersky Endpoint Security は、OpenIOC 1.1 標準に準拠した IOC ファイルの編集をサポートしています。OpenIOC バージョン 1.0 に準拠した IOC ファイルの内容を変更することはできません。
    IOC コレクションに IOC ファイルが追加されます。必要に応じて、IOC ファイルをタスク範囲から一時的に除外できます。

タスク実行後の IOC ファイルの追加または削除は推奨されません。前回実行された IOC スキャン結果が正しく表示されないことがあります。IOC ファイルの侵害インジケーターを検索するには、新しいタスクを追加するようにしてください。

11. 必要に応じて、［**遡及的 IOC スキャン**］をオンにします。*遡及的 IOC スキャン*は、Kaspersky Endpoint Security が一定期間のデータを使用してセキュリティ侵害インジケーターをスキャンする *IOC スキャン*タスクのモードです。このモードは、コンピューターのネットワーク動作のデータ内のセキュリティ侵害インジケーターを検知することを目的としています。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムのログとブラウザーのログ内のデータを分析します。

    遡及的 IOC スキャンは、Google Chrome、Mozilla Firefox、Microsoft Edge（バージョン 79 以降）のブラウザーのログを分析します。

12. IOC 検知時の動作の設定：

    - **デバイスをネットワークから分離する**：このオプションを選択した場合、Kaspersky Endpoint Security は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。分離時間はEndpoint Detection and Response コンポーネントの設定で設定できます。

      このチェックボックスをオフにすると、タスクを手動で実行した後でコンピューターをネットワークから分離できます。*IOC スキャン*タスクで IOC が検知された場合、IOC から直接コンピューターをネットワークから分離することができます（*IOC スキャン*のプロパティ→［**アプリケーション設定**］→［**IOC スキャン結果**］タスク）。Kaspersky Endpoint Security では、ネットワーク分離の無効化期間やネットワーク分離の除外リストなど、追加の設定をすぐに管理することもできます。

    - **コピーを隔離に移動し、オブジェクトを削除する**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。

      このチェックボックスをオフにすると、タスクを手動で実行した後でファイルを手動で隔離できます。*IOC スキャン*タスクでデータを危険にさらす可能性のあるファイルが検知された場合、IOC スキャン結果からこのファイルを直接隔離することができます（［**アプリケーション設定**］→［**IOC スキャン結果**］）。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

    - **簡易スキャンを実行する**：このオプションを選択した場合、Kaspersky Endpoint Security は*簡易スキャン*タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。

13. ［**詳細**］に移動します。

14. タスクの一部として分析される必要のあるデータ種別（IOC ドキュメント）を選択します。

    Kaspersky Endpoint Security は、読み込まれた IOC ファイルの内容に従って *IOC スキャン*タスク用のデータ種別（IOC ドキュメント）を自動で選択します。選択されたデータ種別の選択解除は推奨されません。

    次のデータ種別に対してスキャン範囲を追加で設定できます：

    - **ファイル - FileItem**：事前定義された範囲を使用してコンピューター上の IOC スキャン範囲を設定します。

      既定では、Kaspersky Endpoint Security はコンピューターの重要な領域（ダウンロードフォルダー、デスクトップ、一時的なオペレーティングシステムのファイルがあるフォルダーなど）のみの IOC をスキャンします。スキャン範囲を手動で追加することもできます。

- **Windows イベントログ - EventLogItem**：イベントが記録された際の時間周期を入力します。IOC スキャンに使用する必要のある Windows イベントログを選択することもできます。既定では、次のイベントログが選択されています：アプリケーションイベントログ、システムイベントログ、セキュリティイベントログ。

- **Windows レジストリ - RegistryItem**：レジストリで IOC スキャン範囲を設定します。

  既定では、Kaspersky Endpoint Security はレジストリキー一式をスキャンします。

15. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

16. タスクのスケジュールを設定します。

> このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

17. 変更内容を保存します。

18. タスクの横にあるチェックボックスをオンにします。

19. ［**開始**］をクリックします。

Kaspersky Endpoint Security はコンピューター上にある侵害インジケーターの検索を実行します。［**履歴**］のタスクのプロパティでタスクの結果を確認できます。［**アプリケーション設定**］→［**IOC スキャン結果**］の順に選択して、タスクのプロパティで侵害インジケーターに関する情報を表示することができます。IOC スキャン結果では、手動で検知されたファイルを隔離することも、コンピューターをネットワークから分離することもできます。

Kaspersky Endpoint Security は、同じ IOC ファイルに対して作成されたレコード間で重複を検索し、タスク結果に一意のレコードのみを保持します。重複とは、すべての比較対象フィールドの値が同じである同じ種別のレコードです。また、1 つ以上のフィールドに値がない場合、本製品はレコードを作成しないこともあります（下の表を参照）。

種別	比較対象フィールド	レコードを作成しない条件
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• FullPath、Md5sum、Sha256sum フィールドの値が欠落している。 • FullPath フィールドの値が欠落しており、Md5sum と Sha256sum のフィールドの値が同一。
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Hive、KeyPath、ValueName の 1 つ以上のフィールドの値が欠落している。
ProcessItem	• startTime • PID	startTime または PID フィールドの値が欠落している。

> ［**警告の詳細**］ウィンドウには、同一のフィールド値を持つ RegistryItem レコードが表示される場合があります。このようなレコードは、インターフェイスに表示されないテキストフィールドの値が異なるため、重複ではありません。

> IOC スキャン結果は 30 日間保持されます。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータを自動的に削除します。

IOC スキャンの拡張テレメトリ

遡及的 IOC スキャンを行う場合、コンピューターで拡張テレメトリを有効にすることを推奨します。拡張テレメトリにより IOC 検知の精度は向上しますが、コンピューターのリソースの消費量も増加します。

拡張テレメトリには、次の追加タームのサポートが含まれます：

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

拡張テレメトリが無効になっている場合、Kaspersky Endpoint Security は検知されたセキュリティ侵害インジケーターに関する情報を置き換えることがあります。

拡張テレメトリを有効にするには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**詳細なシステム動作の記録を有効にする**］チェックボックスをオンにします。
6. 変更内容を保存します。

ファイルを隔離する

脅威への対応として、Kaspersky Endpoint Detection and Response は*ファイルの隔離*タスクを作成します。これは脅威の影響を最小限にとどめるために必要です。*隔離*はコンピューター上にある特別なローカル保管領域です。ユーザーがコンピューターに対して危険だと判断したファイルを隔離することができます。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は、Detection and Response ソリューション (EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox) と連携する際にのみ隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、Kaspersky Sandbox のヘルプ、Kaspersky Endpoint Detection and Response Optimum のヘルプ、および Kaspersky Endpoint Detection and Response Expert のヘルプ、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

次の方法で*ファイルの隔離*タスクを作成できます：

- アラートの詳細（EDR Optimum のみ）で作成する。

  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

- タスクウィザードを使用する。

  ファイルのパスまたはハッシュ（SHA256 または MD5）、もしくはファイルのパスとハッシュの両方を入力する必要があります。

- *IOC スキャンタスク設定*を使用する。

  *IOC スキャンタスク*でデータを危険にさらす可能性のあるファイルが検知された場合、IOC スキャン結果からこのファイルを直接隔離することができます（[**アプリケーション設定**] → [**IOC スキャン結果**]）。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

*ファイルの隔離*タスクには次の制限事項があります：

1. ファイルのサイズは 100 MB を超えることはできません。
2. 重要なシステムオブジェクト（SCO）は隔離できません。SCO とはオペレーティングシステムと Kaspersky Endpoint Security for Windows アプリケーションが実行できる必要のあるファイルです。
3. EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。
4. *ファイルの隔離*タスクの結果として隔離されたオブジェクトをスキャンすることはできません。

［ファイルの隔離］タスクを作成するには：

1. Web コンソールのメインウィンドウで、[**アセット（デバイス）**] → [**タスク**] の順に選択します。

   タスクのリストが表示されます。

2. [**追加**] をクリックします。

   タスクウィザードが起動します。

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］から［**ファイルの隔離**］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。［**次へ**］をクリックします。

5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。［**次へ**］をクリックします。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

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

7. 新しいタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. ファイルのリストで、［**追加**］をクリックします。
   ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

    ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにドライブ文字があると、*ファイルが見つかりません*というエラーになります。

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

    このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

Kaspersky Endpoint Security はファイルを隔離します。

ファイルが別のプロセスでロックされている場合は、タスクは*完了*として表示されますが、ファイルそのものはコンピューターが再起動されてから隔離されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

実行中のファイルを隔離しようとした場合、*ファイルの隔離*タスクはエラー「*アクセスが拒否されました*」で終了することがあります。ファイルに対して[プロセスの終了タスクを作成](#)してから再度実行してください。

サイズが大きいファイルを隔離しようとした場合、*ファイルの隔離*タスクはエラー「*隔離の保管領域に十分な空き容量がありません*」で終了することがあります。隔離の中身を空にするか、[隔離のサイズを拡大](#)してください。再度実行してください。

Web コンソールを使用して隔離からファイルを復元したり、隔離の中身を空にすることができます。[コマンドライン](#)を使用してオブジェクトをローカルコンピューター上に復元できます。

ファイルを取得する

ユーザーのコンピューターからファイルを取得することができます。たとえば、サードパーティ製品によって作成されたイベントログファイルを取得するよう設定することができます。そのタスクの実行結果として、ファイルは[隔離に保存されます](#)。*隔離*はコンピューター上にある特別なローカル保管領域です。Web コンソールを使用して隔離に保存されたこのファイルをダウンロードすることができます（［**操作**］→［**保管領域**］→［**隔離**］）。ユーザーのコンピューターでは、ファイルは元のフォルダーに残ります。

ファイルのサイズは 100 MB を超えることはできません。

EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

［ファイルの取得］タスクを作成するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**ファイルの取得**］を選択します。
   c. ［**タスク名**］に簡潔な内容を入力します。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。［**次へ**］をクリックします。

5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。［**次へ**］をクリックします。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

6. ［**終了**］をクリックして、ウィザードを終了します。

   タスクのリストに新しいタスクが表示されます。

7. 新しいタスクをクリックします。

   タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. ファイルのリストで、［**追加**］をクリックします。

   ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

    ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにドライブ文字があると、*ファイルが見つかりません*というエラーになります。

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

    このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

    この結果、Kaspersky Endpoint Security はファイルのコピーを作成し、コピーを隔離に移動します。Web コンソールで隔離からファイルをダウンロードします。

ファイルを削除する

*ファイルの削除*タスクを使用してリモートからファイルを削除できます。たとえば、脅威への対応としてリモートからファイルを削除する場合などです。

*ファイルの削除*タスクには次の制限事項があります：

- 重要なシステムオブジェクト（SCO）は削除できません。SCO とはオペレーティングシステムと Kaspersky Endpoint Security アプリケーションが実行できる必要のあるファイルです。
- EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

［ファイルの削除］タスクを作成するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**ファイルの削除**］を選択します。
   c. ［**タスク名**］に簡潔な内容を入力します。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。［**次へ**］をクリックします。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。［**次へ**］をクリックします。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

6. ［**終了**］をクリックして、ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. ファイルのリストで、［**追加**］をクリックします。
   ファイルの追加ウィザードが開始されます。
10. ファイルを追加するには、ファイルの完全パス、ファイルのハッシュとパスの両方を入力する必要があります。

    ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにドライブ文字があると、*ファイルが見つかりません*というエラーになります。

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

    このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

    Kaspersky Endpoint Security はコンピューターからファイルを削除します。ファイルが別のプロセスでロックされている場合は、タスクは*完了*として表示されますが、ファイルそのものはコンピューターが再起動されてから削除されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

実行中のファイルを隔離しようとした場合、*ファイルの削除*タスクはエラー「*アクセスが拒否されました*」で終了することがあります。ファイルに対して*プロセスの終了タスクを作成*してから再度実行してください。

プロセスの開始

*プロセスの開始*タスクを使用してリモートからファイルを実行できます。たとえば、コンピューターの設定ファイルを作成するユーティリティをリモートから実行したりすることができます。次に、*ファイルの取得*タスクを使用して Kaspersky Security Center Web コンソールで作成されたファイルを受け取ります。

EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

［プロセスの開始］タスクを作成するには：

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

2. ［**追加**］をクリックします。
   タスクウィザードが起動します。

3. タスクの設定を指定します：

   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。

   b. ［**タスク種別**］から［**プロセスの開始**］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

4. タスク範囲の指定方法に応じて、対象デバイスを選択します。［**次へ**］をクリックします。

5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。［**次へ**］をクリックします。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

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

7. 新しいタスクをクリックします。

8. タスクのプロパティウィンドウが表示されます。

9. ［**アプリケーション設定**］タブを選択します。

10. プロセスの開始コマンドを入力します。
    現在のフォルダー（既定）で「`conf.txt`」というファイルにコンピューターの設定に関する情報を保存する「`utility.exe`」というユーティリティを実行するとします。ユーティリティは `C:\Users\admin\Diagnostic\` フォルダーにあります。設定ファイルは `C:\Users\admin\Documents\Configuration` フォルダーに保存する必要があります。次の値を入力します：

    - **実行コマンド** – `C:\Users\admin\Diagnostic\utility.exe`
    - **コマンドライン引数（省略可能）** – `/R conf.txt`
    - **作業フォルダーのパス（省略可能）** – `C:\Users\admin\Documents\Configuration`

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

    このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

    この結果、Kaspersky Endpoint Security はコマンドをサイレントモードで実行し、プロセスを開始します。［**実行結果**］のタスクのプロパティでタスクの結果を確認できます。

プロセスの終了

*プロセスの終了*タスクを使用してリモートからプロセスを終了することができます。たとえば、*プロセスを実行*タスクを使用して開始されたインターネットの速度テストツールをリモートから終了する場合などです。

ファイルの実行をブロックする場合は、実行防止機能を設定することができます。実行ファイル、スクリプト、Office 形式のファイルの実行を禁止することができます。

プロセスの終了タスクには次の制限事項があります：

- 重要なシステムオブジェクト（SCO）のプロセスは終了できません。SCO とはオペレーティングシステムと Kaspersky Endpoint Security アプリケーションが実行できる必要のあるファイルです。
- EDR Optimum のタスクは、Web コンソールおよび Cloud コンソールで設定できます。EDR Expert のタスク設定は Cloud コンソールのみで使用可能です。

［プロセスの終了］タスクを作成するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］から［**Kaspersky Endpoint Security for Windows 12.12.0**］を選択します。
   b. ［**タスク種別**］から［**プロセスの終了**］を選択します。
   c. ［**タスク名**］に簡潔な内容を入力します。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
4. タスク範囲の指定方法に応じて、対象デバイスを選択します。［**次へ**］をクリックします。
5. タスクの実行に使用するユーザーアカウントの認証情報を入力します。［**次へ**］をクリックします。

   既定では、Kaspersky Endpoint Security はタスクをシステムユーザーアカウント（SYSTEM）として開始します。

6. ［**終了**］をクリックして、ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。
7. 新しいタスクをクリックします。
   タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. 手順を完了するには、強制終了するファイルを選択する必要があります。次のいずれかの方法でファイルを選択することができます：
   - ファイルの完全名を入力します。
   - ファイルのハッシュとパスを入力します。
   - プロセスの PID を入力します（ローカルタスクのみ）。

ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにドライブ文字があると、*ファイルが見つかりません*というエラーになります。

10. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。
11. タスクのスケジュールを設定します。

    このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

12. ［**保存**］をクリックします。
13. タスクの横にあるチェックボックスをオンにします。
14. ［**開始**］をクリックします。

    この結果、Kaspersky Endpoint Security はコンピューター上でそのプロセスを終了します。たとえば、アプリケーション「ゲーム」が実行中で、game.exe プロセスを終了すると、データを保存せずにアプリケーションは終了されます。［**履歴**］のタスクのプロパティでタスクの結果を確認できます。

実行防止

実行防止を使用して、実行ファイルやスクリプトの実行や Office 形式のファイルを開く動作を管理することができます。こうすることで、安全でないと考えられるアプリケーションの実行をブロックしたりすることができます。結果、脅威の拡散を止めることができます。実行防止は、Office ファイルの拡張子のセットおよびスクリプトインタープリターのセットをサポートしています。

実行防止ルール

実行防止ルールを含むファイルへのユーザーのアクセスを管理することができます。*実行防止ルール*とは、オブジェクトの実行のブロックなど、製品がオブジェクトの実行時への対応時に適用する一連の条件です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。

実行防止ルールは次の方法で作成できます：

- アラートの詳細（EDR Optimum のみ）で作成する。

  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

- グループポリシーまたはローカルアプリケーション設定を使用する。

  ファイルのパスまたはハッシュ（SHA256 または MD5）、もしくはファイルのパスとハッシュの両方を入力する必要があります。

ローカルでコマンドラインを使用して実行防止を管理することもできます。

実行防止には次の制限事項があります：

1. CD や IOS イメージ上のファイルは実行防止の対象外です。これらのファイルの実行はブロックされません。
2. システムで重要なオブジェクト（SCO）の開始をブロックすることはできません。SCO とはオペレーティングシステムと Kaspersky Endpoint Security アプリケーションが実行できる必要のあるファイルです。
3. 5000 以上の実行防止ルールの作成は、システムが不安定になる可能性があるため推奨されません。

実行防止ルールのモード

実行防止機能は以下の 2 つのモードで動作します：

- **統計のみ**

  このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。

- **有効**

  このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。

実行防止の管理

Web コンソールでのみこの機能を設定できます。

実行を防止するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**実行防止**］タブを選択します。
6. ［**実行防止は有効です**］をオンにします。

7. ［**禁止されたオブジェクトを実行、または開いたときの処理**］ブロックで、機能の操作モードを選択します：

   - **ブロックしイベントログへ追加する**：このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。

   - **イベントログに追加する**：このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。

8. 実行防止ルールのリストを作成します：

   a. ［**手動で追加**］をクリックします。

   b. 表示されるウィンドウで、「*アプリケーション A*」のように実行防止ルールの名前を入力します。

   c. ［**種別**］で、［**実行ファイル**］、［**スクリプト**］、［**Microsoft Office ドキュメント**］からブロックするオブジェクトを選択します。

      オブジェクト種別を誤って選択すると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。

   d. ファイルを追加するには、ファイルのハッシュ（SHA256 または MD5）、ファイルの完全パス、ハッシュとパスの両方を入力する必要があります。

      > ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにネットワークドライブ文字が含まれていると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。

      実行防止は、Office ファイルの拡張子のセットおよびスクリプトインタープリターのセットをサポートしています。

9. 変更内容を保存します。

この結果、Kaspersky Endpoint Security はオブジェクトの実行（実行ファイルやスクリプトの実行、Office 形式のファイルを開く動作）をブロックします。スクリプトの実行がブロックされていても、例えばスクリプトファイルをテキストエディタで開くことなどは可能です。オブジェクトの実行をブロックする際、製品設定で有効にされている場合は Kaspersky Endpoint Security は標準の通知（下の図を参照）を表示します。



実行防止の通知

コンピューターのネットワーク分離

コンピューターのネットワーク分離を使用して、セキュリティ侵害インジケーター（IOC）の検知時の対応として、コンピューターを自動的にネットワークから分離できます。これは*自動モード*です。検知した脅威を調査している最中など、ネットワーク分離を手動でオンにできます。これは*手動モード*です。

ネットワーク分離がオンになると、本製品はすべてのアクティブな接続を切断し、コンピューターのすべての新規 TCP/IP 接続をブロックしますが、以下の接続は切断されません：

- ネットワーク分離の除外リストに追加されている接続。
- Kaspersky Endpoint Security サービスによって開始された接続。
- Kaspersky Security Center ネットワークエージェントによって開始された接続。
- アプリケーションが Light Agent モードで使用されている場合の SVM および Integration Server への接続。

Web コンソールでのみこの機能を設定できます。

ネットワーク分離の自動モード

IOC 検知時の対応として、ネットワーク分離を自動的にオンにするよう設定できます。グループポリシーを使用してネットワーク分離の自動モードを設定できます。

IOC 検知時の対応として、ネットワーク分離を自動的に有効にするよう設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **IOC スキャン**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
   必要に応じて、*IOC スキャン*タスクを作成します。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**IOC 検知時の処理**］ブロックで、［**IOC が見つかった後に応答処理を実行する**］および［**コンピューターをネットワークから分離する**］を選択します。
5. 変更内容を保存します。

この結果、IOC が検知されると、本製品は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。

一定期間が経過した後に自動ネットワーク分離を無効にするように設定できます。既定では、ネットワーク分離がオンになってから 8 時間が経過すると、本製品はネットワーク分離をオフにします。ネットワーク分離は手動でオフにすることもできます（以下の手順を参照）。ネットワーク分離をオフにした後は、コンピューターは制限されることなくネットワークを使用することができます。

コンピューターのネットワーク分離を自動モードでオフにする時間の遅延を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**ネットワーク分離**］タブを選択します。
6. ネットワーク分離をオフにする時間の遅延を設定します。
7. 変更内容を保存します。

ネットワーク分離の手動モード

手動でネットワーク分離をオンまたはオフにすることができます。Kaspersky Security Center コンソールで、コンピューターのプロパティを使用してネットワーク分離の手動モードを設定できます。

ネットワーク分離は次の方法でオンにできます：

- アラートの詳細（EDR Optimum のみ）で作成する。
  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。
- 個別のローカル環境用の製品設定を使用する。
- *IOC* スキャンタスク設定を使用する。
  IOC スキャンタスクで IOC が検知された場合、IOC から直接コンピューターをネットワークから分離することができます（*IOC* スキャンのプロパティ→［**アプリケーション設定**］→［**IOC スキャン結果**］タスク）。Kaspersky Endpoint Security では、ネットワーク分離の無効化期間やネットワーク分離の除外リストなど、追加の設定をすぐに管理することもできます。

手動でコンピューターのネットワーク分離を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。
   コンピューターのプロパティが表示されます。
3. ［**アプリケーション**］タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。

5. ［**アプリケーション設定**］タブを選択します。

6. ［**Detection and Response**］→［**Endpoint Detection and Response**］に移動します。

7. ［**ネットワーク分離**］ブロックで、［**コンピューターをネットワークから分離する**］をクリックします。

指定した時間が経過した後にネットワーク分離を自動でオフにするよう設定することができます。既定では、ネットワーク分離がオンになってから 8 時間が経過すると、本製品はネットワーク分離をオフにします。ネットワーク分離をオフにした後は、コンピューターは制限されることなくネットワークを使用することができます。

コンピューターのネットワーク分離を手動モードでオフにする時間の遅延を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ローカル環境用の製品設定を行うコンピューターを選択します。
   コンピューターのプロパティが表示されます。

3. ［**タスク**］タブを選択します。
   これにより、コンピューターで使用可能なタスクのリストが表示されます。

4. ［**ネットワーク分離**］タスクを選択します。

5. ［**アプリケーション設定**］タブを選択します。

6. 表示されるウィンドウで、ネットワーク分離をオフにする時間の遅延を設定します。

7. 変更内容を保存します。

手動でコンピューターのネットワーク分離を無効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. ローカル環境用の製品設定を行うコンピューターを選択します。
   コンピューターのプロパティが表示されます。

3. ［**アプリケーション**］タブを選択します。

4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。

5. ［**アプリケーション設定**］タブを選択します。

6. ［**Detection and Response**］→［**Endpoint Detection and Response**］に移動します。

7. ［**ネットワーク分離**］ブロックで、［**コンピューターの分離を解除する**］をクリックします。

ローカルでコマンドラインを使用してネットワーク分離を無効にすることもできます。

Kaspersky Endpoint Security 12.10 for Windows から、アラートの詳細でネットワーク分離を管理できるようになりました。さらに、アラートの詳細では、コンピューターのネットワーク分離期間を指定できます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプ および Kaspersky Endpoint Detection and Response Expert のヘルプ を参照してください。

ネットワーク分離の除外リスト

ネットワーク分離の除外リストを設定できます。ネットワーク分離がオンになっても、ルールに一致するネットワーク接続はブロックされません。

*標準のネットワークプロファイル*のリストを使用してネットワーク分離の除外リストを設定できます。既定では、除外リストには DNS/DHCP サーバーおよび DNS/DHCP クライアントロールを持つデバイスの動作が妨げられないようにするルールを含むネットワークプロファイルが含まれています。標準のネットワークプロファイルまたは除外リストの設定は手動で変更できます（以下の手順を参照してください）。

ポリシーのプロパティで指定された除外リストは、脅威の検知時の対応としてネットワーク分離が自動的にオンになった場合にのみ適用されます。コンピューターのプロパティで指定された除外リストは、Kaspersky Security Center のコンソールのコンピューターのプロパティまたはアラートの詳細から手動でネットワーク分離をオンにした場合にのみ適用されます。

これらのパラメータは異なる使用シナリオを持つため、有効なポリシーはコンピューターのプロパティで設定されたネットワーク分離の除外リストの適用をブロックしません。

自動モードでネットワーク分離の除外リストを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**ネットワーク分離**］タブを選択します。
6. ［**ネットワーク分離の除外リスト**］ブロックで、［**除外リスト**］をクリックします。
7. 表示されるウィンドウで、［**追加**］→［**プロファイルから追加**］をクリックして例外を設定する標準ネットワークプロファイルを選択します。

   プロファイルからネットワーク分離の除外リストがネットワーク分離の除外リストのリストに追加されます。ネットワーク接続のプロパティが表示されます。必要に応じて、ネットワーク接続設定を編集できます。
8. 必要に応じて、ネットワーク分離の除外リストを手動で追加してください。ネットワーク分離の除外リストを手動で追加するには、除外リストのウィンドウで［追加］→［**手動で追加**］をクリックしてネットワーク接続設定を手動で編集してください。
9. 変更内容を保存します。

手動モードでネットワーク分離の除外リストを追加する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。

   コンピューターのプロパティが表示されます。
3. ［**タスク**］タブを選択します。

   これにより、コンピューターで使用可能なタスクのリストが表示されます。
4. ［**ネットワーク分離**］タスクを選択します。
5. ［**アプリケーション設定**］タブを選択します。
6. 表示されるウィンドウで、［**除外リスト**］をクリックします。
7. 表示されるウィンドウで、［**プロファイルから追加**］をクリックして例外を設定する標準ネットワークプロファイルを選択します。

   プロファイルからネットワーク分離の除外リストがネットワーク分離の除外リストのリストに追加されます。ネットワーク接続のプロパティが表示されます。必要に応じて、ネットワーク接続設定を編集できます。
8. 必要に応じて、ネットワーク分離の除外リストを手動で追加してください。ネットワーク分離の除外リストを手動で追加するには、除外リストのウィンドウで［**追加**］をクリックしてネットワーク接続設定を手動で編集してください。
9. 変更内容を保存します。

ローカルでコマンドラインを使用してネットワーク分離の除外リストを表示することもできます。この場合、コンピューターは分離されている必要があります。

Kaspersky Endpoint Security 12.10 for Windows から、アラートの詳細でネットワーク分離の除外リストを追加できるようになりました。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

Cloud Sandbox

Cloud Sandbox はコンピューター上のより高度な脅威を検知する技術です。Kaspersky Endpoint Security は、検知したファイルを自動的に Cloud Sandbox に送って分析します。Cloud Sandbox はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してそのファイルの評価を決定します。これらのファイルのデータは Kaspersky Security Network に送られます。このため、Cloud Sandbox が悪意のあるファイルを検知すると、Kaspersky Endpoint Security はこのファイルが検出されたすべてのコンピューター上でこの脅威を除去するための適切な操作を実行します。

Cloud Sandbox が動作するには、Kaspersky Security Network の使用を有効にする必要があります。

Kaspersky Private Security Network を使用している場合は、Cloud Sandbox 技術は使用できません。

Cloud Sandbox 技術は、使用しているライセンス種別にかかわらずすべての Kaspersky Security Network ユーザーに対して有効で使用可能です。Endpoint Detection and Response ソリューション（EDR Optimum または EDR Expert）を導入済みの場合は、Cloud Sandbox で検知された脅威向けの個別のカウンターを有効にすることができます。検知した脅威の分析中にこのカウンターを使用して統計を生成することができます。

Cloud Sandbox カウンターを有効にするには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**Cloud Sandbox**］タブを選択します。
6. ［**Cloud Sandbox は有効です**］をオンにします。
7. 変更内容を保存します。

脅威が見つかった場合、Kaspersky Endpoint Security は［**脅威検知技術**］の下のメインウィンドウで Cloud Sandbox を使用して検知された脅威向けのカウンターを有効にします。また、Kaspersky Endpoint Security では Kaspersky Security Center コンソールの*脅威レポート*で Cloud Sandbox 脅威検知技術が表示されます。

EDR Optimum の KEA から KES への移行ガイド

Kaspersky Endpoint Security for Windows には Kaspersky Endpoint Detection and Response Optimum ソリューション向けの組み込みエージェントが含まれるようになりました。EDR Optimum と連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security を導入する場合は、Kaspersky Endpoint Detection and Response Optimum ソリューションと Kaspersky Endpoint Security は継続して連携します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Security をバージョン 11.7.0 以降にアップデートすると、システムで同じ動作が発生します。

Kaspersky Endpoint Security は Kaspersky Endpoint Agent と互換性はありません。同じコンピューターにこれらの製品の両方をインストールすることはできません。

Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum の一部として機能するには、次の条件を満たしている必要があります：

- Kaspersky Endpoint Detection and Response Optimum バージョン 2.0 以降。
- Kaspersky Security Center のバージョンが 13.2 以降である (ネットワークエージェントを含む)。以前のバージョンの Kaspersky Security Center では、EDR Optimum 機能をアクティベートすることはできません。
- EDR Optimum は、Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。

- 管理サーバーへのデータ転送が有効になっている。このデータは Web コンソール経由でコンピューター上で隔離されたファイルに関する情報を取得するために必要となります。
- Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されている。Kaspersky Security Center Web コンソールを経由した管理サーバーと EDR Optimum が連携するためには、新しい保護された接続であるバックグラウンド*接続*を確立する必要があります。

EDR Optimum で［KES + KEA］設定から［KES + 組み込みエージェント］に移行する手順

1. **Kaspersky Endpoint Security Web プラグインのアップグレード**

   EDR Optimum コンポーネントは、Kaspersky Endpoint Security の Web プラグインのバージョン 11.7.0 以降を使用して管理できます。

2. **ポリシーおよびタスクの移行**

   Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。そのためには、Web コンソールの Kaspersky Endpoint Agent からの移行ウィザードを使用します。

   Web コンソールで Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行する方法

   Web コンソールのメインウィンドウで、［**操作**］→［**Kaspersky Endpoint Agent からの移行**］の順に選択します。

   ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

   ステップ 1：ポリシーの移行

   移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Agent のポリシーをクリックして、設定を統合する Kaspersky Endpoint Security のポリシーを選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

   ステップ 2：タスクの移行

   移行ウィザードが Kaspersky Endpoint Security 向けの新しいタスクを作成します。タスクのリストで、Kaspersky Endpoint Security のポリシー向けに作成する Kaspersky Endpoint Agent のタスクを選択します。次の手順に進みます。

   ステップ 3：ウィザードの完了

   ウィザードを終了します。ウィザードは以下の処理を実行します：

   - 新規の Kaspersky Endpoint Security のポリシーを作成する

ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには *<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>* という名前が付けられます。新しいポリシーのステータスは*非アクティブ*になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ*非アクティブ*にして、新しく統合されたポリシーを有効にします。

Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行後、新しいポリシーに管理サーバーへのデータ転送機能（隔離されたファイルのデータと脅威の活動連鎖のデータ）が設定されていることを確認してください。データ転送のパラメータ値は Kaspersky Endpoint Agent ポリシーからは移行されません。

- 新規の Kaspersky Endpoint Security のタスクを作成する

  新しいタスクは、Kaspersky Endpoint Agent のタスクのコピーです。同時に、ウィザードは Kaspersky Endpoint Agent タスクには変更を加えません。

3 EDR Optimum 機能のライセンス

共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Security for Windows および Kaspersky Endpoint Agent をアクティベートした場合は、本製品をバージョン 11.7.0 以降にアップグレードした後に EDR Optimum 機能は自動的にアクティベートされます。追加で操作する必要はありません。

スタンドアロンの Kaspersky Endpoint Detection and Response Optimum アドオンのライセンスを使用して EDR Optimum 機能をアクティベートした場合は、EDR Optimum のライセンスが Kaspersky Security Center リポジトリに追加されていて、ライセンスの自動配信機能が有効になっていることを確認してください。本製品をバージョン 11.7.0 以降にアップグレードした後に、EDR Optimum 機能が自動的にアクティベートされます。

Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Agent をアクティベートしており、別のライセンスを使用して Kaspersky Endpoint Security for Windows をアクティベートしていた場合、Kaspersky Endpoint Security for Windows のライセンスを共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security のライセンスで置き換える必要があります。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。

4 Kaspersky Endpoint Security のインストールまたはアップグレード

製品のインストールまたはアップグレード中に EDR Optimum 機能を移行するには、リモートインストールタスクの使用を推奨します。リモートインストールタスクを作成する場合、インストールパッケージの設定で EDR Optimum コンポーネントを選択する必要があります。

次の方法で本製品をアップグレードすることもできます：

- Kaspersky Update サービスを使用する。
- クライアントデバイスのローカルで、インストールウィザードを使用する。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security をインストールする場合、コンポーネントの自動選択がサポートされます。自動選択されるコンポーネントは、本製品のアップグレードを実行するユーザーアカウントの権限により異なります。

Kaspersky Endpoint Security をシステムアカウント（SYSTEM）で EXE または MSI ファイルを使用してアップグレードする場合は、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されます。そのため、たとえばコンピューターに Kaspersky Endpoint Agent がインストールされており、EDR Optimum ソリューションがアクティベートされていた場合、Kaspersky Endpoint Security のインストーラーは自動的にコンポーネントのセットを構成して EDR Optimum コンポーネントを選択します。これにより、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。通常、システムアカウント (SYSTEM) を使用した MSI インストーラーの実行は、カスペルスキーのアップデートサービス経由または Kaspersky Security Center 経由でのインストールパッケージの配信時などに行われます。

権限のないユーザーアカウントで MSI ファイルを使用して Kaspersky Endpoint Security をアップグレードすると、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されません。この場合、Kaspersky Endpoint Security は Kaspersky Endpoint Agent 構成に基づいて、コンポーネントを選択します。それから、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

Kaspersky Endpoint Security は、コンピューターを再起動することなくアップグレードをサポートします。ポリシーのプロパティで製品のアップグレードモードを選択できます。

5. **本製品の動作の確認**

製品のインストール後またはアップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。コンポーネントのステータスが「*ライセンスに含まれていません*」となっている場合は、組み込みエージェント機能をアクティベートしていることを確認してください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows には Kaspersky Sandbox ソリューションとの連携用の組み込みエージェントが含まれるようになりました。*Sandbox* コンポーネントはコンピューター上の高度な脅威を検知し、自動的にブロックします。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。ソリューションについて詳しくは、Kaspersky Sandbox のヘルプ および Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください。

組み込みエージェントと Kaspersky Sandbox の連携

Kaspersky Sandbox コンポーネントと連携させるには、Sandbox コンポーネントを追加する必要があります。Sandbox コンポーネントは、インストール中またはアップグレード中、または*コンポーネントの変更*タスクを使用して選択できます。

この機能を使用するには、次の条件を満たす必要があります：

- Kaspersky Security Center 13.2。Kaspersky Security Center の以前のバージョンでは、脅威応答のスタンドアロンの IOC スキャンタスクの作成は許可されません。
- この機能は Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。
- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- 管理サーバーへのデータ転送が有効になっている。

Kaspersky Sandbox のすべての機能を使用するには、隔離するファイルのデータ転送が有効になっていることを確認してください。このデータは Web コンソール経由でコンピューター上で隔離されたファイルに関する情報を取得するために必要となります。たとえば、Web コンソールで分析用に隔離からファイルをダウンロードすることができます。

Web コンソールで管理サーバーへのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**KSC 連携**］に移動します。
5. ［**管理サーバーへのデータ転送**］ブロックで、［**隔離ファイルの情報**］をオンにします。
6. 変更内容を保存します。

- Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されました。

  Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Sandbox が連携するためには、 新しい保護された接続である*バックグラウンド接続*を確立する必要があります。Kaspersky Security Center とその他のカスペルスキーのソリューションとの統合について詳しくは、Kaspersky Security Center ヘルプを参照してください。

  Web コンソールとのバックグラウンド接続を確立する

  1. Web コンソールのメインウィンドウで、［**設定**］→［**連携**］の順に選択します。
  2. ［**連携**］に移動します。
  3. ［**連携用のバックグラウンド接続が［有効］です**］をオンにします。
  4. 変更内容を保存します。

  Kaspersky Security Center Web コンソールと管理サーバー間でバックグラウンド接続が確立されていない場合、脅威への対応の一部としてのスタンドアロンの IOC スキャンタスクは作成されません。

- Sandbox サーバーと信頼済み接続を設定するには、TLS 証明書を準備する必要があります。次に、ポリシーを使用してこの証明書をコンピューターに追加する必要があります。また、証明書を Sandbox サーバーに追加する必要もあります。

  > 暗号コンテナーを使用した双方向認証は、Kaspersky Sandbox では使用できません。

  コマンドラインを使用して TLS 証明書を Web コンソールまたはローカルで追加することができます。

- Kaspersky Sandbox コンポーネントが有効になっている。

- Sandbox の動作を保証する製品コンポーネントが有効になっており、動作可能である。次のコンポーネントが Sandbox の動作を確保するために必要となります：
  - ファイル脅威対策
  - ホスト侵入防止
  - ファイアウォール
  - AMSI 保護
  - バックグラウンドスキャン

Kaspersky Sandbox との連携を有効または無効にするには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Sandbox**］に移動します。
5. ［**Sandbox との連携は有効です**］トグルスイッチを使用して機能を有効または無効にします。
6. ［**連携モード**］ブロックで、機能の操作モードを選択します：**Kaspersky Sandbox**。
7. ［**接続設定**］リンクをクリックします。
   Sandbox サーバーの接続設定ウィンドウが表示されます。
8. ［**サーバー TLS 証明書**］ブロックで、［**アップロード**］を選択して TLS 証明書ファイルを選択します。
   Kaspersky Endpoint Security は、1 つの Sandbox サーバーに対して 1 つの TLS 証明書のみ持つことができます。以前に TLS 証明書を追加していた場合、その証明書は取り消されます。一番新しい証明書が使用されます。
9. Sandbox サーバーの詳細な接続設定を行います。
   - **タイムアウト（ミリ秒）**：Sandbox サーバーの接続タイムアウトです。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、サーバーの接続タイムアウトの時間を長くすることができます。要求のタイムアウトは 0.5 秒以下を推奨します。
   - **要求のキュー**：要求のキューフォルダーのサイズです。Sandbox でスキャンするために複数のオブジェクトを送信する場合、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは 100 MB に制限されています。最大サイズに到達すると、Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。
10. ［**Sandbox サーバーへの接続**］ブロックの［**追加**］をクリックします。

11. 表示されるウィンドウで、Sandbox のサーバーのアドレス（IPv4、IPv6、DNS）およびポートを入力します。

    仮想イメージの配備と Sandbox サーバーの設定について詳しくは、Kaspersky Sandbox のヘルプを参照してください。

12. 変更内容を保存します。

TLS 証明書が検証されます。証明書の検証が正常に完了すると、Kaspersky Endpoint Security は次回の Kaspersky Security Center との同期の際に証明書をコンピューターに送信します。2 つの TLS 証明書を追加した場合、Kaspersky Sandbox は新しいほうの証明書を使用して信頼済み接続を確立します。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Sandbox**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

コマンドラインを使用して、Web コンソールまたはローカルで Kaspersky Sandbox との連携を有効または無効にすることができます。

Kaspersky Endpoint Security は Kaspersky Sandbox コンポーネントの動作に関する情報をレポートに保存します。レポートにはエラーに関する情報も記録されます。「`Error code: XXX`」という形式のエラー（例：`0xa67b01f4`）が表示された場合は、テクニカルサポートにお問い合わせください。

セキュリティ侵害インジケーターのスキャン（スタンドアロンタスク）

*セキュリティ侵害インジケーター（IOC）*とは、コンピューターへの認証されないアクセス（コンピューターの侵害）の痕跡を示すオブジェクトまたは活動に関する一連のデータです。たとえば、システムへのログインを複数回失敗すると、セキュリティ侵害インジケーターの構成要素となります。*IOC スキャンタスク*は、コンピューターのセキュリティ侵害インジケーターを検索し、脅威への対応方法を確立するのに役立ちます。

Kaspersky Endpoint Security は IOC ファイルを使用して侵害インジケーターを検索します。*IOC ファイル*は、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。IOC ファイルは OpenIOC 標準に準拠している必要があります。Kaspersky Endpoint Security は自動的に Kaspersky Sandbox 向けの IOC ファイルを作成します。

IOC スキャンタスクの実行モード

Kaspersky Sandbox 向けのスタンドアロンの IOC スキャンタスクが作成されます。*スタンドアロンの IOC スキャンタスク*は、Kaspersky Sandbox で検知された脅威に到達した際に自動的に作成されるタスクのグループです。Kaspersky Endpoint Security は IOC ファイルを自動で作成します。カスタム IOC ファイルはサポートされていません。タスクは作成されてから 30 日が経過すると自動的に削除されます。スタンドアロンの IOC スキャンタスクについて詳しくは、Kaspersky Sandbox のヘルプを参照してください。

［IOC スキャン］タスクの設定

脅威への対応時に、Kaspersky Sandbox が *IOC* スキャンタスクを自動で作成および実行することがあります。

Web コンソールでのみ設定できます。

Kaspersky Sandbox のスタンドアロンの IOC スキャンタスクには Kaspersky Security Center 13.2 が必要です。

IOC スキャンタスクの設定を変更するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. Kaspersky Endpoint Security の **IOC スキャン**タスクを選択します。
   タスクのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**IOC スキャン設定**］に移動します。
5. IOC 検知時の動作の設定：
   - **コピーを隔離に移動し、オブジェクトを削除する**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。
   - **簡易スキャンを実行する**：このオプションを選択した場合、Kaspersky Endpoint Security は*簡易スキャン*タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。
   - **コンピューターを使用していないときにのみ実行する**：コンピューターのリソースの負荷が高い場合にタスクの開始を延期します。スクリーンセーバーの実行中またはコンピューターのロック時にのみ、スケジュールされたスキャンが実行されます。タスクの実行をコンピューターのロック解除などで中断した場合、Kaspersky Endpoint Security はタスクが中断された時点から自動でタスクを実行します。このスケジュールのオプションを使用して、コンピューター使用時のリソース消費量を抑えることができます。
6. 変更内容を保存します。

［**履歴**］のタスクのプロパティでタスクの結果を確認できます。［**アプリケーション設定**］→［**IOC スキャン結果**］の順に選択して、タスクのプロパティで侵害インジケーターに関する情報を表示することができます。

IOC スキャン結果は 30 日間保持されます。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータを自動的に削除します。

Kaspersky Sandbox の KEA から KES への移行ガイド

Kaspersky Endpoint Security for Windows には Kaspersky Sandbox ソリューション向けの組み込みエージェントが含まれるようになりました。Kaspersky Sandbox と連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security を導入する場合は、Kaspersky Sandbox ソリューションと Kaspersky Endpoint Security は継続して連携します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Security をバージョン 11.7.0 以降にアップデートすると、システムで同じ動作が発生します。

Kaspersky Endpoint Security は Kaspersky Endpoint Agent と互換性はありません。同じコンピューターにこれらの製品の両方をインストールすることはできません。

Kaspersky Endpoint Security が Kaspersky Sandbox の一部として機能するには、次の条件を満たしている必要があります：

- Kaspersky Sandbox のバージョンが 2.0 以降である。
- Kaspersky Security Center のバージョンが 13.2 以降である (ネットワークエージェントを含む)。以前のバージョンの Kaspersky Security Center では、Kaspersky Sandbox 機能をアクティベートすることはできません。
- Kaspersky Sandbox は、Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。
- 管理サーバーへのデータ転送が有効になっている。このデータは Web コンソール経由でコンピューター上で隔離されたファイルに関する情報を取得するために必要となります。
- Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されている。Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Sandbox が連携するためには、 新しい保護された接続である*バックグラウンド接続*を確立する必要があります。

Kaspersky Sandbox で［KES + KEA］設定から［KES + 組み込みエージェント］に移行する手順

1. **Kaspersky Endpoint Security Web プラグインのアップグレード**

   Kaspersky Sandbox コンポーネントは、Kaspersky Endpoint Security の Web プラグインのバージョン 11.7.0 以降を使用して管理できます。

2. **ポリシーおよびタスクの移行**

   Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。そのためには、Web コンソールの Kaspersky Endpoint Agent からの移行ウィザードを使用します。

   Web コンソールで Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行する方法

   Web コンソールのメインウィンドウで、［**操作**］→［**Kaspersky Endpoint Agent からの移行**］の順に選択します。

ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

ステップ1：ポリシーの移行

移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Agent のポリシーをクリックして、設定を統合する Kaspersky Endpoint Security のポリシーを選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

ステップ2：タスクの移行

移行ウィザードが Kaspersky Endpoint Security 向けの新しいタスクを作成します。タスクのリストで、Kaspersky Endpoint Security のポリシー向けに作成する Kaspersky Endpoint Agent のタスクを選択します。次の手順に進みます。

ステップ3：ウィザードの完了

ウィザードを終了します。ウィザードは以下の処理を実行します：

- 新規の Kaspersky Endpoint Security のポリシーを作成する

  ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには *<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>* という名前が付けられます。新しいポリシーのステータスは*非アクティブ*になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ*非アクティブ*にして、新しく統合されたポリシーを有効にします。

  > Kaspersky Endpoint Agent から Kaspersky Endpoint Security for Windows への移行後、新しいポリシーに管理サーバーへのデータ転送機能（隔離されたファイルのデータと脅威の活動連鎖のデータ）が設定されていることを確認してください。データ転送のパラメータ値は Kaspersky Endpoint Agent ポリシーからは移行されません。

- 新規の Kaspersky Endpoint Security のタスクを作成する

  新しいタスクは、Kaspersky Endpoint Agent のタスクのコピーです。同時に、ウィザードは Kaspersky Endpoint Agent タスクには変更を加えません。

3 Kaspersky Sandbox 機能のライセンス管理

Kaspersky Sandbox ソリューションの一部として Kaspersky Endpoint Security をアクティベートするには、Kaspersky Sandbox のアドオンの個別のライセンスが必要です。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。結果として、*Kaspersky Endpoint Security* および *Kaspersky Sandbox* の 2 種類のライセンスがアプリケーションに追加されることになります。

4 Kaspersky Endpoint Security のインストールまたはアップグレード

製品のインストールまたはアップグレード中に Kaspersky Sandbox 機能を移行するには、リモートインストールタスクの使用を推奨します。リモートインストールタスクを作成する場合、インストールパッケージの設定で Kaspersky Sandbox コンポーネントを選択する必要があります。

次の方法で本製品をアップグレードすることもできます：

- Kaspersky Update サービスを使用する。
- クライアントデバイスのローカルで、インストールウィザードを使用する。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security をインストールする場合、コンポーネントの自動選択がサポートされます。自動選択されるコンポーネントは、本製品のアップグレードを実行するユーザーアカウントの権限により異なります。

Kaspersky Endpoint Security をシステムアカウント（SYSTEM）で EXE または MSI ファイルを使用してアップグレードする場合は、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されます。そのため、たとえばコンピューターに Kaspersky Endpoint Agent がインストールされており、Kaspersky Sandbox ソリューションがアクティベートされていた場合、Kaspersky Endpoint Security のインストーラーは自動的にコンポーネントのセットを構成して Kaspersky Sandbox コンポーネントを選択します。これにより、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。通常、システムアカウント (SYSTEM) を使用した MSI インストーラーの実行は、カスペルスキーのアップデートサービス経由または Kaspersky Security Center 経由でのインストールパッケージの配信時などに行われます。

権限のないユーザーアカウントで MSI ファイルを使用して Kaspersky Endpoint Security をアップグレードすると、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されません。この場合、Kaspersky Endpoint Security は Kaspersky Endpoint Agent 構成に基づいて、コンポーネントを選択します。それから、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

Kaspersky Endpoint Security は、コンピューターを再起動することなくアップグレードをサポートします。ポリシーのプロパティで製品のアップグレードモードを選択できます。

5 本製品の動作の確認

製品のインストール後またはアップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。コンポーネントのステータスが「*ライセンスに含まれていません*」となっている場合は、組み込みエージェント機能をアクティベートしていることを確認してください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security for Windows は、Kaspersky Anti Targeted Attack Platform (EDR (KATA)) ソリューションとの連携をサポートしています。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。本製品には、EDR、NDR コンポーネント用の組み込みエージェントが含まれています。本製品は、KATA の一部である Sandbox コンポーネントとの連携もサポートします。

脅威インテリジェンスツール

Kaspersky Endpoint Detection and Response は次の脅威インテリジェンスツールを使用します。

- Kaspersky Threat Intelligence Portal との連携。ファイルや Web アドレスの評価に関する情報を蓄積し、表示できます。
- Kaspersky Threats データベース。
- Kaspersky Security Network（以下、「KSN」とも表記）。クラウドサービスのインフラストラクチャで、カスペルスキーの情報基盤に基づいたリアルタイムのファイル、Web サイト、ソフトウェアの評価情報を提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。

ソリューションの動作原理

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリデータ）は Kaspersky Anti Targeted Attack Platform サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検出した脅威に関する情報およびその脅威の処理結果についての情報を Kaspersky Anti Targeted Attack Platform サーバーに 送信します。

EDR (KATA) および NDR (KATA) 連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Kaspersky Anti Targeted Attack Platform コンソールを使用して管理されるようになります。

EDR / NDR (KATA) 連携のための Kaspersky Endpoint Security の設定

EDR / NDR (KATA) と連携するには、以下の設定を使用できます：

- **[KES + 組み込みエージェント]**：この設定において、Kaspersky Endpoint Security は、コンピューターのセキュリティを確保するアプリケーションと EDR / NDR (KATA) を操作するアプリケーションの両方の役割を果たします。EDR (KATA) の組み込みエージェントは、Kaspersky Endpoint Security 12.1 for Windows 以降で使用できます。NDR (KATA) の組み込みエージェントは、Kaspersky Endpoint Security 12.7 for Windows 以降で使用できます。

- **[サードパーティ製 EPP+EDR エージェント]**.この設定において、IT インフラストラクチャのセキュリティはサードパーティエンドポイント保護プラットフォーム（EPP）によって確保されます。EDR / NDR (KATA) との連携は、Kaspersky Endpoint Security の Endpoint Detection and Response Agent (EDR Agent) の設定で提供されます。この設定において、EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。EDR (KATA) の EDR Agent は、Kaspersky Endpoint Security 12.3 for Windows 以降で使用できます。NDR (KATA) の EDR Agent は、Kaspersky Endpoint Security 12.7 for Windows 以降で使用できます。

Kaspersky Endpoint Security の旧バージョン向けサポート

Kaspersky Endpoint Security 11.2.0～11.8.0 を Kaspersky Anti Targeted Attack Platform (EDR) との連携に使用している場合は、製品には Kaspersky Endpoint Agent が含まれます。Kaspersky Endpoint Security のインストール中に並行して Kaspersky Endpoint Agent をインストールできます。

Kaspersky Endpoint Security 11.9.0 から Kaspersky Endpoint Security の配信キットには Kaspersky Endpoint Agent の配布パッケージが含まれなくなったため、Kaspersky Endpoint Security 11.9.0～12.0 を使用している場合、Kaspersky Endpoint Agent を個別にインストールする必要があります。

組み込みエージェントと EDR / NDR (KATA) の連携

EDR / NDR (KATA) との連携には、次の関連コンポーネントを追加する必要があります：Endpoint Detection and Response (KATA) または Network Detection and Response (KATA)。EDR / NDR (KATA) との連携用コンポーネントは、本製品のインストール中またはアップグレード中に選択するか、*コンポーネントの変更*タスクを使用して選択することができます。

Kaspersky Endpoint Security for Windows のバージョン 12.11 以降、EDR (KATA) コンポーネントの名前が **Endpoint Detection and Response Expert（バージョン 8.0 以降）** に変更されました。本製品の本バージョンでは、コンポーネントは Kaspersky Anti Targeted Attack Platform 7.1 以前のバージョン、および Kaspersky Endpoint Detection and Response Expert（オンプレミス）と互換性があります。

EDR Optimum、EDR Expert および EDR (KATA) コンポーネント間には互換性はありません。

EDR / NDR (KATA) を使用するには、次の条件を満たす必要があります：

- EDR (KATA)：Kaspersky Anti Targeted Attack Platform のバージョンが 5.0 ～ 7.1 である。

- NDR (KATA)：Kaspersky Anti Targeted Attack Platform のバージョンが 7.0 以降である。

- EDR (KATA)：Kaspersky Endpoint Security for Windows 12.1 以降である。KATA の Kaspersky Endpoint Security の各種バージョンとの対応について詳しくは、Kaspersky Anti Targeted Attack Platform ヘルプを参照してください。
- NDR (KATA)：Kaspersky Endpoint Security for Windows 12.7 以降である。
- Kaspersky Security Center のバージョンが 14.2 以降である。以前のバージョンの Kaspersky Security Center では、EDR / NDR (KATA) 機能をアクティベートすることはできません。
- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- Endpoint Detection and Response (KATA) および Network Detection and Response (KATA) コンポーネントが有効になっている。
- EDR/NDR (KATA) の動作を保証する製品コンポーネントが有効になっており、動作可能である。次のコンポーネントが EDR / NDR (KATA) の動作を確保するために必要となります：
  - ファイル脅威対策
  - ウェブ脅威対策
  - メール脅威対策
  - 脆弱性攻撃ブロック
  - ふるまい検知
  - ホスト侵入防止
  - AMSI 保護
  - バックグラウンドスキャン
  - Kaspersky Security Network

Endpoint Detection and Response (KATA) とは次の手順で連携されます：

1. **Endpoint Detection and Response (KATA) および Network Detection and Response (KATA) コンポーネントのインストール**

   EDR (KATA) および NDR (KATA) コンポーネントは、インストール中またはアップグレード中、または*コンポーネントの変更*タスクを使用して選択できます。

   > 新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2. **Endpoint Detection and Response (KATA) と Network Detection and Response (KATA) のアクティベーション**

   EDR (KATA) および NDR (KATA) (たとえば、Kaspersky Endpoint Detection and Response (KATA) アドオン) の個別ライセンスを購入する必要があります。

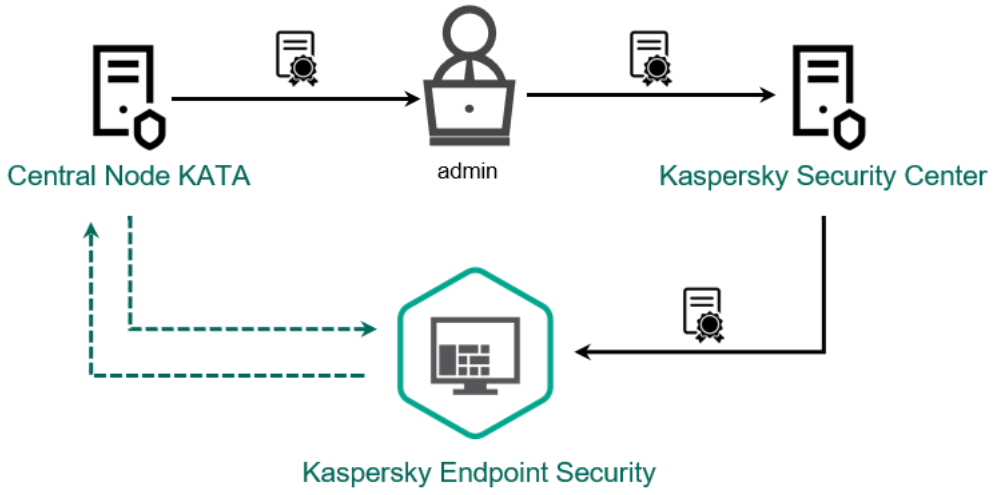
   この機能は、EDR (KATA) および NDR (KATA) 機能をカバーする別のライセンスを追加した後に使用可能になります。結果として、Kaspersky Endpoint Security のライセンスと、Kaspersky Endpoint Detection and Response (KATA) および Network Detection and Response (KATA) のライセンスという複数のライセンスがコンピューターに追加されることになります。

スタンドアロンの EDR (KATA) および NDR (KATA) 機能のライセンス認証は、Kaspersky Endpoint Security のライセンス認証と同じです。

EDR (KATA) と NDR (KATA) の両方の機能がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

3 Central Node への接続

Kaspersky Anti Targeted Attack Platform では、Kaspersky Endpoint Security と Central Node コンポーネント間に信頼済みの接続を確立する必要があります。信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。



TLS 証明書の Kaspersky Endpoint Security への追加

既定では、Kaspersky Endpoint Security は Central Node の TLS 証明書のみを確認します。接続の安全性をより高めるには、追加で Central Node のコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、Central Node および Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

管理コンソール（MMC）を使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、**Detection and Response** を選択し、設定するコンポーネントを選択します：**Endpoint Detection and Response Expert（オンプレミス）** または **Network Detection and Response (KATA)**。
5. 対応するチェックボックスをオンにします：**Endpoint Detection and Response Expert（バージョン 7.1 以前）** または **Network Detection and Response (KATA)**。
6. ［**サーバーの接続設定**］をクリックします。

7. サーバー接続を設定します：

   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。

   - **サーバー TLS 証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

   - **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

     暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

8. ［**OK**］をクリックします。

9. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

   複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

10. 必要に応じて、テレメトリを設定してください。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールを使用して Kaspersky Endpoint Security 端末を Central Node に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**組み込みエージェントの設定**］セクションに移動し、設定するコンポーネントを選択します：**Endpoint Detection and Response Expert（オンプレミス）** または **Network Detection and Response (KATA)**。

5. 対応するスイッチをオンにします：**Endpoint Detection and Response Expert（オンプレミス）が有効です** または **Network Detection and Response (KATA) は有効です**。

6. EDR (KATA) を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 7.1 以前）**］を選択します。

7. ［**接続設定**］をクリックします。

8. サーバー接続を設定します：

   - **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。

   - **サーバー証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。

   - **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

     暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

9. ［**OK**］をクリックします。

10. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

    複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

11. 必要に応じて、テレメトリを設定してください。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

コマンドラインを使用して TLS 証明書をローカルで追加することもできます。

コンピューターが Kaspersky Anti Targeted Attack Platform コンソールに追加されます。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Endpoint Detection and Response Expert（バージョン 8.0 以降）**］および［**Network Detection and Response (KATA)**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

Kaspersky Security Center コンソールでは、コンピューターのプロパティの［**コンポーネント**］セクションでコンポーネントの状態を確認できます。コンソールでコンポーネントのステータスを確認する際は、次の点に留意してください：コンポーネントがインストールされておらず、機能がライセンスに含まれていない場合は、コンソールには［**未インストール**］ではなく［**ライセンスでサポートされていません**］のステータスが表示されます。

Kaspersky Endpoint Security 12.6 for Windows から、Kaspersky Security Center 管理コンソール（MMC）で EDR (KATA) コンポーネントのステータスを監視できるようになりました。コンポーネントの現在のステータスは、［**Endpoint Sensor ステータス**］列のコンピュータープロパティに表示されます（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）。Web コンソールに Endpoint Sensor のステータスは表示されません。

EDR (KATA) テレメトリの設定

*テレメトリ*とは、保護対象コンピューター上で発生したイベントのリストです。Kaspersky Endpoint Security はテレメトリデータを分析し、同期中に Kaspersky Anti Targeted Attack Platform へ送信します。テレメトリイベントはほぼ継続的にサーバーに届きます。次の条件のいずれかが満たされると、Kaspersky Endpoint Security はサーバーとの同期を開始します。

- 同期間隔が経過した。
- バッファ内のイベント数が上限を超えた。

既定では、本製品は 30 分間隔またはバッファ内のイベントが 1024 件に達すると同期します。同期については Kaspersky Endpoint Security のポリシーで設定できるので、ネットワーク負荷に応じて最適な値を選択することができます（以下の手順を参照）。

Kaspersky Endpoint Security とサーバー間に接続がない場合は、本製品は新しいイベントをキューに入れます。接続が復元されると、Kaspersky Endpoint Security はキューのイベントを順にサーバーに送信します。サーバーの過負荷を避けるため、イベントの一部がスキップされることがあります。イベント転送設定で、1 時間ごとの最大イベントを設定するなどしてイベント転送を最適化することができます（以下の手順を参照）。

テレメトリを使用する別のソリューションとあわせて Kaspersky Anti Targeted Attack Platform を使用している場合は、KATA (EDR) 向けのテレメトリをオフにすることができます（以下の説明を参照してください）。これにより、これらのソリューションのサーバー負荷を最適化することができます。例えば、Managed Detection and Response ソリューションと KATA (EDR) を導入している場合、MDR テレメトリを使用して KATA (EDR) で脅威応答タスクを作成することができます。

管理コンソール（MMC）で テレメトリを設定する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、**Detection and Response** を選択し、設定するコンポーネントを選択します：**Endpoint Detection and Response Expert（オンプレミス）** または **Network Detection and Response (KATA)**。
5. ［**KATA サーバーに同期リクエストを送信する間隔（分）**］を設定します。サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。
6. ［**KATA にテレメトリを送信する**］がオンになっていることを確認してください。
7. 必要に応じて、［**データ転送設定**］ブロックで、サーバー設定との同期を設定します：
   - **最大イベント転送遅延時間（秒）**：指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。
   - **イベントパッケージの最大数**：バッファがイベントでいっぱいになると、本製品はサーバーと同期します。既定値は 1024 イベントです。

8. 必要に応じて、［**リクエストの調整**］ブロックの［**リクエストの調整を有効にする**］をオンにします。

   これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。

9. サーバーへのイベント送信の最適化を設定します：

   - **1 時間ごとのイベントの最大数**：本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1 時間後にイベントの送信は再開されます。1 時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を 1 時間あたり 60,000 イベントに増やすことを推奨します。

   - **イベントの制限超過のパーセンテージ**：本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールで テレメトリを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（オンプレミス）**］に移動します。

5. EDR (KATA) を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 7.1 以前）**］を選択します。

6. ［**データ転送設定**］ブロックで［**KATA サーバーにテレメトリを送信する**］がオンになっていることを確認します。

7. ［**サーバーに同期リクエストを送信する間隔（分）**］を設定します。サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。

8. ［**KATA サーバーにテレメトリを送信する**］がオンになっていることを確認してください。

9. 必要に応じて、［**データ転送設定**］ブロックで、サーバー設定との同期を設定します：

   - **最大イベント転送遅延時間（秒）**：指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。

   - **イベントパッケージの最大数**：バッファがイベントでいっぱいになると、本製品はサーバーと同期します。既定値は 1024 イベントです。

10. 必要に応じて、［**リクエストの調整**］ブロックの［**リクエストの調整を有効にする**］をオンにします。

    これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。

11. サーバーへのイベント送信の最適化を設定します：

    - **1 時間ごとのイベントの最大数**：本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1 時間後にイベントの送信は再開されます。1 時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を 1 時間あたり 60,000 イベントに増やすことを推奨します。

    - **イベントの制限超過のパーセンテージ**：本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**KATA 連携**］→［**製品利用統計情報収集（テレメトリ）の除外リスト**］セクションの順に選択します。

5. ［**データ転送設定**］で、［**除外リストを使用する**］をオンにします。

6. ［**追加**］をクリックして除外リストを設定します：

   条件は「*AND.*」で結合できます。

   - **パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。除外リストが機能するには、ファイルのパスを指定する必要があります。

   - **コマンドライン**：オブジェクトを実行するために使用されるコマンド。

   - **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。
     VersionInfo リソースについて詳しくは、Microsoft の Web サイトの情報を参照してください。

   - **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。

   - **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。

   - **MD5**：ファイルの MD5 ハッシュ。

- **SHA256**：ファイルの SHA256 ハッシュ。
- **イベント種別**：除外リストが機能するには、少なくとも 1 つのイベント種別を指定する必要があります。

7. 変更内容を保存します。

1. Kaspersky Security Center の管理コンソールツリーで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

ステップ 1：タスク種別の選択

1. ［**Kaspersky Endpoint Security for Windows (12.12)**］→［**アップデートのロールバック**］の順に選択します。

ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

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

ステップ 3：タスク開始スケジュールの設定

タスクのスケジュールを設定します（たとえば、［手動］など）。

ステップ 4：タスク名の定義

タスクの名前を入力します。

ステップ7：タスク作成の完了

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

EDR (KATA) テレメトリの除外リスト

パフォーマンスを向上させ、テレメトリサーバーへのデータ送信を最適化するために、テレメトリの除外リストを設定できます。たとえば、個々のアプリケーションのネットワーク通信データを送信しないように選択できます。

管理コンソール（MMC）でテレメトリの除外リストを作成する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
4. ［**テレメトリの設定**］→［**EDR (KATA) / NDR (KATA) のテレメトリ**］ブロックの［**設定**］をクリックします。
5. 開いたウィンドウで、テレメトリの除外リストを設定します（下の表を参照）。

   本製品は、除外条件を論理 AND と組み合わせます。ルールを作成するには、［**完全パス**］フィールドで値を指定して、［**次のイベント種別に使用する**］リストでイベント種別を少なくとも1つ選択します。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールでテレメトリの除外リストを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**テレメトリの設定**］に移動します。
5. ［**EDR (KATA) / NDR (KATA) のテレメトリ**］タブを選択します。
6. 開いたウィンドウで、テレメトリの除外リストを設定します（下の表を参照）。

   本製品は、除外条件を論理 AND と組み合わせます。ルールを作成するには、［**完全パス**］フィールドで値を指定して、イベント種別を少なくとも1つ選択します。
7. 変更内容を保存します。

パラメータ	説明
除外されるプロセス	**送信するテレメトリのサイズを最適化**：Kaspersky Endpoint Security では、Microsoft SMB プロトコル、WinRM サービス、およびネットワークエージェントの klnagent.exe プロセスについて、データの送信量を最適化したり、コードが 102（基本的な通信）および 8（プロセスのネットワークアクティビティ）のイベントをテレメトリから除外できます。また、すべての種類のネットワークプロトコルについて、ネットワークパケットの種類に関する拡張情報を最適化できます。 Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **次のイベント種別に使用する**： • **ファイルの変更** • **ネットワークイベント** • **プロセス：コンソールでの対話的入力** • **モジュールの読み込み** • **レジストリの変更** • **DNS ログ** • **プロセスへのアクセス** • **コード埋め込み** • **WMI クエリ** • **パイプ** • LDAP • AMSI
除外されるネットワークコミュニケーション	**ルール名** **通信方向** **プロトコル** **生ソケット** **プロトコル番号** **TLS 証明書** **ローカルポートまたは範囲** **リモートポートまたは範囲** **ローカルアドレス**：Kaspersky Endpoint Security がネットワークトラフィックからテレメトリを除外するコンピューターのネットワークアドレス。 **リモートアドレス**：Kaspersky Endpoint Security がネットワークトラフィックからテレメトリを除外するコンピューターのネットワークアドレス。 IP アドレスでは IPv4 形式のみがサポートされます。 **アプリケーション**：Kaspersky Endpoint Security がネットワークトラフィックから EDR テレメトリを除外しているアプリケーションの実行ファイルのリスト。

パラメータ	説明
除外されるファイル操作	**ルール名** **ファイル名またはマスク**：ファイルまたはフォルダーの名前またはマスク。Kaspersky Endpoint Security は、このファイルまたはフォルダーにアクセスがあると除外ルールを適用します。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。 **操作種別** **以前のパス** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。
除外されるDNS 操作	**ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 DNS： • **DNS サーバー IP アドレス** • **クエリオプション** • **ステータス** • **ドメイン名** • **設定種別 ID** • **応答データ**

パラメータ	説明
除外されるLDAP 操作	**ルール名** **LDAP 検索範囲** **フィルター** **LDAP オブジェクト検索用の識別名** **オブジェクトの属性** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。
除外されるプロセスのアクセスクエリ	**ルール名** **操作種別** **要求されたプロセスへのアクセス** **コールスタックトレース** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**、**親プロセス**、**ターゲットプロセス**、**ソースプロセスのファイル**：および**ターゲットプロセスのファイル**。 • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **このルールを使用するルールの適用条件とイベント種別を指定してください**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。

パラメータ	説明
除外されるコード埋め込み	**ルール名** **アクセス方法** **コールスタック** **変更されたコマンドライン** **埋め込みアドレス** **挿入された DLL 名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。
除外されるWMI クエリ	**ルール名** **WMI 操作種別** **リモートクエリ** **WMI コマンドを実行したコンピューターの名前** **WMI ユーザーアカウント** **実行された WMI コマンド** **WMI 名前空間** **WMI イベントコンシューマーフィルター** **作成した WMI イベントコンシューマーの名前** **WMI イベントコンシューマーのソースコード** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。

パラメータ	説明
除外されるパイプ操作	**ルール名** **パイプの名前** **操作種別** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。
除外されるレジストリ変更	**ルール名** **操作種別** **パス** **値の名前** **値** **レジストリファイルの完全名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**：および**親プロセス**： • **完全パス**：名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**：ファイルを実行するために使用されるコマンド。 • **説明**：RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**：RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**：RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**：MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。
除外されるデバイスの操作	**ルール名** **デバイス種別** **デバイス ID** **デバイス名**

例 1。除外されるプロセス

サードパーティの製品（プロセス）のイベントをテレメトリから除外するには、[**除外されるプロセス**] タブの EDR テレメトリ除外リストのウィンドウを開き、製品の実行ファイルを追加します。

Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。

Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。例：

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



プロセスの除外

例 1。ファイルの変更

Notepad++ アプリケーションでスクリプトを頻繁に変更しており、対応するスクリプトの変更イベントを除外したい場合は、 Notepad++ の実行ファイルをテレメトリの除外リストに追加します。

次のように設定します。

- **完全パス**：`C:\Program Files\Notepad++\notepad++.exe`
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34
- **次のイベント種別に使用する**：ファイルの変更

例 2。ネットワークイベント

リモートサーバー上のファイルを管理するために WinSCP アプリケーションを使用している場合にネットワークイベントを除外したい場合は、WinSCP の実行ファイルをテレメトリの除外リストに追加します。

次のように設定します。

- **完全パス**：`C:\Program Files (x86)\WinSCP\WinSCP.exe`
- **SHA256**：47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74（任意）
- **次のイベント種別に使用する**：ネットワークイベント

例 2。除外されるネットワークコミュニケーション

テレメトリからリモートサービス接続イベントを除外するには、[**除外されるネットワークコミュニケーション**] タブで EDR テレメトリの除外リストのウィンドウを開き、接続設定（プロトコル、ポート、方向、IP アドレス、TLS 証明書など）を追加します。

Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。

サブネットアドレス（例：10.28.0.0/24）を指定することはできません。本製品では、1 つの IP アドレス（例：10.28.0.105）のみを指定できます。



ネットワークコミュニケーションの除外

企業の Web サーバーを使用しており、その Web サーバーに接続する際のブラウザーのイベントを除外する場合は、サーバーの IP アドレスとブラウザーの実行ファイルをテレメトリの除外リストに追加します。

次のように設定します。

- **プロトコル**：TCP
- **リモートポートまたは範囲**：443
- **リモートアドレス**：10.28.0.105
- **アプリケーション**：`C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`、`C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`

例 3。除外されるファイル操作

信頼するファイル操作に関連するイベントをテレメトリから除外するには、[**除外されるファイル操作**] タブで EDR テレメトリの除外リストのウィンドウを開いて、信頼するファイルを追加します。

Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。



ファイル操作の除外

アプリケーションがログに書き込み、このログファイルの変更イベントを除外する場合は、テレメトリからアプリケーションのログファイルと実行ファイルを追加します。

次のように設定します。

- **ファイル名またはマスク**：`C:\Apache24\logs\error.log`
- **操作種別**：ファイルの変更
- **完全パス**：`C:\Apache24\bin\httpd.exe`
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

例 4。除外されるレジストリ変更

レジストリ変更イベントをテレメトリから除外するには、[**除外されるレジストリ変更**] タブで EDR テレメトリの除外リストのウィンドウを開いて、レジストリキーを追加します。

Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。

アプリケーションがレジストリ値を頻繁に変更し、これらのレジストリ変更イベントをテレメトリから除外する場合は、アプリケーションのレジストリキーと実行ファイルをテレメトリの除外に追加します。

次のように設定します。

- **操作種別**：変更
- **パス**：HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64
- **完全パス**：`C:\Program Files\PuTTY\putty.exe`
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

KATA Sandbox

Kaspersky Anti Targeted Attack Platform には、Sandbox (KATA Sandbox) コンポーネントが含まれています。*Sandbox* はコンピューター上のより高度な脅威を検知する技術です。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

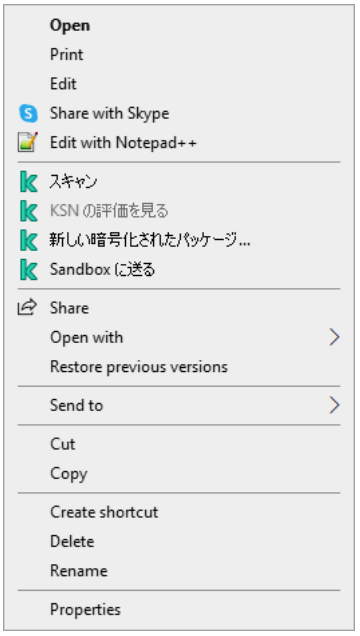
KATA Sandbox をアクティベートするには、KATA または KEDR 機能を含むライセンスが必要です。使用可能な機能について詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

KATA Sandbox では、次のモードでファイルをスキャンできます：

- *手動*.ユーザーはコンテキストメニューから手動でスキャン用ファイルを送信します（[**Sandbox に送る**]）。ファイルを Sandbox に送る時に、本製品は定義データベースを使用してファイルをスキャンします。
- *自動*.本製品はオブジェクトを自動的に検知し、スキャンのために Sandbox に送信します。

ファイルが Sandbox に送られた後も、ユーザーはそのファイルに引き続きアクセスできます。Kaspersky Endpoint Security は対応するイベントを記録し、そのイベントを Kaspersky Security Center と Kaspersky Anti Targeted Attack Platform コンソールに送信します。Sandbox が悪意のあるアクティビティを検知した場合、Kaspersky Endpoint Security は Threat Response 処理を自動的に実行します（たとえば、オブジェクトを削除し、簡易スキャンを開始します）。

KATA Sandbox を手動モードで動作させるには、Kaspersky Anti Targeted Attack Platform 7.0 以降を導入する必要があります。KATA Sandbox を自動モードで動作させるには、Kaspersky Anti Targeted Attack Platform 8.0 以降を導入する必要があります。



KATA Sandbox でのコンテキストメニューからのスキャン

組み込みエージェントと KATA Sandbox の連携

KATA Sandbox コンポーネントと連携するには、Sandbox コンポーネントを追加する必要があります。Sandbox コンポーネントは、インストール中またはアップグレード中、または*コンポーネントの変更*タスクを使用して選択できます。

スキャン用にファイルを送信するには、KATA Sandbox との統合を有効にし、ソリューション内に導入されている Central Node サーバーを追加する必要があります。この機能は Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。

KATA Sandbox との連携を有効または無効にするには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Sandbox**］に移動します。

5. ［**Sandbox との連携は有効です**］トグルスイッチを使用して機能を有効または無効にします。

6. KATA Sandbox の動作モードを選択します：

   - **手動**：ユーザーはコンテキストメニューから手動でスキャン用ファイルを送信します（［**Sandbox に送る**］）。
   - **自動**：本製品はオブジェクトを自動的に検知し、スキャンのために Sandbox に送信します。
   - **複合**

7. ［**接続設定**］リンクをクリックします。

8. Central Node サーバーの接続を設定します：

   - **タイムアウト（ミリ秒）**：Central Node サーバーの接続タイムアウトです。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、サーバーの接続タイムアウトの時間を長くすることができます。要求のタイムアウトは 0.5 秒以下を推奨します。
   - **要求のキュー**：要求のキューフォルダーのサイズです。Sandbox でスキャンするために複数のオブジェクトを送信する場合、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは 100 MB に制限されています。最大サイズに到達すると、Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。
   - **サーバー TLS 証明書**：Central Node サーバーと信頼済み接続を設定するには、TLS 証明書を準備する必要があります。次に、ポリシーを使用してこの証明書をコンピューターに追加する必要があります。また、証明書を Central Node サーバーに追加する必要もあります。
   - **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

9. ［**Sandbox サーバーへの接続**］ブロックの［**追加**］をクリックします。

10. 表示されるウィンドウで、Central Node のサーバーのアドレス（IPv4、IPv6、DNS）およびポートを入力します。

    仮想イメージの配備と Central Node サーバーの設定について詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

Sandbox コンポーネントが有効になりました。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Sandbox**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

Threat Response 処理の設定

Sandbox が悪意のあるアクティビティを検知した場合、Kaspersky Endpoint Security は Threat Response 処理を自動的に実行します（たとえば、オブジェクトを削除し、簡易スキャンを開始します）。

Threat Response 処理を設定するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Sandbox**］に移動します。
5. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。
   - **コピーを隔離に移動し、オブジェクトを削除する**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。
   - **簡易スキャンを実行する**：このオプションを選択した場合、Kaspersky Endpoint Security は*簡易スキャン*タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。
   - **IOC スキャンタスクを作成する**：このオプションを選択した場合、Kaspersky Endpoint Security は自動的に *IOC スキャン*（*自動 IOC スキャンタスク*）を作成します。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、簡易スキャンタスクの実行）を設定できます。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、*簡易スキャンタスク*の実行）を設定できます。その他の *IOC スキャンタスク*の設定を変更するには、タスクの設定に移動してください。
6. 必要に応じて、［**IOC スキャン範囲**］ブロックの［*IOC スキャン*］タスクを設定します。
   - **重要なファイル領域**：このオプションを選択した場合、Kaspersky Endpoint Security はカーネルメモリやブートセクターのような、コンピューター上の重要なファイル領域にのみ IOC スキャンを実行します。
   - **コンピューターのシステムドライブのファイル領域**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターのシステムドライブで IOC スキャンを実行します。

7. 必要に応じて、［**IOC スキャンタスクを実行する**］ブロックの［*IOC スキャン*］タスクを設定します。

- **手動**：都合の良いときに手動で *IOC* スキャンタスクを開始できる実行方法です。
- **自動**：脅威が検知されたときに自動で Kaspersky Endpoint Security が *IOC* スキャンタスクを実行する実行モードです。
- **コンピューターを使用していないときにのみ実行する**：スクリーンセーバーが動作しているまたは画面がロックされているときに Kaspersky Endpoint Security が *IOC* スキャンタスクを実行する実行モードです。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はタスクを一時停止します。このため、タスクの完了まで数日かかることがあります。

8. *IOC スキャンのタスクの詳細設定を指定します*。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

EDR の KEA から KES への移行ガイド（KATA）

Kaspersky Endpoint Security for Windows バージョン 12.1 から、Kaspersky Anti Targeted Attack Platform (KATA EDR) ソリューションの一部である Kaspersky Endpoint Detection and Response コンポーネントの管理用の組み込みエージェントが含まれるようになりました。EDR (KATA) と連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。Kaspersky Endpoint Agent のすべての機能は、Kaspersky Endpoint Security によって実行されます。Kaspersky Anti Targeted Attack Platform サーバーの負荷は変わりません。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security を導入する場合は、Kaspersky Anti Targeted Attack Platform (EDR) ソリューションと Kaspersky Endpoint Security は継続して連携します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。Kaspersky Endpoint Security をバージョン 12.1 以降にアップデートすると、システムで同じ動作が発生します。

Kaspersky Endpoint Security は Kaspersky Endpoint Agent と互換性はありません。同じコンピューターにこれらの製品の両方をインストールすることはできません。

Kaspersky Endpoint Security が Endpoint Detection and Response (KATA) の一部として機能するには、次の条件を満たしている必要があります。

- Kaspersky Anti Targeted Attack Platform のバージョンが 5.0 以降である。
- Kaspersky Security Center のバージョンが 14.2 以降である (ネットワークエージェントを含む)。以前のバージョンの Kaspersky Security Center では、Endpoint Detection and Response (KATA) をアクティベートすることはできません。

EDR (KATA) で［KES + KEA］設定から［KES + 組み込みエージェント］に移行する手順

1. **Kaspersky Endpoint Security の管理プラグインのアップグレード**

   EDR (KATA) コンポーネントは、Kaspersky Endpoint Security の管理プラグインのバージョン 12.1 以降を使用して管理できます。使用している Kaspersky Security Center コンソールの種類に応じて、管理コンソール (MMC) で管理プラグインをアップデートするか、Web コンソールで Web プラグインをアップデートします。

2. **ポリシーおよびタスクの移行**

Kaspersky Endpoint Agent の設定を Kaspersky Endpoint Security for Windows に移行します。次の設定方法があります：

- Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザード。Kaspersky Endpoint Agent から Kaspersky Endpoint Security への移行ウィザードは、Web コンソールでのみ動作します。

  Web コンソールで Kaspersky Endpoint Agent から Kaspersky Endpoint Security にポリシーおよびタスクの設定を移行する方法

  Web コンソールのメインウィンドウで、［**操作**］→［**Kaspersky Endpoint Agent からの移行**］の順に選択します。

  ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

ステップ 1：ポリシーの移行

移行ウィザードでは Kaspersky Endpoint Security および Kaspersky Endpoint Agent のポリシーの設定を統合する新しいポリシーが作成されます。ポリシーのリストで、Kaspersky Endpoint Security のポリシーと統合する Kaspersky Endpoint Agent のポリシーを選択します。Kaspersky Endpoint Agent のポリシーをクリックして、設定を統合する Kaspersky Endpoint Security のポリシーを選択します。正しいポリシーを選択したことを確認してから次の手順に進みます。

ステップ 2：タスクの移行

移行ウィザードは、EDR (KATA) タスクをサポートしていません。この手順をスキップします。

ステップ 3：ウィザードの完了

ウィザードを終了します。ウィザードを実行した結果、新規の Kaspersky Endpoint Security ポリシーが作成されます。ポリシーは Kaspersky Endpoint Security および Kaspersky Endpoint Agent の設定を統合します。ポリシーには *<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>* という名前が付けられます。新しいポリシーのステータスは*非アクティブ*になっています。続行するには、Kaspersky Endpoint Agent と Kaspersky Endpoint Security のポリシーをそれぞれ*非アクティブ*にして、新しく統合されたポリシーを有効にします。

Web コンソールの移行ウィザードは、次のポリシー設定をスキップするため、移行は実行されません。

- 設定の変更の禁止（［**接続設定**］が鍵のかかったアイコンの状態）。

  既定では、設定は編集可能です（鍵が開いたアイコン）。このため、コンピューターに設定が適用されません。設定の変更を禁止して、アイコンは鍵がかかった状態にする必要があります。

- 暗号化コンテナー。

  Central Node サーバーとの接続に相互認証を使用している場合は、暗号化コンテナーを再度追加する必要があります。

移行ウィザードでは、これらの設定が移行されないため、Central Node サーバーにコンピューターを接続するときにエラーが発生することがあります。エラーを修正するには、ポリシーのプロパティに移動して接続設定を指定する必要があります。

- 標準ポリシーとタスクの一括置換ウィザード。ポリシーとタスクの一括変換ウィザードは、管理コンソール (MMC) でのみ使用可能です。ポリシーとタスクの一括変換ウィザードについて詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。

サーバー上で Kaspersky Endpoint Security が正常に動作するため、サーバーの動作に重要なファイルを信頼ゾーンに追加することを推奨します。SQL サーバーでは、MDF と LDF データベースファイルを追加する必要があります。Microsoft Exchange サーバーでは、CHK、EDB、JRS、LOG、JSL ファイルを追加する必要があります。例えば、`C:\Program Files (x86)\Microsoft SQL Server\*.mdf` のようにマスクを使用することができます。

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

EDR テレメトリの除外リストでは、Kaspersky Endpoint Agent ポリシーから Kaspersky Endpoint Security ポリシーへの移行が行われません。Kaspersky Endpoint Security には信頼するアプリケーションという独自の除外ツールがあります。Kaspersky Endpoint Security の動作は最適化されているため、個別の EDR テレメトリ除外リストが存在しなくても、Kaspersky Endpoint Agent と比較してコンピューターに追加の負荷をかけることはありません。Kaspersky Endpoint Security はテレメトリを EDR (KATA) だけでなく、製品の保護機能の動作にも使用します。このため、個別の EDR テレメトリ除外リストを移動する必要がありません。コンピューターのパフォーマンスが低下する場合は、アプリケーションの動作を確認してください（「ステップ 7 パフォーマンスの確認」を参照）。

3 EDR (KATA) 機能のライセンス

Kaspersky Anti Targeted Attack Platform ソリューションの一部として Kaspersky Endpoint Security をアクティベートするには、Kaspersky Endpoint Detection and Response（KATA）のアドオンの個別のライセンスが必要です。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。結果として、*Kaspersky Endpoint Security* および *Kaspersky Endpoint Detection and Response（KATA）* の 2 種類のライセンスがアプリケーションに追加されることになります。

EDR Optimum または EDR Expert の機能がアクティベートされているコンピューター上で Kaspersky Endpoint Detection and Response (KATA) アドオンをライセンス認証するには、以下の事項を特別に考慮する必要があります：

- EDR Optimum または EDR Expert 機能を備えた Kaspersky Endpoint Security のライセンス認証に *ライセンス情報ファイル*を使用している場合、Kaspersky Endpoint Detection and Response (KATA) アドオンに別のライセンスを追加することはできません。ライセンス認証にアクティベーションコードを使用する方法に切り替えるか、サービスプロバイダーに連絡して Kaspersky Endpoint Security および EDR の機能をアクティベートするための新しいライセンス情報ファイルを入手することができます。サービスプロバイダーは、ライセンス認証用に 1 つまたは複数のライセンス情報ファイルを提供します。

- EDR Optimum または EDR Expert 機能がない Kaspersky Endpoint Security のライセンス認証に *ライセンス情報ファイル*を使用している場合、ライセンス情報ファイルを再発行する必要なく、Kaspersky Endpoint Detection and Response (KATA) アドオンに別のライセンスを追加できます。

- ライセンス認証にアクティベーションコードを使用している場合、カスペルスキーのアクティベーションサーバーが自動的にライセンス情報ファイルを再発行し、EDR (KATA) 機能が自動的に使用可能になります。この場合、EDR Optimum と EDR Expert は無効になります。

- Kaspersky Endpoint Security では、最大 2 つの現在のライセンスを追加することができます。これは、Kaspersky Endpoint Security ライセンスとアドオンタイプのライセンスです。また、予備のライセンスを 2 つまで追加することができます。Kaspersky Endpoint Security の予備のライセンス 1 つと、アドオンタイプの予備のライセンス 1 つです。

4 Kaspersky Endpoint Security のインストールまたはアップグレード

製品のインストールまたはアップグレード中に EDR (KATA) 機能を移行するには、リモートインストールタスクの使用を推奨します。リモートインストールタスクを作成する場合、インストールパッケージの設定で EDR (KATA) コンポーネントを選択する必要があります。

次の方法で本製品をアップグレードすることもできます：

- Kaspersky Update サービスを使用する。

- クライアントデバイスのローカルで、インストールウィザードを使用する。

Kaspersky Endpoint Agent がインストールされているコンピューターに Kaspersky Endpoint Security をインストールする場合、コンポーネントの自動選択がサポートされます。自動選択されるコンポーネントは、本製品のアップグレードを実行するユーザーアカウントの権限により異なります。

Kaspersky Endpoint Security をシステムアカウント（SYSTEM）で EXE または MSI ファイルを使用してアップグレードする場合は、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されます。そのため、コンピューターに Kaspersky Endpoint Agent がインストールされており、EDR (KATA) ソリューションがアクティベートされている場合、Kaspersky Endpoint Security のインストーラーは自動的にコンポーネントのセットを構成して EDR (KATA) コンポーネントを選択します。これにより、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。通常、システムアカウント (SYSTEM) を使用した MSI インストーラーの実行は、カスペルスキーのアップデートサービス経由または Kaspersky Security Center 経由でのインストールパッケージの配信時などに行われます。

権限のないユーザーアカウントで MSI ファイルを使用して Kaspersky Endpoint Security をアップグレードすると、Kaspersky Endpoint Security にはカスペルスキーソリューションの現在のライセンスへのアクセス権が付与されません。この場合、Kaspersky Endpoint Security は、Kaspersky Endpoint Agent のコンポーネントの組み合わせに基づいて、自動的にコンポーネントを選択します。それから、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

Kaspersky Endpoint Security は、コンピューターを再起動することなくアップグレードをサポートします。ポリシーのプロパティで製品のアップグレードモードを選択できます。

5 本製品の動作の確認

製品のインストール後またはアップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。

- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。コンポーネントのステータスが「*ライセンスに含まれていません*」となっている場合は、組み込みエージェント機能をアクティベートしていることを確認してください。

- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

6 Kaspersky Anti Targeted Attack Platform サーバーとの接続の確認

Kaspersky Anti Targeted Attack Platform サーバーとの接続を確認します。次の手順に従います：

1. 有効な証明書があるか確認します。
2. サーバーの接続設定を確認します。
3. イベントログを確認します。

   サーバーとの接続が確立されたら、本製品はイベント［*EDR Expert サーバーに正常に接続しました*］を送信します。正常な接続イベントがなく、接続エラーに関するイベントもない場合は、イベントログ設定を確認して、Endpoint Detection and Response (KATA) へのイベント送信を有効にしてください。

サーバーの接続ステータスは Kaspersky Security Center コンソールのコンピューターのステータスに影響しません。そのため、サーバーとの接続がない場合も、コンピューターのステータスは *OK* と表示されます。サーバーとの接続を検証するには、イベントログを確認してください。

7 パフォーマンスの確認

アプリケーションのインストールやアップデート後にコンピューターのパフォーマンスが低下した場合、データ転送を最適化することができます。次の手順に従います：

1. EDR (KATA) コンポーネントを無効化し、性能劣化が EDR (KATA) に起因するものであるかを確認します。
2. 信頼するアプリケーションでは、コンソール入力操作のテレメトリ収集をオフにします（既定で有効になっています）。
3. コンピューターのパフォーマンスを低下させるアプリケーションを、信頼するアプリケーションのリストに追加します。
4. カスペルスキーのテクニカルサポートにお問い合わせください。Kaspersky Anti Targeted Attack Platform のテレメトリフィルタリングの設定について、サポートエキスパートがお手伝いします。これにより、トラフィック量を減少させることができます。特定のアプリケーションによってコンピューターのパフォーマンスに影響がある場合は、そのアプリケーションの配布パッケージをご依頼内容に添付してください。

Endpoint Detection and Response Expert（オンプレミス）



Kaspersky Endpoint Security for Windows は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションとの連携をサポートしています。*Kaspersky Endpoint Detection and Response Expert（オンプレミス）*は、組織がほとんどの種別のサイバーリスクを防ぎ、最も重要な脅威の拡散シナリオに対応できるようにするカスペルスキー製品を含むエンタープライズ向けのサイバーセキュリティソリューションです。EDR Expert（オンプレミス）コンポーネントは、Open Single Management Platform (OSMP) に配備されます。このプラットフォームは、単一のインターフェイスでクロスプラットフォームのシナリオを実行し、カスペルスキー製品とサードパーティ製品を包括的なセキュリティシステムに統合することを可能にします。

ソリューションの中心的な要素の 1 つは *SIEM* です。SIEM は、すべてのコンポーネントからのイベントを追跡し、ベンダーおよびユーザー定義のルールを使用してこれらのイベントを相互に関連付けます。EDR Expert（オンプレミス）は、企業インフラストラクチャから受信したログとテレメトリを調べて攻撃を自動的に検出し、 カスペルスキー製品やサードパーティの情報セキュリティ製品からのイベントを含む、EDR Expert（オンプレミス）で収集されたすべてのイベントを組み合わせた統合調査グラフを使用してインシデントの調査を可能にします。

高度なインシデントに対応するために、EDR Expert（オンプレミス）は、事前設定されたシナリオとユーザー定義のシナリオを使用します。サードパーティ製品からの対応処理や、複数のアプリケーションが関係する対応シナリオを使用することもできます。

脅威インテリジェンスツール

Kaspersky Endpoint Detection and Response は次の脅威インテリジェンスツールを使用します。

- Kaspersky Threat Intelligence Portal との連携。ファイルや Web アドレスの評価に関する情報を蓄積し、表示できます。
- Kaspersky Threats データベース。
- Kaspersky Security Network（以下、「KSN」とも表記）。クラウドサービスのインフラストラクチャで、カスペルスキーの情報基盤に基づいたリアルタイムのファイル、Web サイト、ソフトウェアの評価情報を提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。

ソリューションの動作原理

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューター上のイベントに関する情報（テレメトリ）が EDR Expert（オンプレミス）サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検知した脅威に関する情報およびその脅威の処理結果についての情報をテレメトリ収集サーバーに送信します。

EDR Expert（オンプレミス）連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Open Single Management Platform (OSMP) を使用して管理されるようになります。

EDR Expert（オンプレミス）連携のための Kaspersky Endpoint Security の設定

EDR Expert（オンプレミス）と連携するには、以下の設定を使用できます：

- **[KES + 組み込みエージェント]**：この設定において、Kaspersky Endpoint Security は、コンピューターのセキュリティを確保するアプリケーションと EDR Expert（オンプレミス）を操作するアプリケーションの両方の役割を果たします。EDR Expert（オンプレミス）の組み込みエージェントは、Kaspersky Endpoint Security 12.11 for Windows 以降で使用できます。
- **[サードパーティ製 EPP+EDR エージェント]**.この設定において、IT インフラストラクチャのセキュリティはサードパーティエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）によって確保されます。EDR Expert（オンプレミス）との連携は、Kaspersky Endpoint Security の Endpoint Detection and Response Agent (EDR Agent) の設定で提供されます。この設定において、EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。EDR Expert（オンプレミス）の EDR Agent は、Kaspersky Endpoint Security 12.11 for Windows 以降で使用できます。

組み込みエージェントと EDR Expert（オンプレミス）の連携

Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションと連携するには、Endpoint Detection and Response Expert（オンプレミス）コンポーネントを追加し、Kaspersky Endpoint Security を設定する必要があります。

EDR Optimum、EDR Expert および EDR Expert（オンプレミス）コンポーネント間には互換性はありません。

Endpoint Detection and Response Expert（オンプレミス）が動作するには次の条件を満たしている必要があります。

- OSMP（Open Single Management Platform）がインストールされている。
- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- Endpoint Detection and Response Expert（オンプレミス）コンポーネントがオンになっている。
- EDR Expert（オンプレミス）の動作を保証する製品コンポーネントが有効になっており、動作可能である。次のコンポーネントが EDR Expert（オンプレミス）の動作を確保するために必要となります：
  - ファイル脅威対策
  - ウェブ脅威対策
  - メール脅威対策
  - 脆弱性攻撃ブロック
  - ふるまい検知
  - ホスト侵入防止
  - 修復エンジン
  - アダプティブアノマリーコントロール

EDR Expert（オンプレミス）の連携を設定するには、次の手順を実行します：

1. **EDR Expert（オンプレミス）コンポーネントのインストール**

   EDR Expert（オンプレミス）コンポーネントは、インストール中またはアップグレード中、または*コンポーネントの変更*タスクを使用して選択できます。

   新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2. **Kaspersky Endpoint Detection and Response Expert（オンプレミス）のアクティベーション**

   EDR Expert（オンプレミス）（Kaspersky Endpoint Detection and Response Expert（オンプレミス）アドオン）の個別ライセンスを購入する必要があります。

この機能は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）向けの別のライセンスを追加すると使用できるようになります。結果として、Kaspersky Endpoint Security のライセンスおよび Kaspersky Endpoint Detection and Response Expert（オンプレミス）のライセンスの 2 種類のライセンスがコンピューターに追加されることになります。

スタンドアロンの Endpoint Detection and Response Expert（オンプレミス）のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

EDR Expert（オンプレミス）がライセンスでサポートされており、本製品のローカルインターフェイスで実行中であることを確認してください。

3 テレメトリ収集サーバーと応答サーバーへの接続

Kaspersky Endpoint Detection and Response Expert（オンプレミス）では、Kaspersky Endpoint Security と次の 2 つのサーバーとの信頼済みの接続が必要です：

- *テレメトリの収集サーバー*は、コンピューター上で発生するイベントに関する情報を収集、正規化、関連付け、分析、保存する SIEM ソリューションの一部であるサーバーです。
- *応答サーバー*は、データを受信してスキャンし、オブジェクトのふるまいを調査し、そのような調査結果を公開するためのサーバーです。

信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。

既定では、Kaspersky Endpoint Security はサーバーの TLS 証明書のみを確認します。接続の安全性をより高めるには、追加でサーバーのコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、サーバーおよび Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。

Web コンソールを使用して Kaspersky Endpoint Security 端末を EDR Expert（オンプレミス）に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（オンプレミス）**］に移動します。
5. ［**Endpoint Detection and Response Expert（オンプレミス）が有効です**］をオンにします。
6. EDR Expert（オンプレミス）を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 8.0 以降）**］を選択します。

7. *テレメトリ収集サーバー*の接続を設定します：

a. ［**テレメトリ収集サーバーへの接続**］セクションで、［**接続設定**］をクリックします。

b. テレメトリ収集サーバーの接続を設定します：

- **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。
- **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。
- **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

c. ［OK］をクリックします。

d. テレメトリ収集サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

   複数のテレメトリ収集サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

e. 必要に応じて、テレメトリを設定してください。

8. *応答サーバー*の接続を設定します：

a. ［**応答サーバーへの接続**］ブロックで、［**サーバーに同期リクエストを送信する間隔（分）**］を設定します：サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は脅威対応タスクを受信し、タスクの結果を送信します。

b. ［**接続設定**］リンクをクリックします。

c. 応答サーバーの接続を設定します：

- **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。
- **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。

- **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

  暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

d. ［**OK**］をクリックします。

e. 応答サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

   複数の応答サーバーアのドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

その結果、コンピューターが Open Single Management Platform (OSMP) に追加されます。コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**Endpoint Detection and Response Expert（オンプレミス）**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

EDR Expert（オンプレミス）のテレメトリ設定

*テレメトリ*とは、保護対象コンピューター上で発生したイベントのリストです。Kaspersky Endpoint Security はテレメトリデータを分析し、同期中にテレメトリ収集サーバーに送信します。テレメトリイベントはほぼ継続的にサーバーに届きます。次の条件のいずれかが満たされると、Kaspersky Endpoint Security はサーバーとの同期を開始します。

- 同期間隔が経過した。
- バッファ内のイベント数が上限を超えた。

既定では、本製品は 30 分間隔またはバッファ内のイベントが 1024 件に達すると同期します。同期については Kaspersky Endpoint Security のポリシーで設定できるので、ネットワーク負荷に応じて最適な値を選択することができます（以下の手順を参照）。

Kaspersky Endpoint Security とサーバー間に接続がない場合は、本製品は新しいイベントをキューに入れます。接続が復元されると、Kaspersky Endpoint Security はキューのイベントを順にサーバーに送信します。サーバーの過負荷を避けるため、イベントの一部がスキップされることがあります。イベント転送設定で、1 時間ごとの最大イベントを設定するなどしてイベント転送を最適化することができます（以下の手順を参照）。

テレメトリを設定するには、次の手順を実行します：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（オンプレミス）**］に移動します。

5. EDR Expert（オンプレミス）を設定するには、ソリューションのリストから［**Endpoint Detection and Response Expert（バージョン 8.0 以降）**］を選択します。

6. ［**データ転送設定**］ブロックで［**テレメトリ収集サーバーにテレメトリを送信する**］がオンになっていることを確認します。

7. 必要に応じて、［**IOA のあるテレメトリのみ送信する**］をオンにします。*攻撃の痕跡（IOA）*は、標的型攻撃を示す可能性のあるシステム内の疑わしい動作の説明を含むルールです。本製品は、システム内で進行中の動作をこれらのルールと比較し、標的型攻撃を示唆するイベントをログに記録します。本製品は、このようなイベントをリアルタイムで追跡できる*ストリーミングスキャン*の技術を採用しています。

8. 必要に応じて、［**データ転送設定**］ブロックで、サーバー設定との同期を設定します：

   - **最大イベント転送遅延時間（秒）**：指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。

   - **イベントパッケージの最大数**：バッファがイベントでいっぱいになると、本製品はサーバーと同期します。既定値は 1024 イベントです。

9. 必要に応じて、［**リクエストの調整**］ブロックの［**リクエストの調整を有効にする**］をオンにします。

   これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。

10. サーバーへのイベント送信の最適化を設定します：

    - **1 時間ごとのイベントの最大数**：本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1 時間後にイベントの送信は再開されます。1 時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を 1 時間あたり 60,000 イベントに増やすことを推奨します。

    - **イベントの制限超過のパーセンテージ**：本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。

11. ［**応答サーバーへの接続**］ブロックで、［**サーバーに同期リクエストを送信する間隔（分）**］パラメータに値を入力します。

12. サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。

13. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

EDR Expert（オンプレミス）のテレメトリ除外

パフォーマンスを向上させ、テレメト収集リサーバーへのデータ送信を最適化するために、テレメトリの除外リストを追加できます。たとえば、個々のアプリケーションのネットワーク通信データを送信しないように選択できます。

使用するルールが多すぎると、テレメトリの収集サーバーへの負荷が増えて、コンピューターのパフォーマンスが低下することがあります。必要なルールのみを追加することを推奨します。

Web コンソールと Cloud コンソールでテレメトリの除外リストを作成するには、次の操作を行います：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**テレメトリの設定**］に移動します。

5. ［**EDR Expert（オンプレミス）のテレメトリ**］タブを選択します。

6. ［**全般的な除外**］ブロックの［**追加**］をクリックします。
   ［**除外ルールを追加**］ウィンドウが表示されます。

7. 必要に応じて、ルールのステータスを変更します。既定では、ルールは有効になっています。

8. ルール名を入力します。

9. ルールが適用された際に実行する処理を選択します：

   - **収集しない**：フィルタリングされたイベントは、送信対象のテレメトリから除外されます。

   - **IOA を除外**：IOA ルールの適用イベントは、送信対象のテレメトリから除外されます。

10. ［**IOA を除外**］を選択した場合は、除外対象に追加する IOA ルールを指定します：

    - **すべて除外**：指定した条件が満たされると、本製品はすべての IOA ルールに基づいて生成されたイベントをテレメトリから除外します。

    - **GUID による除外**：IOA ルールの GUID を指定します。「**,**」を使用すると、複数の GUID を指定できます。IOA ルールについて詳しくは、EDR Expert（オンプレミス）のヘルプを参照してください。

11. フィルタリング条件を指定します：

    a. フィルタリングに使用するフィールド名を選択します。

    b. 演算子を選択して（下記の表を参照）、イベントからのフィールド値と比較する値を指定します。

条件演算子の一覧

演算子	説明
<	フィールド値が条件で指定された値よりも小さい場合、イベントは除外されます。
≤	フィールド値が条件で指定された値以下の場合、イベントは除外されます。
=	フィールドの値が条件で指定された値と等しい場合、イベントは除外されます。
≥	フィールドの値が条件で指定された値以上である場合、イベントは除外されます。
>	フィールド値が条件で指定された値より大きい場合、イベントは除外されます。
≠	フィールドの値が条件で指定された値と等しくない場合、イベントは除外されます。
次の表現に一致する	フィールド値が条件で指定されたマスクと一致する場合、イベントは除外されます。マスクの入力時の文字「*」および「?」がサポートされます。
次の表現に一致しない	フィールド値が条件で指定されたマスクと一致しない場合、イベントは除外されます。マスクの入力時の文字「*」および「?」がサポートされます。
次のうち1つと一致する	フィールド値が条件で指定されたリスト内の値のいずれかと一致する場合、イベントはフィルタリングされたとみなされます。
次の1つとも一致しない	フィールド値が条件で指定されたリスト内のいずれの値とも一致しない場合、イベントはフィルタリングされたとみなされます。
次の表現のうち1つに一致する	フィールド値が条件で指定されたマスクのいずれかに一致する場合、イベントは除外されます。Kaspersky Endpoint Security はマスクの入力において「*」文字と「?」文字をサポートします。
次の表現のうち1つに一致しない	フィールド値が条件で指定されたマスクのいずれにも一致しない場合、イベントは除外されます。Kaspersky Endpoint Security はマスクの入力において「*」文字と「?」文字をサポートします。
次が存在する	条件で指定されたフィールドがイベントに存在する場合、イベントは除外されます。
次が存在しない	条件で指定されたフィールドがイベントに存在しない場合、イベントは除外されます。
次を含む	条件で指定された値がフィールド値に存在する場合、イベントは除外されます。
が次と等しい	フィールドの値が条件で指定された値と等しい場合、イベントは除外されます。スキャンでは大文字と小文字は区別されません。
ビットごとの AND	フィールド値と条件で指定された値とのビットごとの AND（&）演算の結果が1の場合、イベントは除外されます。

12. 必要に応じて、複数のフィルター条件や条件グループを追加することで、複雑なフィルター条件を作成できます。条件グループには、ネストされた条件や条件グループを追加することもできます。次の演算子を指定できます：

    - **AND**：は、フィルターが指定されたすべての条件を満たすイベントを選択することを意味します。
    - **OR**：は、フィルターが指定された条件のいずれかを満たすイベントを選択することを意味します。
    - **NOT**：（この演算子を使用するには、**前に NOT を追加**オプションを選択します）は、フィルターが指定された条件のいずれにも該当しないイベントを選択することを意味します。

    条件と第1レベルの条件グループは、**AND** 演算子で結合されます。

13. コンピューターが Open Single Management Platform (OSMP) を実行している場合は、作成したフィルタリングルールをスキャンできます。スキャンを実行するには、［**ルールの確認**］ボタンをクリックします。

    表示されたウィンドウに、作成したルールでフィルタリングされたイベントの表が表示されます。詳細については、EDR Expert（オンプレミス）のヘルプを参照してください。

14. 必要に応じて、［**すべてのイベント種別**］で、イベントの種別ごとにテレメトリ除外を追加します。

    a. イベントの種別名をクリックします。

    b. 表示されたウィンドウで、［**手動で設定する**］をクリックします。

    c. 必要に応じて、［**イベントを送信**］ トグルスイッチを使用して、選択したイベント種別のテレメトリ送信を設定します。既定では、すべてのイベント種別でテレメトリ送信が有効になっています。

    d. ［**除外ルール**］ブロックの［**追加**］をクリックします。
    ［**除外ルールを追加**］ウィンドウが表示されます。

    e. 追加するルールごとに、手順 7〜13 で説明されている操作を実行してください。

15. イベントの種別によっては、収集するテレメトリを拡張するための包含ルールを追加することもできます。

    a. ［**包含ルール**］ブロックの［**追加**］をクリックします。
    ［**包含ルールを追加**］ウィンドウが表示されます。

    b. ルール名を入力します。

    c. ［**条件**］の下に表示されているフィールドに値を入力します。使用できるフィールドの種別は、選択したイベントによって異なります。

> 除外ルールは包含ルールよりも優先されます。

16. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

EDR Expert（オンプレミス）のイベントフィルターのエクスポートとインポート

除外リストを JSON ファイルにエクスポートすることができます。これにより、たとえば多数のイベント ID をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、イベントフィルターのバックアップをとったり、別のサーバーにリストを移行することができます。

> 使用するルールが多すぎると、テレメトリの収集サーバーへの負荷が増えて、コンピューターのパフォーマンスが低下することがあります。必要なルールのみを追加することを推奨します。

管理コンソール（MMC）でイベントフィルターをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。

2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。

5. ［**テレメトリの設定**］→［**EDR Expert（オンプレミス）のテレメトリ**］ブロックの［**設定**］をクリックします。

6. イベントフィルターをエクスポートするには：

   a. ［**エクスポート**］をクリックします。

   表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。

   b. ファイルを保存します。

   Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。

7. イベントフィルターをインポートするには：

   a. ［**インポート**］をクリックします。

   b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。

   c. ファイルを開きます。

   コンピューターにイベントフィルタリングルールが既に存在する場合、Kaspersky Endpoint Security はインポート時にそれらを置き換えます。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールでイベントフィルターをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**テレメトリの設定**］に移動します。

5. ［**EDR Expert（オンプレミス）のテレメトリ**］タブを選択します。

6. イベントフィルターをエクスポートするには：

   a. ［**エクスポート**］をクリックします。

   b. 表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。

   c. ファイルを保存します。

   Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。

7. イベントフィルターをインポートするには：

   a. ［**インポート**］をクリックします。

   b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。

c. イベントフィルタリングルールをインポートする方法として、既存のルールに追加するか、既存のルールを破棄して新しいルールに置き換えるかを選択します。

d. ファイルを開きます。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（🔒）。

コマンドラインでイベントフィルターをエクスポートまたはインポートすることもできます。

隔離の管理

*隔離*はコンピューター上にある特別なローカル保管領域です。ユーザーがコンピューターに対して危険だと判断したファイルを隔離することができます。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は、Detection and Response ソリューション (EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox) と連携する際にのみ隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、Kaspersky Sandbox のヘルプ、Kaspersky Endpoint Detection and Response Optimum のヘルプ、および Kaspersky Endpoint Detection and Response Expert のヘルプ、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security はシステムアカウント（SYSTEM）を使用してファイルを隔離します。

Kaspersky Security Center コンソールでのみ隔離を設定できます。Web コンソールを使用して、隔離されたオブジェクトを管理（復元、削除、追加など）することもできます。ローカルのコンピューター上では、コマンドラインを使用したオブジェクトの復元のみ可能です。

隔離フォルダーの最大サイズの設定

既定では隔離のサイズは 1024 MB に制限されています。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security はファイルの送信を停止し、*隔離の保管領域に十分な空き容量がありません*のイベントを生成します。隔離のディスク空き容量が不足しないように、Kaspersky Endpoint Security が*隔離の保管領域の容量がまもなく上限に達します*のイベントを生成するしきい値を設定できます。隔離されたファイルを自動的に削除する保管期間を設定することはできません。

組織で Kaspersky Anti Targeted Attack Platform (EDR) ソリューションが導入されている場合は、隔離の容量を増加しておくことをお勧めします。YARA スキャンを実行すると、メモリダンプが増大することがあります。メモリダンプが隔離のサイズより大きくなると、YARA スキャンはエラーで終了し、メモリダンプは隔離されません。隔離のサイズをコンピューターの RAM と同等（例：8 GB）にしておくか、隔離のサイズ制限を無効にしておくことを推奨します。

管理コンソール（MMC）で隔離の最大サイズを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**レポートと保管領域**］の順に選択します。

4. ［**隔離**］ブロックで隔離のサイズを設定します：

   - **隔離のサイズを制限する：<N>MB**：このチェックボックスをオンにすると、隔離の最大サイズは指定した値に制限されます。既定では、最大サイズは 1024 MB です。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security は*隔離の保管領域に十分な空き容量がありません*のイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を停止します。隔離の中身を手動で空にしてください。

     チェックボックスをオフにすると、隔離のサイズは使用可能なディスクの空き容量によって制限されます。

   - **隔離の容量が次の割合に到達した際に通知する：<N>%**：隔離のしきい値です。たとえば、「50%」のように隔離のしきい値を設定できます。隔離のサイズのしきい値に到達すると、Kaspersky Endpoint Security は対応するイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を継続します。

     このチェックボックスをオフにすると、隔離のしきい値に達した際にイベントが生成されません。

5. 変更内容を保存します。

Web コンソールと Cloud コンソールで隔離の最大サイズを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**レポートと保管領域**］に移動します。

5. ［**隔離**］ブロックで隔離のサイズを設定します：

   - **隔離のサイズを制限する**：このチェックボックスをオンにすると、隔離のサイズは指定した値に制限されます。チェックボックスをオフにすると、隔離のサイズは使用可能なディスクの空き容量によって制限されます。本製品はサイズの大きいメモリダンプファイルを保存する可能性があるため、YARA スキャンでこれが必要になる場合があります。

   - **隔離の最大サイズ（MB）**：このチェックボックスをオンにすると、隔離の最大サイズは指定した値に制限されます。既定では、最大サイズは 1024 MB です。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security は*隔離の保管領域に十分な空き容量がありません*のイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を停止します。隔離の中身を手動で空にしてください。

     チェックボックスをオフにすると、隔離のサイズは使用可能なディスクの空き容量によって制限されます。

   - **隔離の容量が次の割合に到達した際に通知する（%）**：隔離のしきい値です。たとえば、「50%」のように隔離のしきい値を設定できます。隔離のサイズのしきい値に到達すると、Kaspersky Endpoint Security は対応するイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を継続します。

6. 変更内容を保存します。

隔離されたファイルの Kaspersky Security Center への送信

Web コンソールで隔離されたオブジェクトの処理を実行するには、隔離されたファイルのデータの管理サーバーへの送信を有効にする必要があります。たとえば、Web コンソールで分析用に隔離からファイルをダウンロードすることができます。Kaspersky Sandbox および Kaspersky Endpoint Detection and Response のすべての機能が動作するため、隔離されたファイルのデータの送信を有効にする必要があります。

管理コンソール（MMC）で隔離されたファイルのデータ転送を有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**レポートと保管領域**］の順に選択します。
4. ［**管理サーバーへのデータ転送**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、［**ファイルの隔離**］をオンにします。
6. 変更内容を保存します。

管理コンソール（MMC）で隔離されたファイルのデータ転送を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**KSC 連携**］に移動します。
5. ［**管理サーバーへのデータ転送**］ブロックで、［**隔離ファイルの情報**］をオンにします。
6. 変更内容を保存します。

Kaspersky Security Center コンソールで、コンピューター上で隔離されたファイルのリストを表示できるようになりました。Kaspersky Security Center コンソールを使用して、隔離されたオブジェクトを管理（復元、削除、追加など）できます。隔離されたファイルの操作について詳しくは、Kaspersky Security Center ヘルプ を参照してください。

隔離からのファイルの復元

既定では、Kaspersky Endpoint Security はファイルを元のフォルダーに復元します。復元先のフォルダーが削除されていたり、ユーザーにそのフォルダーへのアクセス権がない場合、ファイルはフォルダー「`%DataRoot%\QB\Restored`」に保存されます。その後、ファイルを手動で移動先のフォルダーに移動する必要があります。

隔離からファイルを復元するには：

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］→［**隔離**］をクリックします。
2. 隔離にあるファイルのリストが表示されます。リストから復元したいファイルを選択して［**復元**］をクリックします。

Kaspersky Endpoint Security はこのファイルを復元します。復元先のフォルダーに同じ名前のファイルがある場合は、ファイルの復元がキャンセルされます。EDR Optimum と EDR Expert ソリューションでは、復元後にファイルは削除されます。その他のソリューションでは、隔離にファイルのコピーが保存されます。

EDR 処理の監視

Kaspersky Endpoint Security for Windows 12.9 では、EDR 処理監視センターが導入されています。*EDR 処理監視センター*は、すべての Kaspersky Detection and Response ソリューションの脅威対応履歴を確認できるコンソールです。組織に複数の Detection and Response（EDR Optimum と MDR など）が導入されている場合は、すべてのソリューションの脅威対応履歴が表示されます。これにより、個別のコンピューターのそれぞれの Detection and Response ソリューションのパフォーマンスを分析して、これらのソリューションの設定を最適化できます。

監視センターでは以下の情報が提供されます：

- 脅威対応タスク（*プロセスの終了*タスクなど）に関する情報
- ネットワーク分離と実行防止ルールの変更

脅威対応でネットワーク共有へのアクセスに関連するエラーが発生した場合、そのエラーは、表示される脅威対応履歴で省略されます。

EDR 処理監視センターに移動するには：

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ローカル環境用の製品設定を行うコンピューターを選択します。
   コンピューターのプロパティが表示されます。
3. ［**アプリケーション**］タブを選択します。
4. **Kaspersky Endpoint Security for Windows** をクリックします。
   ローカルアプリケーション設定が表示されます。
5. ［**アプリケーション設定**］タブを選択します。
6. ［**Detection and Response**］→［**応答履歴**］に移動します。

これにより、EDR 処理監視センターコンソールが開きます。コンソールを使用すると、脅威対応タスクのステータス、タスクの実行時間、ルールの変更、イニシエーターの詳細を確認することができます。

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows は、Kaspersky Unified Monitoring and Analysis Platform ソリューションをサポートしています。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* は、組織の IT インフラストラクチャ向けの SIEM (Security Information and Event Management) ソリューションです。KUMA を使用すると、セキュリティ上の脅威が被害をもたらす前にそれを検知、分析し、緩和することができます。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリ）は Kaspersky Unified Monitoring and Analysis Platform (KUMA) サーバーに送信されます。KUMA のコンソールには、Windows イベントログと同様に、イベントがマークアップなしのリストとして表示されます。

Kaspersky Endpoint Security は、KUMA のエージェントのすべての機能を提供するわけではありません。本製品はマークアップなしでイベントのみを KUMA に送信します。KUMA のすべての機能にアクセスするには、ライセンスを購入し、KUMA 管理者ガイドに従ってソリューションを導入する必要があります。

Kaspersky Endpoint Security と KUMA の連携

KUMA を使用するには、次の条件を満たす必要があります：

- Kaspersky Security Center のバージョンが 14.2 以降である。以前のバージョンの Kaspersky Security Center では、KUMA 連携機能をアクティベートすることはできません。
- 本製品がアクティベートされており、ライセンスがこの機能をサポートしている。
- KUMA 連携コンポーネントが有効になっている。

KUMA 連携を設定するには、次の手順を実行します：

1. **KUMA 連携コンポーネントのインストール**

   KUMA 連携コンポーネントは、本製品のインストール中またはアップグレード中に選択するか、*コンポーネントの変更*タスクを使用して選択することができます。

   新機能を持つ製品にアップグレードを完了するにはコンピューターを再起動する必要があります。

2. **KUMA のアクティベーション**

   Kaspersky Endpoint Security のライセンス（たとえば Kaspersky Endpoint Security for Business Standard）に加えて、Kaspersky Endpoint Security と KUMA の連携（Kaspersky Endpoint Security for Windows KUMA 統合アドオン）用に個別のライセンスが必要です。

本製品を EDR Agent モードでインストールする場合は、Kaspersky Endpoint Security を KUMA と連携させるためのライセンスと、Kaspersky Anti Targeted Attack Platform (KATA) ライセンスまたは Kaspersky Managed Detection and Response (MDR) ライセンスが必要です。KUMA のみに EDR Agent を導入することはできません。

別途 KUMA のライセンスを追加することで機能を使用できるようになります。その結果、Kaspersky Endpoint Security を KUMA と連携させるためのアクティブなキーがコンピューター上にもう 1 つ存在することになります。

スタンドアロンの KUMA 機能のライセンス認証は、Kaspersky Endpoint Security のライセンス認証と同じです。

KUMA がライセンスでサポートされており、本製品のローカルインターフェイスで稼働していることを確認してください。

3 KUMA への接続

Kaspersky Endpoint Security アプリケーションを搭載したコンピューターを KUMA ソリューションに接続するには：

1. Kaspersky Endpoint Security ポリシーに KUMA サーバーのアドレスを追加し、接続のネットワーク設定を指定します。
2. KUMA コンソールで、種別が TCP または UDP のコネクターを持つコレクターを追加し、接続の基本的なネットワーク設定を指定します。コレクターの管理について詳しくは、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください。

Kaspersky Endpoint Security と KUMA サーバーの間に信頼済みの接続を確立できます。信頼する接続を設定するには、TLS 証明書を使用してください。TLS 証明書は KUMA Core サーバーで取得できます（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。それから、TLS 証明書を Kaspersky Endpoint Security に追加してください（以下の手順を参照）。

接続の安全性をより高めるには、追加で KUMA のコンピューターの検証をオンにすることができます（相互認証）。この検証をオンにするには、KUMA および Kaspersky Endpoint Security の設定で相互認証をオンにしておく必要があります。相互認証を使用するには、暗号化コンテナーも必要となります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。外部の認証局で、PKCS#12 コンテナー形式の秘密鍵を含む証明書を生成する必要があります。次に、KUMA コンソールと Kaspersky Endpoint Security に PFX アーカイブを追加する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。

管理コンソール（MMC）を使用して Kaspersky Endpoint Security 端末を KUMA に接続する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**KUMA 連携**］を選択します。
4. ［**KUMA 連携**］チェックボックスをオンにします。
5. ［**連携の設定**］ブロックで、［**$IsKUMATelemetry ? "KUMA サーバーへの Windows イベント転送を有効にする": "SIEM サーバーへの Windows イベント転送を有効にする**］をオンにします。
6. 必要に応じて、［**KUMA サーバーへの接続設定**］ブロックの［**TLS 暗号化を使用する**］をオンにします。

7. 信頼済みの接続を設定します。

   a. ［**KUMA サーバーへの接続設定**］をクリックします。

   b. サーバー接続を設定します：

   - **タイムアウト（秒）**：KUMA サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の KUMA サーバーに接続を試みます。

   - **サーバー TLS 証明書**：KUMA サーバーと信頼済みの接続を確立するための TLS 証明書。Kaspersky Unifield Monitoring and Analysis Platform コンソールで TLS 証明書を取得できます（Kaspersky Unified Monitoring and Analysis Platform の手順を参照してください）。

     信頼済みの接続を確立するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**With verification**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。

   - **相互認証を使用する**：Kaspersky Endpoint Security と KUMA 間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**Custom PFX**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。次に、暗号化コンテナーを取得し、暗号コンテナーを保護するためのパスワードを設定する必要があります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。KUMA を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

     > 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

   c. ［**OK**］をクリックします。

8. KUMA サーバーを追加します。

   a. ［**追加**］をクリックします。

   これにより、KUMA サーバーを追加できるフォームが開きます。

   b. KUMA サーバーに接続するためのプロトコル（**HTTP / HTTPS**、**TCP**、**UDP**）を選択します。

   HTTP / HTTPS プロトコルを選択した場合、本製品は既定で KUMA サーバーへの接続に HTTPS を使用します。HTTP を使用するには、サーバーアドレスにこのプロトコルを手動で指定する必要があります（例：`http://server.com`）。

   c. サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定します。

   d. ［**OK**］をクリックします。

   Kaspersky Endpoint Security はリストの 1 番目の KUMA サーバーに接続します。接続に失敗した場合、リストの 2 番目の KUMA サーバーに接続します。

9. 必要に応じて、［**データ転送設定**］ブロックの［**最大イベント転送遅延時間（秒）**］を設定します。指定された時間が経過すると、Kaspersky Endpoint Security は同じサーバーへの接続を試みます。サーバーが複数ある場合はリスト内の次のサーバーに接続します。既定値は 30 秒です。

10. 変更内容を保存します。

Web コンソールを使用して Kaspersky Endpoint Security 端末を KUMA に接続する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**組み込みエージェントの設定**］→［**KUMA 連携**］に移動します。
5. ［**KUMA 連携は有効です**］をオンにします。
6. 必要に応じて、［**サーバーの接続設定**］ブロックの［**TLS 暗号化を使用する**］トグルスイッチをオンにします。
7. 信頼済みの接続を設定します。
   a. ［**接続設定**］をクリックします。
   b. サーバー接続を設定します：
      - **タイムアウト（秒）**：KUMA サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の KUMA サーバーに接続を試みます。
      - **サーバー TLS 証明書**：KUMA サーバーと信頼済みの接続を確立するための TLS 証明書。Kaspersky Unifield Monitoring and Analysis Platform コンソールで TLS 証明書を取得できます（Kaspersky Unified Monitoring and Analysis Platform の手順を参照してください）。
        信頼済みの接続を確立するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**With verification**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。
      - **相互認証を使用する**：Kaspersky Endpoint Security と KUMA 間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**Custom PFX**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。次に、暗号化コンテナーを取得し、暗号コンテナーを保護するためのパスワードを設定する必要があります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。KUMA を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。

        > 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

   c. ［**OK**］をクリックします。
8. KUMA サーバーを追加します。
   a. ［**追加**］をクリックします。
      これにより、KUMA サーバーを追加できるフォームが開きます。

b. KUMA サーバーに接続するためのプロトコル（**HTTP / HTTPS**、**TCP**、**UDP**）を選択します。

HTTP / HTTPS プロトコルを選択した場合、本製品は既定で KUMA サーバーへの接続に HTTPS を使用します。HTTP を使用するには、サーバーアドレスにこのプロトコルを手動で指定する必要があります（例：`http://server.com`）。

c. サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定します。

d. ［**OK**］をクリックします。

Kaspersky Endpoint Security はリストの 1 番目の KUMA サーバーに接続します。接続に失敗した場合、リストの 2 番目の KUMA サーバーに接続します。

9. 必要に応じて、［**サーバーの接続設定**］ブロックの［**イベント送信時の最大遅延（秒）**］を設定します。指定された時間が経過すると、Kaspersky Endpoint Security は同じサーバーへの接続を試みます。サーバーが複数ある場合はリスト内の次のサーバーに接続します。既定値は 30 秒です。

10. 変更内容を保存します。

KUMA 連携が正しく設定されているかどうかは、KUMA コンソールで確認できます（詳しくは Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照）。コンポーネントの動作状態は、Kaspersky Security Center コンソールの*製品コンポーネントのステータスレポート*で表示できます。また、コンポーネントの動作状態を Kaspersky Endpoint Security のローカルインターフェイス内のレポートで表示して確認することもできます。［**KUMA連携**］は Kaspersky Endpoint Security のコンポーネントのリストに追加されます。

4 KUMA サーバーへのテレメトリ送信の有効化

既定では、KUMA サーバーへのイベント送信は無効になっています。KUMA を正しく動作させるには、テレメトリ送信を有効にする必要があります。［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。

管理コンソール（MMC）で KUMA サーバーへのテレメトリの送信を有効にする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
5. ［**テレメトリの設定**］→［**KUMA テレメトリ**］ブロックの［**設定**］をクリックします。
6. イベントソースとして使用するイベントログ（*Application*、*Security*、または*System*）を選択します。

   標準ログに加えて、サードパーティ製品のログを指定できます。
7. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

Web コンソールで KUMA サーバーへのテレメトリの送信を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**テレメトリの設定**］に移動します。
5. ［**KUMA テレメトリ**］タブを選択します。
6. イベントソースとして使用するイベントログ（*Application*、*Security*、または*System*）を選択します。

   標準ログに加えて、サードパーティ製品のログを指定できます。
7. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

KUMA に送信するイベントのフィルタリング

既定では、KUMA サーバーへのイベント送信は無効になっています。KUMA を正しく動作させるには、テレメトリ送信を有効にする必要があります。［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。パフォーマンスを向上させ、KUMA サーバーへのデータ転送を最適化するために、テレメトリに個々のイベントを手動で追加したり除外したりできます。たとえば、Sysmon イベントを除外できます。

管理コンソール（MMC）で KUMA に送信するイベントのリストを作成する方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。
3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
4. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。
5. ［**テレメトリの設定**］→［**KUMA テレメトリ**］ブロックの［**設定**］をクリックします。
6. 表示されるウィンドウで、KUMA に送信するイベントフィルターを設定します。

   標準の*Application*ログ、*Security*ログ、*System*ログのイベントフィルタリングを設定することも、手動で別のログを追加することもできます。

   a. ［**追加**］をクリックするか、ログのプロパティを開きます。

   b. イベント送信モードを選択します：

   - **すべてのイベントを送信する**：このモードでは、本製品は除外ルールに追加されたイベントを除くすべてのイベントを Windows ログから送信します。
   - **選択したイベントのみ送信する**：このモードでは、本製品は包含ルールに追加されたイベントのみを送信します。

   c. 関連するイベント送信モードの除外ルールまたは包含ルールのリストを作成します。

   ルールを追加するには、Windows イベントログ内のイベントの ID を指定する必要があります。ルール内に複数のイベント ID をリストできます。複数のイベント ID を指定するには、カンマ（,）を使用します。
7. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

Web コンソールで KUMA に送信するイベントのリストを作成する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**テレメトリの設定**］に移動します。
5. ［**KUMA テレメトリ**］タブを選択します。
6. 表示されるウィンドウで、KUMA に送信するイベントフィルターを設定します。
   標準の*Application*ログ、*Security*ログ、*System*ログのイベントフィルタリングを設定することも、手動で別のログを追加することもできます。
   a. ［**追加**］をクリックするか、ログのプロパティを開きます。
   b. イベント送信モードを選択します：
      - **すべてのイベントを送信する**：このモードでは、本製品は除外ルールに追加されたイベントを除くすべてのイベントを Windows ログから送信します。
      - **選択したイベントのみ送信する**：このモードでは、本製品は包含ルールに追加されたイベントのみを送信します。
   c. 関連するイベント送信モードの除外ルールまたは包含ルールのリストを作成します。
      ルールを追加するには、Windows イベントログ内のイベントの ID を指定する必要があります。ルール内に複数のイベント ID をリストできます。複数のイベント ID を指定するには、カンマ（,）を使用します。
7. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

KUMA イベントフィルターのエクスポートとインポート

除外リストを JSON ファイルにエクスポートすることができます。これにより、たとえば多数のイベント ID をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、イベントフィルターのバックアップをとったり、別のサーバーにリストを移行することができます。

使用するルールが多すぎると、KUMA サーバーへの負荷が増えて、コンピューターのパフォーマンスが低下することがあります。必要なルールのみを追加することを推奨します。

管理コンソール（MMC）でイベントフィルターをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**ポリシー**］を選択します。

3. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

4. ポリシーウィンドウで、［**全般設定**］→［**除外リストとオブジェクト種別**］の順に選択します。

5. ［**テレメトリの設定**］→［**KUMA テレメトリ**］ブロックの［**設定**］をクリックします。

6. イベントフィルターをエクスポートするには：

   a. エクスポートするフィルター付きのイベントログを選択します。

   b. → ［**エクスポート**］を選択します。

   c. 表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。

   d. ファイルを保存します。

   Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。

7. イベントフィルターをインポートするには：

   a. → ［**インポート**］を選択します。

   b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。

   c. ファイルを開きます。

   コンピューターにイベントフィルタリングルールが既に存在する場合、Kaspersky Endpoint Security はインポート時にそれらを置き換えます。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

Web コンソールでイベントフィルターをエクスポートおよびインポートする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］タブを選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**テレメトリの設定**］に移動します。

5. ［**KUMA テレメトリ**］タブを選択します。

6. イベントフィルターをエクスポートするには：

   a. エクスポートするフィルター付きのイベントログを選択します。

   b. → ［**エクスポート**］を選択します。

   c. 表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。

d. ファイルを保存します。

Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。

7. イベントフィルターをインポートするには：

a. → ［**インポート**］を選択します。

b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。

c. ファイルを開きます。

コンピューターにイベントフィルタリングルールが既に存在する場合、Kaspersky Endpoint Security はインポート時にそれらを置き換えます。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、南京錠を閉じます（）。

コマンドラインでイベントフィルターをエクスポートまたはインポートすることもできます。

KSWS から KES への移行ガイド

バージョン 11.8.0 から、Kaspersky Endpoint Security for Windows は Kaspersky Security for Windows Server (KSWS) ソリューションの基本的な機能をサポートするようになりました。*Kaspersky Security for Windows Server* は、Microsoft Windows オペレーティングシステムで動作するサーバーとネットワーク接続ストレージを、ファイル交換を介してサーバーやネットワーク接続ストレージに影響を及ぼすウイルスなどのコンピューターセキュリティの脅威から保護します。ソリューションについて詳しくは、Kaspersky Security for Windows Server のヘルプを参照してください。Kaspersky Endpoint Security 11.8.0 より、Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows に移行して、ワークステーションおよびサーバーを保護する同一のソリューションを使用できるようになりました。

ソフトウェア要件

KSWS から KES への移行を開始する前に、Kaspersky Endpoint Security for Windows のハードウェアおよびソフトウェアの要件を満たしていることを確認してください。サポートされるオペレーティングシステムは KES と KSWS で異なります。例えば、KES は Windows Server 2003 を実行しているサーバーをサポートしていません。

KSWS から KES へ移行するための最小ソフトウェア要件：

- Kaspersky Endpoint Security for Windows 12.0
- Kaspersky Security 11.0.1 for Windows Server

  Kaspersky Security for Windows Server の以前のバージョンがインストールされている場合は、最新版にアップデートしてください。ポリシーとタスクの一括変換ウィザードは、Kaspersky Security for Windows Server の以前のバージョンをサポートしていません。
- Kaspersky Security Center 14.2

  Kaspersky Security Center の以前のバージョンがインストールされている場合は、14.2 以降のバージョンにアップデートしてください。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、ポリシーではなくプロファイルに移行することができます。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、より広い範囲のポリシー設定を移行することができます。
- Kaspersky Endpoint Agent 3.10

  Kaspersky Endpoint Agent の以前のバージョンがインストールされている場合は、最新版にアップデートしてください。Kaspersky Endpoint Agent 3.10 から、Kaspersky Endpoint Security では [KSWS + KEA] 構成から [KES + 組み込みエージェント] への移行がサポートされるようになりました。

移行の推奨事項

KSWS から KES への移行時には、次の推奨事項を検討してください：

- あらかじめ KSWS から KES への移行時刻を検討します。週末など、サーバーの動作中の負荷が一番低い時刻を選択してください。
- 移行後、順次製品コンポーネントをオンにしてください。例えば、ファイル脅威対策を単独で有効にしてから、その他の保護機能をオンにして、その他のコントロールコ機能をオンにするなどの方法をとります。各手順で、本製品が正常に動作していることを確認し、またサーバーのパフォーマンスを監視してください。KES のアーキテクチャは KSWS のものと異なるため、オペレーティングシステムが異なる動作を示す可能性があります。
- 移行は段階的に行ってください。単一のサーバーをまず移行してから複数のサーバーを移行し、それから組織のすべてのサーバーを移行してください。
- 異なる種別のサーバーの移行は別々に実行してください。例えば、データベースサーバーを最初に移行してからメールサーバーなどその他のサーバーを移行します。
- 高負荷のサーバーの移行には特別な考慮事項が必要です。

移行手順

KSWS から KES への移行は半自動で実行されます。これはアプリケーションのアーキテクチャが異なるために必要となります。ポリシー設定の移行には、ポリシーとタスクの一括変換ウィザード（移行ウィザード）を実行する必要があります。ポリシー設定を移行した後、移行ウィザードが対応できなかった設定を手動で設定する必要があります（例えば、パスワードによる保護の設定など）。移行後、すべての設定が正しく移行されたかどうか確認してください。

KSWS から KES への移行は、次の順番で行ってください：

1. **KSWS のタスクとポリシーを移行する**

   ポリシーとタスクを移行した後に、追加の設定手順を実行する必要があります。KSWS からの移行後、Kaspersky Endpoint Security が必要なセキュリティレベルを提供していることを確認してください。

   > Kaspersky Security for Windows Server のポリシーとタスクの一括変換ウィザードは、管理コンソール（MMC）でのみ使用可能です。ポリシーとタスクの設定は Web コンソールおよび Kaspersky Security Center Cloud コンソールでは移行できません。

2. **Kaspersky Endpoint Security をインストールする**

   Kaspersky Endpoint Security は、次の方法でインストールすることができます。

   - KSWS のアンインストール後に KES をインストールする（推奨）。

     > kavremover ユーティリティ は KSWS の管理をサポートしていません。

   - KSWS 上に KES をインストールする。

3. KSWS のライセンスで KES をアクティベートする

4. **移行後、本製品が正しく動作していることを確認する**

   KSWS から KES への移行後、本製品が正しく動作していることを確認してください。コンソールでサーバーのステータスを確認します（[*OK*] になっている必要があります）。製品でエラーがレポートされていないことを確認し、管理サーバーに最後に接続された時刻、定義データベースの最終アップデート時刻およびサーバーの保護ステータスも確認してください。

   除外リスト、信頼するアプリケーション、信頼する URL、アプリケーションコントロールルールの移行には特に注意してください。

KSWS と KES のコンポーネントの対応

KSWS から KES に移行する際、アプリケーションがローカルでインストールされる場合のみ、コンポーネントの組み合わせが移行されます。

Kaspersky Security for Windows Server と Kaspersky Endpoint Security for Windows コンポーネントの対応

Kaspersky Security for Windows Server コンポーネント	Kaspersky Endpoint Security for Windows コンポーネント
基本機能	アプリケーションカーネル
Windows イベントログ監視	Windows イベントログ監視
デバイスコントロール	デバイスコントロール
ファイアウォール管理	*（サポートされていません）* KSWS のファイアウォール機能はシステムレベルのファイアウォールで実行されます。KES では、ファイアウォール機能は個別のコンポーネントが実行されています。移行後、Kaspersky Endpoint Security のファイアウォールを設定できます。
ファイル変更監視	システム変更監視
脆弱性攻撃ブロック	脆弱性攻撃ブロック
システムトレイアイコン	*（サポートされていません）* 製品インターフェイスの設定でユーザーの操作を設定できます。
Kaspersky Security Center との連携	ネットワークエージェントコネクター
Endpoint Agent	*（サポートされていません）* Kaspersky Endpoint Security 11.9.0 では、Kaspersky Endpoint Agent 配布パッケージは Kaspersky Endpoint Security 配信キットには含まれません。Kaspersky Endpoint Agent 配布パッケージは別途ダウンロードする必要があります。
ネットワーク脅威対策	ネットワーク脅威対策
アンチクリプター	ふるまい検知
NetApp のアンチクリプター	*（サポートされていません）*
トラフィックセキュリティ	ウェブ脅威対策 メール脅威対策 ウェブコントロール
オンデマンドスキャン	アプリケーションカーネル
ICAP ネットワークストレージの保護	*（サポートされていません）* Kaspersky Endpoint Security は、ネットワーク接続ストレージの保護コンポーネントをサポートしません。これらのコンポーネントが必要な場合は、Kaspersky Security for Windows Server を引き続き使用することができます。

Kaspersky Security for Windows Server コンポーネント	Kaspersky Endpoint Security for Windows コンポーネント
RPC ネットワークストレージの保護	*（サポートされていません）* Kaspersky Endpoint Security は、ネットワーク接続ストレージの保護コンポーネントをサポートしません。これらのコンポーネントが必要な場合は、Kaspersky Security for Windows Server を引き続き使用することができます。
ファイルのリアルタイム保護	ファイル脅威対策
スクリプト監視	*（サポートされていません）* スクリプト監視は AMSI 保護など、別のコンポーネントにより扱われます。
KSN の使用	Kaspersky Security Network
アプリケーション起動コントロール	アプリケーションコントロール
パフォーマンスカウンター	*（サポートされていません）*

KSWS と KES の設定の対応

ポリシーとタスクの移行時に、KES は KSWS の設定に従って設定されます。KSWS に含まれないアプリケーションコンポーネントの設定は既定値で設定されます。

製品設定

スケーラビリティ、インターフェイスおよびスキャン設定

製品設定は Kaspersky Endpoint Security for Windows ではサポートされません。

製品設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
スケーラビリティ設定	*（移行されません）* Kaspersky Endpoint Security がすべての処理対象プロセスを管理します。
システムトレイアイコンの表示	*（移行されません）* クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウとWindows の通知領域のアイコンが既定で利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。製品インターフェイスの設定でユーザーの操作を設定できます。
スキャン後にファイル属性を復元する	*（移行されません）* ファイルのスキャン後、Kaspersky Endpoint Security は自動的にファイルの属性を復元します。
スレッドのスキャン時に CPU の使用を制限する	*（移行されません）* Kaspersky Endpoint Security はスキャン時の CPU の使用を制限しません。コンピューターの負荷が最も少ないタイミングでタスクを実行するよう設定することができます。
スキャン中に作成された一時ファイルのフォルダー	*（移行されません）* Kaspersky Endpoint Security は一時ファイルを `C:\Windows\Temp` フォルダーに配置します。
HSM システムの設定	*（移行されません）* Kaspersky Endpoint Security は HSM システムをサポートしません。

セキュリティと信頼性

KSWS のセキュリティ設定は［**全般設定**］セクション、［**アプリケーション設定**］および［**インターフェイス**］サブセクションに移行されます。

製品のセキュリティ設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
アプリケーションプロセスを外部の脅威から保護する	**セルフディフェンスを有効にする**（［**アプリケーション設定**］サブセクション）
パスワードによる保護を適用する	*（移行されません）* Kaspersky Endpoint Security には組み込みのパスワードによる保護機能があります（［**インターフェイス**］サブセクションを参照してください）。
タスク復元を実行する	*（移行されません）* Kaspersky Endpoint Security はマルウェアのスキャンのみ自動で復元します。その他のタスクはスケジュールに沿って実行されます。
スケジュール設定済みのスキャンタスクを開始しない	**バッテリー使用中はスケジュールタスクを延期する**（［**アプリケーション設定**］サブセクション）
現在のスキャンタスクを中止する	*（移行されません）* コンピューターが UPS 電源に切り替えた場合、Kaspersky Endpoint Security は既に実行中のスキャンタスクを中止しません。

接続設定

管理サーバーとのインタラクション設定は［**全般設定**］セクション、［**ネットワーク設定**］および［**アプリケーション設定**］サブセクションに移行されます。

管理サーバーのインタラクション設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
プロキシサーバー設定	**プロキシサーバー設定**（［**ネットワーク設定**］サブセクション）
ローカルアドレスへの接続時はプロキシサーバーを使用しない	**ローカルアドレスにはプロキシサーバーを使用しない**（［**ネットワーク設定**］サブセクション）
プロキシサーバーの認証設定	**プロキシサーバー認証を使用する**（［**ネットワーク設定**］サブセクション） プロキシサーバー認証のパスワードは移行されません。ポリシーの移行後、パスワードを手動で入力する必要があります。
アプリケーションのアクティベーション時に Kaspersky Security Center をプロキシサーバーとして使用する	**アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する**（［**アプリケーション設定**］サブセクション）

ローカルシステムタスクの実行

Kaspersky Endpoint Security では Kaspersky Security for Windows Server のローカルシステムタスクの実行に関する設定は無視されます。［**ローカルタスク**］、［**タスク管理**］で、ローカル KES タスクを設定することができます。*マルウェアのスキャン*および*定義データベースと製品機能のアップデート*タスクは、タスクのプロパティで実行スケジュールを設定することができます。

詳細設定

信頼ゾーン

KSWS の信頼ゾーンの設定は［**全般設定**］セクション、［**除外リスト**］サブセクションに移行されます。

信頼ゾーンの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
スキャン対象オブジェクト（除外リスト）	**信頼するオブジェクト**（信頼するオブジェクト） KSWS および KES により、オブジェクトの選択に使用される方法は異なります。移行時に、KES は個別のファイルまたはファイルまたはフォルダーのパスとして定義された除外リストをサポートします。KSWS が事前定義された領域またはスクリプト URL に対する除外リストを持っていた場合は、これらの除外リストは移行されません。移行後にこれらの除外リストを手動で追加する必要があります。事前定義された領域としての除外リストは、［*マルウェアのスキャン*］タスク設定で設定する必要があります。スクリプト Web アドレスとしての除外リストは、ウェブ脅威対策の信頼する Web アドレスに追加する必要があります。
サブフォルダーにも適用（除外リスト）	**サブフォルダーを含む**（信頼するオブジェクト）
検知対象オブジェクト（除外リスト）	**検知するオブジェクトの種別**（信頼するオブジェクト）
除外の適用範囲（除外リスト）	**保護機能**（信頼するオブジェクト） 少なくとも 1 つのコンポーネントが KSWS で選択されていた場合は、KES は除外リストをすべての製品コンポーネントに適用します。
コメント（除外リスト）	**コメント**（信頼するオブジェクト）
信頼するプロセス（信頼するプロセス）	**信頼するアプリケーション** 信頼するプロセス / アプリケーションの選択方法は KSWS と KES では異なります。移行時に、実行ファイルへのパスまたはマスクとして設定された信頼するアプリケーションをサポートします。KSWS にファイルのハッシュとして設定された信頼するプロセスがある場合、このような信頼するプロセスは移行されません。移行後にこれらの信頼するプロセスを手動で追加する必要があります。
ファイルのバックアップ処理を確認しない（信頼するプロセス）	**アプリケーションの動作を監視しない**（信頼するアプリケーション）

リムーバブルドライブのスキャン

リムーバブルドライブのスキャンの設定は［**ローカルタスク**］セクション、［**リムーバブルドライブスキャン**］サブセクションに移行されます。

リムーバブルドライブスキャンの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
USB 経由の接続でリムーバブルドライブをスキャンする	**リムーバブルドライブ接続時の処理**
格納データ容量がこの値以下ならリムーバブルドライブをスキャンする（MB）	**リムーバブルドライブの最大サイズ**
次のセキュリティレベルでスキャンする： • **最大の保護** • **推奨** • **最高のパフォーマンス**	**リムーバブルドライブ接続時の処理**： • **最大の保護** • **推奨** KSWS のセキュリティレベルは次のように KES スキャンモードに対応します： • 最大の保護 – 最大の保護 • 推奨 – 推奨 • 最高のパフォーマンス – 推奨

アプリケーション管理用のユーザー権限

Kaspersky Endpoint Security はアプリケーション管理用のユーザーアクセス権限およびアプリケーションサービスの管理の割り当てはサポートしません。アプリケーションの管理用のユーザーおよびユーザーグループのアクセス権の設定は Kaspersky Security Center で設定できます。

Kaspersky Security サービス管理用のユーザーアクセス権限

Kaspersky Endpoint Security はアプリケーション管理用のユーザーアクセス権限およびアプリケーションサービスの管理の割り当てはサポートしません。アプリケーションの管理用のユーザーおよびユーザーグループのアクセス権の設定は Kaspersky Security Center で設定できます。

保管領域

KSWS 保管領域の設定は［**全般設定**］セクション、［**レポートと保管領域**］サブセクション、［**脅威対策**］セクション、［**ネットワーク脅威対策**］サブセクションに移行されます。

保管領域の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
バックアップフォルダー	*（移行されません）* Kaspersky Endpoint Security はファイルのバックアップコピーを `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` フォルダーに保存します。
バックアップの最大サイズ（MB）	**バックアップのサイズを制限する**（［**全般設定**］→［**レポートと保管領域**］セクション）
空き容量のしきい値（MB）	*（移行されません）* Kaspersky Endpoint Security はしきい値 50% に達した場合、イベント「*隔離の保管領域の容量がまもなく上限に達します*」を記録します。
オブジェクトの復元先フォルダー	*（移行されません）* Kaspersky Endpoint Security はファイルを元のフォルダーに復元します。
隔離フォルダー	*（移行されません）* Kaspersky Endpoint Security はファイルのバックアップコピーを `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` フォルダーに保存します。
隔離の最大サイズ（MB）	*（移行されません）* Kaspersky Endpoint Security は感染の可能性のあるオブジェクトをバックアップに保存します。移行中、Kaspersky Endpoint Security は隔離の設定を無視します。
空き容量のしきい値（MB）	*（移行されません）* Kaspersky Endpoint Security は感染の可能性のあるオブジェクトをバックアップに保存します。移行中、Kaspersky Endpoint Security は隔離の設定を無視します。
オブジェクトの復元先フォルダー	*（移行されません）* Kaspersky Endpoint Security はファイルを元のフォルダーに復元します。
自動的にブロック解除するまでの時間	**攻撃元の端末をブロックする時間**（［**脅威対策**］→［**ネットワーク脅威対策**］セクション）

サーバーのリアルタイム保護

ファイルのリアルタイム保護

KSWS のファイルのリアルタイム保護の設定は［**脅威対策**］セクション、［**ファイル脅威対策**］サブセクションに移行されます。

ファイルのリアルタイム保護の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
オブジェクトの保護モード： • **スマートモード** • **実行時** • **アクセス時** • **アクセス時と変更時**	**スキャンモード：** • **スマートモードでスキャン** • **ファイルの実行時にスキャン** • **ファイルのアクセス時にスキャン** • **ファイルのアクセス時と更新時にスキャン**
起動プロセスのより詳細な分析	*（移行されません）* Kaspersky Endpoint Security は最適なモードの分析モードを 1 つのみサポートします。
ヒューリスティックアナライザー： • **低** • **中** • **高**	**ヒューリスティック分析：** • **スキャン（レベル低）** • **スキャン（レベル中）** • **スキャン（レベル高）**
信頼ゾーンを適用する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントに信頼ゾーンを適用します。信頼ゾーンの設定内で除外を設定することができます。
保護に KSN を使用する	*（移行されません）* Kaspersky Endpoint Security はすべての製品コンポーネントに KSN を使用します。
悪意のある活動を示すコンピューターのネットワーク共有リソースへのアクセスをブロックする	*（移行されません）* 既定では、Kaspersky Endpoint Security は、悪意のある動作を示すホストに対してネットワーク共有リソースへのアクセスをブロックします。
アクティブな脅威の検知時に簡易スキャンを起動する	*（移行されません）* Kaspersky Endpoint Security はアクティブな脅威が検知された場合は簡易スキャンタスクを実行しません。
保護に Kaspersky Sandbox を使用する	*（移行されません）* 既定では、Kaspersky Endpoint Security はスキャンのため Kaspersky Sandbox にオブジェクトを送ります。
保護範囲	**保護範囲**
スケジュール設定	*（移行されません）* Kaspersky Endpoint Security はファイル脅威対策の一時停止に Kaspersky Endpoint Security のスケジュールを使用します。

KSN の使用

KSWS の Kaspersky Security Network の設定は［**先進の脅威対策**］セクション、［**Kaspersky Security Network**］サブセクションに移行されます。

Kaspersky Security Network の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
Kaspersky Security Network への参加に関する条項をすべて確認し、理解した上で同意する	**Kaspersky Security Network に関する声明** Kaspersky Endpoint Security は製品インストール時、ポリシーの新規作成時、Kaspersky Security Network の使用が有効にされたときに Kaspersky Security Network に関する声明への同意を求めます。
スキャンしたファイルに関するデータを送信	*（移行されません）* KSN が有効になると、Kaspersky Endpoint Security はスキャンしたファイルに関するデータを自動的に送信します。
要求した URL に関するデータを送信	*（移行されません）* KSN が有効になると、Kaspersky Endpoint Security は要求された URL に関するデータを自動的に送信します。
Kaspersky Security Network に統計情報を送信	**拡張 KSN モードを有効にする**
Kaspersky Managed Protection に関する声明の条項に同意する	*（移行されません）* Kaspersky Endpoint Security には KMP サービスは含まれません。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
KSN で信頼されていないオブジェクトに対する処理	*（移行されません）* 保護機能の設定およびスキャンタスクの設定で、脅威の検知時の処理を設定することができます。
ファイルサイズが次の値を超えたら KSN に送信する前にチェックサムを計算しない	*（移行されません）* 保護機能の設定およびスキャンタスクの設定で、サイズの大きいファイルに対するスキャンの制限を設定することができます。
Kaspersky Security Center を KSN プロキシとして使用する	**管理サーバーを KSN プロキシサーバーとして使用する**
スケジュール設定	*（移行されません）* コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

トラフィックセキュリティ

KSWS のトラフィックセキュリティの設定は［**脅威対策**］セクション、［**ウェブ脅威対策**］および［**メール脅威対策**］サブセクション、［**セキュリティコントロール**］セクション、［**ウェブコントロール**］サブセクション、［**全般設定**］セクション、［**ネットワーク設定**］サブセクションに移行されます。

トラフィックセキュリティの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
URL ベースのルールを適用する	**ウェブコントロール**（［**ウェブコントロール**］サブセクション） URL ベースのルールは Kaspersky Endpoint Security の別個のルールに移行されます。
証明書ベースのルールを適用する	*（移行されません）* Kaspersky Endpoint Security は、証明書ベースのルールをサポートしません。
Web トラフィックカテゴリコントロールにルールを適用する	**ウェブコントロール**（［**ウェブコントロール**］サブセクション） Web トラフィックカテゴリコントロールのブロックルールは Kaspersky Endpoint Security では単一のブロックルールに移行されます。カテゴリコントロールの許可ルールは Kaspersky Endpoint Security では無視されます。 KSWS と KES のカテゴリの対応は下記にあります。
Web ページをカテゴリに分類できない場合はアクセスを許可する	*（移行されません）* Kaspersky Endpoint Security は Web ページをカテゴリに分類できない場合はアクセスを許可します。
保護対象デバイスに損害を与えるために使用される可能性がある、正規の Web リソースへのアクセスを許可する	*（移行されません）* Kaspersky Endpoint Security は保護対象デバイスに損害を与えるために使用される可能性がある、正規の Web リソースへのアクセスを許可します。
正規の広告へのアクセスを許可する	*（移行されません）* ウェブコントロールの設定で Web リソース［*バナー広告*］を使用して正規の広告へのアクセスを管理することができます。
動作モード： • **ドライバーインターセプター** • **リダイレクター** • **外部プロキシ**	*（移行されません）* Kaspersky Endpoint Security はドライバーインターセプターモードのみサポートします。
ICAP サービス接続設定	*（移行されません）* Kaspersky Endpoint Security は ICAP ネットワークストレージの保護をサポートしません。
HTTPS プロトコル経由の安全な接続をスキャンする	［**暗号化された接続をスキャン**］/［**常に暗号化された接続をスキャンする**］モード（［**ネットワーク設定**］サブセクション）
次の TLS プロトコルバージョンを使用する	*（移行されません）* Kaspersky Endpoint Security は次のプロトコルを介して通信される暗号化されたネットワークトラフィックをスキャンします： • SSL 3.0 • TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3 暗号化された接続のスキャンの設定で SSL 2.0 接続を追加でブロックすることができます。
証明書が無効の Web サーバーを信頼しない	**アドレス**（［**ネットワーク設定**］サブセクション）

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
ポートの監視（監視領域）	**監視対象のポート**（［**ネットワーク設定**］サブセクション） 移行中、KES は［**カスペルスキー推奨のリストに登録されているアプリケーションのすべてのポートを監視する**］、および［**選択したアプリケーションのすべてのポートを監視する**］をオフにします。
ポートの除外（監視領域）	*（移行されません）*
IP アドレスの除外（監視領域）	**信頼するアドレスを設定**（［**ネットワーク設定**］サブセクション）
プロセスの除外（監視領域）	**信頼するアプリケーションを設定**（［**ネットワーク設定**］サブセクション） 移行中、KES は次の信頼するアプリケーションを設定します： • ［**ネットワークトラフィックをスキャンしない**］をオンにします。KES はいずれの IP アドレスおよびポートのネットワークトラフィックをスキャンしません。 • その他の信頼するアプリケーションの設定のチェックボックスはオフになります。
セキュリティポート	*（移行されません）*
悪意のある URL データベースを使用して Web リンクをスキャンする	**悪意のある Web アドレスのデータベースで Web アドレスをチェックする**（［**ウェブ脅威対策**］サブセクション）
アンチフィッシングデータベースを使用して Web ページをスキャンする	**フィッシングサイトのデータベースで Web アドレスをチェックする**（［**ウェブ脅威対策**］サブセクション）
保護に KSN を使用する	*（移行されません）* Kaspersky Endpoint Security はすべての製品コンポーネントに KSN を使用します。
信頼ゾーンを使用する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントに信頼ゾーンを適用します。信頼ゾーンの設定内で除外を設定することができます。
ヒューリスティックアナライザーを使用する	**ヒューリスティック分析を使用する**（［**ウェブ脅威対策**］および［**メール脅威対策**］サブセクション）
セキュリティレベル	*（移行されません）* Kaspersky Endpoint Security にはウェブ脅威対策およびメール脅威対策コンポーネントに独自のセキュリティレベルがあります。既定では、Kaspersky Endpoint Security は推奨されるセキュリティレベルを設定します。
メール脅威対策を有効にする	**メール脅威対策**（［**メール脅威対策**］サブセクション） **Microsoft Outlook アドインに接続** **受信メッセージ**（保護範囲） **メール受信時にスキャンする**（メール保護）
スケジュール設定	*（移行されません）* コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

脆弱性攻撃ブロック

KSWS の脆弱性攻撃ブロックの設定は［**先進の脅威対策**］セクション、［**脆弱性攻撃ブロック**］サブセクションに移行されます。

脆弱性攻撃ブロックの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
脆弱なプロセスに対する攻撃から防御する： • **脆弱性攻撃時に終了する** • **通知のみ**	**攻撃を検知したとき**： • **ブロックする** • **通知する**
脆弱性攻撃を受けたプロセスについてターミナルサービスから通知する	*（移行されません）* Kaspersky Endpoint Security はターミナルサービスをサポートしません。
Kaspersky Security サービスが無効の場合にも脆弱なプロセスに対する攻撃を防御する	*（移行されません）* Kaspersky Endpoint Security は継続的に脆弱なプロセスに対する攻撃から防御します。
保護対象プロセス	**システムプロセスのメモリ保護を有効にする** Kaspersky Endpoint Security は、保護されたプロセスの選択をサポートしません：システムプロセスのメモリ保護を有効にすることのみ可能です。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
脆弱性攻撃ブロック技術： • **利用できるすべての脆弱性攻撃ブロック技術を適用する** • **選択した脆弱性攻撃ブロック技術を適用する**	*（移行されません）* Kaspersky Endpoint Security は利用できるすべての脆弱性攻撃ブロック技術を適用します。

ネットワーク脅威対策

KSWS のネットワーク脅威対策の設定は［**脅威対策**］セクション、［**ネットワーク脅威対策**］サブセクションに移行されます。

ネットワーク脅威対策の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
動作モード： • **処理しない** • **ネットワーク攻撃の通知のみ行う** • **攻撃の検知時に接続をブロックする**	**ネットワーク脅威対策** ［**処理しない**］が選択されている場合、ネットワーク脅威対策は無効になります。 ［**ネットワーク攻撃の通知のみ行う**］または［**攻撃の検知時に接続をブロックする**］が選択されている場合、ネットワーク脅威対策は有効になります。Kaspersky Endpoint Security は常に［**攻撃の検知時に接続をブロックする**］モードで動作します。
タスクが実行されていない時にトラフィック分析を停止しない	*（移行されません）* Kaspersky Endpoint Security はコンポーネントが有効にされている場合継続的にトラフィックを分析します。
除外された IP アドレスを管理しない	**除外リスト**
スケジュール設定	*（移行されません）* コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

スクリプト監視

Kaspersky Endpoint Security は、スクリプト監視コンポーネントをサポートしません。スクリプト監視は AMSI 保護など、別のコンポーネントにより扱われます。

Web サイトのカテゴリ

Kaspersky Endpoint Security では Kaspersky Security for Windows Server のカテゴリのすべてはサポートされません。Kaspersky Endpoint Security に存在しないカテゴリは移行されません。そのため、サポートされないカテゴリを持つ Web リソースの分類ルールは移行されません。

Web サイトのカテゴリ

Kaspersky Security for Windows Server のカテゴリ	Kaspersky Endpoint Security for Windows のカテゴリ
戦争ゲーム	ビデオゲーム
妊娠中絶	*（移行されません）*
宝くじ（広域）	ギャンブル、宝くじ、懸賞
アルコール	アルコール、タバコ、ドラッグ
匿名プロキシサーバー	アノニマイザー
拒食症	*（移行されません）*
不動産の賃貸	*（移行されません）*
音楽、映像、ソフトウェア	ソフトウェア、音声、映像
銀行	銀行
ブログ	ブログ
軍隊	武器、爆発物、軍事
子ども向け	*（移行されません）*

Kaspersky Security for Windows Server のカテゴリ	Kaspersky Endpoint Security for Windows のカテゴリ
差別	暴力、不寛容
家庭と家族	*（移行されません）*
ホスティングとドメインサービス	インターネットコミュニケーション
ペットと動物	*（移行されません）*
法律と政治	国・地域の法律による禁止対象
ロシア通信規制当局による制限（ロシア連邦）	ロシア連邦の法律による禁止対象
連邦法 436 による制限（ロシア連邦）	ロシア連邦の法律による禁止対象
ロシア連邦法による制限	ロシア連邦の法律による禁止対象
グローバルな法的制限	国・地域の法律による禁止対象
成人向け出会い系サイト	アダルト
インターネットサービス	*（移行されません）*
アダルトショップ	アダルト
情報技術	*（移行されません）*
カジノ、トランプゲーム	ギャンブル、宝くじ、懸賞
書籍と著作物	*（移行されません）*
コンピューターゲーム	ビデオゲーム
健康と美容	*（移行されません）*
文化と社会	*（移行されません）*
LGBT	アダルト
宝くじ	ギャンブル、宝くじ、懸賞
薬剤	*（移行されません）*
ファッション	*（移行されません）*
音楽	*（移行されません）*
ドラッグ	アルコール、タバコ、ドラッグ
暴力	暴力、不寛容
不満	*（移行されません）*
違法ドラッグ	アルコール、タバコ、ドラッグ
憎悪と差別	暴力、不寛容
わいせつな語彙	過激な表現、わいせつな表現
ランジェリー	アダルト
ニュース	ニュース
ヌード	アダルト
教育	*（移行されません）*
オンラインショッピング	オンラインストア
すべての通信媒体	インターネットコミュニケーション
クレジットカードによる決済	決済システム
オンラインショッピング（独自の決済システム）	オンラインストア
オンライン百科事典	*（移行されません）*
オンラインバンキング	銀行
武器	武器、爆発物、軍事
魚釣りと狩猟	*（移行されません）*

Kaspersky Security for Windows Server のカテゴリ	Kaspersky Endpoint Security for Windows のカテゴリ
決済システム	決済システム
求人サイト	求人サイト
検索エンジン	*（移行されません）*
警察機関指定の危険サイト（日本）	日本の警察庁主導の取組みによる禁止対象
KPSN により信頼されている	*（移行されません）*
KPSN により信頼されていない	*（移行されません）*
ポルノ	アダルト
メディアのホスティングとストリーミング	ニュース
Web メール	Web メール
旅行	*（移行されません）*
テレビとラジオ	ニュース
ティーザーと広告サービス	バナー広告
宗教	宗教、宗教団体
レストラン、カフェおよび食品	*（移行されません）*
出会い系サイト	出会い系サイト
性教育	アダルト
SNS	SNS
スポーツ	*（移行されません）*
賭博	ギャンブル、宝くじ、懸賞
自殺	暴力、不寛容
タバコ	アルコール、タバコ、ドラッグ
Torrent	Torrent
国の過激派リストに記載（ロシア連邦）	ロシア連邦の法律による禁止対象
ファイル共有	ファイル共有
薬局	*（移行されません）*
趣味とエンターテインメント	*（移行されません）*
チャットとフォーラム	チャット、フォーラム、メッセンジャー
学校と大学のページ	*（移行されません）*
占星術と秘儀	*（移行されません）*
過激思想と人種差別	暴力、不寛容
電子商取引	オンラインストア
性愛	アダルト
ユーモア	*（移行されません）*

ローカル活動の管理

アプリケーション起動コントロール

KSWS のアプリケーションコントロールの設定は［**セキュリティコントロール**］セクション、［**アプリケーションコントロール**］サブセクションに移行されます。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
動作モード： • **統計のみ** • **処理を実行**	**処理**（アプリケーションコントロール）： • **ルールをテスト運用** • **ルールを適用**
最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す	*（移行されません）* Kaspersky Endpoint Security はアプリケーションの実行の試行を常にスキャンします。
実行するコマンドのないコマンドインタープリターの起動を拒否する	*（移行されません）* アプリケーションコントロールで禁止されていない場合は、Kaspersky Endpoint Security はコマンドインタープリターの実行を許可します。
ルール	**アプリケーションコントロールルール***（制限付きでサポートされます）* Kaspersky Endpoint Security 11.11.0 ではアプリケーション起動コントロールルールのサポートが導入されました。 アプリケーション起動コントロールルールの移行機能には一部の制限事項があります。規定では、KSWS のアプリケーション起動コントロールには次の 2 つのルールが含まれます： • **OS が信頼する証明書によってスクリプトおよび MSI を許可する** • **OS が信頼する証明書によって実行ファイルを許可する** 元の KSWS の 1 つ以上のルールに［**許可**］種別がある場合、移行中に KES は新しい許可ルール［**信頼するルート証明書**］を作成します。KES のアプリケーションコントロールは信頼するスクリプト、MSI パッケージおよび実行ファイルの実行を許可するために単一のルールを使用します。両方のソースの KSWS ルールに［**ブロック**］種別が含まれる場合は、KES は信頼するルート証明書を持つアプリケーションの管理用のルールを追加しません。
実行ファイルにルールを適用する	*（移行されません）* ルールの適用範囲は KES のアプリケーションコントロールの設定では設定できません。KES のアプリケーションコントロールは、実行ファイル、スクリプトと MSI パッケージのすべての種別のファイルにルールを適用します。すべてのファイル種別が KSWS のルール適用範囲に含まれている場合は、KES は移行中に KSWS のルールを引き継ぎます。一部のファイル種別が KSWS のルール適用範囲から除外されていた場合は、KES は移行中に KSWS ルールを引き継ぎますが、アプリケーションコントロールの処理として［**ルールをテスト運用**］が選択されます。
DLL モジュールの読み込みを監視する	**DLL モジュールの読み込みの監視（システムの負荷が大きくなります）**
スクリプトと MSI パッケージにルールを適用する	*（移行されません）* ルールの適用範囲は KES のアプリケーションコントロールの設定では設定できません。KES のアプリケーションコントロールは、実行ファイル、スクリプトと MSI パッケージのすべての種別のファイルにルールを適用します。すべてのファイル種別が KSWS のルール適用範囲に含まれている場合は、KES は移行中に KSWS のルールを引き継ぎます。一部のファイル種別が KSWS のルール適用範囲から除外されていた場合は、KES は移行中に KSWS ルールを引き継ぎますが、アプリケーションコントロールの処理として［**ルールをテスト運用**］が選択されます。
KSN で信頼されていないアプリケーションを拒否する	*（移行されません）* Kaspersky Endpoint Security はアプリケーションの評価を判断に使用せず、ルールに従ってアプリケーションの実行を許可またはブロックします。
KSN で信頼されているアプリケーションを許可する	移行中、KES は新しい許可ルールを追加します。KL カテゴリ［**その他のソフトウェア\アプリケーション、KSN の評価によって信頼済み**］はルール適用条件として指定されています。
KSN で信頼されているアプリケーションの実行を許可するユーザーまたはユーザーグループ	KL カテゴリ（**その他のソフトウェア\アプリケーション、KSN の評価によって信頼済み**）を含むアプリケーションコントロールの許可ルールの**ユーザーとその権限**。
リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルールを追加します。ファイルのハッシュはルール適用条件として指定されます。
Windows インストーラーによるソフトウェア配布を常に許可する	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルール（［**ソフトウェア配布アプリケーションとパッケージが許可されています**］）を追加します。ファイルのハッシュはルール適用条件として指定されます。アカウントのプロパティ［**信頼するアップデーター**］はオンになります。
バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する	*（移行されません）*

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
許可されているソフトウェア配布アプリケーションおよびパッケージ	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルールを追加します。ファイルのハッシュはルール適用条件として指定されます。アカウントのプロパティ［**信頼するアップデーター**］はオンになります。
スケジュール設定	*（移行されません）* KSWS の設定でスケジュールが設定されていた場合、アプリケーションコントロールコンポーネントは移行時に有効になります。KSWS の設定でスケジュールが設定されていなかった場合、アプリケーションコントロールは無効になります。 コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

デバイスコントロール

KSWS のデバイスコントロールの設定は［**セキュリティコントロール**］セクション、［**デバイスコントロール**］サブセクションに移行されます。

デバイスコントロールの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
動作モード： • **処理を実行** • **統計のみ**	*（移行されません）* アプリケーションコントロールはアクティブモードで動作します。デバイスの接続統計は継続的に監査で提供されます。
デバイスコントロールタスクが実行されていない時にすべての外部デバイスの使用を許可する	*（移行されません）* デバイスコントロールは Kaspersky Endpoint Security が実行されているときには常にオンになっています。
デバイスコントロールルール	**信頼するデバイス** 移行中、Kaspersky Endpoint Security は無効にされた KSWS のルールを無視します。
スケジュール設定	*（移行されません）* Kaspersky Endpoint Security は、特定のデバイス種別にアクセスする場合に固有のスケジュールを使用します。

ネットワーク接続ストレージの保護

RPC ネットワークストレージの保護

Kaspersky Endpoint Security は、ネットワーク接続ストレージの保護コンポーネントをサポートしません。これらのコンポーネントが必要な場合は、Kaspersky Security for Windows Server を引き続き使用することができます。

ICAP ネットワークストレージの保護

Kaspersky Endpoint Security は、ネットワーク接続ストレージの保護コンポーネントをサポートしません。これらのコンポーネントが必要な場合は、Kaspersky Security for Windows Server を引き続き使用することができます。

NetApp のアンチクリプター

Kaspersky Endpoint Security は NetApp のアンチクリプターをサポートしません。アンチクリプター機能はふるまい検知など、別の製品コンポーネントにより提供されます。

ネットワーク活動の管理

ファイアウォール管理

Kaspersky Endpoint Security は KSWS のファイアウォール管理をサポートしません。KSWS のファイアウォール機能はシステムレベルのファイアウォールで実行されます。移行後、Kaspersky Endpoint Security のファイアウォールを設定できます。

アンチクリプター

ネットワークのアンチクリプターの設定は［**先進の脅威対策**］セクション、［**ふるまい検知**］サブセクションに移行されます。

アンチクリプターの設定

KSWS の設定	KES の設定
動作モード： • **統計のみ** • **処理を実行**	**外部からの共有フォルダーの暗号化を検知したとき**： • **通知する** • **ブロックする**
ヒューリスティックアナライザー	*（移行されません）* Kaspersky Endpoint Security はふるまい検知にヒューリスティック分析を使用しません。
保護範囲の設定： • **保護対象デバイス上のすべてのネットワーク共有フォルダー** • **指定した共有フォルダーのみ**	*（移行されません）* Kaspersky Endpoint Security は保護対象コンピューターのすべての共有ネットワークフォルダーの暗号化をブロックします。
除外リスト	*（移行されません）* Kaspersky Endpoint Security には固有のふるまい検知コンポーネント向けの除外リストがあります。移行後に手動で除外リストを追加できます。
スケジュール設定	*（移行されません）* コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

システム監査

ファイル変更監視

KSWS のファイル変更監視の設定は［**セキュリティコントロール**］セクション、［**システム変更監視**］サブセクションに移行されます。

ファイル変更監視の設定

KSWS の設定	KES の設定
監視中断期間におけるファイル操作の情報を記録する	*（移行されません）* Kaspersky Endpoint Security は監視中断期間におけるファイル操作の情報は記録しません。
USN ログを不正に利用しようとする動作をブロックする	*（移行されません）* Kaspersky Endpoint Security は USN ログを不正利用しようとする動作をブロックしません。
監視範囲	［**監視範囲**］→［**ファイル**］*（制限付きでサポートされます）* 無効にされた監視範囲の記録は KES に移行されません。Kaspersky Endpoint Security は有効な監視範囲の記録のみ追加します。
信頼するユーザー	**信頼するユーザーまたはユーザーグループ**
ファイル操作マーカー	**ファイル操作マーカー**

KSWS の設定	KES の設定
可能な場合、ファイルのチェックサムを計算する	**ハッシュ**
除外リスト	［**除外リスト**］→［**ファイル**］

Windows イベントログ監視

KSWS の Windows イベントログ監視の設定は［**セキュリティコントロール**］セクション、［**Windows イベントログ監視**］サブセクションに移行されます。

Windows イベントログ監視の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
Windows イベントログ監視にカスタムルールを適用する	*（移行されません）* Kaspersky Endpoint Security すべての有効なカスタムルールを適用します。
カスタムルール	**カスタムルール** 事前定義済みのルール［**システム（Server 2003 OS）にサービスがインストールされました**］は KES には移行されません。
Windows イベントログ監視に定義済みのルールを適用する	*（移行されません）* Kaspersky Endpoint Security はすべての有効な事前定義済みのルールを適用します。
定義済みのルール	**事前定義済みのルール**
パスワードのブルートフォース攻撃の検知	**ブルートフォース攻撃の検知**
ネットワークログオンの検出	**ネットワークログオンの検知**
除外リスト（IP アドレス）	**除外リスト**（IP アドレス）
除外リスト（ユーザー）	**除外リスト**（ユーザー）
スケジュール設定	*（移行されません）* コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

ログと通知

実行ログ

KSWS のログの設定は［**全般設定**］セクション、［**インターフェイス**］および［**レポートと保管領域**］サブセクションに移行されます。

ログの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
イベントログ	**通知**（［**インターフェイス**］サブセクション）
ログフォルダー	*（移行されません）* Kaspersky Endpoint Security はレポートを `C:\ProgramData\Kaspersky Lab\KES.12.12\Report` フォルダーに保存します。
実行ログの保管日数	*（移行されません）* KES のレポートの保管期間は［**全般設定**］、［**レポートと保管領域**］で設定できます。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
監査ログイベントから削除	*（移行されません）* Kaspersky Endpoint Security はシステム監査レポートを含むすべてのレポートにレポート保管領域の制限を適用します。
SIEM との連携	*（移行されません）* Kaspersky Security Center で SIEM との連携を設定できます。

イベント通知

KSWS の通知の設定は［**全般設定**］セクション、［**インターフェイス**］サブセクションに移行されます。

通知の設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
通知	**通知**
ユーザーへの通知： • **ターミナルサービスを使用** • **Windows Messenger サービスコマンドを使用**	*（移行されません）* Kaspersky Endpoint Security では、通知用テキストの編集はサポートされません。Kaspersky Endpoint Security では標準の通知が表示されます。
管理者への通知： • **Windows Messenger サービスコマンドを使用** • **実行ファイルを実行** • **メールを送信**	メール通知の設定のみ Kaspersky Endpoint Security に移行されます。［**メール通知の設定**］（**通知**ブロック）その他方法での管理者への通知はサポートされません。
定義データベースがアップデートされていません	**定義データベースの未アップデートを通知する未アップデート期間**
定義データベースが長期間アップデートされていません	**定義データベースの長期間未アップデートを通知する未アップデート期間**
簡易スキャンが長期間実行されていません	*（移行されません）* Kaspersky Endpoint Security は 3 日経過後に簡易スキャンが実行されていないイベントを生成します。

管理サーバーとのインタラクション

KSWS の管理サーバーとのインタラクション設定は［**全般設定**］セクション、［**レポートと保管領域**］サブセクションに移行されます。

管理サーバーのインタラクション設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
隔離されたファイル	**ファイルの隔離**
バックアップされたファイル	**ファイルのバックアップ**
ブロック対象コンピューター	*（移行されません）* Kaspersky Endpoint Security はブロック対象コンピューターに関する情報を自動的に送信します。

タスク

製品のアクティベーション

Kaspersky Endpoint Security は、*アクティベーションの完了*タスク（KSWS）をサポートしません。KES で［*ライセンスの追加*］タスクを作成し、ライセンスをインストールパッケージに追加するか、ライセンスの自動配信機能を有効にすることができます。

アップデートのコピー

KSWS の*アップデートのコピー*タスクの設定は KES の［*定義データベースと製品機能のアップデート*］タスクに移行されます。

アップデートのコピータスクの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
アップデート元： • **Kaspersky Security Center 管理サーバー** • **カスペルスキーのアップデートサーバー** • **カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**	**アップデート元**： • **Kaspersky Security Center** • **カスペルスキーのアップデートサーバー** • **ユーザーが指定**
指定したサーバーが使用できない場合はカスペルスキーのアップデートサーバーを使用する	*（移行されません）* Kaspersky Endpoint Security では、カスペルスキーのアップデートサーバーを含む複数のアップデート元の指定が許可されています。最初のアップデート元が利用できない場合は、Kaspersky Endpoint Security はリスト内の別のアップデート元を使用してアップデートを取得します。
プロキシサーバー設定を使用してカスペルスキーのアップデートサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
プロキシサーバー設定を使用して他のサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
アップデートのコピーの設定： • **定義データベースのアップデートをコピーする** • **ソフトウェアモジュールの重要なアップデートをコピーする** • **定義データベースとソフトウェアモジュールの重要なアップデートをコピーする**	*（移行されません）* Kaspersky Endpoint Security は定義データベースのアップデートとアプリケーションの重要なアップデートを単一のパッケージとして追加します。
コピーしたアップデートのローカル用保存フォルダー	**アップデートをフォルダーにコピーする**

ベースラインファイル変更監視

*ベースラインファイル変更監視*タスクの設定（KSWS）は、［*システム変更チェック*］タスクと、ポリシーセクション［**セキュリティコントロール**］、サブセクション［**システム変更監視**］に移行されます。

ベースラインファイル変更監視タスクの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
ハッシュ計算アルゴリズム： • **MD5**： • **SHA256**：	*（移行されません）* Kaspersky Endpoint Security はチェックサムの計算に SHA256 アルゴリズムを使用します。
スキャン範囲	**監視範囲**（［**システム変更監視**］サブセクション）

定義データベースのアップデート

KSWS の*定義データベースのアップデート*タスクの設定は KES の［*定義データベースと製品機能のアップデート*］タスクに移行されます。

定義データベースのアップデートタスクの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
アップデート元： • **Kaspersky Security Center 管理サーバー** • **カスペルスキーのアップデートサーバー** • **カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**	**アップデート元：** • **Kaspersky Security Center** • **カスペルスキーのアップデートサーバー** • **ユーザーが指定**
指定したサーバーが使用できない場合はカスペルスキーのアップデートサーバーを使用する	*（移行されません）* Kaspersky Endpoint Security では、カスペルスキーのアップデートサーバーを含む複数のアップデート元の指定が許可されています。最初のアップデート元が利用できない場合は、Kaspersky Endpoint Security はリスト内の別のアップデート元を使用してアップデートを取得します。
プロキシサーバー設定を使用してカスペルスキーのアップデートサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
プロキシサーバー設定を使用して他のサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
ディスク I/O の負荷の低減	*（移行されません）*

ソフトウェアモジュールのアップデート

KSWS の *ソフトウェアモジュールのアップデートタスク*の設定は KES の［*定義データベースと製品機能のアップデート*］タスクに移行されます。

ソフトウェアモジュールのアップデートタスクの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
アップデート元： • **Kaspersky Security Center 管理サーバー** • **カスペルスキーのアップデートサーバー** • **カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー**	**アップデート元：** • **Kaspersky Security Center** • **カスペルスキーのアップデートサーバー** • **ユーザーが指定**
指定したサーバーが使用できない場合はカスペルスキーのアップデートサーバーを使用する	*（移行されません）* Kaspersky Endpoint Security では、カスペルスキーのアップデートサーバーを含む複数のアップデート元の指定が許可されています。最初のアップデート元が利用できない場合は、Kaspersky Endpoint Security はリスト内の別のアップデート元を使用してアップデートを取得します。
プロキシサーバー設定を使用してカスペルスキーのアップデートサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
プロキシサーバー設定を使用して他のサーバーに接続する	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントにプロキシサーバーを使用します。本製品のネットワークのオプションでプロキシサーバーの接続を設定できます。
ソフトウェアモジュールの重要なアップデートをコピーしインストールする	**重要なアップデートおよび承認済みのアップデートをインストールする**
適用可能になったソフトウェアの重要なアップデートを確認する	*（移行されません）* Kaspersky Endpoint Security は継続的に製品機能の重要なアップデートが適用可能かどうか確認します。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
システムの再起動を許可する	*（移行されません）* Kaspersky Endpoint Security はユーザーにコンピューターを再起動する権限を求める画面を表示します。
適用可能になったソフトウェアモジュールの定期アップデートの情報を受信する	*（移行されません）* Kaspersky Endpoint Security はソフトウェアモジュールのアップデートに関する通知を表示します。

定義データベースのロールバック

KSWS の*定義データベースのロールバック*タスクの設定は KES の［*アップデートのロールバック*］タスクに移行されます。新しい［*アップデートのロールバック*］タスク（KES）には、タスク開始スケジュール［*手動*］があります。

オンデマンドスキャン

KSWS の*オンデマンドスキャン*タスクの設定は KES の［*マルウェアのスキャン*］タスクに移行されます。

スキャンタスクの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
スキャン範囲	**スキャン範囲**
保護レベル： • **最大の保護** • **推奨** • **最高のパフォーマンス**	**セキュリティレベル**： • **高** • **推奨** • **低** セキュリティレベルの設定は KSWS と KES で異なります。
スキャン対象オブジェクト： • **すべてのオブジェクト** • **ファイル形式によってオブジェクトをスキャン** • **定義データベース指定の拡張子リストによってオブジェクトをスキャン** • **指定の拡張子リストによってオブジェクトをスキャン**	**ファイル種別**： • **すべてのファイルをスキャン** • **ファイル形式でファイルをスキャン** • **拡張子でファイルをスキャン** Kaspersky Endpoint Security ではカスタマイズした拡張子リストは許可されません。Kaspersky Endpoint Security は［**指定の拡張子リストによってオブジェクトをスキャン**］の値を［**拡張子でファイルをスキャン**］の値で置き換えます。
サブフォルダー	**サブフォルダーを含む**
サブファイル	*（移行されません）*
ディスクのブートセクターと MBR をスキャン	*（移行されません）*
NTFS 代替データストリームをスキャン	*（移行されません）*
作成または変更されたファイルのみをスキャン	**新規作成または変更されたファイルのみスキャン**
複合オブジェクトのスキャン： • **すべてのアーカイブ** • **すべての SFX アーカイブ** • **すべてのメールデータベース** • **すべての圧縮されたオブジェクト** • **すべての通常のメール** • **すべての OLE 埋め込みオブジェクト**	**複合ファイルのスキャン**： • **アーカイブをスキャン** • **パスワードで保護されているアーカイブをスキャン** • **配布パッケージをスキャン** • **メール形式のファイルをスキャン** • **Microsoft Office 形式のファイルをスキャン**
感染などの問題があるオブジェクトの処理： • **駆除** • **駆除する。駆除できない場合は削除する** • **削除** • **推奨処理を実行** • **通知のみ**	**脅威の検知時の処理**： • **駆除する。駆除できない場合は削除する** • **駆除する。駆除できない場合は通知する** • **通知する**

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
感染の可能性があるオブジェクトの処理： • **隔離** • **削除** • **推奨処理を実行** • **通知のみ**	*（移行されません）* Kaspersky Endpoint Security は脅威が検知されると処理を適用します。
検知したオブジェクトの種別に応じて処理を実行	*（移行されません）*
埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する	*（移行されません）*
除外するファイル	*（移行されません）* Kaspersky Endpoint Security はすべてのコンポーネントに信頼ゾーンを適用します。信頼ゾーンの設定内で除外を設定することができます。
検知しない	*（移行されません）*
スキャン時間が次を超えたら停止する	**ファイルの最大スキャン時間**
スキャンする複合オブジェクトの最大サイズ	**大きな複合ファイルをスキャンしない**
iSwift を使用する	**iSwift**
iChecker を使用する	**iChecker**
オフラインファイルの処理： • **スキャンしない** • **ファイルの常駐部分のみスキャン** • **ファイル全体をスキャン** • **指定した期間（日数）にアクセスされた場合のみ** • **可能な場合はローカルのハードディスクにファイルをコピーしない**	*（移行されません）* Kaspersky Endpoint Security はオフラインファイル全体をスキャンします。

アプリケーション整合性チェック

KSWS の *アプリケーションの整合性チェック*タスクの設定は KES の［*アプリケーション整合性チェック*］タスクに移行されます。

アプリケーション起動コントロールルールの自動作成

Kaspersky Endpoint Security では *アプリケーション起動コントロールルールの自動作成*タスクはサポートされません。アプリケーションコントロールの設定でルールを作成することができます。

デバイスコントロールルールの自動作成

Kaspersky Endpoint Security では *デバイスコントロールルールの自動作成*タスクはサポートされません。デバイスコントロールの設定でルールを作成することができます。

KSWS コンポーネントの移行

ローカルでのインストール前に、Kaspersky Endpoint Security はコンピューターにカスペルスキー製品が存在するかどうかを確認します。コンピューター上に Kaspersky Security for Windows Server がインストールされている場合、KES はインストール済みの KSWS コンポーネント一式を検知し、同じコンポーネントをインストールするよう選択します。

KSWS にない KES コンポーネントは次のようにインストールされます：

- AMSI 保護、ホスト侵入防止、修復エンジンは既定の設定でインストールされます。
- 有害 USB 攻撃ブロック、アダプティブアノマリーコントロール、データ暗号化、Detection and Response コンポーネントは無視されます。

リモートからインストールした場合は、KES はインストールされた KSWS コンポーネントを無視します。インストーラーは[インストールパッケージのプロパティ]で選択したコンポーネントをインストールします。[Kaspersky Endpoint Security のインストール]と[ポリシーとタスクの移行]後、[KES の設定は KSWS の設定に従って設定されます]。

KSWS のタスクとポリシーの移行

KSWS のポリシーおよびタスクの設定は次の方法で移行することができます：

- ポリシーとタスクの一括変換ウィザード（以下、「移行ウィザード」とも表記）を使用する。

  > KSWS の移行ウィザードは管理コンソール（MMC）でのみ使用可能です。ポリシーとタスクの設定は Web コンソールおよび Cloud コンソールでは移行できません。

  一括変換ウィザードは、Kaspersky Security Center のバージョンにより異なる動作をします。ソリューションをバージョン 14.2 以降のバージョンにアップグレードすることをお勧めします。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、ポリシーではなくプロファイルに移行することができます。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、より広い範囲のポリシー設定を移行することができます。

- Kaspersky Endpoint Security for Windows の新規ポリシーウィザードを使用する。

  新規ポリシーウィザードを使用して KSWS のポリシーに基づいた KES ポリシーを作成することができます。

移行ウィザードや新規ポリシーウィザードを使用した場合、KSWS ポリシーの移行手順は異なります。

ポリシーとタスクの一括置換ウィザード

移行ウィザードは KSWS のポリシー設定を KES ポリシー設定の代わりにポリシーのプロファイルに移動します。*ポリシーのプロファイル*とは、コンピューターが設定されたアクティベーションルールを満たしている場合にコンピューター上でアクティベートされる、一連のポリシー設定です。デバイスのタグ「`UpgradedFromKSWS`」がポリシーのプロファイルの適用条件として選択されます。Kaspersky Security Center は、リモートインストールタスクを使用して KSWS 上に KES をインストールしたすべてのコンピューターにタグ「`UpgradedFromKSWS`」を自動的に追加します。別のインストール方法を選択した場合は、デバイスに手動でタグを割り当てることができます。

タグをデバイスに追加するには：

1. サーバー向けの新しいタグ「`UpgradedFromKSWS`」を作成します。

   デバイスのタグの作成について詳しくは、[Kaspersky Security Center ヘルプ]を参照してください。

2. Kaspersky Security Center コンソールで新しい管理グループを作成し、このグループにタグを割り当てるサーバーを追加します。

   抽出ツールを使用してサーバーを分類することができます。抽出の操作について詳しくは、Kaspersky Security Center ヘルプを参照してください。

3. Kaspersky Security Center コンソールで管理グループのすべてのサーバーを選択し、選択したサーバーのプロパティを開いてタグを割り当てます。

複数の KSWS ポリシーを移行している場合は、各ポリシーは単一の包括的なポリシーのプロファイルに変換されます。KSWS ポリシーに既にプロファイルが含まれる場合は、これらもプロファイルとして移行されます。結果、すべての KSWS ポリシーに対応するプロファイルを含む単一のポリシーが作成されます。

ポリシーとタスクの一括変換ウィザードを使用して KSWS のポリシーの設定を移行する方法

1. 管理コンソールで、管理サーバーを選択して右クリックしてコンテキストメニューを開きます。
2. ［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

ポリシーとタスクの一括変換ウィザードが開始されます。ウィザードの指示に従います。

ステップ 1：ポリシーとタスクを変換するアプリケーションの選択

ここでは、Kaspersky Endpoint Security for Windows を選択します。次の手順に進みます。

ステップ 2：ポリシーの変換

移行ウィザードは KES ポリシー内に KSWS ポリシーのプロファイルを作成します。ポリシーのプロファイルに変換する Kaspersky Security for Windows Server ポリシーを選択します。次の手順に進みます。

移行ウィザードはポリシーの返還を開始します。新しいポリシープロファイルの名前は元の KSWS ポリシーに対応した名前になります。

ステップ 3：ポリシーの移行レポート

移行ウィザードはポリシーの移行レポートを作成します。ポリシーの移行レポートには、ポリシーが変換された日時、元の KSWS ポリシーの名前、変換先の KES ポリシー名、新しいポリシープロファイル名が含まれます。

ステップ 4：タスクの変換

移行ウィザードは Kaspersky Endpoint Security for Windows 向けの新しいタスクを作成します。タスクのリストで、 Kaspersky Endpoint Security 向けに作成する KSWS のタスクを選択します。新しいタスクは「*<KSWS タスク名>（変換済み）*」という名前になります。次の手順に進みます。

ステップ 5：ウィザードの完了

ウィザードを終了します。ウィザードは以下の処理を実行します：

- 新しいポリシープロファイルの Kaspersky Endpoint Security ポリシーへの追加

  ポリシーには Kaspersky Security for Windows Server の設定のプロファイルが含まれます。新しいポリシーのステータスは*有効*になっています。ウィザードは KSWS のポリシーを変更しません。

- 新規の Kaspersky Endpoint Security のタスクを作成する

  新しいタスクは KSWS のタスクのコピーになります。ウィザードは KSWS のポリシーを変更しません。

KSWS の設定を含む新しいポリシープロファイルは「*UpgradedFromKSWS <Kaspersky Security for Windows Server のポリシー名>*」という名前になります。プロファイルのプロパティで、移行ウィザードは自動的にデバイスのタグ「`UpgradedFromKSWS`」を適用基準として選択します。このように、ポリシープロファイルからの設定はサーバーに自動的に適用されます。

KSWS ポリシーに基づいたポリシーの作成用ウィザード

KSWS ポリシーに基づく KES ポリシーが作成されると、それに応じてウィザードは新しいポリシーの設定を転送します。つまり、1 つの KES ポリシーが 1 つの KSWS ポリシーに対応することになります。ウィザードはポリシーをプロファイルに変換しません。

KSWS のポリシーを移行する新規ポリシーウィザードを使用する方法

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

   ポリシーウィザードが起動します。
5. ポリシーウィザードの指示に従います。

ステップ 1：グループポリシーを作成するにアプリケーションの選択

Kaspersky Endpoint Security for Windows (12.12) のアプリケーションを選択します。

ステップ 2：グループポリシー名の入力

グループポリシーの名前を入力します（「*オフィスのポリシー*」など）。

［**旧バージョンのアプリケーションのポリシー設定を使用する**］チェックボックスをオンにします。［**参照**］をクリックして KSWS のポリシーを選択します。

ステップ 3：Kaspersky Security Network への参加

Kaspersky Security Network（KSN）に関する声明の内容を確認し、同意するかどうかを選択します。

ステップ 4：コンピューターでのアプリケーション使用モードの選択

［**標準モード**］を選択します。Kaspersky Endpoint Security は、すべての製品モードと OS の種別に対して共通のポリシーを提供します。

さまざまなモードやオペレーティングシステムの種類に応じて異なるポリシーを使用することを推奨します。

ステップ 5：信頼ゾーンの設定

信頼ゾーンを設定します。設定済みの信頼するオブジェクトとアプリケーションを追加できます。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Light Agent モードの Kaspersky Endpoint Security を迅速に設定することもできます。

ステップ 6：ポリシーステータスの選択

- **アクティブ**：次の同期の実行後、このポリシーがクライアントコンピューター上でアクティブなポリシーとして使用されます。

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

- **非アクティブ**：バックアップ用のポリシーです。必要に応じて、非アクティブなポリシーのステータスをアクティブに変更できます。

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

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

ウィザードを終了します。

移行後のポリシーとタスクの追加設定

KSWS と KES ではコンポーネントの組み合わせとポリシー設定が異なるため、移行後にはポリシー設定が企業のセキュリティ要件を満たしていることを検証する必要があります。

次の標準ポリシー設定を確認します：

- パスワードによる保護：KSWS のパスワードによる保護の設定は移行されません。Kaspersky Endpoint Security には組み込みのパスワード保護機能があります。必要に応じて、パスワードによる保護をオンにしてパスワードを設定してください。
- 信頼ゾーン：KSWS および KES により、オブジェクトの選択に使用される方法は異なります。移行時に、KES は個別のファイルまたはファイルまたはフォルダーのパスとして定義された除外リストをサポートします。KSWS が事前定義された領域またはスクリプト URL に対する除外リストを持っていた場合は、これらの除外リストは移行されません。移行後にこれらの除外リストを手動で追加する必要があります。

  > サーバー上で Kaspersky Endpoint Security が正常に動作するため、サーバーの動作に重要なファイルを信頼ゾーンに追加することを推奨します。SQL サーバーでは、MDF と LDF データベースファイルを追加する必要があります。Microsoft Exchange サーバーでは、CHK、EDB、JRS、LOG、JSL ファイルを追加する必要があります。例えば、`C:\Program Files (x86)\Microsoft SQL Server\*.mdf` のようにマスクを使用することができます。

  > Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

- ファイアウォール：KSWS のファイアウォール機能はシステムレベルのファイアウォールで実行されます。KES では、ファイアウォール機能は個別のコンポーネントが実行されています。移行後、Kaspersky Endpoint Security のファイアウォールを設定できます。
- Kaspersky Security Network：Kaspersky Endpoint Security では個別のコンポーネントにおける KSN 設定はサポートされません。Kaspersky Endpoint Security はすべての製品コンポーネントに KSN を使用します。KSN を使用するには、新しい Kaspersky Security Network に関する声明の内容に同意する必要があります。
- ウェブコントロール：Web トラフィックカテゴリコントロールのブロックルールは Kaspersky Endpoint Security では単一のブロックルールに移行されます。カテゴリコントロールの許可ルールは Kaspersky Endpoint Security では無視されます。Kaspersky Endpoint Security では Kaspersky Security for Windows Server のカテゴリのすべてはサポートされません。Kaspersky Endpoint Security に存在しないカテゴリは移行されません。そのため、サポートされないカテゴリを持つ Web リソースの分類ルールは移行されません。必要に応じて、ウェブコントロールルールを追加します。
- プロキシサーバー：プロキシサーバー接続のパスワードは移行されません。プロキシサーバーへの接続に使用されるパスワードは手動で入力してください。
- 個別のコンポーネントのスケジュール：Kaspersky Endpoint Security では個別のコンポーネントにおけるスケジュール設定はサポートされません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

- コンポーネントの組み合わせ：Kaspersky Endpoint Security で利用できる機能の組合せは、オペレーティングシステムの種別（ワークステーションまたはサーバー）によって異なります。例えば、暗号化ツールの中では、サーバーで利用可能なものは BitLocker ドライブ暗号化のみです。

- 属性：属性の状態は移行されません。属性には既定の設定が適用されます。既定では、新しいポリシー内のほぼすべての設定で、子ポリシーおよびローカルの製品インターフェイスでの設定の変更は禁止されています。［**Managed Detection and Response (Industrial CyberSecurity)**］セクションおよび［**ユーザーサポート**］の設定グループ（［**インターフェイス**］セクション）内のポリシー設定の属性の値は となっています。必要に応じて、親ポリシーからの設定の継承を設定してください。

- アクティブな脅威に対する操作：特別な駆除はワークステーションとサーバーに対して異なる動作をします。［*マルウェアのスキャン*］タスクの設定および製品設定で特別な駆除を設定できます。

- 本製品のアップグレード：再起動せずにメジャーアップデートやパッチをインストールするには、製品のアップグレードモードを変更する必要があります。既定では、再起動せずに製品アップデートをインストールする機能は無効になっています。

- Kaspersky Endpoint Agent：Kaspersky Endpoint Security には、Managed Detection and Response ソリューションと動作する組み込みエージェントが含まれています。必要に応じて、Kaspersky Endpoint Agent のポリシー設定を Kaspersky Endpoint Security のポリシーに移行してください。

- ［*定義データベースと製品機能のアップデート*］タスク：［*定義データベースと製品機能のアップデート*］タスクの設定が正常に移行されたことを確認してください。KSWS の 3 つのタスクの代わりに、KES では 1 つの KES タスクを使用します。［*定義データベースと製品機能のアップデート*］タスクを最適化して、不要なタスクを削除することができます。

- その他のタスク：アプリケーションコントロール、デバイスコントロール、ファイル変更監視機能の動作は KSWS と KES では異なります。KES では*ベースラインファイル変更監視*、*アプリケーション起動コントロールルールの自動作成*、*デバイスコントロールルールの自動作成*タスクは使用しません。そのため、これらのタスクは移行されません。移行後、ファイル変更監視、アプリケーションコントロール、デバイスコントロールコンポーネントを設定することができます。

KSWS の信頼ゾーンの移行

*信頼*ゾーンは Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。*ポリシーとタスクの一括変換ウィザード*または*KSWS ポリシーに基づいて新しい KES ポリシーを作成するためのウィザード*を使用して、KSWS から KES に信頼ゾーンオブジェクトを移行できます。KSWS と KES ではコンポーネントと機能の組み合わせが異なるため、移行後には除外リストが企業のセキュリティ要件を満たしていることを検証する必要があります。信頼ゾーンへの除外リストの追加方法も、KES と KSWS で異なります。移行ウィザードには、KSWS のすべての除外リストを移行するツールはありません。つまり、移行後には、KSWS の除外リストの一部を手動で追加する必要があります。

サーバー上で Kaspersky Endpoint Security が正常に動作するため、サーバーの動作に重要なファイルを信頼ゾーンに追加することを推奨します。SQL サーバーでは、MDF と LDF データベースファイルを追加する必要があります。Microsoft Exchange サーバーでは、CHK、EDB、JRS、LOG、JSL ファイルを追加する必要があります。例えば、`C:\Program Files (x86)\Microsoft SQL Server\*.mdf` のようにマスクを使用することができます。

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

KSWS		KES
スキャン対象オブジェクト		
• 定義済みの範囲	*（移行されません）*	
• ディスク、フォルダーまたはネットワーク上の場所	→	**ファイルまたはフォルダー**
• ファイル	→	**ファイルまたはフォルダー**
• スクリプトファイルまたは Web アドレス	*（移行されません）*	
検知したオブジェクト	→	**検知するオブジェクトの種別**
信頼するプロセス	→	**信頼するアプリケーション**

スキャン対象オブジェクトの移行

プロパティで［**スキャン対象オブジェクト**］の方法が選択されている KSWS の除外リストは、いくつかの制限を伴って、プロパティで［**ファイルまたはフォルダー**］の方法が選択されている KES の除外リストに移行されます。除外の移行は、オブジェクトの選択方法によって異なります：

- 定義済みの範囲：*移行しません*。

  移行後にこれらの除外リストを手動で追加する必要があります。事前定義された領域としての除外リストは、［*マルウェアのスキャン*］タスク設定で設定する必要があります。

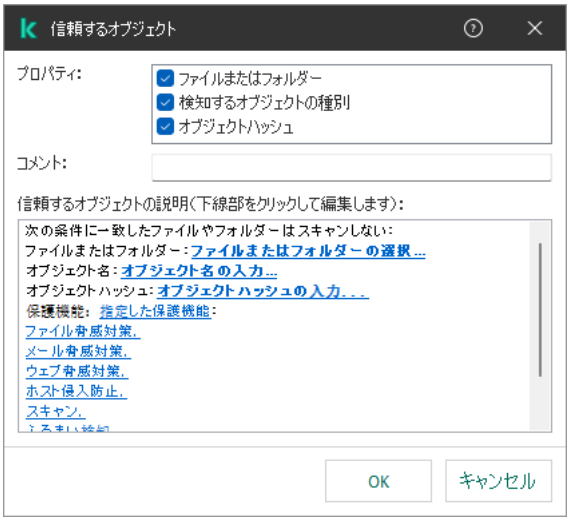
- ディスク、フォルダーまたはネットワーク上の場所：プロパティで［ファイルまたはフォルダー］の方法が選択されている KES の除外リストに移行します。

- ファイル：プロパティで［ファイルまたはフォルダー］の方法が選択されている KES の除外リストに移行します。

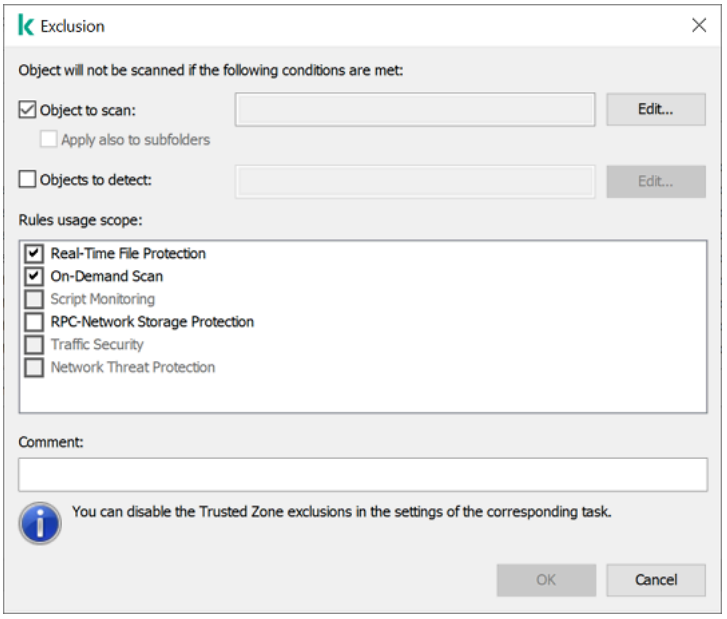
- スクリプトファイルまたは Web アドレス：*移行しません*。

  移行後にこれらの除外リストを手動で追加する必要があります。スクリプト Web アドレスとしての除外リストは、ウェブ脅威対策の信頼する Web アドレスに追加する必要があります。

スキャン対象オブジェクトの［**サブフォルダーにも適用**］がオンになっている場合、この設定は KES の除外リスト（［**サブフォルダーを含む**］）に移行されます。



KES の除外の設定



KSWS の除外の設定

検知したオブジェクトの移行

プロパティで［**検知したオブジェクト**］の方法が選択されている KSWS の除外リストは、プロパティで［**検知するオブジェクトの種別**］の方法が選択されている KES の除外リストに移行されます。検知したオブジェクトの名前は、「ウイルス百科事典」の分類に対応します（例：「`Email-Worm`」、「`Rootkit`」、「`RemoteAdmin`」）。Kaspersky Endpoint Security は、疑問符 `?`（任意の 1 文字に一致）とアスタリスク `*`（任意の連続した文字に一致）を使用したマスクをサポートします。

除外の適用範囲の移行

除外の適用範囲は、除外が適用されるコンポーネントのセットです。KES と KSWS でコンポーネントのセットが異なるため、移行ウィザードで除外の適用範囲を移行することはできません。そのため、少なくとも1つのコンポーネントが KSWS の適用範囲で選択されていた場合は、KES は除外をすべての製品コンポーネントに適用します。

KSWS の適用範囲の設定は、信頼ゾーンの設定で行うことも、KSWS 保護機能の設定で行うこともできます。この目的で、ポリシーの対応するセクションにある［**信頼ゾーンを適用する**］をオンまたはオフにすることができます。KES 保護機能の設定には、このようなチェックボックスは含まれていません。つまり、個々のコンポーネントの設定の信頼ゾーンのステータスは、移行時に失われます。移行が完了したら、KES ポリシーの信頼ゾーンの設定で、除外が適用されるコンポーネントを選択します。

コメントの移行

KSWS の信頼ゾーンのコメントは、変更されずに KES の除外のコメントに移行されます。

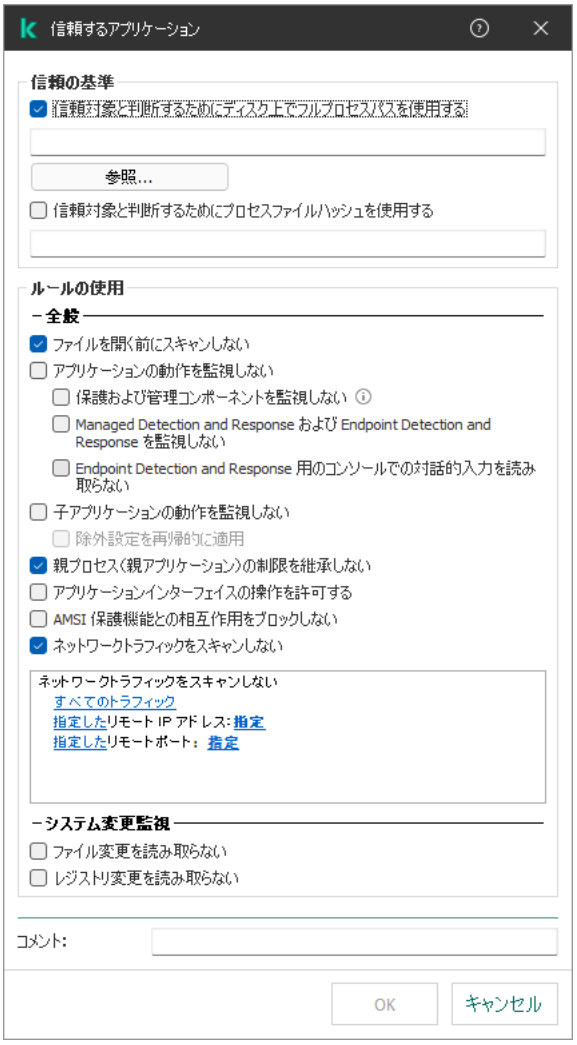
信頼するプロセスの移行

KSWS の信頼するプロセスは、いくつかの制限を伴って、KES の信頼するプロセスに移行されます。信頼するプロセスの移行は、オブジェクトの選択方法によって異なります：

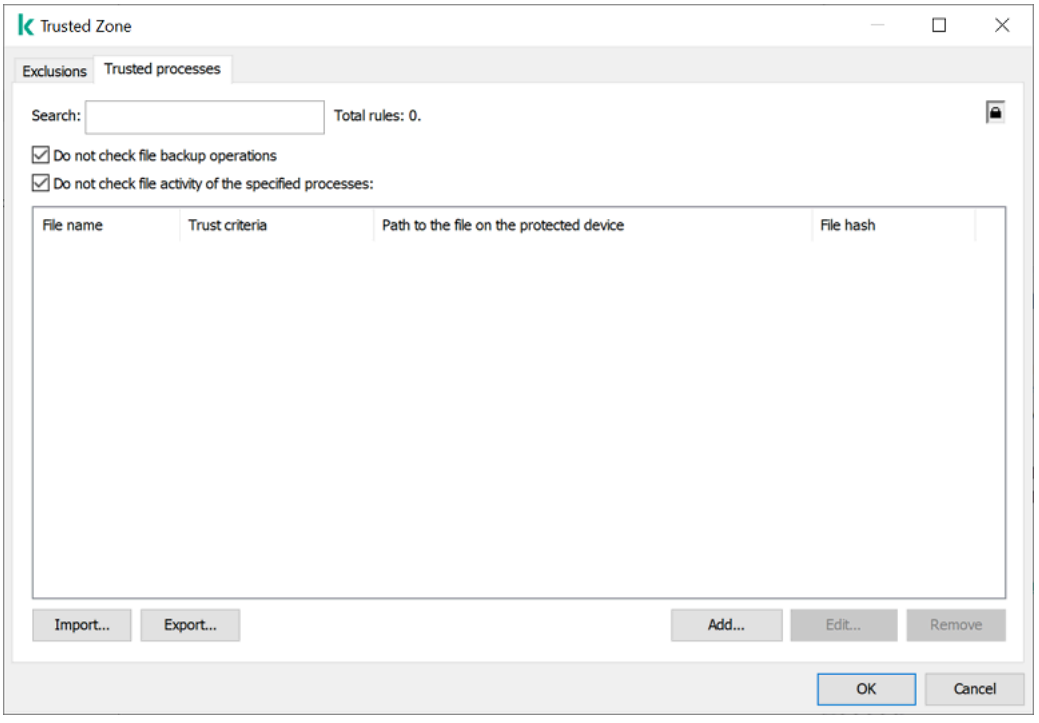
- 保護対象デバイス上のファイルへのパス：KES の信頼するアプリケーションに移行します。
- ファイルのハッシュ：*移行しません*。

KSWS にファイルのハッシュとして設定された信頼するプロセスがある場合、このような信頼するプロセスは移行されません。移行後にこれらの信頼するプロセスを手動で追加する必要があります。

信頼するプロセスの設定で［**ファイルのバックアップ処理を確認しない**］がオンになっている場合、この設定はKESの信頼するアプリケーション（［**アプリケーションの動作を監視しない**］）に移行されます。



KESの信頼するアプリケーションの設定



KSWSの信頼するプロセスの設定

KSWSのアプリケーション起動コントロールルールの移行

KSWS のアプリケーション起動コントロールは、既定ですべてをブロックします。つまり、アプリケーション起動コントロールは、許可するアプリケーションとルールで指定されていないすべてのアプリケーションを自動的にブロックします。そのため、KES のアプリケーションコントロールの移行ウィザードでは、既定ですべてをブロックする原則に対応する**許可リスト**コントロールモードが自動的に設定されます。

*ポリシーとタスクの一括変換ウィザード*または*KSWS ポリシーに基づいて新しい KES ポリシーを作成するためのウィザード*を使用して、KSWS から KES にルールを移行できます。

アプリケーション起動コントロールのモードの移行

KSWS のアプリケーション起動コントロールのモードは、次のように KES のアプリケーションコントロールに移行されます：

- ［**統計のみ**］→［**ルールをテスト運用**］
- ［**アクティブ**］→［**ルールを適用**］

KSWS のアプリケーション起動コントロールの事前定義済みのルールの移行

規定では、KSWS のアプリケーション起動コントロールには次の 2 つのルールが含まれます：

- **OS が信頼する証明書によってスクリプトおよび MSI を許可する**
- **OS が信頼する証明書によって実行ファイルを許可する**

事前定義済みのルールにより、信頼するルート証明書によって署名された*スクリプト*、*MSI パッケージ*、および*実行ファイル*を実行することができます。少なくとも 1 つの KSWS の事前定義済みのルールに［**許可**］種別がある場合、移行ウィザードは新しい許可ルール［**信頼するルート証明書**］を作成します。KES のアプリケーションコントロールは信頼するスクリプト、MSI パッケージおよび実行ファイルの実行を許可するために単一のルールを使用します。

両方の KSWS の事前定義済みのルールに［**拒否**］種別がある場合、KES は事前定義済みのルールを無視します。

KSWS のアプリケーション起動コントロールのカスタムルールの移行

KSWS のアプリケーション起動コントロールルールは、次の条件に従ってファイルの実行を制限します：

- デジタル証明書による署名
- SHA256 ハッシュ
- ファイルパス

KSWS と KES ではルールの作成方法が異なります。そのため、移行ウィザードによって、KSWS のルールからの条件と除外リストが含まれた*アプリケーションカテゴリ*が作成されて、これらのアプリケーションカテゴリが KES のルールに追加されます。ウィザードは、アプリケーションカテゴリの［**証明書**］、［**フォルダーパス**］、および［**ファイルのハッシュ**］の条件を使用します。Kaspersky Security Center 管理コンソールの［**アプリケーションの管理**］→［**アプリケーションカテゴリ**］セクションで新しいアプリケーションカテゴリを使用できます。

移行ウィザードで、KSWS のルールが種別ごと、およびユーザーごとにグループ化されます。次に、ウィザードで、KSWS のルールからの条件と除外リストを含むアプリケーションカテゴリが作成されて、そのアプリケーションカテゴリが新しい KES のルールに追加されます。ウィザードで、KES のルールの［**説明**］フィールドに、KSWS のルールの名前が指定されます。

KSWS のアプリケーション起動コントロールの詳細設定の移行

KSWS のアプリケーション起動コントロールと KES のアプリケーションコントロールの動作原理は異なるため、移行ウィザードでは設定の一部しか移行されない場合があります。

アプリケーション起動コントロールの設定

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す	*（移行されません）* Kaspersky Endpoint Security はアプリケーションの実行の試行を常にスキャンします。
実行するコマンドのないコマンドインタープリターの起動を拒否する	*（移行されません）* アプリケーションコントロールで禁止されていない場合は、Kaspersky Endpoint Security はコマンドインタープリターの実行を許可します。
実行ファイルにルールを適用する	*（移行されません）* ルールの適用範囲は KES のアプリケーションコントロールの設定では設定できません。KES のアプリケーションコントロールは、実行ファイル、スクリプトと MSI パッケージのすべての種別のファイルにルールを適用します。すべてのファイル種別が KSWS のルール適用範囲に含まれている場合は、KES は移行中に KSWS のルールを引き継ぎます。一部のファイル種別が KSWS のルール適用範囲から除外されていた場合は、KES は移行中に KSWS ルールを引き継ぎますが、アプリケーションコントロールの処理として［**ルールをテスト運用**］が選択されます。
DLL モジュールの読み込みを監視する	**DLL モジュールの読み込みの監視（システムの負荷が大きくなります）**
スクリプトと MSI パッケージにルールを適用する	*（移行されません）* ルールの適用範囲は KES のアプリケーションコントロールの設定では設定できません。KES のアプリケーションコントロールは、実行ファイル、スクリプトと MSI パッケージのすべての種別のファイルにルールを適用します。すべてのファイル種別が KSWS のルール適用範囲に含まれている場合は、KES は移行中に KSWS のルールを引き継ぎます。一部のファイル種別が KSWS のルール適用範囲から除外されていた場合は、KES は移行中に KSWS ルールを引き継ぎますが、アプリケーションコントロールの処理として［**ルールをテスト運用**］が選択されます。

Kaspersky Security for Windows Server の設定	Kaspersky Endpoint Security for Windows の設定
KSN で信頼されていないアプリケーションを拒否する	*（移行されません）* Kaspersky Endpoint Security はアプリケーションの評価を判断に使用せず、ルールに従ってアプリケーションの実行を許可またはブロックします。
KSN で信頼されているアプリケーションを許可する	移行中、KES は新しい許可ルールを追加します。KL カテゴリ［**その他のソフトウェア\アプリケーション、KSN の評価によって信頼済み**］はルール適用条件として指定されています。
KSN で信頼されているアプリケーションの実行を許可するユーザーまたはユーザーグループ	KL カテゴリ（**その他のソフトウェア\アプリケーション、KSN の評価によって信頼済み**）を含むアプリケーションコントロールの許可ルールの**ユーザーとその権限**。
リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルールを追加します。ファイルのハッシュはルール適用条件として指定されます。
Windows インストーラーによるソフトウェア配布を常に許可する	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルール（［**ソフトウェア配布アプリケーションとパッケージが許可されています**］）を追加します。ファイルのハッシュはルール適用条件として指定されます。アカウントのプロパティ［**信頼するアップデーター**］はオンになります。
バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する	*（移行されません）*
許可されているソフトウェア配布アプリケーションおよびパッケージ	KSWS のソフトウェア配布コントロールと KES は異なる動作をします。移行中、KES はソフトウェアの自動配布が許可されているアプリケーションに対して新しい許可ルールを追加します。ファイルのハッシュはルール適用条件として指定されます。アカウントのプロパティ［**信頼するアップデーター**］はオンになります。
スケジュール設定	*（移行されません）* KSWS の設定でスケジュールが設定されていた場合、アプリケーションコントロールコンポーネントは移行時に有効になります。KSWS の設定でスケジュールが設定されていなかった場合、アプリケーションコントロールは無効になります。 コンポーネントに個別のスケジュールを設定することはできません。コンポーネントは Kaspersky Endpoint Security が動作しているときには常にオンになっています。

KSWS の代替としての KES のインストール

Kaspersky Endpoint Security は、次の方法でインストールすることができます。

- KSWS のアンインストール後に KES をインストールする（推奨）。
- KSWS 上に KES をインストールする。

Kaspersky Security for Windows Server の削除

アプリケーションは、リモートから［*アプリケーションのリモートアンインストール*］タスクを使用して削除するか、サーバー上でローカルに削除することができます。KSWS の削除後、サーバーを再起動する必要がある可能性があります。再起動せずに Kaspersky Endpoint Security をインストールするためには、Kaspersky Security for Windows Server が完全に削除されたことを確認してください。アプリケーションが完全に削除されていないと、Kaspersky Endpoint Security をインストールすることにより、サーバーの誤動作を発生させる可能性があります。kavremover ユーティリティを使用した場合でも、アプリケーションが完全に削除されたことを確認してください。kavremover ユーティリティは KSWS の管理をサポートしていません。

KSWS へのアクセスを制限するためにパスワードによる保護が有効になっている場合、KES インストールパッケージの設定にアンインストール用パスワードを入力します。

KSWS の削除後に、利用可能な方法で Kaspersky Endpoint Security for Windows をインストールしてください。

Kaspersky Endpoint Security のインストール

KES をリモートからインストールする際は、インストールパッケージのプロパティで選択したコンポーネントがサーバーにインストールされます。インストールパッケージのプロパティには、既定のコンポーネントを設定することを推奨します。KSWS 上に KES をインストールする場合は、再起動は必要ありません。

ローカルでのインストール前に、Kaspersky Endpoint Security はコンピューターにカスペルスキー製品が存在するかどうかを確認します。コンピューター上に Kaspersky Security for Windows Server がインストールされている場合、KES はインストール済みの KSWS コンポーネント一式を検知し、同じコンポーネントをインストールするよう選択します。KSWS 上に KES をインストールする場合は、再起動は必要ありません。

KSWS 上への KES のインストールが失敗した場合は、インストールをロールバックすることができます。インストールをロールバックした後は、サーバーを再起動して再度実行することを推奨します。

KSWS の設定およびタスクは Kaspersky Endpoint Security for Windows のインストール時には移行されません。製品設定を移行するには、ポリシーとタスクの一括変換ウィザードを実行します。

インストールされたコンポーネントの一覧は、`status` コマンドを使用して製品インターフェイスの［**セキュリティ**］セクションで確認するか、Kaspersky Security Center コンソールのコンピューターのプロパティで確認できます。インストール後に［*コンポーネントの変更*］を使用してコンポーネントセットを変更することができます。

［KSWS + KEA］構成からの［KES + 組み込みエージェント］構成への移行

EDR (KATA)、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA および MDR の一部としての Kaspersky Endpoint Security for Windows の使用をサポートするため、組み込みエージェントが製品に追加されました。これらのソリューションと連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。

KSWS から KES への移行時、EDR (KATA)、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA および MDR ソリューションは Kaspersky Endpoint Security との動作を続行します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。

[KSWS + KEA] 設定から [KES + 組み込みエージェント] への移行には次の手順が含まれます：

1. **KSWS から KES への移行**

   KSWS から KES への移行には、Kaspersky Security for Windows Server の代わりとしての Kaspersky Endpoint Security のインストールが含まれます。

   KSWS および KEA へのアクセスを制限するために、管理者がパスワードによる保護を有効にしているケースが多くあります。Kaspersky Security Center Linux 15.1 から、*アプリケーションのリモートインストール*タスクの設定にアプリケーションのアンインストール用パスワードを入力できるようになりました。このタスクでは、アンインストール用パスワードを 1 つだけ入力できます。つまり、KSWS と KEA に同じパスワードが設定されていれば、KSWS アプリケーションと KEA アプリケーションは正常に削除されます。パスワードが異なる場合、いずれかのアプリケーションの削除がアクセスエラーで失敗します。移行を完了するには、*アプリケーションのリモートインストール*タスクの設定でパスワードを入力できなかったアプリケーションに対し、パスワードによる保護を無効にする必要があります。

   移行作業を実行するため、Kaspersky Endpoint Security の一部としてDetection and Response ソリューションをサポートするコンポーネントを選択する必要があります。本製品のインストール後、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

2. **ポリシーおよびタスクの移行**

   [KSWS + KEA] のポリシーとタスクからの [KES + 組み込みエージェント] へ移行には、次の手順が含まれます：

   1. ポリシーとタスクの一括置換ウィザード（管理コンソール（MMC）上でのみ使用可能）を使用した、KSWS から KES へのポリシーとタスクの移行。

      「*UpgradedFromKSWS <Kaspersky Security for Windows Server ポリシーの名前>*」という名前のポリシープロファイルが KES のポリシーに追加されます。新しい KES タスクも「*<KSWS タスク名> (変換済み)*」という名前で作成されます。

2. Kaspersky Endpoint Agent からの移行用のウィザード（Web コンソールと Cloud コンソールでのみ使用可能）を使用した、KEA から KES へのポリシーとタスクの移行。

   「*<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>*」という名前の新しいポリシーが作成されます。新しいタスクと KES のタスクも作成されます。

3 ライセンス機能

共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Security for Windows および Kaspersky Endpoint Agent をアクティベートした場合は、本製品をバージョン 11.7.0 にアップグレードした後に EDR Optimum 機能は自動的にアクティベートされます。追加で操作する必要はありません。

スタンドアロンの Kaspersky Endpoint Detection and Response Optimum アドオンのライセンスを使用して EDR Optimum 機能をアクティベートした場合は、EDR Optimum アドオンのライセンスが Kaspersky Security Center リポジトリに追加されていて、ライセンスの自動配信機能が有効になっていることを確認してください。本製品をバージョン 11.7.0 にアップグレードした後に、EDR Optimum 機能が自動的にアクティベートされます。

Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security ライセンスを使用して Kaspersky Endpoint Agent をアクティベートしており、別のライセンスを使用して Kaspersky Endpoint Security for Windows をアクティベートしていた場合、Kaspersky Endpoint Security for Windows のライセンスを共通の Kaspersky Endpoint Detection and Response Optimum または Kaspersky Optimum Security のライセンスで置き換える必要があります。ライセンスは［*ライセンスの追加*］タスクを使用して置き換えることができます。

Kaspersky Sandbox 機能をアクティベートする必要はありません。Kaspersky Sandbox 機能は Kaspersky Endpoint Security for Windows をアップグレードおよびアクティベートした後すぐに利用可能になります。

Kaspersky Anti Targeted Attack Platform のライセンスは、Kaspersky Anti Targeted Attack Platform ソリューションの一部として Kaspersky Endpoint Security のアクティベートに使用することができます。本製品をバージョン 12.1 にアップグレードした後に、EDR (KATA) 機能が自動的にアクティベートされます。追加で操作する必要はありません。

4 Kaspersky Endpoint Detection and Response Optimum および Kaspersky Sandbox の状態を確認する。

アップグレード後に、Kaspersky Security Center コンソールでコンピューターに「緊急」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。

*製品コンポーネントのステータスレポート*を使用して EDR Optimum 機能がアクティベートされているかどうかを確認してください。コンポーネントの状態が「*ライセンスに含まれていません*」と表示されている場合は、EDR Optimum の自動ライセンス配信機能がオンになっていることを確認してください。

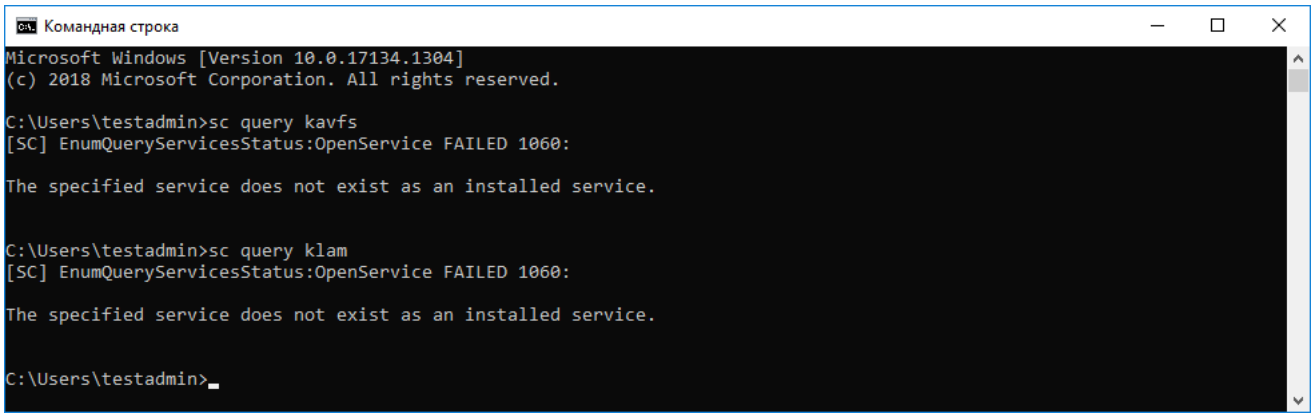
Kaspersky Security for Windows Server が正常に削除されたことの確認

Kaspersky Security for Windows Server が完全に削除されたことを確認してください：

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` フォルダーが存在しない。
- 次のサービスが存在しない：
  - Kaspersky Security Service（KAVFS）
  - Kaspersky Security Management サービス（AVFSGT）
  - Kaspersky Security Exploit Prevention サービス（KAVFSSLP）
  - Kaspersky Security Script Checker サービス（KAVFSSCS）

  実行されているサービスは、タスクマネージャーまたは `sc query` コマンドを実行することで確認できます（下図を参照）。
- 次のドライバーが存在しない：
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

インストールされたドライバーは `C:\Windows\System32\drivers` フォルダーを確認するか、`sc query` コマンドを実行することで確認できます。サービスまたはドライバーが見つからない場合は、以下のような応答が返されます：



Kaspersky Security for Windows Server のサービスおよびドライバーが正常に削除されたことの確認

アプリケーションまたはドライバーファイルがサーバーに残っていた場合は、それらのファイルを手動で削除してください。Kaspersky Security for Windows Server サービスがサーバーでまだ実行されていた場合は、手動でサービスを停止（`sc stop`）および削除（`sc delete`）してください。klam.sys ドライバーを停止するには、`fltmc unload klam` command.コマンドを使用してください。

KSWS のライセンスでの KES のアクティベート

本製品のインストール後、Kaspersky Security for Windows Server（KSWS）のライセンスを使用して Kaspersky Endpoint Security for Windows（KES）をアクティベートすることができます。移行後のアクティベーションプロセスは、KSWS のアクティベーション方法によって異なります（下の表を参照）。

Kaspersky Endpoint Security では *Kaspersky Security for Storage* のライセンスはサポートされません。このライセンスで作業するには、Kaspersky Security for Windows Server を使用する必要があります。

KES を KSWS のライセンスでアクティベートするには、アクティベーションコードを使用する必要があります。製品のアクティベートにライセンス情報ファイルを使用している場合は、Kaspersky Endpoint Security のライセンス情報ファイルについてテクニカルサポートにお問い合わせいただく必要があります。

Kaspersky Security for Windows Server のライセンスを使用した Kaspersky Endpoint Security for Windows のアクティベート

Kaspersky Security for Windows Server のアクティベーション方法	Kaspersky Endpoint Security for Windows へのライセンスの移行
KSWS ライセンスのコンピューターへの自動配信。	KSWS ライセンスのプロパティでライセンスの自動配信が有効になっていた場合、KES は KSWS のライセンスで自動的にアクティベートされます。
KSWS ライセンスがタスクで追加されている。	KSWS がタスクを使用してローカルでアクティベートされた場合、KSWS のライセンスは KSWS の移行中に削除されます。製品を再度アクティベートする必要があります。例えば、Kaspersky Endpoint Security for Windows のインストールパッケージにライセンスを追加することが可能です。
KSWS のライセンスが製品のインターフェイスでローカルに追加されている。	KSWS が製品のアクティベーションウィザードを使用してローカルでアクティベートされている場合、KSWS のライセンスは KSWS の移行中に削除されます。製品を再度アクティベートする必要があります。例えば、Kaspersky Endpoint Security for Windows のインストールパッケージにライセンスを追加することが可能です。
KSWS のライセンスがインストールパッケージに追加されている。	KSWS がインストールパッケージのライセンスを使用してアクティベートされている場合、KSWS のライセンスは KSWS の移行中に削除されます。製品を再度アクティベートする必要があります。例えば、Kaspersky Endpoint Security for Windows のインストールパッケージにライセンスを追加することが可能です。

Kaspersky Security for Windows Server のアクティベーション方法	Kaspersky Endpoint Security for Windows へのライセンスの移行
Amazon Web Services（AWS）の有料仮想マシンイメージ（Amazon マシンイメージ：AMI）。	Kaspersky Security Center を Amazon Web Services（AWS）の有料仮想マシンイメージ（Amazon マシンイメージ：AMI）として購入した場合は、KES のアクティベートは必要ありません。この場合、Kaspersky Security Center は本製品に事前に追加されている、AWS のライセンスを使用します。
自分自身のライセンスで購入し追加料金が必要ない、事前準備した Kaspersky Security Center イメージ（Bring Your Own License：BYOL モデル）。	クラウド環境で自身のライセンスを適用した、追加設定の必要がない Kaspersky Security Center イメージ（Bring Your Own License：BYOL モデル）を使用している場合、本製品を可能な方法でアクティベートする必要があります。Kaspersky Hybrid Cloud Security ライセンスが必要になります。

高負荷のサーバーを移行する際の留意点

高負荷のサーバーでは、パフォーマンスと障害を監視することが重要です。Kaspersky Endpoint Security for Windows への移行後、他の機能に関連している、相当量のサーバーリソースを使用するアプリケーションを一時的に無効にすることを推奨します。サーバーが問題なく動作していることを確認してから、これらの製品コンポーネントを有効な状態に戻します。

高負荷のサーバーの移行には、以下を推奨します：

1. 既定の設定で Kaspersky Endpoint Security のポリシーを作成する。

   既定の設定が最適と考えられます。これらの設定はカスペルスキーの専門家が推奨しています。既定の設定により、推奨される保護レベルおよび最適なリソースを使用できます。

2. ポリシーの設定で、次の機能をオフにします：ネットワーク脅威対策、ふるまい検知、脆弱性攻撃ブロック、修復エンジン、アプリケーションコントロール。

   組織で Kaspersky Managed Detection and Response（MDR）ソリューションが導入されている場合は、BLOB 設定ファイルを Kaspersky Endpoint Security のポリシーにアップロードします。

3. サーバーから Kaspersky Security for Windows Server を削除します。

4. 既定の機能セットで Kaspersky Endpoint Security for Windows をインストールします。

   組織に Detection and Response ソリューションが導入されている場合は、インストールパッケージのプロパティで関連するコンポーネントを選択します。

5. 本製品の設定を確認します：

   - 本製品が KSWS のライセンスでアクティベートされている。
   - 新しいポリシーが適用されている。以前に選択されていたコンポーネントが無効になっている。

6. サーバーが動作していることを確認してください。Kaspersky Endpoint Security for Windows がサーバーリソースの 1% 以上を使用していないことを確認してください。

7. 必要に応じて、信頼するオブジェクトを作成、信頼するアプリケーションを追加、信頼する URL のリストを作成してください。

8. ふるまい検知、脆弱性攻撃ブロック、修復エンジンをオンにします。Kaspersky Endpoint Security for Windows がサーバーリソースの 1% 以上を使用していないことを確認してください。

9. ネットワーク脅威対策をオンにします。Kaspersky Endpoint Security for Windows がサーバーリソースの 2% 以上を使用していないことを確認してください。

10. ルールのテストモードでアプリケーションコントロールをオンにします。

11. アプリケーションコントロールが動作していることを確認してください。必要に応じて、新しいアプリケーションコントロールルールを追加して、アプリケーションコントロールが動作していることを確認してからルールのテストモードをオフにします。

KSWS から KES への移行後、本製品が正しく動作していることを確認してください。コンソールでサーバーのステータスを確認します（[*OK*] になっている必要があります）。製品でエラーがレポートされていないことを確認し、管理サーバーに最後に接続された時刻、定義データベースの最終アップデート時刻およびサーバーの保護ステータスも確認してください。

Server Core モードのサーバーでの本製品の管理

Server Core モードのサーバーには GUI がありません。そのため、本製品を管理するにはリモートで Kaspersky Security Center コンソールを使用するか、ローカルでコマンドラインを使用する必要があります。

Kaspersky Security Center コンソールを使用した本製品の管理

Kaspersky Security Center コンソールを使用した本製品のインストールは、通常の本製品のインストールと異なる点はありません。インストールパッケージの作成時に、本製品をアクティベートするライセンスを追加することができます。Kaspersky Endpoint Security for Windows または Kaspersky Security for Windows Server のライセンスを使用できます。

Server Core モードのサーバーでは、次の製品コンポーネントは利用できません：ウェブ脅威対策、メール脅威対策、ウェブコントロール、有害 USB 攻撃ブロック、ファイルレベルの暗号化（FLE）、Kaspersky Disk Encryption（FDE）。

Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。本製品はユーザーにサーバーを再起動するよう要求するウィンドウを表示することはできません。サーバーの再起動が必要かどうかは、Kaspersky Security Center コンソールのレポートで確認できます。

Server Core モードのサーバーでの本製品の管理はコンピューターでの管理と異なる点はありません。本製品の設定にはポリシーおよびタスクを使用できます。

Server Core モードのサーバーで本製品を管理するには次の事項に留意してください：

- Server Core モードのサーバーには GUI がないため、Kaspersky Endpoint Security はユーザーに対して特別な駆除が必要であることを提示する警告を表示することができません。脅威を駆除するには、製品設定で特別な駆除を有効にして、*マルウェアのスキャンタスク*の設定で*すぐに特別な駆除を実行する*よう設定する必要があります。その後 *マルウェアのスキャンタスク*を開始します。

- BitLocker ドライブ暗号化は Trusted Platform Module（TPM）でのみ利用できます。本製品はパスワード入力ウィンドウを起動前認証で表示できないため、暗号化に PIN またはパスワードは使用できません。コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、ドライブの暗号化を開始する前に暗号化鍵を保存するためのリムーバブルドライブを接続してください。

コマンドラインを使用しての製品の管理

GUI を使用できない場合はコマンドラインを使用して Kaspersky Endpoint Security を管理できます。

Server Core モードのサーバーに本製品をインストールするには、次のコマンドを実行します：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

本製品をアクティベートするには、次のコマンドを実行します：

```
avp.com license /add <activation code or key file>
```

製品プロファイルのステータスを確認するには、次のコマンドを実行します：

```
avp.com status
```

アプリケーションの管理コマンドのリストを表示するには、次のコマンドを実行します：

```
avp.com help
```

［KSWS + KEA］から［KES + 組み込みエージェント］への移行

Kaspersky Security for Windows Server（KSWS）から Kaspersky Endpoint Security（KES）へ移行する際、サーバーの保護機能の設定および最適なパフォーマンスのため、必要に応じて次の推奨事項を参考にしてください。単一の組織での移行の例について説明します。

組織のインフラストラクチャ

会社では次のような構成で運用されているものとします：

- Kaspersky Security Center 14.2

  管理者は管理コンソール（MMC）を使用してカスペルスキー製品を管理している。Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) が導入されている

  Kaspersky Security Center では、組織のサーバーを含む次の 3 つの管理グループが作成されている：2 つの SQL サーバーの管理グループと、Microsoft Exchange サーバーの管理グループ。各管理グループはそれぞれのポリシーで管理されている。*定義データベースのアップデート*および*オンデマンドスキャンタスク*が組織のすべてのサーバーで作成されている。

  KSWS のアクティベーション用ライセンスは Kaspersky Security Center に追加されている。ライセンスの自動配信が有効になっている。

- SQL サーバーには Kaspersky Security for Windows Server 11.0.1 と Kaspersky Endpoint Agent 3.11 がインストールされている。SQL サーバーは 2 つのクラスターに統合されている。

  KSWS はポリシー「*SQL_Policy(1)*」および「*SQL_Policy(2)*」で管理されている。*定義データベースのアップデート*、*オンデマンドスキャンタスク*が作成されている。

- Microsoft Exchange Server には Kaspersky Security for Windows Server 11.0.1 と Kaspersky Endpoint Agent 3.11 がインストールされている。

  KSWS はポリシー「*Exchange_Policy*」で管理されている。*定義データベースのアップデート*、*オンデマンドスキャン*タスクが作成されている。

移行の計画

移行には次の手順が含まれます：

1. ポリシーとタスクの一括変換ウィザードを使用して KSWS タスクおよびポリシーを移行する。
2. ポリシーとタスクの一括変換ウィザードを使用して Kaspersky Endpoint Agent のポリシーを移行する。
3. タグを使用して、新しいポリシーのプロパティにあるポリシープロファイルを有効にする。
4. KSWS の代替として KES をインストールする。
5. EDR Optimum を有効にする。
6. KES が動作していることを確認する。

初めの移行シナリオは SQL サーバーのクラスターのうち 1 つで実行されます。次に SQL サーバーの別のクラスターで移行シナリオが実行されます。それから Microsoft Exchange で移行シナリオが実行されます。

ポリシーとタスクの一括変換ウィザードを使用して KSWS タスクおよびポリシーを移行する。

KSWS タスクの移行には、ポリシーとタスクの一括変換ウィザード（移行ウィザード）を使用できます。結果、ポリシー「*SQL_Policy(1)*」、「*SQL_Policy(2)*」および「*Exchange_Policy*」の代わりに、それぞれの SQL と Microsoft Exchange 用の 3 つのポリシーが統合された単一のポリシーが作成されます。KSWS の設定を含む新しいポリシープロファイルは「*UpgradedFromKSWS <Kaspersky Security for Windows Server のポリシー名>*」という名前になります。プロファイルのプロパティで、移行ウィザードは自動的にデバイスのタグ「`UpgradedFromKSWS`」を適用基準として選択します。このように、ポリシープロファイルからの設定はサーバーに自動的に適用されます。

ポリシーとタスクの一括変換ウィザードを使用して Kaspersky Endpoint Agent のポリシーを移行する

Kaspersky Endpoint Agent のポリシーを移行するには、ポリシーとタスクの一括変換ウィザードを使用できます。Kaspersky Endpoint Agent のポリシーおよびタスクの移行ウィザードは Web コンソールでのみ利用可能です。

タグを使用して、新しいポリシーのプロパティにあるポリシープロファイルを有効にする

プロファイルの有効化条件として事前に割り当てたデバイスのタグを選択します。ポリシーのプロパティを開き、［*ポリシープロファイルの有効化に対する全般ルール*］をプロファイルの有効化の条件として選択します。

KSWS の代替としての KES のインストール

KES をインストールする前に、KSWS のポリシーのプロファイルでパスワードによる保護を無効にしておく必要があります。

KES のインストールには次の手順が含まれます：

1. インストールパッケージを準備します。インストールパッケージのプロパティで、Kaspersky Endpoint Security for Windows 12.0 の配信キットを選択して、既定のコンポーネントのセットを選択します。
2. SQL サーバー管理グループの 1 つに *アプリケーションのリモートインストール*タスクを作成します。
3. タスクのプロパティで、インストールパッケージとライセンス情報ファイルを選択します。
4. タスクが正常に完了するまで待ちます。
5. 残りの管理グループに対しても同様の KES のインストールを繰り返します。

KES のインストールが完了すると、Kaspersky Security Center はコンソール上のコンピューターの名前にタグ「`UpgradedFromKSWS`」を自動的に追加します。

KES のインストールを確認するには、*製品導入レポート*を使用してください。デバイスのステータスも確認することができます。製品のアクティベーションを確認するには、*ライセンス使用レポート*を使用してください。

EDR Optimum の有効化

スタンドアロンの Kaspersky Endpoint Detection and Response Optimum のアドオンライセンスを使用して EDR Optimum の機能を有効化することができます。EDR Optimum のライセンスが Kaspersky Security Center のレポジトリに追加されていて、ライセンスの自動配信機能が有効になっていることを確認してください。

EDR Optimum が有効化されたことを確認するには、*製品コンポーネントのステータスレポート* を使用できます。

KES の動作の確認

KES が動作していることを確認するには、エラーが発生してないことを確認してください。デバイスのステータスは *OK* となっている必要があります。アップデートとマルウェアのスキャンタスクは正常に完了しました。

仮想マシンを保護する Light Agent モード

バージョン 12.8 以降では、Kaspersky Endpoint Security for Windows を Kaspersky Security for Virtualization Light Agent の一部として使用できます。*Kaspersky Security for Virtualization Light Agent* は、ネットワーク攻撃やフィッシング攻撃を含む様々なセキュリティ上の脅威から仮想マシンを包括的に保護する統合ソリューションです。このソリューションを使用するには、本製品を Light Agent モードでインストールする必要があります。

バージョン 6.2 以降の Kaspersky Security for Virtualization Light Agent の一部として、Light Agent モードの Kaspersky Endpoint Security を使用することができます。

Light Agent を起動すると、その仮想マシンである SVM（Secure Virtual Machine）への接続が確立され、維持されます。Protection Server は SVM 上に導入されます。*Protection Server* は、ファイルをスキャンしてウイルスやその他のマルウェアを検知し、定義データベースをアップデートし、ライセンスを管理する Kaspersky Security for Virtualization Light Agent ソリューションのコンポーネントです。Light Agent は、スキャンが必要なファイルのフラグメントを SVM に送信します。スキャン結果は、Light Agent がインストールされているすべての仮想マシンで利用できます（SharedCash 技術）。このように、SharedCash 技術によりソリューションの効率が向上し、脅威への対応が迅速化されます。

組織のインフラストラクチャには、Light Agent がインストールされた多数の仮想マシンと、多数の SVM が含まれる場合があります。Integration Server コンポーネントは、ソリューション コンポーネントと仮想インフラストラクチャ間の連携を目的としています。*Integration Server* - Kaspersky Security for Virtualization Light Agent のコンポーネントで、利用可能な SVM のリストを作成してそのデータを Light Agent に送信したり、Light Agent による SVM の検出を管理したり、Light Agent と SVM 間の接続を保護したりします。

Light Agent モードに関する特別な考慮事項

Kaspersky Endpoint Security のポリシーとタスクを使用して、標準モードおよび Light Agent モードの Kaspersky Endpoint Security を管理できます。Light Agent モードでは、本製品の一部のコンポーネントと機能は使用できません。

定義データベースとソフトウェアモジュールのアップデート

Light Agent モードの Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として動作する場合に必要な特別なマルウェア定義データベースを使用します。Kaspersky Endpoint Security は、Protection Server から定義データベースと製品モジュールのアップデートを取得します。

保護された仮想マシン上の定義データベースとモジュール、SVM 上のフォルダーがアップデート元として指定される特別な*定義データベースと製品機能のアップデート*タスクを使用してアップデートされます。Light Agent では*定義データベースと製品機能のアップデート*タスクが自動的に実行されます。別のアップデート元を選択したり、タスクのスケジュールを設定したり、タスクを削除したりすることはできません。

最新のマルウェア定義データベースのアップデートのロールバックも、Protection Server 側で処理されます。SVM で定義データベースと製品モジュールのアップデートがロールバックされると、保護対象仮想マシン上で特別なローカルの*定義データベースと製品機能のアップデート*タスクが開始されます。このタスクにより、Light Agent は以前の一連のマルウェア定義データベースを使用する状態に戻ります。

Light Agent モードの Kaspersky Endpoint Security は、*アップデートのロールバック*タスクをサポートしません。

Light Agent のアクティベーション

本製品をアクティベートするには、Light Agent が接続されている SVM にライセンスを追加する必要があります。本製品を個別にアクティベートする必要はありません。

Light Agent モードに関するその他の特別な考慮事項

- 本製品のポリシーを作成する際に、Light Agent モードを選択することを推奨します。このモードでは、新規ポリシーウィザードで、SVM 接続を設定するよう要求されます。本製品を Light Agent モードで動作させるには、これらの設定が必要です。
- Light Agent モードでは、データ暗号化コンポーネントとアダプティブアノマリーコントロールをインストールできません。コンポーネントのセットは、ゲストオペレーティングシステムの種別（ワークステーションまたはサーバー）によっても異なります。
- Light Agent は Kaspersky Endpoint Detection and Response Expert（クラウド）との統合をサポートしていません。
- Light Agent は、管理コンソール（MMC）と Kaspersky Security Center Web コンソールで管理できます。Kaspersky Security Center Cloud コンソールでは Light Agent を管理できません。
- VDI 仮想マシン上の製品コンポーネントのセットの変更はサポートされていません。
- Kaspersky Endpoint Security は、KSN プロキシサーバーを介して KSN サーバーと通信します。KSN との直接通信には対応していません。
- Kaspersky Security Network のクラウドモードはサポートされていません。
- Integration Server（VIIS）、Protection Server（SVM）、および KSN サーバーに接続する際の本製品のプロキシサーバーの使用はサポートされていません。

仮想マシンの予備設定

仮想プラットフォームテクノロジーを使用する仮想マシンに Kaspersky Endpoint Security をインストールできます。Kaspersky Endpoint Security は、VMware、Microsoft Hyper-V、Citrix 仮想プラットフォームをサポートします。インストールの前に、仮想マシンの予備設定を実行する必要があります。

Citrix App Layering テクノロジーとの互換性

Full User Layer を使用して一時仮想マシンの状態を保存する場合は、仮想マシンテンプレートにインストールする前に次の操作を実行します：

1. C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txtというファイルを作成し、そこに次の除外リストを追加します：

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. オペレーティングシステムのレジストリで、キー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr に、MiniFilterBypass という名前の新しい DWORD 値を作成し、それを 1 に設定します。

3. オペレーティングシステムのレジストリで、キー HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd に、ExcludeKey という名前の新しい MULTI_SZ 値を作成し、それを \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab に設定します。

4. 仮想マシンを再起動します。

Citrix App Layering を使用するインフラストラクチャ内の仮想マシンにインストールする場合は、次の操作を実行します：

1. Application Layer の仮想マシンテンプレートに、Kaspersky Security Center 管理エージェントと Kaspersky Endpoint Security for Windows をインストールします。

2. 複数レイヤーで構成される仮想マシンイメージを作成します。

3. 作成したイメージを、Citrix App Layering ソリューションをサポートするハイパーバイザーに導入します。

4. 作成されたイメージから一時仮想マシンの作成を設定します。

Citrix App Layering と併せてアンチウイルス製品をインストールする方法の詳細については、Citrix App Layering のドキュメント を参照してください。

Citrix Provisioning（Citrix Provisioning Services）テクノロジーとの互換性

本製品が Citrix Provisioning テクノロジー（Citrix Provisioning Services）と互換性があることを確認するには：

- Citrix Provisioning Target Device ソフトウェアが仮想マシンにインストールされている場合は、Kaspersky Endpoint Security をインストールする前に削除する必要があります。本製品のインストール後に、Citrix Provisioning Target Device をインストールする必要があります。
- インストールウィザードを使用して本製品をインストールする場合や、Kaspersky Security Center を使用してリモートで本製品をインストールする場合は、［**Citrix PVS との互換性を確保する**］をオンにする必要があります。

Omnissa App Volumes テクノロジーとの互換性

仮想マシンテンプレートにインストールする前に、%SVAgent%\Config\Custom\snapvol.cfg ファイルを作成し、そこに次の除外リストを追加します：

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

詳細は、Omnissa のドキュメントを参照してください。

Light Agent のインストール

Light Agent モードでの本製品のインストールは、標準モードの場合と同じです。仮想マシンに Light Agent をインストールする前に、Kaspersky Security Center Network Agent がインストールされていることを確認する必要があります。*ネットワークエージェント*は、管理サーバーと仮想マシンのやり取りをサポートします。

Light Agent は、次のいずれかの方法で仮想マシンにインストールできます：

- Kaspersky Security Center を使用してリモートで実行。
- インストールウィザードを使用してローカルで実行。
- コマンドラインを使用してローカルで実行。

Light Agent をインストールするには、インストールパッケージの設定またはインストールウィザードで適切な設定を選択する必要があります。

Light Agent をサーバーにインストールする場合、高度な保護コンポーネント（ふるまい検知、脆弱性攻撃ブロック、修復エンジン）は本製品の既定の設定から除外されます。本製品の既定の設定では、推奨される保護レベルとサーバーリソースの最適な使用が提供されます。Light Agent をワークステーションにインストールすると、高度な保護コンポーネントが本製品の既定の設定に組み込まれます。

Light Agent をインストールする際に、関連する仮想環境に対して、設定済みの信頼するオブジェクトとアプリケーションを選択することを推奨します。設定済みの信頼するオブジェクトとアプリケーションにより、本製品を迅速に設定し、仮想環境の互換性の問題を回避できます。インストール後に、ポリシーで設定済みの信頼するオブジェクトとアプリケーションを設定することもできます。

永続的な仮想マシンに Light Agent をインストールする場合、Sensor ID 生成アルゴリズムを変更する必要があることがあります。Sensor ID は、サーバーにテレメトリを送信するコンピューターを識別するために、Kaspersky Anti Targeted Attack Platform ソリューションで使用されます。一意の Sensor ID を作成するには、コマンドラインで本製品をインストールする際に `EnableUniqueSensorID=1` を設定します。

インストールウィザードを使用して Light Agent をインストールする方法

1. 仮想マシンに配信キットフォルダーをコピーします。
2. Setup_kes.exe を実行します。

   インストールウィザードが起動します。

Kaspersky Endpoint Security の設定



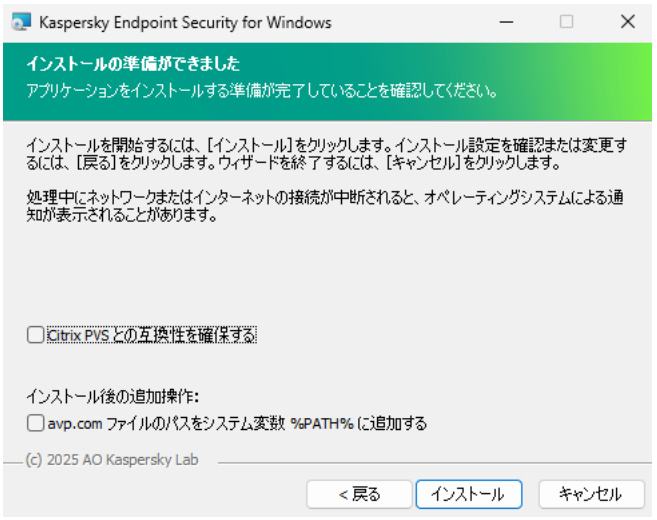
アプリケーションの設定の選択

仮想環境を保護する Light Agent 設定を選択します。この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。

Kaspersky Endpoint Security の各コンポーネント

インストールするコンポーネントを選択します（下図参照）。アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。これを行うには、インストールウィザードを再度実行し、使用可能なコンポーネントの変更を選択する必要があります。

詳細設定



詳細な製品のインストール設定

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

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

avp.com ファイルのパスをシステム変数 %PATH% に追加するコマンドラインインターフェイスの使用で便利なように、%PATH% 変数にインストール先のパスを追加できます。

コマンドラインを使用して Light Agent をインストールする方法

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   または

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1
   [VDI=1] [/qn]
   ```

   VDI のオプションによって VDI（Virtual Desktop Infrastructure）保護モードが有効になります。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。既定では、VDI 保護モードは無効になっています。

そのため、Light Agent は既定のコンポーネントのセットとともに仮想マシンにインストールされます。ファイル setup.ini を使用して、コンポーネントのセットを編集し、詳細設定を指定できます。コマンドラインでインストール設定を指定することもできます。

管理コンソール（MMC）を使用して Light Agent をインストールする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

   これにより、Kaspersky Security Center にダウンロードされたインストールパッケージのリストが開きます。
3. Kaspersky Endpoint Security for Windows インストールパッケージのプロパティを開きます。

   必要に応じて、新しいインストールパッケージを作成します。
4. ［**設定**］セクションに移動します。
5. **仮想環境を保護する Light Agent** 設定を選択します。この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。
6. インストールするコンポーネントを選択します。

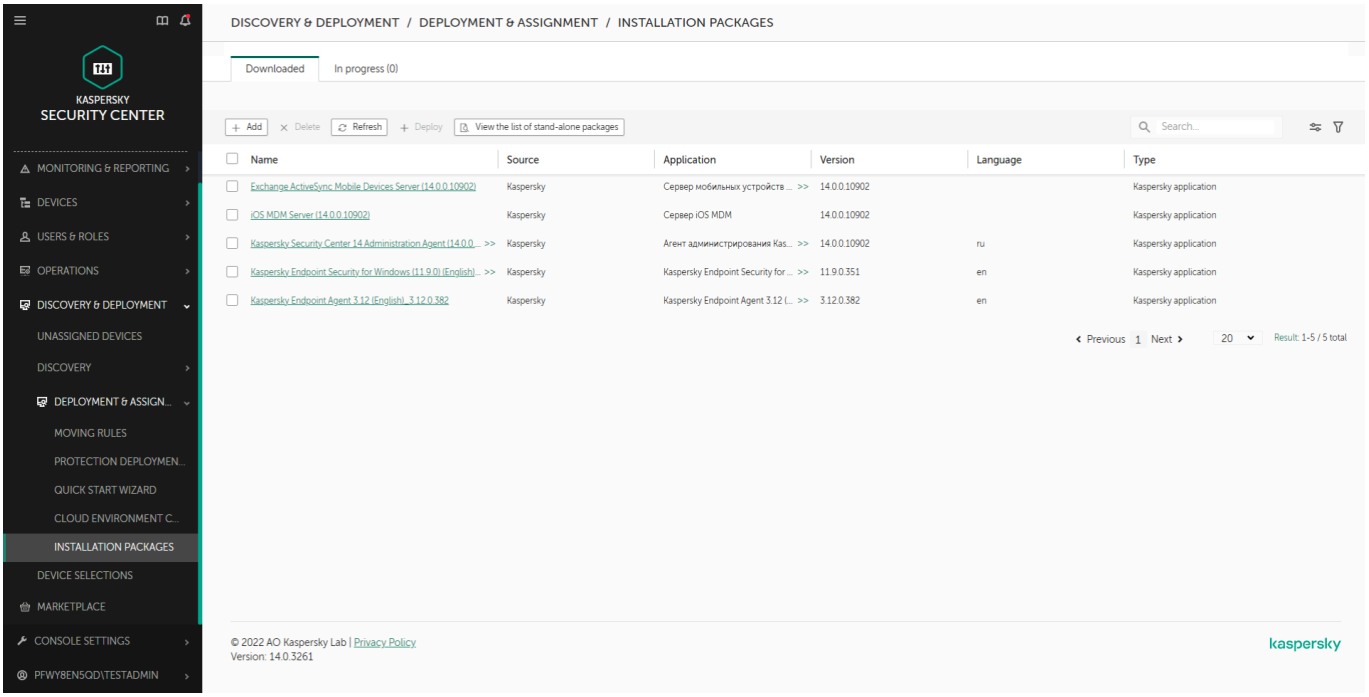
   アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。
7. 信頼ゾーンを設定します。本製品をインストールする仮想環境に対して、設定済みの信頼するオブジェクトとアプリケーションを選択します。

   設定済みの信頼するオブジェクトとアプリケーションにより、本製品を迅速に設定し、仮想環境の互換性の問題を回避できます。
8. 変更内容を保存します。
9. リモートインストールタスクを作成します。タスクのプロパティで、作成したインストールパッケージを選択します。

Web コンソールを使用して Light Agent をインストールする方法

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

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

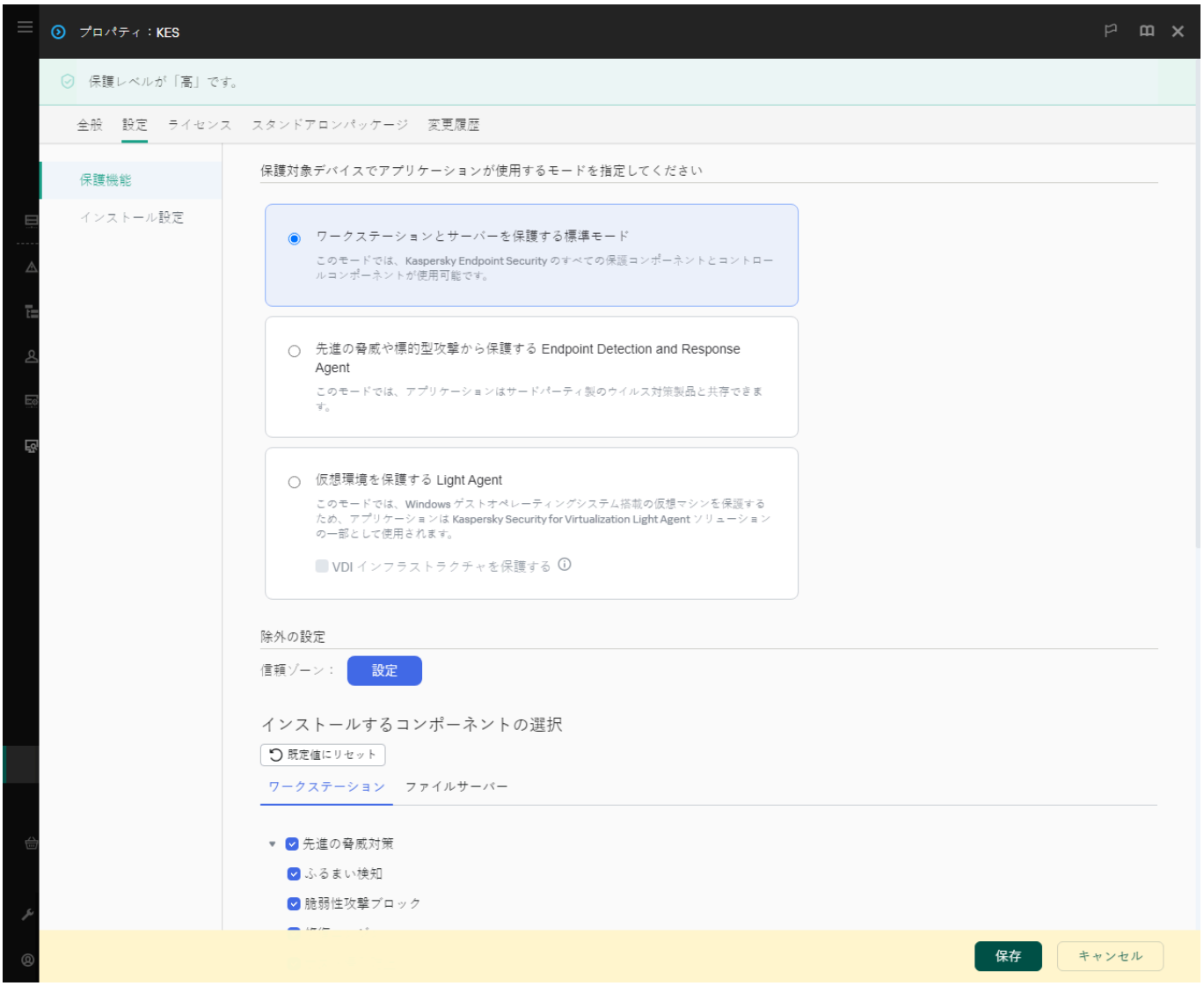


インストールパッケージのリスト

2. Kaspersky Endpoint Security for Windows インストールパッケージのプロパティを開きます。
   必要に応じて、新しいインストールパッケージを作成します。

3. ［**設定**］タブを選択します。

4. ［**保護機能**］セクションに移動します。



インストールパッケージに含まれるコンポーネント

5. **仮想環境を保護する Light Agent** 設定を選択します。この設定は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用される本製品を対象としています。Light Agent は、このソリューションを使用して保護する必要がある各仮想マシンにインストールする必要があります。この設定では、データ暗号化コンポーネントやアダプティブアノマリーコントロールは使用できません。*非永続的な仮想*マシンの作成に使用される仮想マシンテンプレートに Light Agent をインストールする場合は、［**VDI インフラストラクチャを保護する**］（VDI は Virtual Desktop Infrastructure の略）をオンにします。VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。このモードでは、Light Agent は仮想マシンの再起動を必要とする製品アップデートを拒否します。再起動を必要とする製品アップデートを受信すると、Light Agent は保護対象仮想マシンのテンプレートをアップデートする必要があることについてのイベントを生成します。

6. インストールするコンポーネントを選択します。

   アプリケーションのインストール後に、使用可能なアプリケーションコンポーネントを変更できます。

7. 信頼ゾーンを設定します。本製品をインストールする仮想環境に対して、設定済みの信頼するオブジェクトとアプリケーションを選択します。

   設定済みの信頼するオブジェクトとアプリケーションにより、本製品を迅速に設定し、仮想環境の互換性の問題を回避できます。

8. 変更内容を保存します。

9. リモートインストールタスクを作成します。タスクのプロパティで、作成したインストールパッケージを選択します。

これにより、Light Agent が仮想マシンにインストールされます。アプリケーションのインターフェイスを使用することができます。また、アプリケーションのアイコンが通知領域に表示されます。次に、Light Agent と SVMの接続を設定する必要があります。



Light Agent のメインウィンドウ

Light Agent と SVM の接続

Kaspersky Security for Virtualization Light Agent ソリューションでは、Light Agent と SVM の継続的な通信が必要です。これは、Light Agent によって送信されたファイルをスキャンしてウイルスやその他のマルウェアを検知するために必要です。SVM 接続がないと、Light Agent はスキャン用にファイルを送信できません。接続を確立できない時間が 5 分を超えると、スキャンがエラーで終了します。

Light Agent を SVM に接続するには、次の手順を実行します：

1. Light Agent が、使用可能な SVM のリストを取得します。

2. Light Agent が、SVM 選択アルゴリズムに基づいて、接続に最適である使用可能な Protection Server（SVM）を決定します。

3. Light Agent が、追加の SVM 接続設定（タグ、接続の保護ステータス、ライセンスに含まれる製品機能）を確認します。

4. Light Agent を SVM に接続します。

Light Agent の SVM への接続ステータスに関する情報は、Kaspersky Endpoint Security 内で、または本製品のコマンドを使用して取得できます。本製品は、Light Agent の SVM 接続が失われたり確立されたりするたびにイベントを生成して、これらのイベントを Kaspersky Security Center に送信します。SVM 検出に Integration Server を使用している場合は、Integration Server コンソールで、SVM のステータスと、接続されている Light Agent の数に関する情報を取得できます。SVM のステータスの監視について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

SVM 検出

Light Agent の SVM 検出方法を 1 つ選択できます：

- Integration Server (VIIS) の使用

  Integration Server は、Kaspersky Security for Virtualization Light Agent と仮想インフラストラクチャとの通信を可能にするソリューションのコンポーネントです。Integration Server は、接続できる SVM のリストを保持します。Light Agent は、Integration Server との接続を確立し、SVM アドレスのリストを取得します。

  Integration Server は、SVM 間で負荷を自動的に分散するので、大規模な仮想インフラストラクチャで役立ちます。Integration Server は、使用可能な SVM に関する情報を取得し、分析して、接続に最適な Protection Server（SVM）のリストを Light Agent に提供します。

  Light Agent が SVM のリストを取得できるようにするのに必要な操作は、Integration Server のアドレスを入力することだけです。

- SVM アドレスのカスタムリストの使用。

  Light Agent が接続する個々の SVM を指定する必要がある場合は、リストを手動で準備できます。

  Light Agent が接続できる使用可能な SVM のアドレスをリストアップする必要があります。

管理コンソール（MMC）で Light Agent による SVM 検出を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**Light Agent モード**］→［**SVM 検出設定**］の順に選択します。

4. SVM 検出方法を選択します。

   - **Integration Server を使用する**：Integration Server の接続設定を入力します。Integration Server がインストールされているデバイスの IPv4 形式による IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

   - **SVM アドレスのカスタムリストを使用する**：Light Agent が接続できる SVM のリストを作成します。SVM の IP アドレス（IPv4 形式）、または完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。

     SVM アドレスのリストで、単一の IP アドレスと一致する完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、ソリューションでエラーが発生する可能性があります。

5. 変更内容を保存します。

Web コンソールで Light Agent による SVM 検出を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。

   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**Light Agent モード**］→［**SVM 検出設定**］に移動します。

5. SVM 検出方法を選択します。

   - **Integration Server を使用する**：Integration Server の接続設定を入力します。Integration Server がインストールされているデバイスの IPv4 形式による IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

   - **SVM アドレスのカスタムリストを使用する**：Light Agent が接続できる SVM のリストを作成します。SVM の IP アドレス（IPv4 形式）、または完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。

     SVM アドレスのリストで、単一の IP アドレスと一致する完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、ソリューションでエラーが発生する可能性があります。

6. 変更内容を保存します。

製品インターフェイスで Light Agent による SVM 検出を設定する方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウの［**Light Agent モード**］で、［**SVM 検出設定**］をクリックします。

3. SVM 検出方法を選択します。

   - **Integration Server を使用する**：Integration Server の接続設定を入力します。Integration Server がインストールされているデバイスの IPv4 形式による IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

   - **SVM アドレスのカスタムリストを使用する**：Light Agent が接続できる SVM のリストを作成します。SVM の IP アドレス（IPv4 形式）、または完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。

     SVM アドレスのリストで、単一の IP アドレスと一致する完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、ソリューションでエラーが発生する可能性があります。

4. 変更内容を保存します。

Light Agent の SVM 選択アルゴリズムの設定

組織のインフラストラクチャには、Light Agent が接続できる SVM が複数導入されている場合があります。仮想インフラストラクチャのネットワークとリソースの負荷を分散するには、Light Agent を複数の SVM に分散させる必要があります。

Light Agent では、次のいずれかの SVM 選択アルゴリズムを使用して接続できます：

- **標準アルゴリズム**（既定）

  標準アルゴリズムには次の手順が含まれます：

  1. Light Agent が、*ローカルの SVM* を識別します。

     SVM をローカルとして識別するために、Light Agent は主に仮想インフラストラクチャ内の SVM の場所を使用します。SVM が Light Agent と同じハイパーバイザーに配置されている場合、Light Agent はそのような SVM をローカルと判断します。一部の仮想インフラストラクチャでは、設定ファイルを使用してローカルの SVM を手動で指定する必要があります。

  2. Light Agent が複数のローカルの SVM を検出した場合、Light Agent は接続されている Light Agent の数が最も少ない SVM を選択します。ローカルの SVM を識別できなかった場合、Light Agent は仮想インフラストラクチャ全体で接続されている Light Agent の数が最も少ない SVM を選択します。

  ローカルの SVM について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

- **拡張アルゴリズム**

  拡張アルゴリズムを使用すると、ローカルの SVM の選択条件を手動で指定したり、ローカルの SVM 検出を無効にしたりできます。そのためには、仮想インフラストラクチャ内の SVM パス（ハイパーバイザー、クラスタ、またはデータセンター）を選択する必要があります。つまり、ローカルの SVM を検出する範囲を選択する必要があります。Light Agent は、設定された検出範囲にあるローカルの SVM に接続できない場合、接続の試行を停止します。拡張アルゴリズムを使用して、Light Agent に対して、ローカルの SVM の検出を無効にすることもできます。この場合、Light Agent は、仮想インフラストラクチャ全体で接続されている Light Agent の数が最も少ない SVM を選択します。

SVM 接続アルゴリズムに加えて、タグを使用して複数の SVM に対する複数の Light Agent の接続を制限できます。

管理コンソール（MMC）で Light Agent の SVM 選択アルゴリズムを設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Light Agent モード**］→［**SVM 選択アルゴリズム**］の順に選択します。
4. アルゴリズムを選択します：
   - **標準の SVM 選択アルゴリズムを使用する**：Light Agent は、同じハイパーバイザーに導入された SVM を選択します。
   - **拡張 SVM 選択アルゴリズムを使用する**：Light Agent は、選択された種別の SVM パスに導入された SVM を選択します（既定では、［**ハイパーバイザー**］）。
5. 必要に応じて、拡張 SVM 選択アルゴリズムの SVM パスを選択します：
   - **ハイパーバイザー**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。
     - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザー上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。
     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のサーバーグループに配置されます。

     使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーまたはサーバーグループにない場合、Light Agent は SVM へ接続しません。
   - **クラスター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。
     - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザークラスタ上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。
     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一の OpenStack プロジェクトに配置されます。

     使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーのクラスタまたは OpenStack プロジェクトにない場合、Light Agent は SVM へ接続しません。
   - **データセンター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。
     - SVM は、Light Agent がインストールされた仮想マシンと同じデータセンター上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。
     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のアベイラビリティゾーンに配置されます。

Light Agent のある仮想マシンが配置されている同じデータセンターまたはアベイラビリティゾーンに接続可能な SVM がない場合、Light Agent は SVM に接続しません。

- **無視**：Light Agent は、Protection Server に接続するための SVM パスを無視します。Light Agent は、タグ、SVM に接続されている Light Agent の数など、他の条件を考慮します。

6. 変更内容を保存します。

Web コンソールで Light Agent の SVM 選択アルゴリズムを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**Light Agent モード**］→［**SVM 選択アルゴリズム**］に移動します。
5. アルゴリズムを選択します：
   - **標準の SVM 選択アルゴリズムを使用する**：Light Agent は、同じハイパーバイザーに導入された SVM を選択します。
   - **拡張 SVM 選択アルゴリズムを使用する**：Light Agent は、選択された種別の SVM パスに導入された SVM を選択します（既定では、［**ハイパーバイザー**］）。
6. 必要に応じて、拡張 SVM 選択アルゴリズムの SVM パスを選択します：
   - **ハイパーバイザー**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。
     - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザー上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。
     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のサーバーグループに配置されます。

     使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーまたはサーバーグループにない場合、Light Agent は SVM へ接続しません。
   - **クラスター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。
     - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザークラスタ上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。
     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一の OpenStack プロジェクトに配置されます。

使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーのクラスタまたは OpenStack プロジェクトにない場合、Light Agent は SVM へ接続しません。

- **データセンター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。

  - SVM は、Light Agent がインストールされた仮想マシンと同じデータセンター上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。

  - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のアベイラビリティゾーンに配置されます。

  Light Agent のある仮想マシンが配置されている同じデータセンターまたはアベイラビリティゾーンに接続可能な SVM がない場合、Light Agent は SVM に接続しません。

- **無視**：Light Agent は、Protection Server に接続するための SVM パスを無視します。Light Agent は、タグ、SVM に接続されている Light Agent の数など、他の条件を考慮します。

7. 変更内容を保存します。

製品インターフェイスで Light Agent の SVM 選択アルゴリズムを設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウの［**Light Agent モード**］で、［**SVM 検出設定**］をクリックします。
3. アルゴリズムを選択します：

   - **標準の SVM 選択アルゴリズムを使用する**：Light Agent は、同じハイパーバイザーに導入された SVM を選択します。

   - **拡張 SVM 選択アルゴリズムを使用する**：Light Agent は、選択された種別の SVM パスに導入された SVM を選択します（既定では、［**ハイパーバイザー**］）。

4. 必要に応じて、拡張 SVM 選択アルゴリズムの SVM パスを選択します：

   - **ハイパーバイザー**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。

     - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザー上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。

     - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のサーバーグループに配置されます。

     使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーまたはサーバーグループにない場合、Light Agent は SVM へ接続しません。

- **クラスター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。

  - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザークラスタ上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。

  - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一の OpenStack プロジェクトに配置されます。

  使用可能な SVM が、Light Agent がインストールされた仮想マシンが配置されたハイパーバイザーのクラスタまたは OpenStack プロジェクトにない場合、Light Agent は SVM へ接続しません。

- **データセンター**：Light Agent は、特定の基準を満たす SVM を接続先として選択します（仮想インフラストラクチャのタイプに応じて異なります）。

  - SVM は、Light Agent がインストールされた仮想マシンと同じデータセンター上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、または Numa xServer 上の仮想インフラストラクチャ）。

  - SVM は、Light Agent がインストールされた仮想マシン（TIONIX Cloud Platform または OpenStack Platform の仮想インフラストラクチャ）と同一のアベイラビリティゾーンに配置されます。

  Light Agent のある仮想マシンが配置されている同じデータセンターまたはアベイラビリティゾーンに接続可能な SVM がない場合、Light Agent は SVM に接続しません。

- **無視**：Light Agent は、Protection Server に接続するための SVM パスを無視します。Light Agent は、タグ、SVM に接続されている Light Agent の数など、他の条件を考慮します。

5. 変更内容を保存します。

複数の SVM に対する複数の Light Agent の接続の分散（タグ）

複数の Light Agent を 1 つの SVM に接続することができます。複数の Light Agent の接続のバランスをとるために、SVM の個別のリストを指定することができます。SVM 検出に Integration Server を使用している場合は、タグを使用して、複数の SVM に対する複数の Light Agent の接続のバランスをとることができます。つまり、1 つの Light Agent に対して、タグを使用して、接続する SVM のリストを割り当てることができます。これを行うには、タグを Light Agent に割り当てて、SVM 設定でこのタグを指定する必要があります。SVM 設定でのタグの指定について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

例：Kaspersky Endpoint Detection and Response Optimum ソリューションは、指定された仮想マシンホストのインフラストラクチャに導入されます。この場合、`[EDROptimum]` タグを Light Agent に割り当てて、EDR Optimum（EDR Optimum アドオン）ライセンスが追加された SVM に接続することができます。これにより、Light Agent がインストールされている仮想マシンで EDR Optimum 機能を使用できるようになります。EDR Optimum ライセンスのない SVM に Light Agent を接続した場合、Kaspersky Endpoint Detection and Response Optimum 機能は使用できません。

管理コンソール（MMC）で Light Agent に SVM 接続タグを割り当てる方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**Light Agent モード**］→［**SVM 接続タグ**］の順に選択します。

4. ［**接続タグを使用する**］をオンにして、SVM 接続タグを入力します。
   タグには 255 文字までのテキスト文字列を入力できます。［;］以外のすべての文字を使用できます。

5. 変更内容を保存します。

Web コンソールで Light Agent に SVM 接続タグを割り当てる方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**Light Agent モード**］→［**SVM 接続タグ**］に移動します。

5. ［**接続タグを使用する**］をオンにして、SVM 接続タグを入力します。
   タグには 255 文字までのテキスト文字列を入力できます。［;］以外のすべての文字を使用できます。

6. 変更内容を保存します。

製品インターフェイスで Light Agent に SVM 接続タグを割り当てる方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウの［**Light Agent モード**］で、［**SVM 接続タグ**］をクリックします。

3. ［**接続タグを使用する**］をオンにして、SVM 接続タグを入力します。
   タグには 255 文字までのテキスト文字列を入力できます。［;］以外のすべての文字を使用できます。

4. 変更内容を保存します。

Light Agent と SVM の間の接続の保護

Light Agent と Protection Server 間の接続の暗号化を設定できます。これを行うには、SVM の Protection Server 設定および Light Agent 設定で、Light Agent と Protection Server 間のデータチャネルの暗号化を有効にする必要があります。

接続保護が有効になっている Light Agent は、Light Agent と Protection Server 間のデータチャネルの暗号化が有効になっている SVM にのみ接続できます。接続保護が無効になっている Light Agent は、チャネル暗号化が無効になっているか、Protection Server と Light Agent 間のセキュアでない接続が許可されている SVM にのみ接続できます。

Protection Server での接続の保護の設定について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプ を参照してください。

暗号化を使用して接続を保護すると、Kaspersky Security for Virtualization Light Agent のパフォーマンスに影響する可能性があります。

管理コンソール（MMC）で Light Agent の接続の保護を設定する方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**Light Agent モード**］→［**接続の保護**］の順に選択します。
4. ［**Light Agent と Protection Server 間のデータチャネルを暗号化する**］チェックボックスをオンにします。
5. 変更内容を保存します。

Web コンソールの Light Agent で接続保護を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**Light Agent モード**］→［**接続の保護**］に移動します。
5. ［**Light Agent と Protection Server 間のデータチャネルを暗号化する**］チェックボックスをオンにします。
6. 変更内容を保存します。

製品インターフェイスで Light Agent の接続の保護を設定する方法

1. メインウィンドウで、⚙ をクリックします。
2. 本製品の設定ウィンドウの［**Light Agent モード**］で、［**接続の保護**］をクリックします。
3. ［**Light Agent と Protection Server 間のデータチャネルを暗号化する**］チェックボックスをオンにします。
4. 変更内容を保存します。

Light Agent のアクティベーション

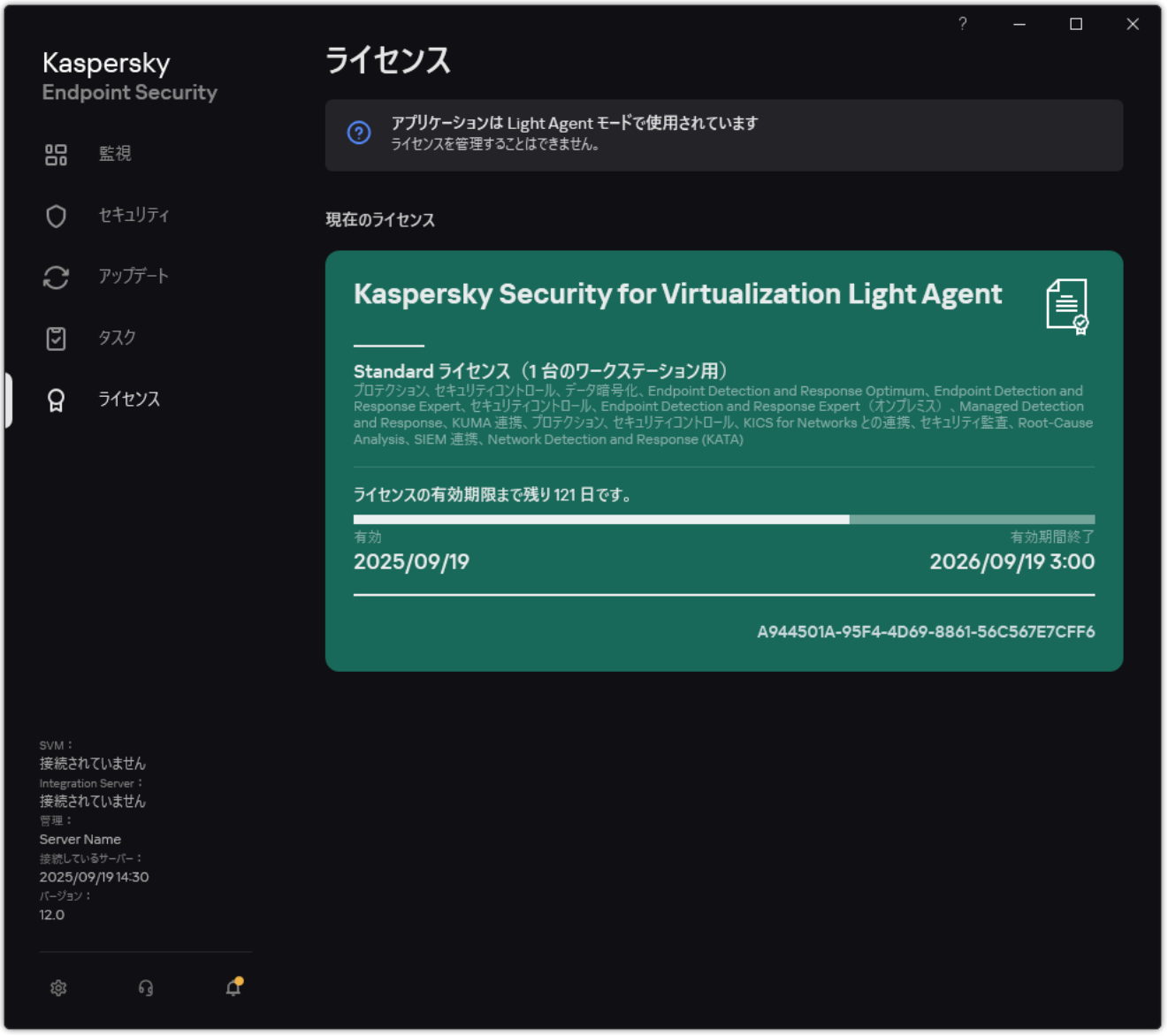
Kaspersky Endpoint Security を仮想環境保護用 Light Agent モードで使用する場合、製品を個別にアクティベートする必要はありません。本製品をアクティベートするには、SVM にライセンスを追加する必要があります。Kaspersky Security Center コンソールで特別なタスクを使用してライセンスを追加できます。Light Agent インターフェイスではライセンスを管理することはできませんが、ライセンス情報を表示することはできます（下の図を参照）。Light Agent のライセンス情報はコマンドラインでも表示できます（以下の手順を参照）。Light Agent は、この情報を SVM から取得します。ソリューションのアクティベーションとライセンスの管理について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプ を参照してください。

Light Agent のライセンス情報を表示するには：

1. 管理者としてコマンドラインインタープリタ（cmd）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   avp.com LICENSE /CHECK
   ```

これにより、Kaspersky Endpoint Security にライセンス情報（Light Agent の接続先の SVM のアドレス、ライセンスの有効期限までの日数などの情報）が表示されます。Light Agent のアクティベーション時に問題が発生した場合は、テクニカルサポートのナレッジベースの記事を参照してください。



［ライセンス］ウィンドウ

KSVLA Light Agent から KES Light Agent への移行ガイド

Kaspersky Security for Virtualization 5.2 Light Agent には、Light Agent for Windows 5.2 コンポーネント（以降、「KSVLA Light Agent」とも表記）が含まれています。Kaspersky Security for Virtualization Light Agent 6.2 では、Light Agent モードの Kaspersky Endpoint Security が Light Agent コンポーネントとして使用されます。ソリューションをバージョン 6.2 にアップデートするには、KSVLA Light Agent 5.2 から Light Agent モードの Kaspersky Endpoint Security（以下、「KES Light Agent」とも表記）に移行する必要があります。Kaspersky Security for Virtualization Light Agent ソリューションのバージョンのアップデートについて詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

ソフトウェア要件

KSVLA Light Agent から KES Light Agent への移行を開始する前に、Kaspersky Endpoint Security for Windows のハードウェアおよびソフトウェアの要件を満たしていることを確認してください。サポートされるオペレーティングシステムは KES と KSWS で異なります。例えば、KES は Windows Server 2003 を実行しているサーバーをサポートしていません。

KSVLA Light Agent から KES Light Agent へ移行するための最小ソフトウェア要件：

- Kaspersky Endpoint Security for Windows 12.8
- Kaspersky Security for Virtualization Light Agent 6.2（Protection Server と Integration Server のコンポーネントを含む）
- Kaspersky Security Center 14.2

  Kaspersky Security Center の以前のバージョンがインストールされている場合は、14.2 以降のバージョンにアップデートしてください。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、ポリシーではなくプロファイルに移行することができます。このバージョンの Kaspersky Security Center を使用すると、ポリシーとタスクの一括変換ウィザードは、より広い範囲のポリシー設定を移行することができます。

移行手順

KSVLA Light Agent から KES Light Agent への移行は半自動的に実行されます。これはアプリケーションのアーキテクチャが異なるために必要となります。

次の順序で KSVLA Light Agent から KES Light Agent に移行します：

1. **KSVLA Light Agent のタスクとポリシーを移行する**

   ポリシー設定の移行には、ポリシーとタスクの一括変換ウィザード（移行ウィザード）を実行する必要があります。ポリシー設定を移行した後、移行ウィザードが対応できなかった設定を手動で設定する必要があります（たとえば、定義データベースのアップデートの設定など）。移行後、すべての設定が正しく移行されたかどうか確認してください。

   > KSVLA Light Agent へのアクセスを制限するためにパスワードによる保護が有効になっている場合は、KES Light Agent をインストールする前に、KSVLA Light Agent のポリシーでパスワードによる保護を無効にする必要があります。KES Light Agent インストールパッケージの設定では、アンインストールのパスワードを入力することはできません。KSVLA Light Agent 上への KES Light Agent のインストールが完了したら、KES ポリシーでパスワードによる保護を有効にする必要があります。

2. **Kaspersky Endpoint Security を Light Agent モードでインストールする**

   次の方法で KES Light Agent をインストールすることができます。

   - KSVLA Light Agent のアンインストール後にKES Light Agent をインストールする（推奨）。
   - KSVLA Light Agent 上に KES Light Agent をインストールする。

3. **移行後、本製品が正しく動作していることを確認する**

   KSVLA Light Agent から KES Light Agent への移行後、本製品が正しく動作していることを確認してください。変換されたポリシーをアクティブにします。Kaspersky Security Center コンソールで仮想マシンのステータスを確認します（[*OK*] になっている必要があります）。本製品についてのエラーが報告されていないことを確認し、SVM に最後に接続した時間と仮想マシンの保護の状態も確認します。ライセンスは SVM に追加されるため、Light Agent をアクティベートする必要はありません。

KSVLA Light Agent の代替として KES Light Agent のインストール

KES Light Agent は、次の方法でインストールすることができます。

- KSVLA Light Agent のアンインストール後にKES Light Agent をインストールする（推奨）。
- KSVLA Light Agent 上に KES Light Agent をインストールする。

KSVLA Light Agent の削除

本製品の削除は、アプリケーションのリモートインストールタスクを使用してリモートから実行することも、仮想マシン上でローカルに実行することも、仮想マシンテンプレートで実行することもできます。
KSVLA Light Agent を削除した後で、仮想マシンを再起動する必要がある場合があります。

KSVLA Light Agent を削除したら、適切な方法を使用して KES Light Agent をインストールします。

KSVLA Light Agent へのアクセスを制限するためにパスワードによる保護が有効になっている場合は、KES Light Agent をインストールする前に、KSVLA Light Agent のポリシーでパスワードによる保護を無効にする必要があります。KES Light Agent インストールパッケージの設定では、アンインストールのパスワードを入力することはできません。KSVLA Light Agent 上への KES Light Agent のインストールが完了したら、KES ポリシーでパスワードによる保護を有効にする必要があります。

Kaspersky Endpoint Security のインストール時に、［**仮想環境を保護する Light Agent**］モードをオンにする必要があります。仮想マシンに KES Light Agent をインストールする前に、インストーラーによって KSVLA Light Agent が共存できないソフトウェアとして検出されて、削除されます。KSVLA Light Agent の設定の移行はサポートされていません。つまり、KES Light Agent をインストールする際にインストールされるコンポーネントのセットは、インストールパッケージのプロパティまたはインストールウィザードで選択した内容によって決まります。KSVLA Light Agent を削除した後で、仮想マシンを再起動する必要があります。

KES Light Agent のインストール時には、KSVLA Light Agent の設定とタスクは移行されません。製品設定を移行するには、ポリシーとタスクの一括変換ウィザードを実行します。

インストールされたコンポーネントの一覧は、`status` コマンドを使用して製品インターフェイスの［**セキュリティ**］セクションで確認するか、Kaspersky Security Center コンソールのコンピューターのプロパティで確認できます。インストール後に［*コンポーネントの変更*］を使用してコンポーネントセットを変更することができます。

KSVLA Light Agent と KES Light Agent のコンポーネントの対応

KSVLA Light Agent と KES Light Agent のコンポーネントのセットは実質的に同じです。KES Light Agent には、KSVLA Light Agent よりも多くの設定があります。移行すると、新しい設定に既定値が設定されます。

KSVLA Light Agent と KES Light Agent のコンポーネントの対応

Light Agent 5.2	KES Light Agent
カーネルをスキャンする	アプリケーションカーネル
ファイルアンチウイルス	ファイル脅威対策
メール保護メールアンチウイルス	メール脅威対策
ウェブアンチウイルス	ウェブ脅威対策
ファイアウォール	ファイアウォール
ネットワーク攻撃防御	ネットワーク脅威対策
アプリケーション権限コントロール	ホスト侵入防止
アプリケーション起動コントロール	アプリケーションコントロール
ウェブコントロール	ウェブコントロール
デバイスコントロール	デバイスコントロール
システムウォッチャー	Kaspersky Endpoint Security では、このコンポーネントは次のコンポーネントに分かれています： • 脆弱性攻撃ブロック • ふるまい検知 • 修復エンジン
システム変更監視	システム変更監視

Light Agent 5.2	KES Light Agent
Kaspersky Endpoint Agent との統合	*（サポートされていません）* Kaspersky Endpoint Security for Windows 11.9.0 以降では、Kaspersky Endpoint Agent 配布パッケージは配信キットには含まれません。
AMSI 保護	AMSI 保護

KSVLA Light Agent のタスクとポリシーの移行

ポリシーとタスクの一括変換ウィザード（以降、「移行ウィザード」とも表記）を使用して、KSVLA Light Agent のポリシーとタスクの設定を移行することができます。

KSVLA Light Agent の移行ウィザードは管理コンソール（MMC）でのみ使用可能です。ポリシーとタスクの設定は Web コンソールおよび Cloud コンソールでは移行できません。

ポリシーとタスクの移行時には、次の特別な考慮事項が適用されます：

- 新しいポリシーは「*<ポリシー>（変換済み）*」という名前になります。
- 新しいポリシーのステータスは*非アクティブポリシー*になっています。
- 設定の変更が禁止されたもの（「南京錠」）は移行されません。移行ウィザードで既定値が設定されます。
- ポリシーのプロファイルは移行されません。手動でポリシーのプロファイルを追加する必要があります。
- 信頼ゾーンの管理が改善されました。KSVLA Light Agent では、設定済みの除外リストを追加できるのは、ポリシーを作成する時のみでした。これ以降、ポリシーのプロパティで、以前に追加した設定済みの除外リストを設定したり、除外リストを手動で追加したりできるようになりました。ポリシーのプロパティで、設定済みの除外リストを追加することはできません。KES Light Agent では、ポリシーの作成中でも、作成されたポリシーのプロパティでも、設定済みの除外リストを追加することができます。インストールパッケージで、設定済みの除外リストを選択することもできます。
- Kaspersky Endpoint Security の製品ユーザーインターフェイスの設定は、インストーラーからポリシーに移動されました。たとえば、製品のユーザーインターフェイスを非表示にする必要がある場合は、ポリシーの設定を管理します。
- 権限ベースのアクセス制御（RBAC）を設定するための機能セットは、Kaspersky Endpoint Security と KSVLA Light Agent で異なります。機能領域へのユーザーアクセス権を、最初から設定する必要があります。

ポリシーとタスクの一括変換ウィザードを使用して KSVLA Light Agent のポリシーの設定を移行する方法

1. 管理コンソールで、管理サーバーを選択して右クリックしてコンテキストメニューを開きます。
2. ［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

ポリシーとタスクの一括変換ウィザードが開始されます。ウィザードの指示に従います。

ステップ1：ポリシーとタスクを変換するアプリケーションの選択

ここでは、Kaspersky Endpoint Security for Windows を選択します。次の手順に進みます。

ステップ2：ポリシーの変換

変換する Kaspersky Security for Virtualization 5.2 Light Agent for Windows ポリシーを選択します。次の手順に進みます。

移行ウィザードはポリシーの返還を開始します。変換中に、移行ウィザードで Kaspersky Security Network に関する声明の諸条件に同意する必要があります。新しいポリシーは「*<ポリシー>（変換済み）*」という名前になります。

ステップ3：タスクの変換

移行ウィザードは Kaspersky Endpoint Security for Windows 向けの新しいタスクを作成します。タスクのリストで、 Kaspersky Endpoint Security 向けに作成する KSVLA Light Agent のタスクを選択します。新しいタスクは「*<タスク名>（変換済み）*」という名前になります。次の手順に進みます。

ステップ4：ウィザードの完了

ウィザードを終了します。

ポリシーの移行後に、ポリシーのプロパティを開いて、その設定を確認して、ポリシーを保存する必要があります。これらのステップを完了しないと、変換されたポリシーが KES Light Agent で無視される場合があります。

Light Agent の SVM 接続設定、除外リスト、信頼するアプリケーション、信頼する URL、アプリケーションコントロールルールの移行には特に注意してください。

[KSVLA Light Agent+KEA] 設定から [KES Light Agent+組み込みエージェント] への移行

EDR (KATA)、EDR Optimum、Kaspersky Sandbox の一部としての Kaspersky Endpoint Security for Windows の使用をサポートするため、組み込みエージェントが製品に追加されました。これらのソリューションと連携するために Kaspersky Endpoint Agent を別途インストールする必要がなくなりました。

KSVLA Light Agent から KES Light Agent への移行時、EDR (KATA)、EDR Optimum、Kaspersky Sandbox ソリューションは Kaspersky Endpoint Security との動作を続行します。また、Kaspersky Endpoint Agent はコンピューターから削除されます。

KSVLA Light Agent から KES Light Agent に移行する前に、Protection server と Integration server を含む Kaspersky Security for Virtualization のすべてのコンポーネントをバージョン 6.2 にアップデートする必要があります。Kaspersky Security for Virtualization Light Agent ソリューションのバージョンのアップデートについて詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

[KSVLA Light Agent+KEA] 設定から [KES Light Agent+組み込みエージェント] への移行には次の手順が含まれます：

1 ポリシーおよびタスクの移行

[KSVLA Light Agent+KEA] のポリシーとタスクからの [KES Light Agent+組み込みエージェント] へ移行には、次の手順が含まれます：

1. ポリシーとタスクの一括置換ウィザード（管理コンソール（MMC）上でのみ使用可能）を使用した、KSVLA Light Agent から KES Light Agent へのポリシーとタスクの移行。

   「*<ポリシー> (変換済み)*」という名前の新しいポリシーが作成されます。新しい KES タスクも「*<タスク名> (変換済み)*」という名前で作成されます。

2. Kaspersky Endpoint Agent からの移行用のウィザード（Web コンソールと Cloud コンソールでのみ使用可能）を使用した、KEA から KES へのポリシーとタスクの移行。

   「*<Kaspersky Endpoint Security ポリシー名> & <Kaspersky Endpoint Agent ポリシー名>*」という名前の新しいポリシーが作成されます。新しいタスクと KES のタスクも作成されます。

2 KSVLA Light Agent から KES Light Agent への移行

KSVLA Light Agent から KES Light Agent への移行には、KSVLA Light Agent の代わりとしての KES Light Agent のインストールが含まれます。

KSVLA Light Agent および KEA へのアクセスを制限するために、管理者がパスワードによる保護を有効にしているケースが多くあります。KEA のアンインストールのパスワードは、*アプリケーションのリモートインストール*タスクのプロパティでのみ入力できます。移行するには、KSVLA Light Agent のパスワードによる保護を無効にする必要があります。

移行作業を実行するため、Kaspersky Endpoint Security の一部としてDetection and Response ソリューションをサポートするコンポーネントを選択する必要があります。本製品のインストール後、Kaspersky Endpoint Security は組み込みエージェントを使用するよう切り替えられ、Kaspersky Endpoint Agent は削除されます。

3 ライセンス機能

本製品を Light Agent モードで使用する場合は、本製品をアクティベートする必要はありません。本製品をアクティベートするには、SVM にライセンスを追加する必要があります。追加機能（EDR Optimum など）をアクティベートするためのライセンスを SVM に追加する必要もあります。つまり、機能のライセンスは、移行の一環として自動的に付与されます。

4 Kaspersky Endpoint Detection and Response Optimum および Kaspersky Sandbox の状態を確認する。

アップグレード後に、Kaspersky Security Center コンソールでコンピューターに「*緊急*」ステータスが表示されている場合：

- コンピューターにネットワークエージェントのバージョン 13.2 以降がインストールされていることを確認します。
- 組み込みエージェントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。コンポーネントのステータスが「*未インストール*」となっている場合は、*コンポーネントの変更*タスクを使用してコンポーネントをインストールしてください。
- Kaspersky Endpoint Security for Windows の新しいポリシーで Kaspersky Security Network に関する声明に同意していることを確認してください。
- *製品コンポーネントのステータスレポート*を使用して EDR Optimum 機能がアクティベートされているかどうかを確認してください。コンポーネントの状態が「*ライセンスに含まれていません*」と表示されている場合は、EDR Optimum の自動ライセンス配信機能がオンになっていることを確認してください。
- 仮想マシンと SVM の接続の状態を確認します。Light Agent の SVM への接続ステータスに関する情報は、Kaspersky Endpoint Security 内で、または本製品のコマンドを使用して取得できます。

コマンドラインを使用しての製品の管理

コマンドラインを使用して Kaspersky Endpoint Security を管理できます。本製品の管理に利用できるコマンドのリストは、「`avp.com HELP`」コマンドを実行して確認できます。特定のコマンドの構文を確認するには、「`avp.com HELP <command>`」コマンドを実行します。

コマンド内の特殊文字はエスケープする必要があります。文字「`&`」、「`|`」、「`(`」、「`)`」、「`<`」、「`>`」、「`^`」をエスケープするには、「`^`」を使用します（たとえば、「`&`」を使用するには「`^&`」と入力します）。文字「`%`」をエスケープするには、「`%%`」と入力します。

`1` を設定する代わりに `yes`、`on`、`enable`、`enabled`、`true` も指定できます。`0` を設定する代わりに `no`、`off`、`disable`、`disabled`、`false` も指定できます。

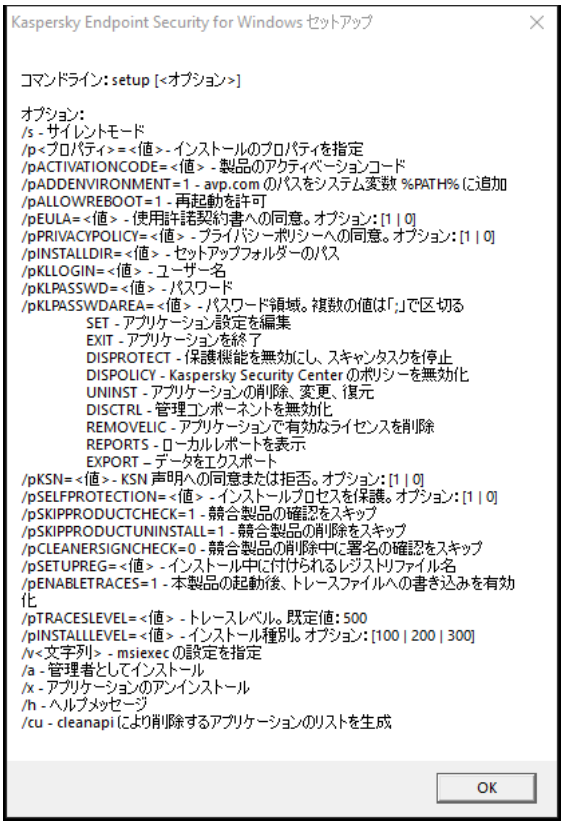
Setup：本製品のインストール

Kaspersky Endpoint Security は次のいずれかのモードでコマンドラインを使用してインストールできます。

- インストールウィザードを使用したインタラクティブモード。
- サイレントモード：サイレントモードでのインストールの開始後は、インストールプロセスでユーザーが操作を行う必要はありません（サイレントインストール）。サイレントモードで本製品をインストールするには、「`/s`」と「`/qn`」パラメータを使用します。

  サイレントモードで本製品をインストールする前には、使用許諾契約書とプライバシーポリシーをよくお読みください。使用許諾契約書とプライバシーポリシーのテキストは、Kaspersky Endpoint Security の配信キットに含まれています。使用許諾契約書の条項をすべて確認し、理解した上でこれに同意しており、なおかつプライバシーポリシーの内容をすべて確認し、理解した上で、プライバシーポリシーに従ってデータの処理と送信（第三国への送信を含む）が行われることに同意している場合にのみ、本製品のインストールに進むことができます。使用許諾契約書の条項とプライバシーポリシーに同意しない場合、Kaspersky Endpoint Security をインストールまたは使用しないでください。

本製品のインストールに利用できるコマンドのリストは、「/h」コマンドを実行して確認できます。インストールコマンドの構文に関するヘルプを表示するには、「setup_kes.exe /h」を入力してください。インストーラーはコマンドオプションの説明のウィンドウを表示します（下図を参照）。



インストールコマンドオプションの説明

本製品をインストールまたは以前のバージョンからアップグレードするには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>] [/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>] [/pSKIPKB5007186CHECK=1] [/s]
   ```

   または

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
   ```

この結果、本製品がコンピューターにインストールされます。本製品がインストールされたこと、また本製品の設定は status コマンドを実行することで確認できます。

`EULA=1`	使用許諾契約書の条項に同意する。使用許諾契約書のテキストは、Kaspersky Endpoint Security の配信キットに含まれています。 製品をインストールまたはアップグレードするには、使用許諾契約書に同意する必要があります。
`PRIVACYPOLICY=1`	プライバシーポリシーに同意する。プライバシーポリシーのテキストは、Kaspersky Endpoint Security の配信キットに含まれています。 本製品のインストールおよびバージョンのアップグレードには、プライバシーポリシーに同意する必要があります。
`KSN`	Kaspersky Security Network (KSN) への参加に同意するかどうか。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security を最初に起動したときに、KSN への参加に同意するかどうかの確認画面が表示されます。次の値を設定できます： • `1`：KSN への参加に同意する • `0`：KSN への参加に同意しない（既定値） Kaspersky Endpoint Security の配布パッケージは、Kaspersky Security Network とともに使用するように最適化されています。Kaspersky Security Network に参加しない場合、インストール後すぐに Kaspersky Endpoint Security をアップデートしてください。
`CONFIGPATH=<path to the configuration file>`	定義済みの設定で本製品をインストール。これには、Kaspersky Endpoint Security の設定を定義した設定ファイルをアップロードする必要があります。製品のローカルインターフェイスで、設定ファイルを作成できます。
`ALLOWREBOOT=1`	製品のインストール後またはアップグレード後にコンピューターの再起動が必要な場合に自動再起動を行うかどうか。このパラメータの値が指定されていない場合、コンピューターの自動再起動はブロックされます。 Kaspersky Endpoint Security のインストールでは再起動は必要ありません。インストール前に競合するアプリケーションをアンインストールする必要がある場合にのみ再起動が必要になります。製品バージョンのアップデートでも、再起動が必要になる場合があります。
`SKIPPRODUCTCHECK=1`	インストール済みのソフトウェアのチェックの実行を無効にします。互換性の問題が発生する可能性のあるソフトウェアのリストは、配信キットに含まれている incompatible.txt ファイルで参照できます。このパラメータの値が指定されておらず、リストに記載されている製品が検知された場合、Kaspersky Endpoint Security のインストールは終了します。
`SKIPPRODUCTUNINSTALL=1`	incompatible.txt リストに記載されたソフトウェアが検知された場合の自動削除を無効にします。このパラメータの値が指定されていない場合、Kaspersky Endpoint Security は互換性の問題が発生する可能性のあるソフトウェアの削除を試みます。 msiexec インストーラーを使用して Kaspersky Endpoint Security をインストールする場合、ソフトウェアの自動削除を有効にすることはできません。互換性の問題が発生する可能性のあるソフトウェアを自動的に削除するには、setup_kes.exe ファイルを使用します。
`CLEANERSIGNCHECK=0|1`	incompatible.txt リストに記載のあるソフトウェアが検出された際の、ソフトウェアのファイルのデジタル署名の検証。ソフトウェアを削除するため、Kaspersky Endpoint Security はソフトウェアのインストーラーファイルを実行します。インストーラーファイルにデジタル署名がない場合は、悪意のあるコードを実行する可能性を避けるため、Kaspersky Endpoint Security はそのファイルを信頼済みでないと判断して、競合するソフトウェアののアンインストールを停止します。Kaspersky Endpoint Security が検出されたソフトウェアのファイルのデジタル署名を検証できない場合、Kaspersky Endpoint Security のインストールはエラーで停止されます。 既定の値はソフトウェアのインストール方法により異なります。 • `0`：デジタル署名の検証は無効です（ソフトウェアが Kaspersky Security Center を介して配信された場合の既定値）。 • `1`：デジタル署名の検証は有効です（ソフトウェアがローカルでインストールされている場合の既定値）。

STANDALONEMODE=1	Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションとの連携のために、Endpoint Detection and Response Agent (EDR Agent) 設定に本製品をインストールします。この設定は、組織の環境に Kaspersky Endpoint Detection and Response クラスのソリューションと並んでサードパーティのエンドポイント保護プラットフォーム（EPP）が導入されている場合に必要です。これにより、Endpoint Detection and Response Agent 設定の Kaspersky Endpoint Security がサードパーティ RPP 製品と互換性を持つようになります。
KLLOGIN	Kaspersky Endpoint Security の機能と設定にアクセスできるユーザー名の指定（パスワードによる保護機能）。ユーザー名は、「KLPASSWD」および「KLPASSWDAREA」の設定と合わせて指定します。既定では、ユーザー名 KLAdmin が使用されます。
KLPASSWD	Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワード（パスワードは「KLLOGIN」および「KLPASSWDAREA」パラメータと合わせて指定します）。 「KLLOGIN」パラメータでユーザー名を指定せずにパスワードを指定した場合、KLAdmin が既定のユーザー名として使用されます。
KLPASSWDAREA	Kaspersky Endpoint Security の機能と設定にアクセスするためのパスワードが必要になる操作の範囲。この範囲内に含まれている操作をユーザーが実行しようとした場合、Kaspersky Endpoint Security でアカウントの認証情報の入力を要求されます（「KLLOGIN」と「KLPASSWD」パラメータ）。複数の値を指定するには、区切り文字として;を使用してください。 次の値を設定できます： • SET：製品設定の変更 • EXIT：製品の終了 • DISPROTECT：保護機能の停止とスキャンタスクの停止 • DISPOLICY：Kaspersky Security Center ポリシーの無効化 • UNINST：コンピューターからの製品の削除 • DISCTRL：管理コンポーネントの停止 • REMOVELIC：ライセンスの削除 • REPORTS：レポートの表示 • EXPORT：本製品の設定のエクスポート 例：「KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT」。 KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。したがって、KLAdmin アカウントのパスワードを要求する操作を設定することはできません。KLAdmin アカウントのパスワードを要求する操作を設定しようとすると、本製品は「Everyone」グループに対して指定された処理を禁止します。
PROTECTOSSERVICES	オペレーティングシステムのサービスの保護機能。オペレーティングシステムのサービスの保護は、サードパーティ製アプリケーションによってオペレーティングシステムのサービスの処理が妨げられるのを防止します。こうしたサービスには、アプリケーションの自動起動サービスなどがあります。 • 1：オペレーティングシステムのサービスの保護は有効です（既定値）。 • 0：オペレーティングシステムのサービスの保護は無効です。
ENABLETRACES	本製品のトレース記録を有効にするかどうか。Kaspersky Endpoint Security は、起動後にトレースファイルを「%ProgramData%\Kaspersky Lab\KES.12.12\Traces」フォルダーに保存します。次の値を設定できます： • 1：トレース記録をオンにする • 0：トレース記録をオフにする（既定値）
TRACESLEVEL	トレース記録の詳細度。次の値を設定できます： • 100（緊急）：深刻なエラーに関するメッセージのみ。 • 200（高）：深刻なエラーを含めたすべてのエラーに関するメッセージ。 • 300（診断）：すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。 • 400（重要）：すべてのエラーに関するメッセージとすべての警告および詳細情報。 • 500（通常）：すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ（既定値）。 • 600（低）：すべてのメッセージ。

ENABLEAZURESUPPORT	Azure WVD 互換モードを有効または無効にします。次の値を設定できます： • 1：Azure WVD 互換モードを有効にする • 0：Azure WVD 互換モードを無効にする（既定値） この機能により、Kaspersky Anti Targeted Attack Platform コンソールに Azure 仮想マシンの状態が正しく表示されるようになります。コンピューターのパフォーマンスを監視するため、Kaspersky Endpoint Security はテレメトリを KATA サーバーに送信します。テレメトリにはコンピューターの ID（Sensor ID）が含まれます。Azure WVD 互換モードはこれらの仮想マシンに永続的に一意な Sensor ID を割り当てることができます。互換モードがオフになっている場合、Azure 仮想マシンの仕組みにより、コンピューターが再起動した後に Sensor ID が変更されることがあります。このため、コンソール上で仮想マシンが重複して表示されることがあります。
AMPPL	AM-PPL 技術（Antimalware Protected Process Light）を使用した Kaspersky Endpoint Security プロセスの保護を有効にするかどうか。AM-PPL 技術について詳しくは、Microsoft の Web サイトの情報を参照してください。 AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。 次の値を設定できます： • 1：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を有効にする • 0：AM-PPL 技術を使用した Kaspersky Endpoint Security プロセスの保護を無効にする
UPGRADEMODE	アプリケーションのアップグレードモード： • Seamless はコンピューターを再起動してアプリケーションをアップグレードすることを意味します（既定値）。 • Force はコンピューターを再起動せずにアプリケーションをアップグレードすることを意味します。 バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。これより前のバージョンのアプリケーションをアップグレードする場合は、コンピューターを再起動する必要があります。バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることもできるようになりました。 Kaspersky Endpoint Security のインストールでは再起動は必要ありません。従って、アプリケーションのアップグレードモードはアプリケーション設定で指定されます。アプリケーション設定またはポリシーでこのパラメータを変更できます。 既にインストールされているアプリケーションをアップグレードする場合、コマンドラインのパラメータの優先度は、アプリケーション設定または setup.ini ファイルで指定されたパラメータの優先度よりも低くなります。たとえば、Force アップグレードモードがコマンドラインで指定され、Seamless モードがアプリケーション設定で指定されている場合、コンピューターを再起動してアップグレードをインストールします（Seamless）。
RESTAPI	REST API を使用した製品の管理。REST API を使用して製品を管理するには、ユーザー名（RESTAPI_User パラメータ）を指定する必要があります。 次の値を設定できます： • 1 – REST API による管理を許可する • 0 – REST API による管理をブロックする（既定値） REST API を使用して製品を管理するには、管理システムを使用した管理を許可する必要があります。許可するには、AdminKitConnector=1 パラメータを設定します。REST API を使用して製品を管理する場合、カスペルスキーの管理システムを使用して製品を管理することはできません。
RESTAPI_User	REST API による製品の管理に使用する Windows ドメインアカウントのユーザー名。REST API による製品の管理はこのユーザーのみ実行できます。ユーザー名は、<DOMAIN>\<UserName> の形式で入力します（例：RESTAPI_User=COMPANY\Administrator）。REST API を利用するユーザーは 1 人しか選択できません。 REST API を使用して製品を管理するには、ユーザー名の追加は必須です。
RESTAPI_Port	REST API による製品の管理に使用するポート。既定ではポート 6782 が使用されます。ポートが使用されていないことを確認してください。
RESTAPI_Certificate	リクエストを識別するための証明書（例：RESTAPI_Certificate=C:\cert.pem）。REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。
ADMINKITCONNECTOR	管理システムを使用した製品管理。管理システムには、Kaspersky Security Center などが含まれます。カスペルスキーの管理システムに加えて、サードパーティ製ソリューションを使用することもできます。Kaspersky Endpoint Security はそのための API を提供します。 次の値を設定できます： • 1 – 管理システムを利用した製品管理を許可する（既定値） • 0 – ローカルインターフェイスを利用した製品管理のみを許可する

`EnableUniqueSensorID`	本製品のインストール中またはアップデート中に、一意のコンピューター識別子（Sensor ID）を作成します。Sensor ID は、サーバーにテレメトリを送信するコンピューターを識別するために、Kaspersky Anti Targeted Attack Platform ソリューションで使用されます。本製品は、Sensor ID の作成時に、マザーボードのシリアル番号などのコンピューターの設定を考慮するアルゴリズムを使用します。本製品を仮想環境で使用する場合など、いくつかのケースでは、Sensor ID が重複する場合があります。その結果、Kaspersky Anti Targeted Attack Platform がテレメトリの送信元コンピューターを識別できなくなります。一意の Sensor ID を作成するには、パラメータ `EnableUniqueSensorID=1` を設定する必要があります。これにより、本製品が、コンピューターに関する他のデータを考慮する別のアルゴリズムを使用して Sensor ID を作成するようになります。これにより、一意の Sensor ID が確保されます。 既定では、パラメータは設定されていません。本製品は次の場合に Sensor ID を継承します： • 製品バージョンのアップデート • ［KES + KEA］設定からの［KES + 組み込みエージェント］設定への移行 インストーラーは、アプリケーション修復の一環として、Sensor ID を継承しようとします。Sensor ID を復元できない場合は、新しい Sensor ID が作成されます。
`SKIPKB5007186CHECK=1`	オペレーティングシステムの更新 KB5007186 がインストールされているかどうかのチェックを無効にします。 本製品をインストールする前に、インストーラーによって、インストールされているオペレーティングシステムの更新がチェックされます。更新 KB5007186 は、本製品で問題を引き起こす可能性があるオペレーティングシステムの更新のリストに含まれています。詳細な情報については、テクニカルサポートのナレッジベースを参照してください。したがって、この更新が検出されると、インストーラーはインストールを中止します。インストールを続行するには、`SKIPKB5007186CHECK=1` を設定します。

例：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

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

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

setup.ini ファイルでアクティベーションコードを指定していない限り、Kaspersky Endpoint Security のインストール後、試用版ライセンスでアクティベーションが行われます。通常、試用版ライセンスには短い有効期間が設定されています。試用版ライセンスの有効期間が終了すると、すべての Kaspersky Endpoint Security 機能が無効になります。製品を引き続き使用するには、アクティベーションウィザードまたは専用のコマンドを使用して、製品版ライセンスで本製品をアクティベートする必要があります。

サイレントモードで製品をインストールまたはアップグレードする場合、以下のファイルの使用がサポートされています：

- setup.ini：製品のインストールの全般設定。

  setup.ini ファイルの設定を適用するには、これらのファイルを Kaspersky Endpoint Security の配布パッケージを同じフォルダーに配置します。

- install.cfg：Kaspersky Endpoint Security の動作に関する設定

  install.cfg ファイルの設定を適用するには、アプリケーションのインストールコマンドで次のようにパスを指定する必要があります：`CONFIGPATH=<path to the configuration file>`

- setup.reg：レジストリキー

  setup.ini ファイルで `SetupReg` パラメータの値として `setup.reg` が設定されている場合にのみ、setup.reg ファイルに含まれるレジストリキーがレジストリに書き込まれます。setup.reg ファイルはカスペルスキーのエキスパートが生成しています。このファイルの内容は変更しないでください。setup.reg ファイルの設定を適用するには、これらのファイルを Kaspersky Endpoint Security の配布パッケージを同じフォルダーに配置します。setup.reg ファイルを別のフォルダーに配置することもできます。この場合、アプリケーションのインストールコマンドで次のようにパスを指定する必要があります：`SETUPREG=<path to the setup.reg file>`

Setup /x：本製品の削除

Kaspersky Endpoint Security は次のいずれかのモードでコマンドラインを使用してアンインストールできます。

- インストールウィザードを使用したインタラクティブモード。
- サイレントモード：サイレントモードでのアンインストールの開始後は、アンインストールプロセスでユーザーが操作を行う必要はありません（サイレントアンインストール）。サイレントモードで本製品をアンインストールするには、「`/s`」と「`/qn`」パラメータを使用します。

サイレントモードで製品をアンインストールするには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：

   - アンインストール操作がパスワードによって保護されていない場合：

     ```
     setup_kes.exe /s /x
     ```

     または

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` は、アプリケーションの固有の識別子です。テクニカルサポートのナレッジベースで、または次のコマンドを使用して、アプリケーションの GUID を確認できます：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
     IdentifyingNumber
     ```

   - アンインストール操作がパスワードによって保護されている場合：

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     または

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

   `SAVEQB` パラメータを使用して、スキャンしたファイルを保存して、バックアップに配置することもできます。ファイルのバックアップコピーは、フォルダー `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` に保存されます。既定では、バックアップへのファイルの保存は無効になっています（`SAVEQB=0`）。

例：

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i：本製品の復元

復元を実行すると、本製品のインストールのプロセスの一環として作成された、すべての破損した製品機能とシステムレジストリキーの整合性がチェックされて、復元されます。

Kaspersky Endpoint Security は次のいずれかのモードでコマンドラインを使用して復元できます。

- インストールウィザードを使用したインタラクティブモード。
- サイレントモード：サイレントモードでの復元の開始後は、復元プロセスでユーザーが操作を行う必要はありません。

Kaspersky Endpoint Security のインストーラーが復元モードで実行されており、本製品の復元が不要な場合、インストーラーは変更を行いません。

Kaspersky Endpoint Security のインストーラーが復元モードで実行されており、本製品がインストールされていない場合、インストーラーはインストールプロセスを開始します。

サイレントモードで製品を復元するには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の配布パッケージがあるフォルダーに移動します。
3. 次のコマンドを実行します：
   - 復元操作がパスワードによって保護されていない場合：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     <GUID> は、アプリケーションの固有の識別子です。テクニカルサポートのナレッジベースで、または次のコマンドを使用して、アプリケーションの GUID を確認できます：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
     IdentifyingNumber
     ```

   - 復元操作がパスワードによって保護されている場合：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

```
例：
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin
KLPASSWD=samplePassword /qn
```

AVP コマンド

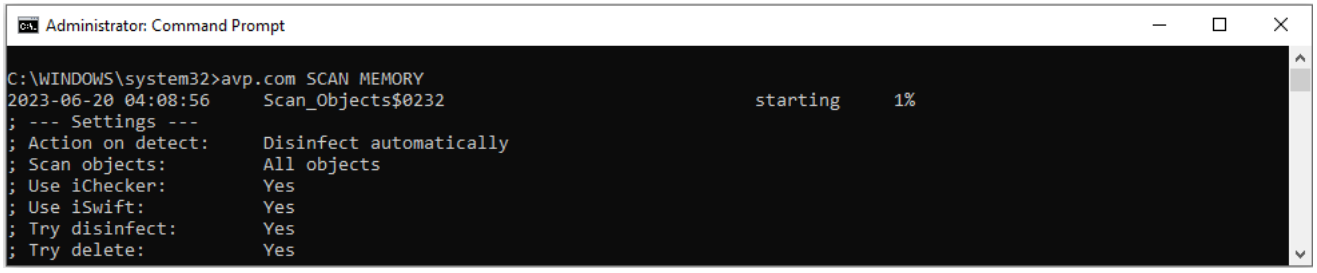
コマンドラインを使用して Kaspersky Endpoint Security を管理するには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
   製品のインストール中に、システム変数 %PATH% を使用して実行ファイルへのパスを追加することができます。

3. コマンドを実行するには、次のテンプレートを使用します：

```
avp.com <コマンド> [オプション]
```

Kaspersky Endpoint Security で、次の図のようにコマンドが実行されます。



コマンドラインを使用しての製品の管理

SCAN：マルウェアのスキャン

マルウェアのスキャンタスクを実行します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

スキャン範囲	
`<files to scan>`	スペース区切りのファイルとフォルダーのリスト。指定するパスが長くスペースを含むときは引用符（"）で囲む必要があります。スペースを含まない短いパス（MS-DOS 短縮形式）は引用符で囲む必要はありません。例： • `"C:\Program Files (x86)\Example Folder"` – 長いパス • `C:\PROGRA~2\EXAMPL~1` – スペースを含まない短いパス
`/ALL`	マルウェアのスキャンタスクを実行します。Kaspersky Endpoint Security が、次のオブジェクトをスキャンします： • カーネルメモリ • オペレーティングシステムの起動時に読み込まれるオブジェクト • ディスクブートセクター • システムバックアップ • すべてのハードディスクドライブとリムーバブルドライブ Kaspersky Endpoint Security for Windows 12.12 では、メールは本製品のスキャン範囲から除外されます。送受信メールのスキャンはメール脅威対策機能によって実行されます。以前のバージョンの管理プラグインを使用している場合、ポリシーにメールが含まれていても、スキャン範囲からメールが除外されます。
`/MEMORY`	カーネルメモリをスキャンします
`/STARTUP`	オペレーティングシステムの起動時に読み込まれるオブジェクトをスキャンします
`/REMDRIVES`	リムーバブルドライブをスキャンします。

/FIXDRIVES	ハードディスクをスキャンします。
/NETDRIVES	ネットワークドライブをスキャンします。
/QUARANTINE	Kaspersky Endpoint Security のバックアップ保管領域のファイルをスキャンします。
/@:<file list.lst>	リストに含まれるファイルとフォルダーをスキャンします。リストに複数のファイルを含める場合は、1行に1つずつ入力して指定するようにします。指定するパスが長くスペースを含むときは引用符（"）で囲む必要があります。スペースを含まない短いパス（MS-DOS 短縮形式）は引用符で囲む必要はありません。例： • "C:\Program Files (x86)\Example Folder" – 長いパス • C:\PROGRA~2\EXAMPL~1 – スペースを含まない短いパス

脅威の検知時の処理	
/i0	**通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
/i1	**駆除する。駆除できない場合は通知する**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
/i2	**駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 既定では、この処理が選択されています。
/i3	**駆除できない場合は削除**：また、複合ファイル（アーカイブなど）の一部に感染したファイルが含まれ、感染したファイルの駆除や削除を実行できない場合、複合ファイル自体を削除します。
/i4	**削除**：また、複合ファイル（アーカイブなど）の一部に感染したファイルが含まれ、感染したファイルを削除できない場合、複合ファイル自体を削除します。

ファイル種別	
/fe	**拡張子でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイル形式はファイルの拡張子に基づいて識別されます。
/fi	**ファイル形式でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。
/fa	**すべてのファイル**：この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。 これは既定の設定です。

信頼するオブジェクト	
-e:a	RAR、ARJ、ZIP、CAB、LHA、JAR、ICE アーカイブはスキャンの対象から除外します。
-e:<file mask>	ファイルマスクと一致するファイルがスキャンの対象から除外されます。例： • 「*.exe」というマスクには、拡張子が「exe」のファイルへのすべてのパスが含まれます。 • 「example*」というマスクには、名前が「EXAMPLE」のファイルへのすべてのパスが含まれます。
-e:<seconds>	指定した上限時間（秒単位）よりもスキャンに時間がかかるファイルは、スキャンの対象から除外されます。
-es:<megabytes>	指定したファイルサイズの上限（MB 単位）よりサイズが大きいファイルは、スキャンの対象から除外されます。

イベントのレポートファイルへの保存モード（スキャン、アップデーターおよびロールバックプロファイルのみ）	
/R:<report file>	緊急イベントのみをレポートファイルに保存します。
/RA:<report file>	すべてのイベントをレポートファイルに保存します。

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

詳細設定	
`/C:<file with scan settings>`	マルウェアのスキャンタスクの設定を指定したファイル。ファイルは手動で作成して TXT 形式で保存する必要があります。ファイルでは次の内容を指定できます：`[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`

```
例：
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE：定義データベースとソフトウェアモジュールのアップデート

定義データベースと製品機能のアップデートタスクを実行します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<アップデートタスクの設定ファイル>]
```

アップデートタスクの設定	
`local`	アプリケーションがインストールされた後に自動で作成された*定義データベースと製品機能のアップデートタスク*の開始です。Kaspersky Security Center のコンソール内またはローカルの製品インターフェイス内で*定義データベースと製品機能のアップデートタスク*の設定を変更することができます。設定されない場合、Kaspersky Endpoint Security は*定義データベースと製品機能のアップデートタスク*を既定の設定またはコマンド内で指定された設定で開始します。*定義データベースと製品機能のアップデートタスク*の設定は次のように指定できます： • `UPDATE`：既定の設定で*定義データベースと製品機能のアップデートタスク*を開始します：アップデート元はカスペルスキーのアップデートサーバーで、アカウントは「System」、その他既定の設定。 • `UPDATE local`：インストール後に自動で作成された*定義データベースと製品機能のアップデートタスク*を開始します（事前定義されたタスク）。 • `UPDATE <update settings>`：手動で定義された設定で*定義データベースと製品機能のアップデートタスク*を開始します（以下を参照）。

アップデート元	
`"<update source>"`	HTTP サーバーまたは FTP サーバーのアドレス、あるいはアップデートパッケージの保存された共有フォルダーのアドレス。アップデート元は1つだけ指定できます。アップデート元が指定されていない場合は、Kaspersky Endpoint Security は既定のアップデート元であるカスペルスキーのアップデートサーバーを使用します。

イベントのレポートファイルへの保存モード（スキャン、アップデーターおよびロールバックプロファイルのみ）	
/R:<report file>	緊急イベントのみをレポートファイルに保存します。
/RA:<report file>	すべてのイベントをレポートファイルに保存します。

詳細設定	
/C:<file with update settings>	*定義データベースと製品機能のアップデートタスクの設定を指定したファイル。ファイルは手動で作成して TXT 形式で保存する必要があります。ファイルでは次の内容を指定できます：*["<update source>"] [/R[A]:<report file>]

例：
avp.com UPDATE local
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt

ROLLBACK：前回のアップデートのロールバック

定義データベースを前のバージョンにロールバックします。これにより、必要に応じて、定義データベースと製品機能を前のバージョンにロールバックすることができます。この機能は、たとえば新しい定義データベースバージョンに無効なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックするような場合に役立ちます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

avp.com ROLLBACK [/R[A]:<report file>]

イベントのレポートファイルへの保存モード（スキャン、アップデーターおよびロールバックプロファイルのみ）	
/R:<report file>	緊急イベントのみをレポートファイルに保存します。
/RA:<report file>	すべてのイベントをレポートファイルに保存します。

例：
avp.com ROLLBACK /RA:rollback.txt

TRACES：トレース

トレースファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。認証エージェントのトレースファイルを除いて、トレースファイルはフォルダー「%ProgramData%\Kaspersky Lab\KES.12.12\Traces」に保存されます。既定では、トレースは無効です。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

トレースレベル	
<tracing level>	トレース記録の詳細度。次の値を設定できます： • 100（緊急）：深刻なエラーに関するメッセージのみ。 • 200（高）：深刻なエラーを含めたすべてのエラーに関するメッセージ。 • 300（診断）：すべてのエラーに関するメッセージと、一部の警告を含むメッセージ。 • 400（重要）：すべてのエラーに関するメッセージとすべての警告および詳細情報。 • 500（通常）：すべてのエラーに関するメッセージとすべての警告、および正常な動作に関する詳細情報を含むメッセージ（既定値）。 • 600（低）：すべてのメッセージ。

詳細設定	
all	以下の「file」と「mem」パラメータを使用するように指定してコマンドを実行します。
file	トレースファイルを1つ保存します（容量の上限なし）。
rot	ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。
mem	トレースの記録をダンプファイルに保存します。

```
例：
avp.com TRACES on 500
avp.com TRACES off
avp.com TRACES on 500 mem
avp.com TRACES off file
```

START：プロファイルの起動

プロファイルを起動します（例：定義データベースのアップデートの開始、保護機能の有効化）。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com START <profile> [/R[A]:<report file>]
```

プロファイル	
<profile>	プロファイル名。*プロファイル*で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能なプロファイルのリストは、「HELP START」コマンドを実行して確認できます。

イベントのレポートファイルへの保存モード（スキャン、アップデーターおよびロールバックプロファイルのみ）	
`/R:<report file>`	緊急イベントのみをレポートファイルに保存します。
`/RA:<report file>`	すべてのイベントをレポートファイルに保存します。

例：
`avp.com START Scan_Objects`

STOP：プロファイルの停止

プロファイルの実行を停止します（例：リムーバブルドライブスキャンの停止、保護機能の無効化）。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーは［**保護機能の停止**］および［**管理コンポーネントの停止**］権限が必要です。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

プロファイル	
`<profile>`	プロファイル名。*プロファイル*で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能なプロファイルのリストは、「`HELP STOP`」コマンドを実行して確認できます。

認証	
`/login=<user name> /password=<password>`	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

STATUS：プロファイルのステータス

プロファイルのステータス情報を表示します（例：`running`、`completed`）。利用可能なプロファイルのリストは、「`HELP STATUS`」コマンドを実行して確認できます。

Kaspersky Endpoint Security は、指定したサービスのステータスも表示できます。カスペルスキーのテクニカルサポートに問い合わせを行って調査が必要になったときに、サービスのプロファイルのステータスに関する情報を取得する場合があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com STATUS [<profile>]
```

プロファイルを指定せずにコマンドを入力した場合、Kaspersky Endpoint Security は本製品のすべてのプロファイルのステータスを表示します。

STATISTICS：プロファイルの動作の統計情報

プロファイルの統計情報を表示します（例：スキャンの所要時間や検知した脅威の数）。利用可能なプロファイルのリストは、「`HELP STATISTICS`」コマンドを実行して確認できます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com STATISTICS <profile>
```

RESTORE：バックアップからのファイルの復元

バックアップ保管領域から元のフォルダーにファイルを復元できます。復元先のフォルダーに同じ名前のファイルが既に存在する場合は、ファイルを置き換えることを確認するよう求められます。バックアップ保管領域から復元されるファイルの名前は元のまま変更されません。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**バックアップから復元**」操作を実行する権限が付与されている必要があります。

*バックアップ保管領域*には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。*バックアップコピー*は、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルのバックアップコピーは、フォルダー `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

詳細設定	
/REPLACE	復元先に同じファイル名のファイルがある場合に、これを上書きします。
<file name>	復元するファイルの名前。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword

EXPORT：本製品の設定のエクスポート

Kaspersky Endpoint Security の設定をファイルにエクスポートします。コマンドに、設定のエクスポート先のファイル名のみが含まれている場合、ファイルは次のように配置されます：

- avp.com へのパスがシステム変数　%PATH%　に追加されている場合、ファイルは「C:\Windows\SysWOW64」フォルダーに配置されます。
- 本製品のインストールフォルダーからコマンドを実行すると、本製品の自己保護機能によってアプリケーションフォルダー内の新規ファイルの作成がブロックされるため、エクスポートは失敗します。アプリケーション設定をファイルにエクスポートするには、ファイルパスを入力します。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**設定のエクスポート**」操作を実行する権限が付与されている必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

プロファイル	
<profile>	プロファイル名。*プロファイル*で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。利用可能なプロファイルのリストは、「HELP EXPORT」コマンドを実行して確認できます。

エクスポートするファイル	
<file name>	本製品の設定をエクスポートするファイルの名前。ファイルパスを入力することもできます。Kaspersky Endpoint Security の設定を DAT または CFG 設定ファイル、TXT テキストファイル、または XML ドキュメントにエクスポートできます。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
avp.com EXPORT fm fm_config.txt

IMPORT：本製品の設定のインポート

EXPORT コマンドで作成したファイルから Kaspersky Endpoint Security の設定をインポートします。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**本製品の設定**」操作を実行する権限が付与されている必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

インポートするファイル	
<file name>	本製品の設定をインポートするファイルの名前。Kaspersky Endpoint Security の設定を DAT または CFG 設定ファイル、TXT テキストファイル、または XML ドキュメントからインポートできます。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword

ADDKEY：ライセンス情報ファイルの適用

アクティベーションコードを使用して Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

```
avp.com ADDKEY <ファイル名> [/login=<ユーザー名> /password=<パスワード>]
```

ライセンス情報ファイル	
<file name>	ライセンス情報ファイルの名前。

認証	
/login=<user name> /password=<password>	ユーザーアカウントの認証情報。これらの認証情報は、パスワードによる保護が有効になっている場合にのみ入力する必要があります。

例：
```
avp.com ADDKEY file.key
```

LICENSE：ライセンス管理

Kaspersky Endpoint Security、EDR Optimum、または EDR Expert（Kaspersky Endpoint Detection and Response アドオン）のライセンスを管理します。

このコマンドを実行してライセンスを削除するには、パスワードによる保護を有効にする必要があります。ユーザーには「**ライセンスの削除**」操作を実行する権限が付与されている必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

実行する操作	
/ADD <file name>	アクティベーションコードを使用して Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。
/ADD <activation code>	アクティベーションコードを使用して Kaspersky Endpoint Security をアクティベートします。製品がすでにアクティベートされている場合、ライセンスは予備のライセンスとして追加されます。
/REFRESH	Kaspersky Endpoint Security のライセンスのステータスを更新します。本製品は最新のライセンスのステータス情報をカスペルスキーのアクティベーションサーバーから受け取ります。

/REFRESH <license ID>	ライセンス ID を使用してライセンスの状態を更新します。このコマンドを使用すると、EDR アドオン、MDR アドオン、KUMA アドオン、またはその他のライセンスの状態を更新できます。ライセンス ID はライセンス証明書から取得できます。本製品は最新のライセンスのステータス情報をカスペルスキーのアクティベーションサーバーから受け取ります。
/CHECK	ライセンス情報を取得します。Kaspersky Endpoint Security で、予備のライセンスや、EDR アドオン、MDR アドオン、KUMA アドオンなどのライセンスを含む、追加されたすべてのライセンスに関する情報が表示されます。 Kaspersky Endpoint Security に次のライセンス情報が表示されます： • ライセンス名 • ライセンスの識別子 • 本製品が Light Agent モードでインストールされている仮想マシンの接続先 Protection Server（SVM）のアドレス • ライセンス種別：試用版、製品版、ベータ版、定額制サービス • 製品のアクティベーション日時 • ライセンスの有効期限の日時 • ライセンスの有効期限までの日数
/CHECK <license ID>	ID でライセンス情報を取得します。このコマンドを使用してライセンス情報を取得できます。ライセンス ID はライセンス証明書から取得できます。
/DEL /login=<user name> /password=<password>	本製品のライセンスを削除します。予備のライセンスも削除されます。
/DEL <license ID> /login=<user name> /password=<password>	ライセンス ID を使用してライセンス情報を削除します。このコマンドを使用すると、EDR アドオン、MDR アドオン、KUMA アドオン、またはその他のライセンスからライセンス情報を削除できます。ライセンス ID はライセンス証明書から取得できます。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

```
例：
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW：ライセンスの更新または購入

カスペルスキーの製品ページが開きます（日本語版ライセンスを更新または購入するときは、販売代理店に直接ご連絡ください）。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

PBATESTRESET：暗号化前のディスクチェックの結果のリセット

ディスク全体の暗号化（FDE）の互換性チェックの結果をリセットします。リセットの対象には、Kaspersky Disk Encryption と BitLocker ドライブ暗号化技術の両方が含まれます。

ディスク全体の暗号化を実行する前に、コンピューターを暗号化できるかどうかのチェックが実行されます。コンピューターが暗号化をサポートしていない場合は、互換性がないという情報が、Kaspersky Endpoint Security により記録されます。その後、暗号化を再び試行した場合は、互換性に関するチェックは実行されず、暗号化を実行できないという警告が表示されます。前回の互換性チェック後に、コンピューターのハードウェア構成が変更された場合、記録されている前回の互換性チェックの結果をリセットし、システムハードディスクと Kaspersky Disk Encryption または BitLocker 暗号化技術との互換性を再チェックする必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

EXIT：本製品の終了

Kaspersky Endpoint Security を終了します。本製品の動作が終了し、コンピューターのメモリ領域が解放されます。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**本製品の終了**」操作を実行する権限が付与されている必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY：ポリシーの無効化

Kaspersky Security Center で設定したポリシーをコンピューター上で無効にします。ポリシーでロックされている設定（状態）も含めて、Kaspersky Endpoint Security のすべての設定を編集できるようになります。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**Kaspersky Security Center ポリシーを無効にする**」操作を実行する権限が付与されている必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY：ポリシーの有効化

Kaspersky Security Center で設定したポリシーをコンピューター上で有効にします。ポリシーで指定した設定が本製品に適用されます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

DISABLE：保護の無効化

Kaspersky Endpoint Security のライセンスの有効期限が切れている場合に、ファイル脅威対策を無効化します。本製品がアクティベーションされていない場合、あるいは有効なライセンスが適用されている場合には、このコマンドは実行できません。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

SPYWARE：スパイウェアの検知の切り替え

スパイウェア検知の管理。既定では、スパイウェアの検知は有効になっています。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com SPYWARE on|off
```

KSN：KSN / KPSN の切り替え

ファイルまたは Web サイトの評価の決定に使用するカスペルスキーのソリューションを選択します。Kaspersky Endpoint Security は、カスペルスキーの評価データベースと連携する、次のインフラストラクチャソリューションをサポートします：

- ほとんどのカスペルスキー製品で使用されるのが *Kaspersky Security Network (KSN)* です。KSN の参加者は、カスペルスキーから情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、評価データベースと統計情報のデータベースに追加されます。

- *Kaspersky Private Security Network (KPSN)* は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。KPSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：

  - コンピューターがインターネットに接続されていない。

  - 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

```
avp.com KSN /global | /private <ファイル名>
```

Kaspersky Security Network 設定ファイル	
`<file name>`	Kaspersky Private Security Network の設定を含む設定ファイルの名前このファイルの拡張子は PKCS7 または PEM です。

例：

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE：サーバー接続の保護の無効化

*管理サーバーの接続の保護*タスクを実行し、管理サーバーへのコンピューターの接続用パスワードを削除します。これにより、管理サーバーの接続の保護が無効になります。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

パスワード	
/password=<password>	KLAdmin ユーザーアカウントのパスワードまたは*管理サーバーの接続の保護*タスクからのパスワード。 パラメータが指定されていない場合、次の行でパスワードを入力するよう求められます。

KESCLI コマンド

KESCLI コマンドを使用すると、OPSWAT コンポーネントを使用してコンピューターの保護の状態に関する情報を受け取ったり、*マルウェアのスキャン*や*定義データベースと製品機能のアップデート*のような標準的なタスクを実行することができます。

`kescli --help` コマンドまたは省略された `kescli -h` コマンドを使用して KSECLI コマンドのリストを表示できます。

コマンドラインを使用して Kaspersky Endpoint Security を管理するには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
   製品のインストール中に、システム変数 %PATH% を使用して実行ファイルへのパスを追加することができます。
3. コマンドを実行するには、次のテンプレートを使用します：

   ```
   kescli <コマンド> [オプション]
   ```

   Kaspersky Endpoint Security で、次の図のようにコマンドが実行されます。



コマンドラインを使用しての製品の管理

Scan：マルウェアのスキャン

マルウェアのスキャン（完全スキャン）タスクを実行します。

タスクを実行するには、管理者はポリシーでローカルタスクの使用を許可する必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

マルウェアのスキャンタスクの完了状況については、`GetScanState` コマンドを使用して確認できます。また、前回のスキャン完了日時については、`GetLastScanTime` コマンドを使用して表示できます。

スキャン範囲	
<scan scope>	「;」で区切られたファイルとフォルダーのリスト。例：「"C:\Program Files (x86)\Example Folder"」。

脅威の検知時の処理	
0	**通知**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルに関する情報をアクティブな脅威のリストに追加します。
1	**駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 既定では、この処理が選択されています。

例：

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState：スキャン完了のステータス

マルウェアのスキャン（完全スキャン）タスクの完了状態についての情報を表示します。

- `1` – スキャンが実行中です。
- `0` – スキャンは実行されていません。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetScanState
```

GetLastScanTime：スキャン完了時刻の判断

前回の *マルウェアのスキャン*（完全スキャン）タスクの完了日時に関する情報を表示します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetLastScanTime
```

GetThreats：検知した脅威に関するデータの取得

検知された脅威のリストを表示します（*脅威レポート*）。このレポートには、レポート作成時より前の 30 日間で検知された脅威およびウイルスに関する情報が含まれます。

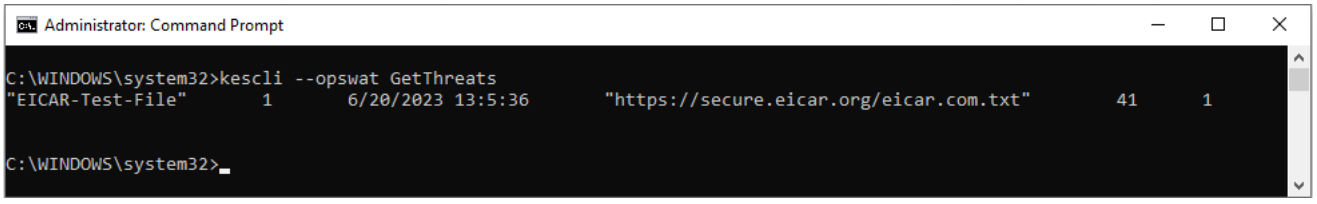
コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetThreats
```

コマンドを実行すると、Kaspersky Endpoint Security は次の形式で応答を送信します：

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



コマンドラインを使用しての製品の管理

オブジェクト種別	
0	不明（Unknown）。
1	ウイルス（Virware）。
2	トロイの木馬（Trojware）。
3	悪意のあるプログラム（Malware）。
4	広告プログラム（Adware）。
5	オートダイヤラープログラム（Pornware）。
6	ユーザーのコンピューターまたはデータに損害を与える目的で犯罪者に悪用される可能性のあるアプリケーション（Riskware）。
7	悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト（Packed）。
20	不明なオブジェクト（Xfiles）。
21	既知のアプリケーション（Software）。

22	隠蔽されたファイル（Hidden）。
23	注意の必要なアプリケーション（Pupware）。
24	異常なふるまい（Anomaly）。
30	決定されていない（Undetect）。
40	広告バナー（Banner）。
50	ネットワーク攻撃（Attack）。
51	レジストリへのアクセス（Registry）。
52	疑わしい動作（Suspicion）。
60	脆弱性（Vulnerability）。
70	フィッシング（Phishing）。
80	望ましくないメール添付（Attachment）。
90	Kaspersky Security Network により検知されたマルウェア（Urgent）。
100	不明なリンク（Suspic URL）。
110	その他のマルウェア（Behavioral）。

脅威の検知時の処理	
0	不明（unknown）。
1	脅威が修復されました（ok）。
2	オブジェクトは感染しており、駆除されていません（infected）。
5	オブジェクトはアーカイブ内にあり、駆除されていません（archive）。
9	オブジェクトは駆除されました（disinfected）。
10	オブジェクトは駆除されていません（not disinfected）。
11	オブジェクトは削除されました（deleted）。
13	オブジェクトのバックアップコピーが作成されました（backupped）。
15	オブジェクトはバックアップに移動されました（quarantined）。
23	オブジェクトはコンピューターの再起動時に削除されました（delete on reboot）。
25	オブジェクトはコンピューターの再起動時に駆除されました（disinfect on reboot）。
29	オブジェクトはユーザーによりバックアップに移動されました（added by user）。
30	オブジェクトは除外リストに追加されました（added to exclude）。
31	オブジェクトはコンピューターの再起動時にバックアップに移動されました（quarantine on reboot）。
36	誤検知（false alarm）。
38	プロセスが中断されました（terminated）。
40	オブジェクトは検出されませんでした（not found）。
41	脅威を解決できませんでした（untreatable）。
42	オブジェクトは復元されました（rolled back）。
43	オブジェクトは脅威の活動の結果作成されました（produced by threat）。
44	オブジェクトはコンピューターの再起動時に復元されました（roll back on reboot）。
0xffffffff	オブジェクトは処理されませんでした（discarded）。

脅威の危険度	
0	不明

1	高
2	スキャン(レベル中)
4	低
8	情報（「*低*」以下）

UpdateDefinitions：定義データベースとソフトウェアモジュールのアップデート

*定義データベースと製品機能のアップデート*タスクを実行します。Kaspersky Endpoint Security は既定のアップデート元であるカスペルスキーのアップデートサーバーを使用します。

タスクを実行するには、管理者はポリシーでローカルタスクの使用を許可する必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

このコマンドは、本製品が Light Agent モードでインストールされている場合は実行できません。

コマンド構文

```
kescli --opswat UpdateDefinitions
```

現在の定義データベースの公開日時については、`GetDefinitionsetState` コマンドを使用して表示できます。

GetDefinitionState：データベースの前回のアップデート日時の決定

使用中の定義データベースの前回のアップデート日時に関する情報を表示します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetDefinitionState
```

EnableRTP：保護の有効化

次の Kaspersky Endpoint Security の保護機能を有効にします：ファイル脅威対策、ウェブ脅威対策、メール脅威対策、ネットワーク脅威対策、ホスト侵入防止。

保護機能を有効にするには、管理者は関連するポリシー設定を編集できる（アイコンが開いている）かどうか確認する必要があります。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat EnableRTP
```

この結果、パスワードによる保護で製品設定の編集が禁止されていても保護機能が有効になります。

ファイル脅威対策の動作状態については、`GetRealTimeProtectionState` コマンドを使用して確認できます。

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

ファイル脅威対策の動作状態に関する情報を受け取ります。

- `1` – 機能が有効です。
- `0` – 機能が無効です。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState：ディスク暗号化のステータス

ディスクの暗号化のステータスに関する情報を表示します：

- `1` は、ディスクがカスペルスキーまたは BitLocker のディスク暗号化技術で保護されていることを意味します。
- `0` は、ディスクが暗号化されていないことを意味します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --opswat GetEncryptionState
```

Version：本製品のバージョンの識別

Kaspersky Endpoint Security for Windows のバージョンを表示します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。

コマンド構文

```
kescli --Version
```

省略したコマンド「`-v`」を使用することもできます。

Detection and Response 管理コマンド

コマンドラインを使用して、Detection and Response ソリューション（Kaspersky Sandbox または Kaspersky Endpoint Detection and Response Optimum など）の組み込み機能を管理することができます。Kaspersky Security Center を使用した管理ができない場合は、Detection and Response ソリューションを管理できます。本製品の管理に利用できるコマンドのリストは、「`HELP`」コマンドを実行して確認できます。特定のコマンドの構文を確認するには、「`HELP <command>`」コマンドを実行します。

コマンドラインを使用して Detection and Response ソリューションの組み込み機能を管理するには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. コマンドを実行するには、次のテンプレートを使用します：

   ```
   avp.com <command> [options]
   ```

   Kaspersky Endpoint Security でコマンドが実行されます。

SANDBOX：Sandbox の管理

Sandbox コンポーネントを管理するコマンド：

- Sandbox コンポーネントを有効または無効にする

  Sandbox コンポーネントは、Kaspersky Sandbox ソリューションおよび KATA Sandbox コンポーネント（Kaspersky Anti Targeted Attack Platform の一部）との連携を提供します。

- Kaspersky Sandbox コンポーネントの設定：
  - Sandbox サーバーにコンピューターを接続する

    サーバーは配備された Microsoft Windows オペレーティングシステムの仮想イメージを使用してスキャンする必要のあるオブジェクトを実行します。IP アドレス（IPv4 または IPv6）、または完全修飾ドメイン名を入力できます。仮想イメージの配備と Sandbox サーバーの設定について詳しくは、Kaspersky Sandbox のヘルプ および Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください。

  - サーバーの接続タイムアウトを設定する

    Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）の接続タイムアウト。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、サーバーの接続タイムアウトの時間を長くすることができます。要求のタイムアウトは 0.5 秒以下を推奨します。

  - コンピューターとサーバーとの間に信頼済み接続を設定する

    Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）との信頼済みの接続を設定するには、TLS 証明書を準備する必要があります。次に、ポリシーを使用してこの証明書をコンピューターに追加する必要があります。また、証明書を Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）に追加する必要があります。

- コンポーネントの現在の設定の表示。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com stop sandbox [/login=<user name> /password=<password>]
avp.com start sandbox
avp.com sandbox /set [--tls=yes|no] [--servers=<server address>:<port>] [--timeout=<Sandbox server connection
timeout (ms)>] [--pinned-certificate=<path to the TLS certificate>][/login=<user name> /password=<password>][--
client-certificate=<path to the PFX archive>]
avp.com sandbox /show
```

実行する操作	
stop	Sandbox コンポーネントを有効にします。
start	Sandbox コンポーネントを無効にします。
set	Sandbox コンポーネントを設定します。次の設定を構成できます： • 信頼済み接続を使用する（--tls） • TLS 証明書を追加する（--pinned-certificate） • サーバーの接続タイムアウトを設定する（--timeout） • Sandbox サーバーを追加する（--servers） • 暗号化コンテナーを追加する（--client-certificate）
show	コンポーネントの現在の設定を表示します。次の応答が表示されます： sandbox.timeout=<Sandbox server connection timeout (ms)> sandbox.tls=<trusted connection status> sandbox.servers=<list of Sandbox servers>

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

PREVENTION：実行防止の管理

実行防止コンポーネントを無効にするか、実行防止ルールのリストを含め、コンポーネントの現在の設定を表示します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com prevention disable
avp.com prevention /show
```

コマンド「`prevention /show`」を実行する値、次の応答が表示されます：

`prevention.enable=true|false`

`prevention.mode=audit|prevent`

`prevention.rules`

`id: <rule ID>`

`target: script|process|document`

`md5: <MD5 hash of the file>`

`sha256: <SHA256 hash of the file>`

`pattern: <path to the object>`

`case-sensitive: true|false`

コマンド戻り値：

- `-1`：コンピューターにインストールされているバージョンの製品ではコマンドがサポートされていません。
- `0`：コマンドが正常に実行されました。
- `1`：必要な引数がコマンドに渡されていません。
- `2`：一般的なエラーが発生しました。
- `4`：構文エラーがあります。
- `9`：操作に誤りがあります（すでに機能が無効にされている状態でその機能を無効にしようとするなど）。

ISOLATION：ネットワーク分離の管理

コンピューターのネットワーク分離を無効にするか、コンポーネントの現在の設定を表示します。コンポーネントの設定には除外リストに追加されたネットワーク接続のリストも含まれます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文：

```
avp.com isolation /OFF /login=<user name> /password=<password>
avp.com isolation /STAT
```

`stat` コマンドを実行すると、次の応答を受け取ります：`Network isolation on|off`。

RESTORE：隔離からのファイルの復元

隔離から元のフォルダーにファイルを復元します。*隔離*はコンピューター上にある特別なローカル保管領域です。ユーザーがコンピューターに対して危険だと判断したファイルを隔離することができます。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は、Detection and Response ソリューション (EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox) と連携する際にのみ隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、Kaspersky Sandbox のヘルプ、Kaspersky Endpoint Detection and Response Optimum のヘルプ、および Kaspersky Endpoint Detection and Response Expert のヘルプ、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

このコマンドを実行するには、パスワードによる保護を有効にする必要があります。ユーザーには「**バックアップから復元**」操作を実行する権限が付与されている必要があります。

オブジェクトはシステムアカウント（SYSTEM）で隔離されます。

隔離からのファイルの復元には次の注意事項があります：

- 復元先のフォルダーが削除されていたり、ユーザーにそのフォルダーへのアクセス権がない場合、ファイルはフォルダー「`%DataRoot%\QB\Restored`」に保存されます。その後、ファイルを手動で移動先のフォルダーに移動する必要があります。
- 本製品は復元されるファイルの名前の大文字小文字を区別します。ファイル名を入力する際に条件を満たしていない場合、ファイルは復元されません。
- 復元先のフォルダーに同じ名前のファイルがある場合は、ファイルの復元がキャンセルされます。
- KATA (EDR) ソリューションを使用している場合は、ファイルの復元後にファイルのコピーが保存されます。隔離の中身は手動で空にすることができます。EDR Optimum と EDR Expert ソリューションでは、復元後にファイルは削除されます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

詳細設定	
/REPLACE	復元先に同じファイル名のファイルがある場合に、これを上書きします。
<file name>	復元するファイルの名前。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword

コマンド戻り値：

- -1：コンピューターにインストールされているバージョンの製品ではコマンドがサポートされていません。
- 0：コマンドが正常に実行されました。
- 1：必要な引数がコマンドに渡されていません。
- 2：一般的なエラーが発生しました。
- 4：構文エラーがあります。

IOCSCAN：セキュリティ侵害インジケーター（IOC）のスキャン

IOC スキャンタスクを実行します。*セキュリティ侵害インジケーター（IOC）*とは、コンピューターへの認証されないアクセス（コンピューターの侵害）の痕跡を示すオブジェクトまたは活動に関する一連のデータです。たとえば、システムへのログインを複数回失敗すると、セキュリティ侵害インジケーターの構成要素となります。*IOC* スキャンタスクは、コンピューターのセキュリティ侵害インジケーターを検索し、脅威への対応方法を確立するのに役立ちます。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

IOC ファイルに記述された侵害インジケーターとの一致が 128 個に達すると、IOC スキャンは中止されます。この動作は、IOC スキャンタスクレポート内の項目数を制限して、分析を容易にし、レポートのオーバーフローを防ぐために必要です。侵害インジケーターの定式化が不正確だと、膨大な数の一致が生成される可能性があるためです。

コマンド構文

avp.com IOCSCAN <IOC ファイルのフルパス>|/path=<IOC ファイルのあるフォルダーのパス> [/process=on|off] [/hint=<プロセスの実行ファイルの完全パス|ファイルの完全パス>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off] [/datetime=<イベントの記録日>] [/channels=<チャネルのリスト>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<除外リスト>] [/scope=<スキャンするフォルダーのリスト>]

IOC ファイル	
`<full path to the IOC file>`	スキャンに使用する IOC ファイルの完全パス。スペースで区切って複数の IOC ファイルを指定することができます。IOC ファイルの完全パスは引数「`/path`」なしで入力する必要があります。 例：`C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	スキャンに使用する IOC ファイルのあるフォルダーのパス。*IOC ファイル*は、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。IOC ファイルは OpenIOC 標準に準拠している必要があります。 例：`C:\Users\Admin\Desktop\IOC`

IOC スキャンのデータ種別	
`/process=on|off`	IOC スキャンの実行中にプロセスデータを分析します（ProcessItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はスキャンの実行時にコンピューター上で実行されているプロセスを分析しません。IOC ファイルに IOC ドキュメント ProcessItem の IOC タームが含まれている場合、無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント ProcessItem が記述されている場合のみプロセスデータを分析します。
`/hint=<full path to the executable file of the process|full path to the file>`	IOC スキャンの実行時にファイルのデータを分析します（ProcessItem および FileItem）。 次のいずれかの方法でファイルを選択することができます： • `<full path to the executable file of the process>` – ProcessItem タ ーム。 • `<full path to the file>` – FileItem タ ーム。
`/registry=on|off`	IOC スキャンの実行中に Windows のレジストリデータを分析します（RegistryItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は Windows レジストリをスキャンしません。IOC ファイルに IOC ドキュメント RegistryItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント RegistryItem が記述されている場合のみ Windows レジストリを分析します。 Kaspersky Endpoint Security はデータ種別 RegistryItem に対しては、レジストリキー一式をスキャンします。
`/dnsentry=on|off`	IOC スキャンの実行中、ローカルの DNS キャッシュ内の項目のデータを分析します（DnsEntryItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はローカルの DNS キャッシュをスキャンしません。IOC ファイルに IOC ドキュメント DnsEntryItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント DnsEntryItem が記述されている場合のみローカルの DNS キャッシュを分析します。
`/arpentry=on|off`	IOC スキャンの実行中、ARP テーブル内の項目のデータを分析します（ArpEntryItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は ARP テーブルをスキャンしません。IOC ファイルに IOC ドキュメント ArpEntryItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント ArpEntryItem が記述されている場合のみローカルの ARP テーブルを分析します。
`/ports=on|off`	IOC スキャンの実行中、待機しているポートに関するデータを分析します（PortItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は端末上のアクティブな接続のテーブルをスキャンしません。IOC ファイルに IOC ドキュメント PortItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント PortItem が記述されている場合のみアクティブな接続のテーブルを分析します。
`/services=on|off`	IOC スキャンの実行中、端末にインストールされているサービスに関するデータを分析します（ServiceItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は端末にインストールされているサービスに関するデータをスキャンしません。IOC ファイルに IOC ドキュメント ServiceItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント ServiceItem が記述されている場合のみサービスのデータを分析します。

`/system=on|off`	IOC スキャンの実行中に環境のデータを分析します（SystemInfoItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は環境データを分析しません。IOC ファイルに IOC ドキュメント SystemInfoItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント SystemInfoItem が記述されている場合のみ環境データを分析します。
`/users=on|off`	IOC スキャンの実行中にユーザーに関するデータを分析します（UserItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はシステムで作成されたユーザーに関するデータを分析しません。IOC ファイルに IOC ドキュメント UserItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント UserItem が記述されている場合のみシステムで作成されたユーザーに関するデータを分析します。
`/volumes=on|off`	IOC スキャンの実行中にボリュームに関するデータを分析します（VolumeItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は端末のボリュームに関するデータをスキャンしません。IOC ファイルに IOC ドキュメント VolumeItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント VolumeItem が記述されている場合のみボリュームに関するデータを分析します。
`/eventlog=on|off`	IOC スキャンの実行中、Windows イベントログの項目のデータを分析します（EventLogItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は Windows イベントログの項目をスキャンしません。IOC ファイルに IOC ドキュメント EventLogItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント EventLogItem が記述されている場合、Windows イベントログを分析します。
`/datetime=<event publication date>`	対応する IOC ドキュメントの IOC スキャン範囲を決定する際には、Windows イベントログにイベントが記録された日付を考慮してください。 IOC スキャンの実行時、Kaspersky Endpoint Security は指定された日時からタスクが実行された時刻までの機関に記録された Windows イベントログの項目をスキャンします。 Kaspersky Endpoint Security では、引数の値にイベントの記録日を指定できます。指定した日付からスキャンが実行されるまでの間に Windows イベントログ内で記録されたイベントに対してのみスキャンが実行されます。 引数が指定されていない場合、Kaspersky Endpoint Security は記録されたすべてのくイベントをスキャンします。設定 `TaskSettings::BaseSettings::EventLogItem::datetime` は編集できません。 スキャン用に提供された IOC ファイルで IOC ドキュメント EventLogItem が記述されている場合のみこの設定が使用されます。
`/channel=<list of channels>`	IOC スキャンを実行するチャネル（ログ）名のリスト。 引数が指定されていない場合、Kaspersky Endpoint Security は指定されたログに記録された項目をスキャンします。IOC ドキュメントには EventLogItem が記載されている必要があります。 ログの名前は、ログのプロパティ（Full Name パラメータ）またはイベントのプロパティ（イベントの XML スキーマ内の `<Channel></Channel>` パラメータ）で指定されたログ（チャネル）の名前に従って文字列で指定されます。スペースで区切って複数のチャネルを指定することができます。 引数が指定されていない場合、Kaspersky Endpoint Security はチャネル `Application`、`System`、`Security` の項目をスキャンします。
`/files=on|off`	IOC スキャンの実行時にファイルのデータを分析します（FileItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はファイルのデータを分析しません。IOC ファイルに IOC ドキュメント FileItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント FileItem が記述されている場合のみファイルに関するデータを分析します。
`/drives=<all|system|critical|custom>`	IOC ドキュメント FileItem のデータを分析する際の IOC スキャン範囲を設定します。 スキャン範囲には次の値を設定できます： • `<all>`：すべての利用可能なファイル範囲 • `<system>`：オペレーティングシステムがインストールされているフォルダーにあるファイル • `<critical>`：ユーザーおよびシステムフォルダー内の一時ファイル • `<custom>`：ユーザー定義の範囲のファイル（`/scope=<list of folders to scan>`） 引数が指定されていない場合、スキャンは重要な領域に対して実行されます。

`/excludes=<list of exclusions>`	IOC ドキュメント FileItem のデータを分析する際に除外する範囲を設定します。スペースで区切って複数のパスを指定することができます。
`/scope=<list of folders to scan>`	IOC ドキュメント FileItem でデータを分析する際のユーザー定義の IOC スキャン範囲です（`/drives=custom`）。スペースで区切って複数のパスを指定することができます。
`/retro /<number of days>`	*遡及的 IOC スキャン*は、Kaspersky Endpoint Security が一定期間のデータを使用してセキュリティ侵害インジケーターをスキャンする *IOC スキャンタスク*のモードです。このモードは、コンピューターのネットワーク動作のデータ内のセキュリティ侵害インジケーターを検知することを目的としています。 期間は 1 日間から 14 日間までに設定できます。既定では、本製品は 1 日間、セキュリティ侵害インジケーターをスキャンします。
`/network=on|off`	ネットワークデータの分析（NetworkItem）。
`/url=on|off`	ブラウザーログのデータ分析（UrlHistoryItem）。 遡及的 IOC スキャンは、Google Chrome、Mozilla Firefox、Microsoft Edge（バージョン 79 以降）のブラウザーのログを分析します。
`/email`	メールオブジェクトの分析（EmailItem）。
`/route`	ルーティングおよび転送テーブルの分析（RouteEntryItem）。

コマンド戻り値：

- `-1`：コンピューターにインストールされているバージョンの製品ではコマンドがサポートされていません。
- `0`：コマンドが正常に実行されました。
- `1`：必要な引数がコマンドに渡されていません。
- `2`：一般的なエラーが発生しました。
- `4`：構文エラーがあります。

コマンドが正常に実行され（戻り値が `0`）、侵害インジケーターが検出された場合、Kaspersky Endpoint Security は次のタスク結果の情報をコマンドラインに出力します：

`Uuid`	IOC ファイル構成のヘッダー部分に基づいた IOC ファイルの ID（`<ioc id="">` タグ）
`Name`	IOC ファイル構成のヘッダー部分に基づいた IOC ファイルの説明（`<description></description>` タグ）
`Matched Indicator Items`	すべての一致したインジケーターの ID のリスト
`Matched objects`	一致した各 IOC ドキュメント箇所のデータ

MDRLICENSE：MDR のアクティベーション

BLOB 設定ファイルを追加して Managed Detection and Response をアクティベートします。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

BLOB ファイルを使用した操作を実行するには、管理者権限が必要です。ポリシーの Managed Detection and Response の設定は編集可能である必要があります（）。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

実行する操作	
`/ADD <file name>`	Kaspersky Managed Detection and Response との連携用の BLOB 設定ファイルを適用します（P7 形式）。BLOB ファイルは 1 ファイルのみ適用可能です。BLOB ファイルがコンピューター上で適用済みの場合は、ファイルが置き換えられます。
`/DEL`	BLOB 設定ファイルを削除します。

認証	
`/login=<user name> /password=<password>`	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA：EDR (KATA) との連携

Endpoint Detection and Response コンポーネント (KATA) の管理用のコマンド：

- EDR (KATA) コンポーネントの有効または無効

  EDR コンポーネント (KATA) は Kaspersky Anti Targeted Attack Platform ソリューションとの連携を提供します。

- Kaspersky Anti Targeted Attack Platform サーバーへの接続を設定します。

- コンポーネントの現在の設定の表示。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com START EDRKATA
avp.com STOP EDRKATA
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
avp.com edrkata /show
```

実行する操作	
`stop`	EDR (KATA) コンポーネントを無効にします。
`start`	EDR (KATA) コンポーネントを有効にします。

set	EDR (KATA) コンポーネントを設定します。次の設定を構成できます： • Central Node サーバーの追加（servers=<server address>:<port>） • TLS 証明書を追加する（server-certificate=<path to the TLS certificate>） • Central Node サーバーの接続タイムアウトの設定（/timeout=<Central Node server connection timeout (s)>） • Central Node サーバーとの同期期間の設定（/sync-period=<Central Node server synchronization period (min)>）
show	コンポーネントの現在の設定を表示します。

KUMA：KUMA との連携

組み込み KUMA エージェントの管理用コマンド：

- KUMA との連携の有効化または無効化。

  組み込み KUMA エージェントは、Kaspersky Unified Monitoring and Analysis Platform ソリューションとの相互運用性を提供します。

- Kaspersky Unified Monitoring and Analysis Platform サーバーへの接続設定。

- コンポーネントの現在の設定の表示。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com START KUMA
avp.com STOP KUMA [/login=<ユーザー名> /password=<パスワード>]
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<暗号化コンテナーへのパス>] [ /client-certificate-
password=<パスワード>] [/maximum-data-transfer-time=<最大イベント転送遅延時間（秒）>]
avp.com KUMA /SHOW
```

実行する操作	
stop	KUMA 連携を無効にします。
start	KUMA 連携を有効にします。
set	組み込みの KUMA エージェントを設定します。次の設定を構成できます： • KUMA サーバーを追加する（/servers=<protocol>://<server address>:<port>） 本製品は、tcp、udp、http、https のサーバー接続プロトコルをサポートしています。 • TLS 証明書を追加する（/server-certificate=<path to the TLS certificate>） • サーバーの接続タイムアウトを設定する（/timeout=<KUMA server connection timeout (s)>） • 暗号化コンテナーを追加する（/client-certificate=<path to the crypto-container> /client-certificate-password=<password>） • イベント転送の遅延を設定する（/maximum-data-transfer-time=<maximum events transmission delay (sec)>）
show	コンポーネントの現在の設定を表示します。

認証	
/login=<user name> /password=<password>	パスワードによる保護の権限に必要なユーザーアカウントの認証情報。

例：

```
avp.com start kuma
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA：YARA スキャンの実行

*YARA スキャンの実行*タスクを実行します。本製品は、YARA ルールのデータベースを使用して、ファイルとオブジェクトをスキャンし、組織の IT インフラストラクチャに対する標的型攻撃のインジケーターを探します。*YARA ルール*は、Kaspersky Endpoint Security がオブジェクトをスキャンするために使用する、標的型攻撃や組織の IT インフラストラクチャへの侵入を示すシグネチャの説明です。

YARA スキャンを実行するには、ルールを記述した YARA ファイルを準備する必要があります。YARA ファイルを作成する際は、次の要件を考慮してください：

- Kaspersky Endpoint Security は、侵害インジケーターを記述するための YARA 4.2.3 オープン標準に準拠した .YARA および .YAR の拡張子の YARA ファイルをサポートしています。
- タスクには YARA ルールを含むファイルのみを指定できます。*YARA スキャンの実行*タスクは、その他のルール種別をサポートしていません。
- Kaspersky Endpoint Security でサポートされていない YARA ファイルを追加した場合、またはルールに構文エラーが含まれている場合、対応するエラーメッセージが表示されてタスクが中止されます。
- 単一のタスクで使用されるすべての YARA ファイルの識別子は一意である必要があります。同じ識別子を持つ YARA ファイルが存在した場合、タスクの実行結果に影響を与えることがあります。
- YARA ルールに記述されたインジケーターとの一致が 128 個に達すると、YARA スキャンは中止されます。この動作は、YARA スキャンレポート内の項目数を制限して、分析を容易にし、レポートのオーバーフローを防ぐために必要です。YARA ルールの定式化が不正確だと、膨大な数の一致が生成される可能性があるためです。

1 つの YARA ファイルに 1 つのルールを作成することを推奨します。こうすることで、スキャン結果が読みやすくなります。

YARA スキャンには時間がかかる場合があります。YARA スキャンは、ドライブのサイズ、タスク設定、ディスク上のオブジェクトの数に応じて、数分から数時間かかる場合があります。本製品では、進行状況のインジケーターは表示されません。YARA スキャンは、停止することも、キャンセルすることもできません。YARA スキャンの結果が得られるまで待つことをお勧めします。

コマンド構文

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA ファイル	
`<full path to the YARA file>`	スキャンに使用する YARA ファイルの完全パス。スペースで区切って複数の YARA ファイルへのパスを指定することができます。 `/path=<path to the folder with YARA files>` 値が指定されていない場合の必須の引数です。 例： `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`

`/path=<path to the folder with YARA files>`	スキャンに使用する YARA ファイルのあるフォルダーの完全パス。 `<full path to the YARA file>` 値が指定されていない場合の必須の引数です。 例： `/path=C:\Users\Admin\Desktop\YARA`

詳細設定	
`/fastScan=<on|off>`	簡易版 YARA スキャン。オブジェクトごとに、検知されたインジケーターの1回の出現がログに記録されます。検知されたインジケーターの重複はログには表示されません。簡易版 YARA スキャンでは、サイズの大きいファイルを迅速にスキャンできます。 この設定が指定されていない場合、標準の YARA スキャンが実行されます。このモードでは、検知されたインジケーターの重複がログに記録されます。
`/maxRules=<maximum number of scan rules>`	適用される一意なルール数の制限値。この値に達すると、アプリケーションは YARA スキャンを停止します。 この設定の値が指定されていない場合、または `0` が指定されている場合、制限なしで YARA スキャンが実行されます。
`/timeOut=<stop scan after the specified time in seconds>`	YARA スキャン時間の制限値（秒）。この時間が経過すると、YARA スキャンが停止します。 この設定の値が指定されていない場合、または `0` が指定されている場合、制限なしで YARA スキャンが実行されます。
`/recursive=<on|off>`	この引数は、`/scanFolders` オブジェクトスキャン内のサブフォルダーの再帰的スキャンを開始します。
`/scanFolders=<list of folders to be scanned>`	この引数は、指定されたフォルダーリスト内のファイルの YARA スキャンを開始します。スペースで区切って複数の値を指定することができます。Kaspersky Endpoint Security はフォルダーのパスのマスクの入力時の文字「`*`」および「`?`」をサポートします。 この設定が指定されていない場合、ネットワーク共有、クラウドドライブ、リムーバブルメディアを除くすべてのローカルドライブの YARA スキャンが実行されます。
`/scanMemory=<on|off>`	実行中のすべてのプロセスのメモリをスキャンします。
`/scanProcess=<process name>`	リストされたプロセスのみメモリをスキャンします。プロセスの実行ファイルへの完全パスをスペース区切りで指定します。マスクを入力する場合は、「`*`」および「`?`」の文字も使用できます。
`/maxSize=<file size in bytes>`	YARA スキャンのファイルサイズの制限値。それよりもサイズの大きいファイルはスキップされます。
`/includes=<list of objects to be scanned>>`	スキャン範囲の編集。スペースで区切って複数の値を指定することができます。次の値が使用可能です： • ファイル名 • ファイルの拡張子 スキャン範囲は、`/scanFolders` パラメータで指定する必要があります。 例： `/scanFolders C:\*.* /includes=*.exe *.dll` – 本製品は、ディスク C 上の EXE および DLL の拡張子を持つすべてのファイルをスキャンします。
`/excludes=<list of objects to be scanned>`	YARA スキャンから除外するファイル。スペースで区切って複数の値を指定することができます。次の値が使用可能です： • ファイルパス • ファイルパスのマスク 除外リストは、`/scanFolders` パラメータで指定する必要があります。 例： `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – ドライブ C のルートフォルダーにある readme.txt ファイル、C:\trusted フォルダーのすべてのファイル、および XML 拡張子のすべてのファイルがスキップされます。
`/scanAutoruns=<on|off>`	自動実行ポイントオブジェクトの YARA スキャン。
`/excludeAutoruns=<list of autorun point areas to skip>`	スキャン範囲からの自動実行ポイントオブジェクトの除外。プロセスの実行ファイルへの完全パスをスペース区切りで指定します。マスクを入力する場合は、「`*`」および「`?`」の文字も使用できます。
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	フォルダーへのパスを指定すると、指定されたパスにある yara_<computer name>_<scan completion time>.txt という名前のファイルにスキャン結果が保存されます。 特定の TXT ファイルへのパスを指定すると、そのファイルにスキャン結果が保存されます。 例：`/logFolder=C:\test` または `/logFolder=C:\test\abc.txt`。 `/logFolder` のオプションが指定されているかどうかに関係なく、スキャン結果はコマンドラインに出力されます。

コマンド戻り値：

- `-1`：コンピューターにインストールされているバージョンの製品ではコマンドがサポートされていません。
- `0`：コマンドは正常に完了しました。
- `1`：必要な引数がコマンドに渡されていません。
- `2`：一般的なエラーが発生しました。
- `4`：構文エラーがあります。
- `5`：引数で指定された1つ以上の YARA ルールファイルが見つかりません。

コマンドが正常に実行され（戻り値が `0`）、侵害インジケーターが検出された場合、Kaspersky Endpoint Security は次のタスク結果の情報をコマンドラインに出力します：

`Started at <time>` `Finished at <time>`	スキャンの開始時刻と完了時刻。
`Host name: <computer name>`	オブジェクトが検知されたコンピューターの名前。
`Result: <error>`	タスクの実行中に発生したエラーのエラーコード。エラーがない場合、`0x00000000` が出力されます。
`Comment: <comment text>`	タスクの実行中に発生したエラーの説明。例：「`Operation timeout`」。
`Object Name:` または `Process:`（プロセスメモリをスキャンする場合）	YARA ルールが適用されたオブジェクトまたはプロセスの名前。
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	YARA ルールが適用されたオブジェクトのハッシュ。
`Rule Name`	適用された YARA ルールの名前。

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	YARA ルールで指定されたメタデータ。

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	オブジェクト内での YARA ルールの条件を満たす一致の検知：
	• 一致が検知されたプロセスメモリまたはファイル内のオフセット（`Offset`）
	• YARA ルール内の一致する文字列の名前（`String name`）
	• プロセスメモリまたはファイル内の一致する文字列（`String data`）

TELEMETRYFILTERS：KUMA に送信するイベントのフィルタリング

パフォーマンスを向上させ、KUMA サーバーへのデータ転送を最適化するために、テレメトリに個々のイベントを手動で追加したり除外したりできます。たとえば、Sysmon イベントを除外できます。

コマンドラインから除外リストを JSON ファイルにエクスポートすることができます。

コマンドに、設定のエクスポート先のファイル名のみが含まれている場合、ファイルは次のように配置されます：

- avp.com へのパスがシステム変数 %PATH% に追加されている場合、ファイルは「`C:\Windows\SysWOW64`」フォルダーに配置されます。
- 本製品のインストールフォルダーからコマンドを実行すると、本製品の自己保護機能によってアプリケーションフォルダー内の新規ファイルの作成がブロックされるため、エクスポートは失敗します。アプリケーション設定をファイルにエクスポートするには、ファイルパスを入力します。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com TELEMETRYFILTERS /export <file name>
avp.com TELEMETRYFILTERS /import <file name>
```

実行する操作	
`export`	KUMA に送信するイベントフィルターをエクスポートします。
`import`	KUMA に送信するイベントフィルターをインポートします。コンピューターにイベントフィルタリングルールが既に存在する場合、Kaspersky Endpoint Security はインポート時にそれらを置き換えます。

エクスポートまたはインポート用のファイル	
`<file name>`	KUMA に送信されるイベントフィルターを含むファイルの名前。ファイルパスを入力することもできます。KUMA に送信するフィルターを JSON ファイルにエクスポートできます。

Light Agent 管理コマンド

コマンドラインで仮想環境保護用 Light Agent モードで本製品を管理できます。Kaspersky Security Center コンソールを使用した管理ができない場合に、Light Agent モードの本製品を管理できます。本製品の管理に利用できるコマンドのリストは、「`HELP`」コマンドを実行して確認できます。特定のコマンドの構文を確認するには、「`HELP <command>`」コマンドを実行します。

コマンドラインから Light Agent モードの本製品を管理するには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。
3. コマンドを実行するには、次のテンプレートを使用します：

```
avp.com <command> [options]
```

Kaspersky Endpoint Security でコマンドが実行されます。

Light Agent モードでインストールされた本製品は、標準モードでインストールされた本製品のほぼすべての AVP コマンドをサポートします。Light Agent モードでは、定義データベースのアップデートタスクとライセンスの管理タスクが制限されます。

KSVLAINFO：Light Agent モードの特定

Light Agent モードの特定。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com KSVLAINFO
```

コマンドは次の情報をコンソールに出力します：

- 仮想環境保護用 Light Agent モード：有効または無効。

  Light Agent モードが有効な場合、アプリケーションは Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用されます。

- VDI 保護モード：有効または無効。

  VDI 保護モードは、非永続的な仮想マシン上での Kaspersky Endpoint Security のパフォーマンスを最適化するのに役立ちます。VDI 保護モードが有効な場合、保護対象仮想マシンの再起動が必要なアップデートは非永続的な仮想マシンにはインストールされません。再起動が必要なアップデートを受信した場合、非永続的な仮想マシンにインストールされている Light Agent は Kaspersky Security Center にメッセージを送信し、保護対象仮想マシンのテンプレートをアップデートする必要があることを通知します。

- 保護対象の仮想マシンの種別：永続的または非永続的。

- 仮想インフラストラクチャにおける仮想マシンの役割：サーバーまたはワークステーション。

- 保護対象の仮想マシンの識別子（UUID）。

VIISINFO：Light Agent と Integration Server との接続のステータス

Light Agent と Integration Server との接続に関する情報の表示。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com VIISINFO
```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続されている Integration Server のアドレスとポート。
- Integration Server 接続ステータス。
- Light Agent と Integration Server の最終接続日時。

SVMINFO：Light Agent と Protection Server との接続のステータス

Light Agent と Protection Server との接続に関する情報の表示。

コマンドを実行するには、Kaspersky Endpoint Security の実行ファイルがあるフォルダーに移動します。システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

コマンド構文

```
avp.com SVMINFO
```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続されている SVM のアドレスと、Light Agent に対する仮想インフラストラクチャ内の SVM の場所：ローカルまたはローカル以外。
- Light Agent が使用する SVM 検出方法：Integration Server の使用または SVM アドレスのカスタムリストの使用。
- SVM 検出方法として SVM アドレスのリストが選択されている場合の SVM アドレスのリスト。
- Light Agent を SVM に接続するためのタグ。
- SVM 選択アルゴリズム：標準または拡張。拡張 SVM 選択アルゴリズムが使用されている場合は、仮想インフラストラクチャ内の SVM パスの種別も表示されます。
- Light Agent と Protection Server 間の接続の保護の状態。

エラーコード

コマンドラインを使用して本製品を使用しているときに、エラーが発生することがあります。エラーが発生すると、Kaspersky Endpoint Security は「`Error: Cannot start task 'EntAppControl'`」のようなエラーメッセージを表示します。さらに、より詳細な状況を確認するためのエラーコード（例：`error=8947906D`）が表示される場合もあります（詳しくは、下記の表を参照してください）。

エラーコード	説明
09479001	このライセンスは既に使用されています。
0947901D	ライセンスの有効期間が終了しています。データベースのアップデートは使用できません。
89479002	ライセンスが見つかりません。
89479003	デジタル署名がないか、破損しています。
89479004	データが破損しています。
89479005	ライセンス情報ファイルが破損しています。
89479006	ライセンスの有効期間が終了しています。
89479007	ライセンス情報ファイルが選択されていません。
89479008	無効なライセンス情報ファイルです。
89479009	データの保存に失敗しました。
8947900A	データの読み取りに失敗しました。
8947900B	入出力エラーです。
8947900C	定義データベースが見つかりません。
8947900E	ライセンスライブラリが読み込まれていません。
8947900F	定義データベースが破損しているか、手動で更新されています。
89479010	定義データベースが破損しています。
89479011	無効なライセンス情報ファイルは、予備のライセンスの追加には使用できません。
89479012	システムエラーです。
89479013	ライセンスの拒否リストが破損しています。
89479014	ファイルの署名が、カスペルスキーのデジタル署名と一致しません。
89479015	試用版ライセンスは製品版のライセンスとして使用できません。
89479016	アプリケーションのベータ版を使用するには、ベータテスト用のライセンスが必要です。
89479017	このライセンス情報ファイルは本製品に対応するものではありません。他の製品のライセンス情報ファイルを使用して Kaspersky Endpoint Security for Windows をアクティベートすることはできません。インストール済みの製品を確認してください。
89479018	ライセンスがカスペルスキーによってブロックされています。
89479019	本製品は既に試用版ライセンスで使用されています。試用版ライセンスのライセンスを再度追加することはできません。
8947901A	ライセンス情報ファイルが破損しています。
8947901B	デジタル署名がないか、破損しているか、カスペルスキーのデジタル署名と一致しません。
8947901C	有効期間が終了している非製品版ライセンスは追加できません。
8947901E	ライセンス情報ファイルの作成日または使用日が無効です。システムの日付を確認してください。
8947901F	試用版ライセンスを追加できません：試用版の他のライセンスが既に有効になっています。
89479020	ライセンスの拒否リストが破損しているか存在しません。
89479021	アップデートの説明が見つからないか、破損しています。
89479022	本製品に適したライセンス情報ではありません
89479023	無効なライセンス情報ファイルは、予備のライセンスの追加には使用できません。
89479025	アクティベーションサーバーへの要求の送信でエラーが発生しました。考えられる原因：インターネットの接続エラーまたはアクティベーションサーバーの一時的な問題。1、2 時間後にアクティベーションコードを使用して製品をアクティベートしてください。このエラーが再度発生する場合は、インターネットプロバイダーにお問い合わせください。
89479026	要求に無効なアクティベーションコードが含まれています。
89479027	応答ステータスを取得できません。

エラーコード	説明
89479028	一時ファイルの保存時にエラーが発生しました。
89479029	無効なアクティベーションコードが入力されたか、無効なシステム日付がコンピューターで設定されました。コンピューターのシステム日付を確認してください。
8947902A	ライセンスが本製品と互換性がないか、ライセンスの有効期間が終了しています
8947902B	ライセンス情報ファイルの取得に失敗しました。無効なアクティベーションコードが入力されました。
8947902C	アクティベーションサーバーがエラー 400 を返しました。
8947902D	アクティベーションサーバーがエラー 401 を返しました。
8947902E	アクティベーションサーバーがエラー 403 を返しました。
8947902F	アクティベーションサーバーで必要なリソースが使用できません。 アクティベーションサーバーがエラー 404 を返しました。インターネットの接続設定を確認してください。
89479030	アクティベーションサーバーがエラー 405 を返しました。
89479031	アクティベーションサーバーがエラー 406 を返しました。
89479032	プロキシ認証が必要です。ネットワーク設定を確認してください。
89479033	要求はタイムアウトしました。
89479034	アクティベーションサーバーがエラー 409 を返しました。
89479035	アクティベーションサーバーで必要なリソースが使用できません。 アクティベーションサーバーがエラー 410 を返しました。インターネットの接続設定を確認してください。
89479036	アクティベーションサーバーがエラー 411 を返しました。
89479037	アクティベーションサーバーがエラー 412 を返しました。
89479038	アクティベーションサーバーがエラー 413 を返しました。
89479039	アクティベーションサーバーがエラー 414 を返しました。
8947903A	アクティベーションサーバーがエラー 415 を返しました。
8947903C	内部サーバーのエラーです。
8947903D	機能がサポートされていません。
8947903E	無効なゲートウェイの応答です。ネットワーク設定を確認してください
8947903F	リソースは一時的に使用できません。
89479040	ゲートウェイ応答はタイムアウトになりました。ネットワーク設定を確認してください。
89479041	サーバーでサポートされていないプロトコルです。
89479043	不明な HTTP エラーです。
89479044	無効なリソース ID です。
89479046	無効な URL です。
89479047	無効な出力先フォルダーです。
89479048	メモリ割り当てエラーです。
89479049	パラメータの ANSI 文字列への変換時にエラーが発生しました（URL、フォルダー、エージェント）。
8947904A	作業者スレッドの作成時にエラーが発生しました。
8947904B	作業者スレッドは既に実行中です。
8947904C	作業者スレッドは実行されていません。
8947904D	ライセンス情報ファイルがアクティベーションサーバーで見つかりません。
8947904E	ライセンスがブロックされています。
8947904F	アクティベーションサーバーの内部エラーです。
89479050	アクティベーション要求に十分なデータがありません。

エラーコード	説明
89479053	追加されたライセンス情報ファイルに対応するライセンスの有効期間が終了しています。
89479054	無効なシステム日付がコンピューターに設定されています。システム日付の値を確認してください
89479055	試用版のライセンスの有効期間が終了しています。
89479056	アプリケーションのアクティベーション期間が終了しています。
89479057	指定したコードを使用した製品のアクティベーションの回数が上限を超えています。
89479058	システムエラーによるアクティベーション処理の完了
89479059	試用版ライセンスは製品版のライセンスとして使用できません。
8947905C	アクティベーションコードが必要です。
89479062	アクティベーションサーバーへ接続できません。
89479064	アクティベーションサーバーが使用できません。インターネット接続を確認してアクティベーションを再試行してください。
89479065	ライセンスの有効期間が終了しています
89479066	現在のライセンスを有効期間が終了したライセンスで置き換えることはできません。
89479067	予備のライセンスに対応するライセンスの有効期間が現在のライセンスよりも先に終了する場合は、予備のライセンスを追加できません。
89479068	更新済みの定額制サービスのライセンスが見つかりません。
8947906A	アクティベーションコードが無効です。
8947906B	このライセンスは既に使用されています
8947906C	現在のライセンスと予備のライセンスのライセンス種別が一致しません。
8947906D	ライセンスがサポートしていないコンポーネントです
8947906E	定額制ライセンスを予備のライセンスとして追加できません
89479213	伝送レイヤーの一般的なエラー
89479214	アクティベーションサーバーに接続できません
89479215	無効な Web アドレス形式です
89479216	プロキシサーバーアドレスを変換できません
89479217	サーバーアドレスを変換できませんでした。インターネット接続の設定を確認してください。
89479218	サーバー接続に失敗しました
89479219	リモートでアクセスが拒否されました
8947921A	操作がタイムアウトしました
8947921B	HTTP 要求の送信でエラーが発生しました
8947921C	SSL 接続エラー
8947921D	コールバックにより操作が中断されました
8947921E	可能な転送試行回数を超過しました
8947921F	受信者を確認できません
89479220	サーバーからの応答が空です
89479221	データの送信でエラーが発生しました
89479222	データの取得でエラーが発生しました
89479223	SSL 証明書に関する問題
89479224	SSL 暗号化に関する問題
89479225	SSL 証明書センターに関する問題
89479226	無効なネットワークパケットのコンテンツ

エラーコード	説明
89479227	アカウントのアクセスが拒否されました
89479228	無効な SSL 証明書ファイル
89479229	SSL 接続を切断できません
8947922A	発生回数が多いエラー
8947922B	失効した証明書が含まれる無効なファイル
8947922C	SSL 証明書の要求エラー
89479401	不明なサーバーエラー
89479402	内部サーバーのエラーです
89479403	入力したアクティベーションコードで利用できるライセンスがありません。
89479404	現在のライセンスがブロックされました
89479405	アクティベーション要求に必要なパラメータがありません
89479406	無効なクライアント番号またはパスワード
89479407	アクティベーションコードが無効です。
89479408	アクティベーションコードは本製品に対応するものではありません。別の製品のアクティベーションコードで Kaspersky Endpoint Security for Windows をアクティベートすることはできません。インストール済みの製品を確認してください
89479409	アクティベーションコードが必要です
8947940B	アクティベーション期間が終了しました
8947940C	このコードを使用したアクティベーションの回数が上限を超えました。
8947940D	無効な形式の要求 ID
8947940E	アクティベーションコードは既に使用されています
8947940F	アクティベーションコードを更新できません
89479410	アクティベーションコードはこの地域で無効です
89479411	このアクティベーションコードは日本語バージョンには適用できません。
89479412	このアクティベーションコードは、本製品の新バージョン用です。インストールされているバージョンをアクティベートするには、別のアクティベーションコードを取得してください
89479413	アクティベーションサーバーがエラー 643 を返しました
89479414	アクティベーションサーバーがエラー 644 を返しました
89479415	アクティベーションサーバーがエラー 645 を返しました
89479416	アクティベーションサーバーがエラー 646 を返しました
89479417	アクティベーションサーバーバージョン 1.0 が必要です
89479418	無効なアクティベーションコード形式
89479419	コンピューターの時刻がアクティベーションサーバーの時刻と同期していません
8947941A	アプリケーションのバージョンが正しくありません
8947941B	定額制サービスの有効期間が終了しています
8947941C	アクティベーション数を超過しました
8947941D	無効なチケット署名
8947941E	追加のデータが必要です
8947941F	データの検証に失敗しました
89479420	定額制サービスを利用できません
89479421	アクティベーションサーバーがメンテナンス中です

エラーコード	説明
89479501	予期しないエラーです
89479502	無効なパラメータが転送されました（アクティベーションサーバーアドレスが記載されていないリストなど）
89479503	アクティベーションコードが無効です(無効なハッシュ)
89479504	無効なユーザー ID です
89479505	無効なユーザーパスワードです
89479506	アクティベーションサーバーからの無効な応答です
89479507	アクティベーション要求が中断されました
89479509	アクティベーションサーバーが空の転送リストを返しました

補足資料：製品プロファイル

*プロファイル*で、Kaspersky Endpoint Security のコンポーネント、タスク、または機能を指定します。コマンドラインから製品を管理するときに、プロファイルを使用します。「`START`」、「`STOP`」、「`STATUS`」、「`STATISTICS`」、「`EXPORT`」コマンドで、プロファイルを使用できます。プロファイルを使用することで、本製品の設定（例：`STOP DeviceControl`）やタスクの実行（例：`START Scan_My_Computer`）を行うことができます。

次のプロファイルを利用できます：

- `AdaptiveAnomaliesControl`：アダプティブアノマリーコントロール。
- `AMSI` – AMSI 保護
- `AntiCryptor`
- `BehaviorDetection` – ふるまい検知
- `DeviceControl`：デバイスコントロール。
- `EntAppControl`：アプリケーションコントロール。
- `File_Monitoring` または `FM`：ファイル脅威対策。
- `Firewall` または `FW`：ファイアウォール。
- `HIPS` – ホスト侵入防止
- `IDS`：ネットワーク脅威対策。
- `IntegrityCheck`：整合性チェック。
- `LogInspector`：Windows イベントログ監視。
- `Mail_Monitoring` または `EM`：メール脅威対策。
- `Rollback`：アップデートのロールバック（本製品が Light Agent モードでインストールされている場合はプロファイルを適用できません）。

- `Scan_ContextScan`：コンテキストメニューからのスキャン。
- `Scan_IdleScan`：バックグラウンドスキャン。
- `Scan_Memory`：カーネルメモリのスキャン。
- `Scan_My_Computer`：完全スキャン。
- `Scan_Objects`：オブジェクトスキャン。
- `Scan_Qscan`：オペレーティングシステムの起動時に読み込まれるオブジェクトのスキャン。
- `Scan_Removable_Drive`：リムーバブルドライブのスキャン。
- `Scan_Startup` または `STARTUP`：簡易スキャン。
- `Updater`：アップデート（本製品が Light Agent モードでインストールされている場合はプロファイルを適用できません）。
- `Web_Monitoring` または `WM`：ウェブ脅威対策。
- `WebControl`：ウェブコントロール。

Kaspersky Endpoint Security では、コマンド指定用のサービス名もサポートされています。カスペルスキーのテクニカルサポートに問い合わせを行って調査が必要になったときに、コマンド指定用のサービス名を使用する場合があります。

REST API を使用した製品の管理

Kaspersky Endpoint Security では、サードパーティ製ソリューションを使用して、製品設定の編集、スキャンの実行、定義データベースのアップデートなどのタスクを実行できます。Kaspersky Endpoint Security はそのための API を提供します。Kaspersky Endpoint Security の REST API は HTTP を介して操作でき、要求と応答の一連のメソッドで構成されています。これにより、製品のローカルインターフェイスまたは Kaspersky Security Center 管理コンソールではなく、サードパーティ製ソリューションを使用して Kaspersky Endpoint Security を管理できます。

REST API を使用するには、REST API のサポートを有効にして Kaspersky Endpoint Security をインストールする必要があります。REST クライアントと Kaspersky Endpoint Security は同じコンピューターにインストールしてください。

Kaspersky Endpoint Security および REST クライアントが安全に相互動作するためには：

- 認証されていないアクセスに対する REST クライアントの保護を REST クライアントの開発者の推奨に従って設定します。任意アクセス制御リスト（DACL）を使用して REST クライアントを書き込みから保護します。
- REST クライアントを実行するには、管理者権限を持つ別のアカウントを使用します。このアカウントのシステムへの対話的なサインインをオフにします。

REST API を使用すると、http://127.0.0.1 または http://localhost を経由して製品が管理されます。REST API を使用してリモートで Kaspersky Endpoint Security を管理することはできません。



REST API のドキュメントを開く

REST API の使用を有効にしての本製品のインストール

REST API を使用して製品を管理するには、REST API のサポートを有効にして Kaspersky Endpoint Security をインストールする必要があります。REST API を使用して Kaspersky Endpoint Security を管理する場合、Kaspersky Security Center を使用して製品を管理できなくなります。

REST API のサポートを有効にした製品のインストールの準備

REST クライアントの Kaspersky Endpoint Security との安全な連携には、リクエストの識別の設定が必要です。そのため、証明書をインストールした後に各リクエストのペイロードに署名する必要があります。

証明書の作成には、 OpenSSL などを使用することができます。

例：

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

鍵長が 2048 ビット以上の RSA 暗号化アルゴリズムを使用してください。

この結果、証明書「`cert.pem`」と秘密鍵「`key.pem`」を入手できます。

REST API のサポートを有効にした本製品のインストール

REST API のサポートを有効にして Kaspersky Endpoint Security をインストールするには：

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. Kaspersky Endpoint Security のバージョン 11.2.0 以降の配布パッケージを含むフォルダーに移動します。
3. 次の設定で Kaspersky Endpoint Security をインストールします：

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     REST API による本製品の管理に使用するユーザー名。ユーザー名は、`<DOMAIN>\<UserName>` の形式で入力します（例：`RESTAPI_User=COMPANY\Administrator`）。このアカウントでのみ、REST API を使用して製品を管理できます。REST API を利用するユーザーは 1 人しか選択できません。
   - `RESTAPI_Port=<port>`

     REST API による製品の管理に使用するポート。既定ではポート 6782 が使用されます。ポートが使用されていないことを確認してください。省略可能なパラメータです。
   - `RESTAPI_Certificate=<path to certificate>`

     リクエストを識別するための証明書（例：`RESTAPI_Certificate=C:\cert.pem`）。

     本製品のインストール後または証明書の有効期間が終了した後に証明書をインストールできます。

     REST API リクエストの識別用の証明書をインストールする方法

     1. Kaspersky Endpoint Security セルフディフェンスを無効にします。

        セルフディフェンスは、ハードディスクのアプリケーションファイル、メモリプロセス、およびシステムレジストリのエントリの改竄や削除を防止します。
     2. REST API 設定を含むレジストリキー `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp` に移動します。
     3. 「`Certificate = C:\Folder\cert.pem`」のように、証明書のパスを入力します。
     4. Kaspersky Endpoint Security セルフディフェンスを有効にします。
     5. 本製品を再起動します。
   - `AdminKitConnector=1`

     管理システムを使用した製品管理。既定では管理が許可されています。

setup.ini ファイルを使用して REST API を使用するための設定を指定することもできます。

```
例：
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

これにより、REST API を使用して製品を管理できます。REST API が動作していることを確認するには、GET 要求を使用して REST API のドキュメントを開きます。

例：
```
GET http://localhost:6782/kes/v1/api-docs
```

REST API のサポートを有効にした本製品がインストールされている場合、Kaspersky Endpoint Security はウェブコントロールの設定内で Web リソースへのアクセスの許可ルール（REST API 用のサービスルール）を自動的に作成します。REST API のサポートを有効にした本製品がインストールされている場合、Kaspersky Endpoint Security はウェブコントロールの設定内で Web リソースへのアクセスの許可ルール（*REST API 用のサービスルール*）を自動的に作成します。このルールは REST クライアントの Kaspersky Endpoint Security へのアクセスを常時許可するために必要です。たとえば、ユーザーの Web リソースへのアクセスを制限した場合、REST API 経由でのアプリケーションの管理には影響しません。*REST API 用のサービスルール*の設定の削除や変更は推奨されません。ルールを削除した場合、Kaspersky Endpoint Security は本製品を再起動した際に復元します。

API の使用

パスワードによる保護を使用して、REST API から製品へのアクセスを制限することはできません。たとえば、ユーザーが REST API を使用して保護を無効にしようとした場合、この操作をブロックすることはできません。一方で、REST API を使用してパスワードによる保護を設定し、ローカルインターフェイスを介した製品へのユーザーアクセスを制限することはできます。

REST API を使用して製品を管理するには、REST API のサポートを有効にして製品をインストールし、なおかつそのときに指定したアカウントで REST クライアントを実行する必要があります。REST API を利用するユーザーは 1 人しか選択できません。

REST API のドキュメントを開く

REST API による製品の管理には次の手順があります：

1. 製品設定の現在の値を取得します。これを行うには GET 要求を送信します。
   例：
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```
2. 製品が設定の構文と値を含む応答を送信します。Kaspersky Endpoint Security は XML 形式と JSON 形式をサポートします。
   例：
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```
3. 製品設定を編集します。GET 要求に対する応答で受信した設定の構文を使用します。
   例：
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```
4. 製品設定（ペイロード）を JSON（payload.json）に保存します。

5. PKCS7 形式で JSON に署名します。

```
例：
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
signed_payload.pem
```

その結果、要求のペイロードを持つ署名済みファイルを入手できます（`signed_payload.pem`）。

6. 製品設定を編集します。これを行うには、POST 要求を送信し、要求のペイロードを持つ署名済みファイル（`signed_payload.pem`）を添付します。

本製品は新しい設定を適用し、製品の設定結果を含む応答を送ります（応答は空白にできます）。設定が更新されたかどうかを GET 要求を送信して確認することができます。

製品の情報源

カスペルスキーの Web サイトの Kaspersky Endpoint Security のページ

Kaspersky Endpoint Security のページでは、本製品に関する情報およびその機能や特性についての概要をご確認いただけます。

Kaspersky Endpoint Security のページにはオンラインストアへのリンクがあります。こちらから本製品を購入、または製品ライセンスを更新することができます。

ナレッジベースの Kaspersky Endpoint Security のページ

*ナレッジベース*は、テクニカルサポートサイトにあるセクションの 1 つです。

ナレッジベースの Kaspersky Endpoint Security のページでは、本製品に関する便利な情報や推奨事項、購入、また本製品のインストールおよび使用に関連したよくある質問（FAQ）と回答に関する情報を参照できます。

ナレッジベースの記事では、Kaspersky Endpoint Security に関するお問い合わせだけでなく、カスペルスキー製品に関するお問い合わせに関しても解凍をご確認いただくことができます。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

カスペルスキー製品のフォーラム

特に緊急の対応が必要ではない場合は、カスペルスキー製品のフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、さまざまなトピックで意見交換しています。

このフォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

テクニカルサポートへのお問い合わせ

製品のドキュメントやその他の Kaspersky Endpoint Security の情報源で問題の解決法が見つからない場合、テクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Endpoint Security のインストール方法や使用方法についてのお問い合わせに回答いたします。

サポート対象期間中、カスペルスキーは Kaspersky Endpoint Security のサポートを提供します（製品のライフサイクルページを参照してください）。テクニカルサポートにご連絡いただく前に、「カスペルスキーのサポートサービス規約」をお読みください。

テクニカルサポートへのご連絡方法は次のとおりです：

- テクニカルサポートの Web サイトにアクセスする
- カスペルスキーカンパニーアカウントポータルからカスペルスキーのテクニカルサポートに要求を送信する

カスペルスキーのテクニカルサポートのスペシャリストに問題を報告した後で、*トレースファイル*の作成を要請される場合があります。このトレースファイルを使用して、アプリケーションコマンドの実行プロセスを段階的に追跡し、エラーが発生した製品動作の段階を特定することができます。

また、テクニカルサポートのスペシャリストから、オペレーティングシステムの詳細な情報や、コンピューターで実行中のプロセス、コンポーネントの動作に関する詳細なレポートを要求される場合があります。

診断の実行中、テクニカルサポートの担当者から次の製品設定を変更するよう要求される場合があります：

- 詳細な診断情報を取得する機能の有効化
- 本製品の個々の機能を、特殊な設定変更によって設定する（これらの設定は、通常のインターフェイスでは設定できないようになっています）
- 取得される診断情報を保存する設定の変更
- ネットワークトラフィックの取得およびログの設定

テクニカルサポートの担当者は、これらの操作に必要なすべての情報（操作の順番に関する詳細、変更する設定、設定ファイル、スクリプト、追加のコマンドライン機能、デバッグモジュール、特定の目的のためのユーティリティなど）を提供し、デバッグ用に取得されるデータの範囲についてお知らせします。取得された詳細な診断情報は、クライアントコンピューターに保存されます。このデータがカスペルスキーに自動送信されることはありません。

上記の操作は、テクニカルサポートのスペシャリストの協力のもと、その指示に従って実行する必要があります。オンラインヘルプで説明されていない、もしくはテクニカルサポートの推奨事項にない方法で製品設定を変更すると、動作が遅くなったりオペレーティングシステムをクラッシュする原因になることがあります。また、お使いのコンピューターの保護レベルが下がり、処理中の情報の可用性や整合性を損なう可能性があります。

トレースファイルの内容と保存場所

お客様は、コンピューターに保存されているデータのセキュリティ、特にカスペルスキーに送信されるまでのデータへのアクセス監視および制限の責任を個人的に負います。

トレースファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。

認証エージェントのトレースファイルを除いて、トレースファイルはフォルダー「`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`」に保存されます。

トレースファイルの命名規則は「`KES<12.12_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`」となります。

トレースファイルに保存されたデータを確認できます。

すべてのトレースファイルには、次の共通データが含まれます：

- イベントの日時
- 実行された脅威の数

  認証エージェントのトレースファイルには、この情報は含まれません。

- イベントを発生させたコンポーネント
- イベントの重大度（情報イベント、警告、緊急イベント、エラー）
- コンポーネントによるコマンド実行およびそのコマンドの実行結果を含むイベントの説明

Kaspersky Endpoint Security は、ユーザーパスワードについて、暗号化したかたちでのみトレースファイルに保存します。

SRV.log、GUI.log、ALL.log トレースファイルの内容

`SRV.log`、`GUI.log`、`ALL.log` トレースファイルは、共通データの他に次の情報を保存する場合があります：

- ローカルコンピューターのファイルのパスに含まれている、姓名を含む個人情報。
- コンピューターにインストールされているハードウェアのデータ（BIOS / UEFI　ファームウェアデータなど）。このデータは、Kaspersky Disk Encryption の実行時にトレースファイルに書き込まれます。
- 平文で転送されたユーザー名とパスワード。このデータは、インターネットトラフィックのスキャン中にトレースファイルに記録されることがあります。

- HTTP ヘッダーに含まれているユーザー名とパスワード。
- ファイル名に含まれている Windows アカウント名。
- 検知されたオブジェクトの名前に含まれている、アカウント名およびパスワードを含むメールアドレスまたは Web アドレス。
- アクセスした Web サイトおよびその Web サイトからのリダイレクト。このデータは、Web サイトがスキャンされる際にトレースファイルに書き込まれます。
- プロキシサーバーにサインインするために使用したプロキシサーバーのアドレス、コンピューター名、ポート、IP アドレス、ユーザー名。このデータは、プロキシサーバーを使用する場合にトレースファイルに書き込まれます。
- コンピューターが接続を確立したリモート IP アドレス。
- ソーシャルネットワークにおけるメッセージの件名、ID、送信者名、メッセージを送信した Web サイトのアドレス。このデータは、ウェブコントロールが有効になっている場合にトレースファイルに書き込まれます。
- ネットワークトラフィックデータトラフィック監視コンポーネントが有効になっている場合（Web Control など）、このデータはトレースファイルに書き込まれます。
- Kaspersky サーバーから受信したデータ（ウイルス対策データベースのバージョンなど）。
- Kaspersky Endpoint Security コンポーネントとその動作データのステータス。
- アプリケーションのユーザーの活動に関するデータ。
- オペレーティングシステムのイベント。

HST.log、BL.log、Dumpwriter.log、WD.log、AVPCon.dll.log トレースファイルの内容

`HST.log` トレースファイルには、共通データの他に、定義データベースと製品機能のアップデートタスクの実行に関する情報が含まれます。

`BL.log` トレースファイルには、共通データの他に、本製品の動作中に発生したイベントの情報と、本製品のエラーを解決するために必要なデータが含まれます。このファイルは、本製品が avp.exe -bl パラメータで開始された場合に作成されます。

`Dumpwriter.log` トレースファイルには、共通データの他に、ダンプファイルが書き込まれる際に発生するエラーの解決に必要なサービス情報が含まれます。

`WD.log` トレースファイルには、共通データの他に、製品機能のアップデートイベントを含め、avpsus サービスの操作中に発生したイベントに関する情報が含まれます。

`AVPCon.dll.log` トレースファイルには、共通データの他に、Kaspersky Security Center 接続モジュールの動作中に発生したイベントに関する情報が含まれます。

パフォーマンスのトレースファイルの内容

パフォーマンスのトレースファイルの命名規則は「KES<12.12_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl」となります。

パフォーマンスのトレースファイルには、共通データの他に、プロセッサでの負荷、オペレーティングシステムとアプリケーションの読み込み時間、実行されていたプロセスに関する情報が含まれます。

AMSI 保護機能のトレースファイルの内容

AMSI.log トレースファイルには、共通データの他に、サードパーティ製品の要求に基づいて実行したスキャン結果に関する情報が含まれます。

メール脅威対策のトレースファイルの内容

mcou.OUTLOOK.EXE.log トレースファイルには、共通データの他に、メールアドレスなど、メールメッセージの一部が含まれます。

コンテキストメニューからのスキャンのトレースファイルの内容

shellex.dll.log トレースファイルには、共通データの他に、スキャンタスクの完了に関する情報と、本製品のデバッグに必要なデータが含まれています。

Web プラグインのトレースファイルの内容

本製品の Web プラグインのトレースファイルは、Kaspersky Security Center Web コンソールサーバーを配備しているコンピューターの「Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs」に保存されます。

本製品の Web プラグインのトレースファイルの命名規則は「 logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log」となります。Web コンソールをインストールするとデータの書き込みが始まり、Web コンソールをアンインストールするとトレースファイルも削除されます。

Web プラグインのトレースファイルには、共通データの他に次の情報が含まれます：

- Kaspersky Endpoint Security のインターフェイスのロックを解除するための KLAdmin ユーザーパスワード（パスワードによる保護）。
- Kaspersky Endpoint Security のインターフェイスのロックを解除するための一時パスワード（パスワードによる保護）。

- SMTP メールサーバーのユーザー名とパスワード（メール通知）。
- 内部プロキシサーバーのユーザー名とパスワード（プロキシサーバー）。
- *コンポーネントの変更*タスクのユーザー名とパスワード。
- Kaspersky Endpoint Security のタスクとポリシーのプロパティで指定されているアカウント認証情報とフォルダーやファイルのパス。

認証エージェントのトレースファイルの内容

認証エージェントのトレースファイルは、次の名前でシステムボリューム情報（System Volume Information）フォルダーに保存されます：`KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`。

認証エージェントのトレースファイルには、共通データの他に、認証エージェントの動作および認証エージェントを使用してユーザーにより実行された動作に関する情報が含まれます。

アプリケーションの動作のトレース

*アプリケーションのトレース*とは、製品が実行する処理の詳細な記録と製品の動作中に発生したイベントに関するメッセージです。トレースプロセス中に、本製品はさまざまなアプリケーションコンポーネントの操作に関するデータ（たとえば、SRV.log、WD.log など）が含まれるファイルセットを作成します。

> アプリケーションのトレースは、カスペルスキーのテクニカルサポート担当者の協力のもと、その指示に従いながら実行してください。

アプリケーションのトレースファイルを作成するには：

1. メインウィンドウで、⚙ をクリックします。
2. 表示されたウィンドウで、［**サポートツール**］をクリックします。
3. ［**アプリケーショントレースを有効にする**］トグルスイッチを使用してアプリケーションの操作の追跡を有効または無効にします。
4. ［**トレース**］で、アプリケーションのトレースモードを選択します：
   - **サイズを制限する**：ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。このモードが選択されている場合、ローテーションするファイルセットの最大数と各ファイルセットの最大サイズを定義することができます。

     既定では、アプリケーションは 5 セットのトレースファイルを保存します。各ファイルセットのは 3072 MB です。この場合、トレースファイルを保存するために 15 GB の空きディスク容量が必要です。
   - **サイズを制限しない**：トレースファイルを 1 つ保存します（容量の上限なし）。

5. ［**レベル**］で、トレースレベルを選択します。

   テクニカルサポートのスペシャリストに、必要なトレースレベルを確認してください。テクニカルサポートのガイダンスを受けることができない場合は、トレースレベルを［**通常**］に設定します。

6. Kaspersky Endpoint Security を再起動します。

7. トレースのプロセスを停止するには、［サポートツール］ウィンドウに戻ってトレースを無効にします。

コマンドラインから本製品をインストールする場合も、setup.ini ファイルを使用して設定することで、トレースファイルを作成できます。

製品動作のトレースファイルがフォルダー「`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`」に作成されます。トレースファイルが作成されたら、カスペルスキーのテクニカルサポートに送信してください。

Kaspersky Endpoint Security は本製品が削除される際に自動でトレースファイルを削除します。手動でファイルを削除することもできます。手動でファイルを削除するには、トレースを無効にして本製品を停止する必要があります。

製品のパフォーマンスのトレース

Kaspersky Endpoint Security では、本製品の使用中にコンピューター上で発生した動作エラーや問題に関する情報を取得できます。たとえば、本製品のインストール後にオペレーティングシステムの読み込みが遅くなったなどの問題に関する情報を取得できます。こうした目的のために、Kaspersky Endpoint Security ではパフォーマンスのトレースファイルを作成できます。*パフォーマンスのトレース*では、Kaspersky Endpoint Security のパフォーマンスに関する問題を診断するために、本製品によって実行される処理に関する情報が記録されます。情報の取得には、Windows イベントトレーシングサービス（ETW）が使用されます。Kaspersky Endpoint Security の問題に関する診断と問題の発生原因の特定は、カスペルスキーのテクニカルサポートが担当します。

アプリケーションのトレースは、カスペルスキーのテクニカルサポート担当者の協力のもと、その指示に従いながら実行してください。

パフォーマンスのトレースファイルを作成するには：

1. メインウィンドウで、 をクリックします。

2. 表示されたウィンドウで、［**サポートツール**］をクリックします。

3. ［**パフォーマンストレースを有効にする**］トグルスイッチを使用してアプリケーションのパフォーマンスの追跡を有効または無効にします。

4. ［**トレース**］で、アプリケーションのトレースモードを選択します：

   - **サイズを制限する**：ローテーションを意味し、指定したファイル容量以内のトレースファイルを、指定した個数を上限に保存します。トレースファイルの数が指定した最大数と同じになり、なおかつ書き込み中のファイルのサイズが指定した最大サイズに達すると、最も古いファイルに上書きして新しいトレースファイルを作成します。このモードが選択されている場合、各ファイルの最大サイズを設定できます。

   - **サイズを制限しない**：トレースファイルを 1 つ保存します（容量の上限なし）。

5. ［**レベル**］で、トレースレベルを選択します。

   - **低**：Kaspersky Endpoint Security は、パフォーマンスに関連するオペレーティングシステムの最も重要なプロセスを分析します。

   - **詳細**：Kaspersky Endpoint Security は、パフォーマンスに関連するオペレーティングシステムのすべてのプロセスを分析します。

6. ［**トレース種別**］で、いずれかのトレース種別を選択します：

   - **基本情報**：Kaspersky Endpoint Security は、オペレーティングシステムの実行中にプロセスを分析します。このトレース種別は、オペレーティングシステムの読み込み後に問題が継続して発生する場合（ブラウザーを使用してインターネットにアクセスするときに問題が発生するなど）に使用してください。

   - **再起動時**：Kaspersky Endpoint Security は、オペレーティングシステムの読み込み中にのみプロセスを分析します。オペレーティングシステムの読み込みが完了すると、Kaspersky Endpoint Security はトレースの実行を停止します。オペレーティングシステムの読み込み時の遅延に関する問題が発生している場合は、このトレース種別を使用してください。

7. コンピューターを再起動して、問題の再現を試行してください。

8. トレースのプロセスを停止するには、［サポートツール］ウィンドウに戻ってトレースを無効にします。

   パフォーマンスのトレースファイルがフォルダー「`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`」に作成されます。トレースファイルが作成されたら、カスペルスキーのテクニカルサポートに送信してください。

ダンプ書き込み

ダンプファイルには、ダンプファイルの作成時点で Kaspersky Endpoint Security のプロセスが作業していたメモリについてのすべての情報が含まれます。

> 保存されたダンプファイルには、機密情報が含まれる可能性があります。データへのアクセスを制御するには、ダンプファイルのセキュリティを個別に確保する必要があります。

ダンプファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。ダンプファイルは、フォルダー「`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`」に保存されます。

管理コンソール（MMC）でダンプへの書き込みを有効にする方法

1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。

4. ［**デバッグ情報**］ブロックの［**設定**］をクリックします。

5. 表示されたウィンドウで、［**ダンプへの書き込みを有効にする**］を使用してアプリケーションのダンプ書き込みを有効または無効にします。

6. 変更内容を保存します。

Web コンソールと Cloud コンソールでダンプへの書き込みを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**全般設定**］→［**テクニカルサポート**］に移動します。

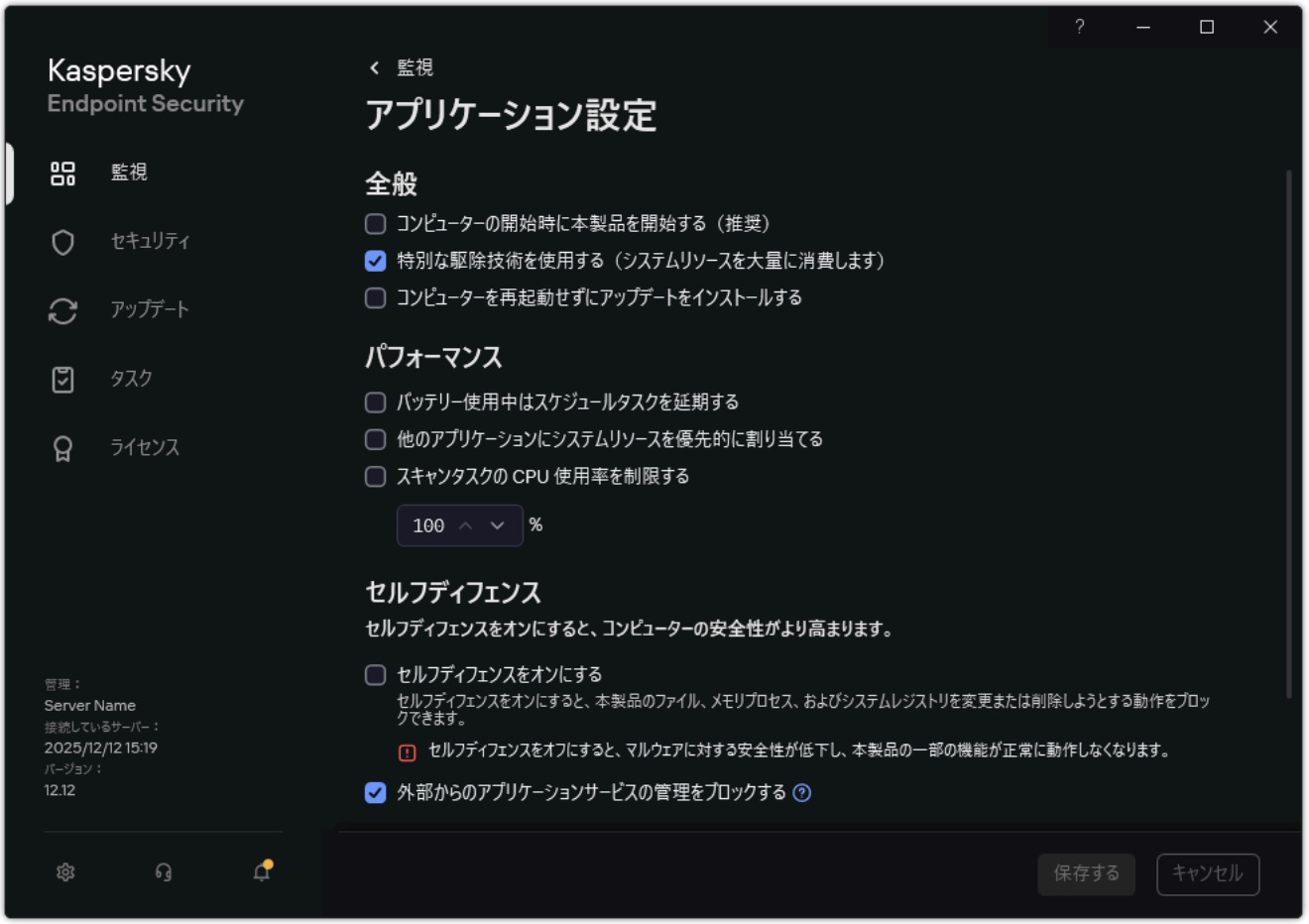
5. ［**デバッグ情報**］ブロックで、［**ダンプへの書き込みは有効です**］を使用してアプリケーションのダンプ書き込みを有効または無効にします。

6. 変更内容を保存します。

製品インターフェイスでダンプへの書き込みを有効にする方法

1. メインウィンドウで、⚙ をクリックします。

2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**デバッグ情報**］ブロックで、［**ダンプへの書き込みを有効にする**］を使用してアプリケーションのダンプ書き込みを有効または無効にします。

4. 変更内容を保存します。

ダンプファイルとトレースファイルの保護

ダンプファイルとトレースファイルには、オペレーティングシステムに関する情報が含まれます。また、ユーザーの個人情報が含まれる場合があります。そのデータに対する不正アクセスを防ぐため、ダンプファイルとトレースファイルの保護を有効にできます。

ダンプファイルとトレースファイルの保護が有効な場合、これらのファイルには次のユーザーがアクセスできます：

- ダンプファイルには、システム管理者と LAN 管理者、およびダンプファイルとトレースファイルの書き出しを有効にしたユーザーがアクセスできます。
- トレースファイルには、システム管理者と LAN 管理者がアクセスできます。

管理コンソール（MMC）でダンプファイルとトレースファイルの保護を有効にする方法

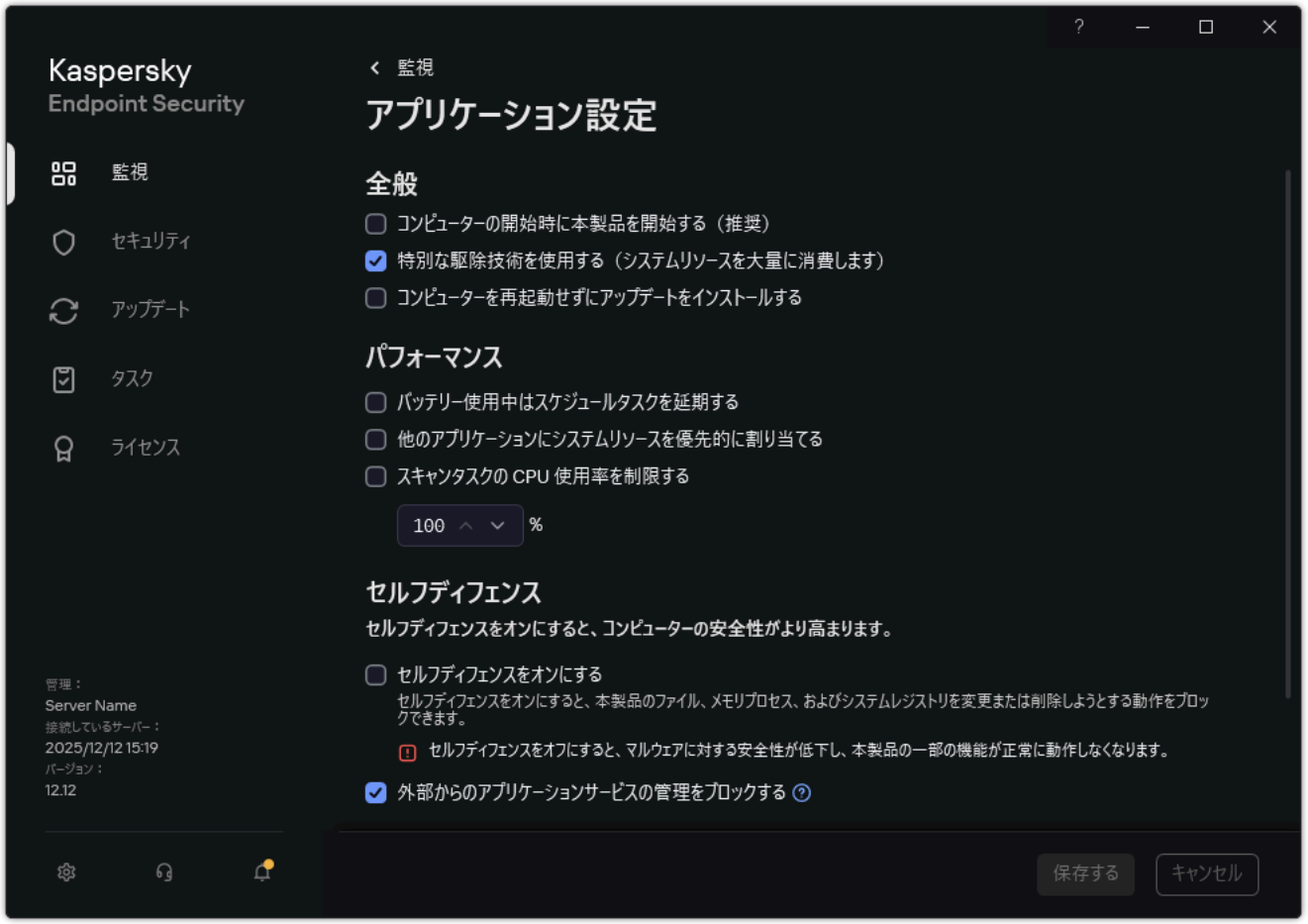
1. Kaspersky Security Center の管理コンソールツリーで、［**ポリシー**］を選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**全般設定**］→［**アプリケーション設定**］の順に選択します。
4. ［**デバッグ情報**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、［**ダンプおよびトレースファイルの保護を有効にする**］を使用してファイルの保護を有効または無効にします。
6. 変更内容を保存します。

Web コンソールと Cloud コンソールでダンプファイルとトレースファイルの保護を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
   ポリシーのプロパティウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**全般設定**］→［**テクニカルサポート**］に移動します。
5. ［**デバッグ情報**］ブロックで、［**ダンプおよびトレースファイルの保護は有効です**］を使用してファイルの保護を有効または無効にします。
6. 変更内容を保存します。

製品インターフェイスでダンプファイルとトレースファイルの保護を有効にする方法

1. メインウィンドウで、⚙をクリックします。
2. 本製品の設定ウィンドウで、［**全般設定**］→［**アプリケーション設定**］を選択します。



Kaspersky Endpoint Security for Windows の設定

3. ［**デバッグ情報**］ブロックで、［**ダンプおよびトレースファイルの保護を有効にする**］を使用してファイルの保護を有効または無効にします。
4. 変更内容を保存します。

保護が有効なときに書き出されたダンプファイルとトレースファイルは、この機能を無効にしても引き続き保護されます。

OS データの取得（Kaspersky Get System Info）

Kaspersky Endpoint Security をインストールした後、オペレーティングシステムまたはアプリケーションが正しく機能しない場合があります。本製品とコンピューターコンポーネントのソフトウェアまたはドライバーの間に競合があります。

問題の原因を特定するために、カスペルスキーのテクニカルサポートは、Kaspersky Get System Info ユーティリティ（以降、「GSI」と表記）からのレポートを要求します。このユーティリティの使用について詳しくは、カスペルスキーのナレッジベースを参照してください。

制限と警告

Kaspersky Endpoint Security には、製品の操作上は重大ではないですがいくつかの制限があります。

本製品のインストール

- Microsoft Windows 10、Microsoft Windows Server 2016 および Microsoft Windows Server 2019 サポートについては、テクニカルサポートサイトのナレッジベースの記事を参照してください。
- Microsoft Windows 11 および Microsoft Windows Server 2022 のサポートについては、テクニカルサポートサイトのナレッジベースの記事を参照してください。
- 感染したコンピューターにインストールされた後、本製品はコンピューターのスキャンを実行する必要があることをユーザーに通知しません。製品のアクティベーションで問題が発生する可能性があります。これらの問題を解決するには、簡易スキャンを実行する必要があります。
- setup.ini および setup.reg ファイルで非 ASCII 文字（たとえばロシア文字など）が使用されていた場合、notepad.exe を使用して編集し、UTF-16LE エンコードで保存する必要があります。その他のエンコーディングはサポートされません。
- インストールパッケージの設定で本製品のインストールパスを指定する際には非 ASCII 文字の使用はサポートされません。
- 製品設定が CFG ファイルからインポートされた場合、Kaspersky Security Network への参加を定義する設定値は適用されません。設定のインポート後、Kaspersky Security Network に関する声明を読み、Kaspersky Security Network への参加の設定に同意してください。製品のインターフェイス、または製品の配信キットに含まれるフォルダーにある ksn_*.txt ファイルで声明の内容を確認できます。
- 暗号化（FLE または FDE）またはデバイスコントロール機能を削除して再インストールする場合は、再インストール前にシステムを再起動する必要があります。
- Microsoft Windows 10 オペレーティングシステムを実行している場合は、ファイルレベルの暗号化（FLE）機能を削除した後にシステムの再起動が必要になります。
- 個別の製品コンポーネントを削除する場合（たとえば*コンポーネントの変更*タスクを使用するなど）、コンピューターの再起動が必要になることがあります。
- *コンポーネントの変更*タスクのプロパティでは、インストールモード（**分離モード / 複合モード**）の切り替え時における、モード間のコンポーネントセットの同期はサポートされていません。モード間のコンポーネントセットの同期は、タスクのプロパティを再度開くと実行されます。
- 本製品のインストールが*名前がないまたは読み込めないアプリケーションがインストールされている*というエラーにより終了することがあります。これは、お使いのコンピューターに互換性のないアプリケーションがあるか、その一部が残っているということを意味します。互換性のない製品の影響を取り除くには、状況の詳細な説明を入力してカスペルスキーのカンパニーアカウントからカスペルスキーのテクニカルサポートにリクエストを送信してください。
- Kaspersky Endpoint Security の削除をキャンセルした場合は、コンピューターを再起動してから本製品の復元を開始してください。
- 本製品の動作には Microsoft .NET Framework 4.0 以降が必要です。Microsoft .NET Framework 4.6.1 には脆弱性があります。Microsoft .NET Framework 4.6.1 を使用している場合は、セキュリティアップデートをインストールする必要があります。Microsoft .NET Framework のセキュリティアップデートに関して詳しくは、Microsoft のテクニカルサポートサイトを参照してください。

- サーバーオペレーティングシステムで選択された Kaspersky Endpoint Agent 機能との本製品のインストールが正常に終了せず、*Windows Installer Coordinator Error* ウィンドウが表示された場合は、Microsoft サポート Web サイトの内容を参照してください。

- 本製品がローカルで対話モードでなくインストールされた場合は、提供されたsetup.ini ファイルを使用してインストールされたコンポーネントを置き換えてください。

- Windows 7 の構成に Kaspersky Endpoint Security for Windows がインストールされた後、Windows Defender は動作を続行します。この場合、システムのパフォーマンスの低下を避けるため、Windows Defender を手動で無効にしてください。

- Kaspersky Endpoint Security for Windows を Kaspersky Security for Windows Server（KSWS）および Windows Defender 製品がインストールされているサーバーにインストールする場合は、システムの再起動が必要です。システムの再起動が不要な製品インストール方法を選択している場合でも、システムの再起動が必要になります。Windows Defender for Windows Server は Kaspersky Endpoint Security for Windows と互換性のない製品のリストに含まれています。本製品のインストール前に、インストーラーは Windows Defender for Windows Server を削除します。互換性のないソフトウェアを削除するには、システムを再起動する必要があります。

- Kaspersky Endpoint Security for Windows（KES）を Kaspersky Security for Windows Server（KSWS）がインストールされたサーバーにインストールするには、KSWS のパスワードによる保護をオフにする必要があります。KSWS から KES への移行後、製品設定でパスワードによる保護を有効にしてください。

- Windows 7 または Veeam Backup & Replication が導入された Windows Server 2008 R2 に本製品をインストールするには、コンピューターを再起動してインストールを再度実行する必要があることがあります。

- パスワードによる保護を有効にしたカスペルスキー スモール オフィス セキュリティ（KSOS）から Kaspersky Endpoint Security（KES）への移行は、KSOS ビルド 21.16.*.* 以降で実行できます。それ以前のバージョンの KSOS を移行するには、パスワードによる保護を無効にするか、KSOS を手動で削除します。パスワードによる保護を無効にした KSOS から KES への移行は、正常に実行されます。

- 起動可能なリムーバブルドライブに Kaspersky Endpoint Security をインストールすることはできません。インストールすると、Kaspersky Endpoint Security で「*インストール先に無効なフォルダーまたはドライブが選択されています。ローカルハードディスクにインストールする必要があります。*」というエラーメッセージが表示されます。サードパーティ製ツールを使用してリムーバブルドライブに本製品をインストールすると、起動プロセス中にオペレーティングシステムがクラッシュ（BSOD）する可能性があります。つまり、Kaspersky Endpoint Security は Windows To Go や同様のソリューションをサポートしていません。リムーバブルドライブからコンピューターをスキャンするには、無料で使用できるレスキューディスク製品を使用できます。

- マルチユーザー RDP セッションがあるターミナルサーバーにネットワークコンポーネントとともに Kaspersky Endpoint Security をインストールする場合は、いくつかの特別な考慮事項があります。管理者セッションが終了すると、オペレーティングシステムはすべてのユーザーセッションを強制的に終了します。ターミナルサーバーに接続するには、サーバーを再起動するか、ローカルでシステムにログインする必要があります。このような挙動は、Windows オペレーティングシステムの動作の特性によって決まります。

- Kaspersky Security Center 16.0 または Kaspersky Security Center 16.1 に、Kaspersky Endpoint Security for Windows （ビルド 12.11.0.2004）および Kaspersky Endpoint Security for Linux （ビルド 12.4.0.1354）の Web プラグインがインストールされている場合、Kaspersky Endpoint Security for Windows Web プラグインをバージョン 12.11.0.6004 にアップデートすると、Kaspersky Endpoint Security for Linux のポリシーが正常に動作しなくなる可能性があります。

  可能な解決策：［**設定**］→［**Web プラグイン**］ウィンドウに移動し、リストから「Kaspersky Endpoint Security for Windows Web Plug-in」「Kaspersky Endpoint Security for Linux Web Plug-in」「Unified Protection and Management Plug-in」を削除してください。その後、まず Kaspersky Endpoint Security for Linux の Web プラグインをインストールし、続いて Kaspersky Endpoint Security for Windows の Web プラグインをインストールしてください。

- Web コンソールで、 Kaspersky Endpoint Security 12.11 for Windows のインストールパッケージのプロパティにコンポーネントのリストが正しく表示されません。別のコンポーネントであるアンチクリプターは、このバージョンの製品では使用できません。外部からの暗号化に対する共有フォルダーの保護は、ふるまい検知コンポーネントに含まれています。Kaspersky Endpoint Security 12.12 for Windows では、この機能は個別のコンポーネントになっています。また、管理コンソール（MMC）では、コンポーネントのリストが正しく表示されます。

本製品のアップグレード

- 本製品のバージョン 11.0.0 から、Kaspersky Endpoint Security for Windows MMC プラグインは、以前のバージョンのプラグインに上書きインストールされるようになりました。以前のバージョンのプラグインに戻すには、現在のプラグインを削除してから以前のバージョンのプラグインをインストールしてください。

- Kaspersky Endpoint Security 11.0.0 または 11.0.1 for Windows をアップグレードする際、*定義データベースと製品機能のアップデート*、*簡易スキャン*、*オブジェクトスキャン*、*アプリケーション整合性チェック*タスクのローカルタスクのスケジュールの設定は保存されません。

- Windows 10 バージョン 1903 および 1909 では、Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3（ビルド 10.3.3.275）、Service Pack 2 Maintenance Release 4（ビルド 10.3.3.304）、ファイルレベルの暗号化（FLE）機能付きの 11.0.0 および 11.0.1 からのアップグレードはエラーで終了することがあります。これは、Windows 10 バージョン 1903 および 1909 でこれらのバージョンの Kaspersky Endpoint Security for Windows がファイルの暗号化をサポートしていないためです。このアップグレードをインストールする前に、ファイル暗号化機能を削除してください。

- 本製品の動作には Microsoft .NET Framework 4.0 以降が必要です。Microsoft .NET Framework 4.6.1 には脆弱性があります。Microsoft .NET Framework 4.6.1 を使用している場合は、セキュリティアップデートをインストールする必要があります。Microsoft .NET Framework のセキュリティアップデートに関して詳しくは、Microsoft のテクニカルサポートサイト を参照してください。

- Kaspersky Endpoint Security のアップグレード時、本製品は Kaspersky Security Network に関する声明が同意されるまで、KSN の使用を無効にします。さらに、*KSN サーバーが使用できません*イベントが受け取られるため、Kaspersky Security Center でコンピューターのステータスが*緊急*に変更されることがあります。Kaspersky Managed Detection and Response を使用している場合、ソリューションの動作で違反に関するイベントを受け取ります。KSN の使用は Kaspersky Managed Detection and Response の操作に必要です。Kaspersky Endpoint Security は、管理者が KSN 利用規約に同意したポリシーの適用後 KSN の使用を有効にします。Kaspersky Security Network に関する声明に同意すると、Kaspersky Endpoint Security は動作を再開します。

- Kaspersky Endpoint Security を 11.10.0 以降のバージョンに再起動せずにアップグレードした後、コンピューターには 2 つの Kaspersky Endpoint Security がインストールされることになります。古いバージョンの製品を手動で削除しないでください。コンピューターが再起動されると、古いバージョンの製品は自動的に削除されます。

- Microsoft Windows 11 を実行するコンピューターで Kaspersky Endpoint Security をアップグレードした後で、ファイルコンテキストメニューにアップグレード前とアップグレード後の両バージョンのアイテムが表示される場合があります。ファイルコンテキストメニューを正しく動作させるには、コンピューターの再起動を 2 回行ってください。

- 製品のセルフディフェンスがオフになっており、すべてのネットワークアダプターが停止している場合、製品のアップグレードが終了してからコンピューターが再起動するまでの間、製品のネットワークコンポーネントが動作しません。このネットワークコンポーネントには、ウェブ脅威対策、メール脅威対策、ネットワーク脅威対策、ファイアウォール、ホスト侵入防止、およびウェブコントロールが含まれます。製品を正しく動作させるには、コンピューターを再起動してください。

- 製品のアップグレードが終了してからコンピューターが再起動するまでの間は、有害 USB 攻撃ブロックコンポーネントが動作しません。製品を正しく動作させるには、コンピューターを再起動してください。

- 前回のアップグレード後にコンピューターの再起動をスキップした場合、製品をアップグレードすることはできません。製品を正しく動作させるには、コンピューターを再起動してください。

- Kaspersky Endpoint Security 11 for Windows より以前のバージョンから本製品がアップグレードされた場合、コンピューターを再起動する必要があります。

- Kaspersky Security Center Cloud コンソールを使用して Kaspersky Endpoint Security を管理する場合、ローカルで本製品をアップデートすることはできません。ローカルで本製品をアップデートする場合、Kaspersky Security Center Cloud コンソールのデータ処理契約に同意することはできません。

サーバープラットフォームのサポート

- *データの重複排除*が有効になっているサーバーで、ファイル fsdmhost.exe を 信頼するアプリケーションのリストに追加する必要があります。これにより、アプリケーションのパフォーマンスが最適化され、CPU への過度の負荷を防ぐことができます。

- ReFS ファイルシステムは次の制限付きでサポートされます：

  - Kaspersky Endpoint Security が脅威の駆除イベントを正しく処理しないことがあります。たとえば、本製品が悪意のあるファイルを削除した際に、レポートにはオブジェクトが処理されていないと記載されることがあります。一方、Kaspersky Endpoint Security は製品の設定に従って脅威を駆除します。また、Kaspersky Endpoint Security は同じオブジェクトに対して*オブジェクトが再起動時に駆除されます*イベントを重複して作成することがあります。

  - ファイル脅威対策は一部の脅威をスキップする可能性があります。一方、マルウェアのスキャンは正常に作動します。

  - *マルウェアのスキャン*タスクが開始された後、iChecker で追加された除外リストはサーバーの再起動時にリセットされます。

  - iSwift はサポートされません。iSwift を使用して追加されたスキャンの除外リストは認識されません。

  - Kaspersky Endpoint Security がインストールされるより前にコンピューター上に meicar.exe ファイルが存在した場合は、eicar.com および susp-eicar.com ファイルは検出されません。

  - 脅威の駆除に関する通知を誤って表示することがあります。たとえば、以前に駆除した脅威に関する通知を表示することがあります。

- ファイルレベルの暗号化（FLE）と Kaspersky Disk Encryption（FDE）技術は、サーバープラットフォームではサポートされません。また、Kaspersky Endpoint Security はデータ暗号化イベントを誤って処理することがあります。

- サーバーオペレーティングシステムでは、特別な駆除の必要性についての警告は表示されません。

- Microsoft Windows Server 2008 はサポート対象外となりました。Microsoft Windows Server 2008 オペレーティングシステムを実行するコンピューターへの本製品のインストールはサポートされません。

- Kaspersky Endpoint Security を Microsoft Data Protection Manager（DPM）が導入されたサーバーにインストールすると、DPM に不具合が発生することがあります。これは DPM の動作の制限事項に関連するものです。不具合を解消するには、ファイル脅威対策機能と *マルウェアのスキャン*でローカルサーバーを除外リストに追加する必要があります。

- Server Core モードは次の制限付きでサポートされます：

  - 通知、ポップアップ通知、その他のインターフェイスコントロールを含む、ローカルのグラフィカルユーザーインターフェイスは利用できません。次のウィンドウを含む入力ウィンドウは表示できません：

    - 製品のバージョンおよびモジュールアップグレードの確認
    - コンピューターの再起動要求
    - プロキシサーバー認証の入力
    - 端末にアクセスする入力（デバイスコントロール）

  - 次の機能は利用できません：ウェブ脅威対策、メール脅威対策、ウェブコントロール、有害 USB 攻撃ブロック。
  - アンチブリッジは使用できません。
  - Kaspersky Security Center コンソールのアプリケーションポリシー内でのみ Kaspersky Security Network に関する声明に同意することができます。
  - BitLocker ドライブ暗号化は Trusted Platform Module（TPM）でのみ利用できます。本製品はパスワード入力ウィンドウを起動前認証で表示できないため、暗号化に PIN またはパスワードは使用できません。コンピューターのオペレーティングシステムで連邦情報処理標準（FIPS）準拠モードが有効になっている場合、ドライブの暗号化を開始する前に暗号化鍵を保存するためのリムーバブルドライブを接続してください。

仮想プラットフォームのサポート

- Hyper-V 仮想マシンでのディスク全体の暗号化（FDE）はサポートされていません。
- Citrix 仮想プラットフォームでのディスク全体の暗号化（FDE）はサポートされていません。
- Windows 10 Enterprise のマルチセッションは次の制限付きでサポートされます：

  - サーバー上でアクティブな脅威を駆除する場合と同様に、Kaspersky Endpoint Security はアクティブな脅威をユーザーに通知せずに駆除します。オペレーティングシステムはマルチセッションモードで継続して実行されており、脅威が直ちに駆除されないとその他のアクティブなユーザーのデータが失われる可能性があるためです。
  - ディスク全体の暗号化（FDE）はサポートされません。
  - BitLocker の管理はサポートされません。
  - リムーバブルドライブでの Kaspersky Endpoint Security の使用はサポートされません。Microsoft Azure インフラストラクチャはリムーバブルドライブをネットワークドライブとして定義します。

- Citrix 仮想プラットフォームでのファイルレベルの暗号化（FLE）のインストールおよび使用はサポートされていません。

- Kaspersky Endpoint Security for Windows と Citrix PVS の互換性をサポートするには、［**Citrix PVS との互換性を確保する**］を有効にしてください。このオプションはインストールウィザードまたはコマンドラインのパラメータ「`/pCITRIXCOMPATIBILITY=1`」を使用して有効にすることが可能です。リモートインストールの場合は、KUD ファイルを編集して次のパラメータを追加する必要があります：`/pCITRIXCOMPATIBILITY=1`。

- Citrix XenDesktop：vDisk を使用する仮想マシンを複製するため、複製の開始前に、セルフディフェンスを無効にする必要があります。

- Citrix XenDesktop で Kaspersky Endpoint Security for Windows および Kaspersky Security Center Network Agent がプリインストールされたマスターイメージのテンプレートを準備する際、設定ファイルに次の種別の除外リストを追加してください：

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Citrix XenDesktop の詳細については、Citrix のサポートサイトを参照してください。

- VMware ESXi ハイパーバイザー上で配備された仮想マシン上で、リムーバブルドライブの安全な接続解除が正常に完了しないことがあります。再度安全な接続解除を実行してください。

- Kaspersky Endpoint Security は VMware ESXi ハイパーバイザーと共存できますが、次の制限があります：

  - Kaspersky Endpoint Security は、Guest Introspection ドライバー（vnetWFP.sys、vnetFLT.sys など）に対応していない可能性があります。非対応を解決するには、ドライバーを最新バージョンにアップデートするか、ドライバーをアンインストールします。

  - 場合によっては、仮想マシンでリムーバブルディスクを安全に取り外そうとすると、失敗することがあります。再度安全な接続解除を実行してください。

- Citrix VDA エージェントを搭載した仮想マシンに Kaspersky Endpoint Security をインストールすると、互換性エラーが発生する可能性があります。これは、Citrix Provisioning Services とアンチウイルスソリューションとの互換性に制限があるために発生します。Citrix Provisioning Services とアンチウイルスソリューションを併用する際のベストプラクティスについては、Citrix のサポートサイトを参照してください。

- Kaspersky Endpoint Security は、ドライブが Citrix ハイパーバイザー上の仮想マシンに接続されている場合、リムーバブルドライブのスキャンをスキップします（*リムーバブルドライブのスキャンタスク*）。このようなデバイスでは、オペレーティングシステムは接続されたリムーバブルドライブをネットワークドライブとして検出します。このような場合、*カスタムスキャンタスク*を使用できます。本製品の動作は、標準モードと Light Agent モードで同じです。

- Citrix App Layering テクノロジーを使用するインフラストラクチャ内の仮想マシンに Kaspersky Endpoint Security がインストールされている場合、本製品が感染を検出して［*オブジェクトが再起動時に削除されます*］という状態になっているファイルは、仮想マシンの再起動時に自動的に削除されません。

  このようなファイルを削除するには、Citrix App Layering 管理者のコンピューター上で、ユーザーレイヤーを含む VHDX ファイルをマウントし、マウントされたディスクに対してマルウェアのスキャンを実行する必要があります。

Kaspersky Security Center との互換性

- Kaspersky Security Center Web コンソールのバージョン 14.1 以前では、管理サーバープロパティのユーザーアクセス権限設定セクションに、ログ監視およびファイル変更監視コンポーネントの機能領域の名前が正しく表示されません。

- Kaspersky Security Center Linux は、Kaspersky Endpoint Security を限定的にサポートします。サポートの制限について詳しくは、Kaspersky Security Center Linux 14.2 のオンラインヘルプを参照してください。

- アプリケーションの修復後、管理サーバーへのコンピューターの接続の保護が無効になります。アプリケーションの修復後、*管理サーバーの接続の保護*タスクを再度実行してください。

- Kaspersky Security Center 15.1 では、数週間間隔でタスクを実行できます（[**曜日ごと**] のスケジュール）。Kaspersky Endpoint Security は、複数週間隔でのタスクの実行をサポートしていません。Kaspersky Endpoint Security のタスクを数週間間隔で実行するようにスケジュール設定している場合、指定された日時に毎週そのタスクが実行されます。

- Kaspersky Security Center 管理コンソールでは、[**ユーザーまたはユーザーグループを選択してください**] ウィンドウには、Kaspersky Security Center ユーザーのリストの最初の 50,000 人のユーザーのみが表示されます。詳細については、Kaspersky Security Center のヘルプを参照してください。

ライセンス管理

- 「*データの取得でエラーが発生しました*」というシステムメッセージが表示された場合、アクティベーションを実行しているコンピューターがネットワークに接続されているかどうかを確認するか、また Kaspersky Security Center Activation Proxy 経由でのアクティベーション設定を設定してください。

- 製品のインターフェイスで、ライセンスの有効期間はコンピューターのローカル時刻で表示されます。

- インターネットアクセスが安定していない状況にあるコンピューターに埋め込みライセンスで本製品をインストールしようとすると、本製品がアクティベートされていない、またはライセンスで機能の動作が制限されているというイベントが一時的に表示されることがあります。これは、インストール処理中に、本製品が埋め込みの試用ライセンスを最初にアクティベートすることが原因で発生します。インターネットアクセスが必要です。

- 試用期間中は、インターネット接続が不安定な環境でアップグレードまたはパッチをインストールしようとすると、本製品がアクティベートされていないというイベントが一時的に表示されることがあります。これは、アップデートのインストール処理中に、本製品が埋め込みの試用ライセンスを最初にアクティベートすることが原因で発生します。インターネットアクセスが必要です。

- 試用版のライセンスが本製品のインストール中に自動的にアクティベートされて、それからライセンス情報を保存せずに本製品をアンインストールすると、本製品の再インストール時には試用版のライセンスが自動で適用されることはありません。この場合は手動で本製品をアクティベートしてください。

- Kaspersky Security Center のバージョン 11 と Kaspersky Endpoint Security のバージョン 12.12 を使用している場合、機能のパフォーマンスレポートは誤動作する可能性があります。お使いのライセンスに含まれない Kaspersky Endpoint Security をインストールしている場合、ネットワークエージェントは Windows イベントログにコンポーネントのステータスエラーを書き込むことがあります。このようなエラーを避けるには、ライセンスに含まれない機能を削除してください。

メール脅威対策

- メール脅威対策の Microsoft Outlook のアドインでメールをスキャンする際、Exchange キャッシュモードの使用オプションで Exchange キャッシュモードを使用してください。

- Kaspersky Endpoint Security は 64 ビットの MS Outlook メールクライアントはサポートしません。つまり、64 ビットの MS Outlook がコンピューターにインストールされていて、スキャン範囲にメールが含まれている場合でも、Kaspersky Endpoint Security は 64 ビットの MS Outlook のファイル（PST および OST ファイル）をスキャンしません。

修復エンジン

- 本製品では、NTFS ファイルシステムまたは FAT32 ファイルシステムを使用しているデバイス上のファイルのみを修復できます。

- 本製品を使用して次の拡張子のファイルを修復できます：ods、odp、odm、odc、odb、doc、docx、docm、wps、xls、xlsx、xlsm、xlsb、xlk、ppt、pptx、pptm、mdb、accdb、pst、dwg、dxf、dxg、wpd、rtf、wb2、pdf、mdf、dbf、psd、pdd、eps、ai、indd、cdr、jpg、jpe、dng、3fr、arw、srf、sr2、bay、crw、cr2、dcr、kdc、erf、mef、mrw、nef、nrw、orf、raf、raw、rwl、rw2、r3d、ptx、pef、srw、x3f、der、cer、crt、pem、pfx、p12、p7b、p7c、1cd。

- ネットワークドライブまたは再書き込み可能な CD / DVD 上に保存されているファイルは修復できません。

- 暗号化ファイルシステム（EFS）を使用して暗号化されたファイルは修復できません。EFS の動作について詳しくは、Microsoft の Web サイトの情報を参照してください。

- 本製品では、オペレーティングシステムのカーネルレベルのプロセスで実行されたファイル変更は監視されません。

- 本製品では、ネットワークインターフェイスを経由して行われたファイル変更は監視されません（例：ファイルが共有フォルダーに保存されていて、プロセスが別のコンピューターからリモートで起動された場合など）。

ファイアウォール

- ネットワークパケットルールまたはアプリケーションネットワークルールで DNS 名が指定されている場合、Kaspersky Endpoint Security はこれらのリソースの IP アドレスを特定するために DNS サーバーに要求を送信することがあります。ファイアウォールは IP アドレスを使用してネットワーク動作を監視します。したがって、本製品では DNS 名が IP アドレスに解決されます。LAN コンピューターまたは内部サービスに対しては、ルールの DNS 名のみを使用することを推奨します。

- すべての IPv6 アドレスにルールを指定するには、::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff のアドレス範囲を追加します。ファイアウォールは ::/0 のマスクをサポートしていません。

- ローカルアドレス、物理インターフェイスおよびパケットの最大生存時間（TTL）によるパケットまたは接続のフィルタリングは次のケースでサポートされます：

  - 送信パケットまたはアプリケーションルール内の TCP および UDP、パケットルールの接続のローカルアドレス

  - 受信パケットまたはブロックアプリケーションルールまたはパケットルール内の接続（UDP を除く）のローカルアドレス

  - 受信および送信パケットのブロックパケットルール内のパケットの最大生存時間（TTL）

  - 受信および送信パケットまたはパケットルール内の接続のネットワークインターフェイス

- 許可するパケットルールにネットワークアダプターまたはパケットの最大生存時間（TTL）を設定していた場合は、このルールの優先度はブロックするアプリケーションルールより低くなります。たとえば、アプリケーションが*強い制限付き*の信頼グループに入っていてネットワーク動作がブロックされていた場合、これらの設定をしたパケットルールを使用してアプリケーションのネットワークの動作を許可することはできません。その他の場合は、パケットルールの優先度はアプリケーションネットワークルールより高くなります。

- ファイアウォールのパケットルールをインポートする際、Kaspersky Endpoint Security がルール名を変更することがあります。本製品は主要なパラメータ（プロトコル、方向、リモートおよびローカルポート、パケット最大生存時間（TTL））のセットでルールを決定します。この主要なパラメータのセットが複数のルール間で同一である場合、本製品は同じ名前を割り当てるか、名前にパラメータのタグを追加します。このように、Kaspersky Endpoint Security はすべてのパケットルールをインポートしますが、主要なパラメータが同一であるルールの名前が変更されることがあります。

- アプリケーションを別の信頼グループに移動する際のネットワークルール内で製品イベントのレポートを有効にしている場合、この信頼グループの制限は適用されません。このため、アプリケーションが信頼済みのグループに属している場合、ネットワークの制限はありません。次に、イベントのレポートを有効にして*ブロック*グループに移動したとします。ファイアウォールはこのアプリケーションに対してネットワーク制限を適用しません。最初にアプリケーションを適切な信頼グループに移動してからイベントのレポートを有効にしてください。この方法が適切でない場合は、ネットワークルール内でアプリケーションの制限を手動で設定してください。制限はアプリケーションのローカルインターフェイスに対してのみ適用されます。ポリシー内でのアプリケーションの信頼グループ間の移動は正常に動作します。

- ファイアウォールと侵入防止機能には、アプリケーション権限と保護対象のリソースという共通の設定があります。ファイアウォールのこれらの設定を変更した場合、Kaspersky Endpoint Security は自動的に侵入防止に新しい設定を適応します。たとえば、ファイアウォールポリシーの全般設定の変更を許可した場合（鍵が開いた状態）、侵入防止も同様に編集可能となります。

- Kaspersky Endpoint Security 11.6.0 以前のバージョンでネットワークパケットルールが適用された時、ファイアウォールのレポートの［**アプリケーション名**］列に *Kaspersky Endpoint Security* の値が常に表示されます。また、すべてのアプリケーションの接続をパケットレベルでブロックします。この動作は Kaspersky Endpoint Security 11.7.0 以降のバージョンでは修正されています。［**ルール種別**］列がファイアウォールのレポートに追加されました。ネットワークパケットルールが適用されると、［**アプリケーション名**］列の値は空白のままになります。

- ファイアウォールを使用してすべてのネットワーク動作を禁止した場合、ネットワーク脅威対策コンポーネントによってポートのスキャンの種別の攻撃が検知される可能性があります。これは、ファイアウォールの前にネットワーク脅威対策が起動されて、ネットワーク内の疑わしい動作が検知されることによって発生する可能性があります。

有害 USB 攻撃ブロック

- Kaspersky Endpoint Security はコンピューターがロック（時間が経過して画面がロックされるなど）されると、USB デバイスのタイムアウトをリセットします。USB デバイスの認証コードを複数回誤って入力し、本製品によって USB デバイスがロックされた場合、コンピューターのロック解除後に再度認証コードを入力することができるようになります。この場合、Kaspersky Endpoint Security は有害 USB 攻撃ブロックの設定で指定された時間 USB をロックしないことになります。

- Kaspersky Endpoint Security はコンピューターの保護機能が一時停止した場合に USB デバイスのロックをリセットします。USB デバイスの認証コードを複数回誤って入力し、本製品によって USB デバイスがロックされた場合、コンピューターの保護機能の再開後に再度認証コードを入力することができるようになります。この場合、Kaspersky Endpoint Security は有害 USB 攻撃ブロックの設定で指定された時間 USB をロックしないことになります。

Kaspersky Security Network

- Kaspersky Endpoint Security は、KSN プロキシに接続する際（KSN プロキシの接続設定で［**HTTPS を使用する**］がオンにされている場合）、サーバーのアドレスに非ラテン文字（ASCII 以外の記号）が含まれている場合、HTTPS をサポートしません。

- Kaspersky Security Center では、グローバル Kaspersky Security Network からプライベート Kaspersky Security Network（KPSN）の使用に切り替えたりその逆に切り替えたりする際に、特定の製品のポリシー内の Kaspersky Security Network への参加設定のオプションが無効になります。切り替え後、Kaspersky Security Network に関する声明を読み、KSN への参加の設定に同意してください。声明の内容については、製品のインターフェイスから、または製品ポリシーの編集時に確認することができます。

- Kaspersky Endpoint Security は、テキストファイル（マクロを含まない TXT、CSV、LOG、DOCX ファイルなど）をスキャン対象として Kaspersky Security Network に送信することはありません。本製品は、脅威となる可能性のあるファイルをスキャン対象として KSN に送信します。これらのファイルには、実行ファイルや、実行コード（DOCX ファイルのマクロなど）を含む可能性のあるファイルなどが挙げられます。本製品のその他のコンポーネントは、テキストファイルのスキャンを実行します。ファイルコンテキストメニューからテキストファイルの評価を手動で確認することもできます。テキストファイルに「*ブロック*」の評価がある場合、本製品は、検知された脅威に対して定義された処理を無視します。

- Kaspersky Endpoint Security 12.9 for Windows 以降では、KPSN からグローバル KSN に切り替える際に、Kaspersky Security Network に関する声明への同意を再確認する必要があります。これを行うには、ポリシーのプロパティまたは製品インターフェイスで Kaspersky Security Network の使用を有効にして、Kaspersky Security Network に関する声明への同意を確認する必要があります。既にグローバル KSN を使用している場合は、まず KSN の使用を無効にしてから再度有効にして、Kaspersky Security Network に関する声明への同意を確認する必要があります。Kaspersky Security Network に関する声明に同意しない場合、本製品は Kaspersky Security Network のデータにアクセスできません。

アプリケーションコントロール

- ハードウェアの最小要件を満たし、Microsoft Windows 10 で動作しているコンピューター上で Kaspersky Endpoint Security が実行されている時にアプリケーションコントロールルールを操作する場合、複数のカテゴリにわたるアプリケーションに対する対象条件や除外条件を、合計 100,000 個を超えて追加することは推奨されません。

- Kaspersky Security Center Web コンソールでアプリケーションコントロールルールを操作する場合、ZIP 形式のアーカイブのみがサポートされます。RAR や 7z など、他の形式のアーカイブはサポートされていません。管理コンソール（MMC）でアプリケーションコントロールルールを操作する場合、このような制限はありません。

- Kaspersky Security Center Web コンソールでアプリケーションコントロールルールを操作する場合、アップロードできるファイルの最大サイズは 104 MB です。管理コンソール（MMC）でアプリケーションコントロールルールを操作する場合、このような制限はありません。

- Microsoft Windows 10 でアプリケーションの拒否リストモードでの動作中に、ブロックルールが誤って適用されてしまい、ルールで指定されていないアプリケーションがブロックされてしまうことがあります。

- Kaspersky Endpoint Security をアップグレードする際に新しい*定義済みのアプリケーションコントロールルール*を追加した場合は、これらのルールを以前のバージョンのアプリケーションに適用することはできません。

- プログレッシブウェブアプリ（PWA）がアプリケーションコントロール機能でブロックされた際に、appManifest.xml がレポート内でブロックされたアプリとして表示されます。

- 標準のメモ帳（Notepad）を Windows 11 のアプリケーションコントロールルールに追加する場合は、アプリケーションのパスを指定しないでください。Windows 11 を実行しているコンピューターでは、オペレーティングシステムは `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` にある Metro のメモ帳を使用しています。オペレーティングシステムの以前のバージョンでは、メモ帳は次のフォルダーにありました：

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  アプリケーションコントロールルールにメモ帳を追加する場合は、製品名や実行中のファイルのプロパティからのファイルのハッシュなどから指定します。

- カテゴリ名に禁止文字（`'` `*` `<` `>` `?` `\` `:` `|`）が含まれている場合、KSWS ポリシーを KES ポリシープロファイルに移行する際に、ポリシーとタスクのバッチ変換ウィザード（移行ウィザード）により、アプリケーションカテゴリの名前が変更されます。移行ウィザードにより、これらの文字が「`_`」文字に上書きされます。例えば、アプリケーションカテゴリ「`KSWS::\Everyone:[C61F-3B7C-4D89-96A1]`」は、「`KSWS_Everyone_[C61F-3B7C-4D89-96A1]`」に名前が変更されます。

デバイスコントロール

- Kaspersky Endpoint Security は、外部デバイスの接続イベントと切断イベントを記録できます。Windows サービスは、システムユーザーアカウントを使用してデバイスを接続または切断します。このため、デバイスを接続または切断したユーザーを知ることが不可能になります。Kaspersky Endpoint Security は、イベントに SYSTEM ユーザーアカウントを指定します。

- 信頼するリストに追加されたプリンタデバイスへのアクセスが、デバイスおよびバスブロックルールによりブロックされます。

- MTP デバイスでは、オペレーティングシステムの組み込み Microsoft ドライバーを使用している場合は読み取り、書き込み、および接続のコントロールがサポートされます。ユーザーがデバイスで作業するために（iTunes または Android Debug Bridge の一部としてなど）カスタムドライバーをインストールする場合、読み取りおよび書き込み操作は機能しないことがあります。

- MTP デバイスで作業する際、デバイスへ再接続したあとにアクセスルールが変更されます。

- デバイスコントロール機能は、監視対象デバイスに関連するイベント（デバイスからファイルを読み取り、ファイルをデバイスに書き込む、またその他のイベントのようなデバイスに接続したり接続を解除したりするイベント）を登録します。Kaspersky Endpoint Security は、次のデバイス種別に対する接続解除イベントのみを登録します：[ポータブルデバイス（MTP）]、[リムーバブルドライブ]、[フロッピーディスク]、[CD/DVD ドライブ]。他のデバイス種別の場合、接続解除イベントは登録されません。本製品は、デバイスをコンピューターに接続する操作をすべてのデバイス種別について登録します。

- デバイスを、ID に含まれるが機種名に含まれない文字を使用した機種のマスクで信頼リストに追加しようとすると、追加されません。ワークステーションでは、デバイスは ID のマスクに基づいた信頼リストに追加されます。

- コンピューターを再起動せずに製品をアップグレードした場合、デバイスコントロールは再接続されたデバイスにアクセスルールを適用しません。ただし、デバイスがアップグレード前に接続されていた場合、デバイスコントロールはルールを正しく適用します。再接続されたデバイスを製品が正しく処理できるようにするには、コンピューターを再起動してください。

- Kaspersky Endpoint Security のバージョン 12.0 がインストールされているコンピューターでは、デバイス種別［**ネットワークプリンター**］のアクセスモード［**許可（ログ記録なし）**］は、Kaspersky Endpoint Security のバージョン 12.1 のポリシーが適用されている場合は［**接続バスに依存**］となります。これらのモードでは、本製品は同様の操作を実行します。Kaspersky Endpoint Security のバージョン 12.1 では、ネットワークプリンターのアクセスモードは、［**許可（ログ記録なし）**］となります。

- Kaspersky Endpoint Security 12.0 for Windows から、プリンターの印刷ルールを設定できるようになりました（印刷コントロール）。印刷コントロールを備えたアプリケーションをインストールした後、または印刷コントロールを備えたアプリケーションにアップグレードした後は、コンピューターを再起動する必要があります。コンピューターが再起動するまでは、Kaspersky Endpoint Security は印刷ルールを適用せず、プリンターへのアクセスのみを制御することができます。コンピュータ-の再起動が組織内のワークフローに悪影響を及ぼす場合は、spoolsv サービス（Print Spooler）のみを再起動することができます。

- Kaspersky Endpoint Security 12.0 for Windows から、本製品で **Wi-Fi** タイプのデバイス用に WPA3 プロトコルがサポートされています。Kaspersky Endpoint Security のバージョン 12.2 のポリシーがコンピューターに適用されている場合、Kaspersky Endpoint Security 11.11.0 以前のバージョンがインストールされたコンピューターには WPA2 プロトコルが選択されます。バージョン 12.0 から 12.1 には WPA2/WPA3 が選択され、12.2 以降のバージョンには WPA3 が選択されます。

- Apple デバイスはポータブルデバイス（MTP）、iTunes デバイスとして分類されます。オペレーティングシステムが Apple デバイスの接続を誤って識別し、Apple デバイスがポータブルデバイス（MTP）として認識されないことがあります。このため、Apple デバイスはファイルマネージャーで利用できず、iTunes アプリケーションではアクセスできる状態になります。このため、Kaspersky Endpoint Security は、iTunes アプリケーション経由でのみ Apple デバイスへのアクセスをコントロールします。ポータブルデバイス（MTP）として Apple デバイスにアクセスするには、デバイスマネージャーを開いて USB コントローラーの一覧から Apple Mobile Device USB Driver を削除する必要があります。コンピューターの再起動後、オペレーティングシステムは Apple デバイスをポータブルデバイス（MTP）と iTunes デバイスとして識別します。Kaspersky Endpoint Security はデバイスへのアクセスを iTunes アプリケーションおよびファイルマネージャーの両方でコントロールします。

- Kaspersky Endpoint Security 12.3 for Windows では、デバイス種別が **Bluetooth** の場合、アクセスの設定が異なります。製品の前のバージョンで［**接続バスに依存**］の値を指定していた場合、バージョン 12.3 へのアップグレード後、設定値が［**許可（ログ記録なし）**］に変わります。これによりデバイスの動作に変更はありません。

- デバイスコントロールは Microsoft Windows Bluetooth スタックを通じてのみ、Bluetooth デバイスをサポートします。デバイスコントロールはサードパーティ製 Bluetooth スタックでは正しく機能しない可能性があります。

- Bluetooth デバイスでデバイスクラス（COD）が隠されているか偽装されている場合、デバイスコントロールが正しく機能しない可能性があります。

- 特定の Realtek Bluetooth ドングルドライバーを搭載した Windows 7 または Windows 8 コンピューターでは、入力デバイス（HID クラス）としてのみ Bluetooth デバイスの接続を許可することができない可能性があります。つまり、アプリケーション設定で Bluetooth デバイスへのアクセスを禁止し、入力デバイスを除外リストに追加した場合、デバイスコントロールは代わりにすべての Bluetooth デバイスへのアクセスを禁止する可能性があります。

ウェブコントロール

- OGV および WEBM 形式はサポートされません。

- RTMP プロトコルはサポートされません。

- ウェブコントロールは WSL1 のみをサポートします。本製品は WSL2 トラフィックを制御しません。

アダプティブアノマリーコントロール

- イベントに基づいて自動で除外リストを作成することをお勧めします。手動で除外リストを追加する際、対象オブジェクトの指定時に「*」をパスの先頭に追加してください。
- サンプルの名前が 1 つでも 260 文字を超える場合はアダプティブアノマリーコントロールルールのレポートは作成できません。
- 対象のオブジェクトのパスなど、オブジェクトやプロセスのプロパティに 256 文字以上の値を持つ場合は、アダプティブアノマリーコントロールルール適用条件リポジトリからの除外の追加はサポートされません。ポリシーの設定で手動で除外を追加できます。また、適用されたアダプティブアノマリーコントロールルールの適用に関するレポートで除外を追加することもできます。
- Kaspersky Security Center 15.1 では、特定のルールに対する詳細な**アダプティブアノマリーコントロールルールのステータスに関するレポート**を生成することはできません。

ドライブの暗号化（FDE）

- 本製品のインストール後、ハードドライブの暗号化が正常に動作するためにオペレーティングシステムの再起動を吸う必要があります。
- 認証エージェントでは記号や特殊文字、| および \ はサポートされません。
- 暗号化後のコンピューターのパフォーマンスを最適に保つため、プロセッサは AES-NI (Intel Advanced Encryption Standard New Instructions) 命令セットをサポートする必要があります。プロセッサが AES-NI をサポートしていない場合、コンピューターのパフォーマンスが低下することがあります。
- 暗号化されたデバイスに本製品がアクセス権を付与する前にプロセスがアクセスしようとすると、本製品はこのようなプロセスを中断するよう警告を表示します。プロセスが中断されない場合、暗号化デバイスを再接続してください。
- ハードドライブの一意な ID はデバイス暗号化の統計では倒置形式で表示されます。
- 暗号化されているデバイスのフォーマットは推奨されません。
- 複数のリムーバブルデバイスが同時にコンピューターに接続されている場合、暗号化ポリシーは 1 つのリムーバブルドライブにのみ適用されます。リムーバブルデバイスが再度接続された際に、暗号化ポリシーは正常に適用されます。
- 過度に断片化されたハードドライブでは暗号化が開始できないことがあります。ハードドライブをデフラグしてください。
- ハードドライブが暗号化されると、Microsoft Windows 7、8、8.1 がインストールされたコンピューターでは暗号化タスクが実行されたときから再起動するまで、また、Microsoft Windows 8、8.1、10 ではハードドライブの暗号化のインストール後から再起動するまで休止状態がブロックされます。ハードドライブが復号化されると、ブートドライブが完全に復号化されたときからオペレーティングシステムが最初に再起動されるまでの間、休眠状態はブロックされます。Microsoft Windows 8、8.1、10 のクイックスタートが有効にされていると、休眠状態がブロックされることでオペレーティングシステムのシャットダウンができなくなることがあります。
- Windows 7 搭載のコンピューターでは、BitLocker でディスクが暗号化された場合、回復中にパスワードの変更が許可されません。回復キーが入力され、オペレーティングシステムが読み込まれた後は、Kaspersky Endpoint Security はユーザーにパスワードまたは PIN コードを変更するよう促しません。このため、新しいパスワードまたは PIN コードを設定することはできません。この問題はオペレーティングシステムの特性によるものです。続行するには、ハードドライブを再度暗号化する必要があります。

- 追加のプロバイダーが有効な状態での xbootmgr.exe ツールの使用はお勧めできません。たとえばディスパッチャ、ネットワーク、またはドライブなどです。
- Kaspersky Endpoint Security for Windows がインストールされているコンピューターでの暗号化されたリムーバブルドライブのフォーマットはサポートされません。
- FAT32 ファイルシステムでの暗号化されたリムーバブルドライブのフォーマットはサポートされません（ドライブは暗号化されていると表示されます）。ドライブをフォーマットするには、NTFS ファイルシステムでフォーマットしなおしてください。
- 1台の暗号化されたコンピューター上で複数のダウンロードエージェントは共存できません。
- 起動可能な GPT ディスクのイメージを暗号化されていない状態で復元しようとすると、オペレーティングシステムが動作不能になる可能性があります。これを回避するために、次の推奨事項に従ってください：
  - バックアップからイメージを復元する前に、ディスクを完全に復号化します。
  - イメージを作成する際に、セクター単位のコピーを使用します。
  - イメージを復元する前に、暗号化されたディスクの最初のセクターからデータを削除し、ディスクを再初期化します。
- 以下の条件を同時に満たす場合は、別のコンピューターで以前暗号化されたリムーバブルドライブにアクセスできません：
  - Kaspersky Security Center のサーバーに接続されていない
  - ユーザーが新しいトークンまたはパスワードで認証しようとしている

  同様の状況が発生する場合は、コンピューターを再起動してください。コンピューターが再起動した後、暗号化されたリムーバブルドライブへのアクセス権が付与されます。
- BIOS 設定で USB の xHCI モードが有効になっている場合、認証エージェントの USB デバイスの検出はサポートされないことがあります。
- 頻繁に使用されているデータをキャッシュするために使用されるデバイスの SSD パーツの Kaspersky Disk Encryption（FDE）技術は SSHD デバイスではサポートされません。
- UEFI モードで実行されている 32 ビットの Microsoft Windows 8、8.1、10 オペレーティングシステムはサポートされていません。
- 復号化されたハードドライブを再度暗号化するには、コンピューターを再起動してください。
- ハードドライブの暗号化は Kaspersky Anti-Virus for UEFI. と互換性がありません。Kaspersky Anti-Virus for UEFI がインストールされているコンピューターでハードドライブの暗号化を使用してください。
- Microsoft アカウントに基づいた認証エージェントアカウントの作成は次の制限付きでサポートされます：
  - シングルサインオン技術はサポートされません。
  - 直近で特定の日数システムにログインしたユーザーにアカウントを作成するオプションを有効にしている場合、認証エージェントの自動アカウント作成はサポートされません。

- 認証エージェントのアカウント名が「<domain>/<Windows account name>」の形式である場合、コンピューター名を変更した後にそのコンピューターのローカルユーザー用に作成されたアカウント名も変更する必要があります。たとえば、コンピューター「Ivanov」のローカルユーザー「Ivanov」があるとして、このユーザーに認証エージェントのアカウント名が「Ivanov/Ivanov」として作成された場合などです。コンピューター名「Ivanov」が「Ivanov-PC」に変更されると、ユーザー名「Ivanov」の認証エージェントのアカウント名ｗｐ「Ivanov/Ivanov」から「Ivanov-PC/Ivanov」に変更する必要があります。認証エージェントのローカルアカウント管理タスクを使用してアカウント名を変更することができます。アカウント名の変更前に、起動前環境の認証は古い名前（例「Ivanov/Ivanov」）を使用して認証することが可能です。

- Kaspersky Disk Encryption 技術を使用して暗号化されたコンピューターに、ユーザーがトークンを使用してのみアクセスが許可されており、このユーザーはアクセスの復元手順を完了する必要がある場合、このユーザーに、暗号化されたコンピューターへのアクセスが復元された後にコンピューターへのパスワードベースでのアクセスが許可されていることを確認してください。アクセスの復元時に設定されたパスワードは保存されない可能性があります。この場合、暗号化されたコンピューターが次回再起動された場合にこのコンピューターへのアクセスの復元手順を完了する必要があります。

- FDE 復元ツールを使用してハードドライブを復号化した場合、元のデバイスのデータが復号化されたデータで上書きされるとエラーが発生する可能性があります。ハードドライブのデータの一部は暗号化されたままになります。FDE 復元ツールを使用する際には、デバイス復号化設定で復号化されたデータを保存するオプションを選択してください。

- 認証エージェントのパスワードが変更された場合、*パスワードは正常に変更されたことを示す文章を含むメッセージが表示されます。OK をクリック*というメッセージが表示されてユーザーがコンピューターを再起動した場合、新しいパスワードは保存されません。起動前環境において続く認証では古いパスワードを使用する必要があります。

- ディスクの暗号化は Intel Rapid Start 技術とは互換性がありません。

- ディスクの暗号化は ExpressCache 技術とは互換性がありません。

- いくつかのケースでは、FDE 復元ツールを使用して暗号化されたドライブを復号化しようとすると、「応答要求」手順が完了した後にツールが誤ってデバイスのステータスを「暗号化されていない」と検知することがあります。ツールのログには、デバイスは正常に復号化されたことを記載するイベントが表示されます。この場合、デバイスの復号化のためにデータ復元手順を再度開始する必要があります。

- Kaspersky Endpoint Security for Windows のプラグインが Web コンソールでアップデートされた後、Web コンソールが再開されるまではクライアントコンピューターのプロパティに BitLocker 回復キーが表示されません。

- ディスク全体の暗号化のサポートの制限事項および制限付きでサポートされるハードドライブの暗号化のデバイスのリストを確認するには、テクニカルサポートのナレッジベースの記事を参照してください。

ファイルレベルの暗号化（FLE）

- ファイルおよびフォルダーの暗号化は Microsoft Windows Embedded ファミリーのオペレーティングシステムではサポートされません。

- アプリケーションのインストール後、ファイルおよびフォルダーの暗号化が正常に動作するためにオペレーティングシステムを再起動する必要があります。

- 本製品は NTFS および FAT32 ファイルシステムのデバイスでのみファイルの暗号化をサポートします。暗号化されたファイルがサポート対象外のファイルシステム（exFAT など）に転送された場合は、デバイス上のファイルは暗号化されておらず、編集可能な状態になります。

- 暗号化されたファイルが利用可能な暗号化機能のあるコンピューターに保存されており、暗号化機能の利用できないコンピューターからそのファイルにアクセスする場合、このファイルへの直接アクセスが提供されます。利用可能な暗号化機能を持つコンピューターのネットワークフォルダーに保存された暗号化されたファイルは、利用可能な暗号化機能を持たないコンピューターにコピーされる場合は復号化された形式でコピーされます。

- Kaspersky Endpoint Security for Windows でファイルを暗号化する前に、Encrypting File System で暗号化されたファイルを復号化してください。

- ファイルが暗号化されると、ファイルのサイズは 4 KB に増えます。

- ファイルの暗号化後、ファイルのプロパティには*アーカイブ*属性が設定されます。

- 復号化されたファイルをリムーバブルメディアなどにコピーすると、ファイルは暗号化されたままになることがあります。これは、ファイルマネージャー（たとえば、explorer.exe）が暗号化されたファイルにアクセスしようとした際にファイルのハッシュがプロセスの特殊なリストに保存されることが原因で発生します。ファイルを復号化した後で、ファイルマネージャーがファイルにアクセスしようとすると、プロセスによってリスト内のファイルのハッシュが検索されます。ハッシュが見つかった場合、Kaspersky Endpoint Security はファイルを暗号化されたままにします。これを回避するために、プロセスのリストから全項目を消去する必要があります。プロセスのリストがいっぱいになると、オペレーティングシステムによって自動的にそのリストから全項目が消去されます。リストの中身は手動で空にすることもできます。これを行うには、コンピューターを再起動し、ファイルにアクセスするために使用しているプロセス（explorer.exe など）を再起動するか、暗号化されたファイルへのアクセスに使用していない別のファイルマネージャーを使用します。

- 暗号化されたアーカイブから解凍されたファイルの名前がコンピューター上に既に存在するファイルと同じ名前だった場合、コンピューター上のファイルは暗号化されたアーカイブから解凍された新しいファイルで上書きされます。ユーザーには上書き操作について通知されません。

- 暗号化されたアーカイブを解凍する前に、解凍されたファイルを保管する空き容量が十分にあるかどうか確認してください。空き容量がない場合、アーカイブの解凍は完了しますが、ファイルが破損することがあります。この場合、Kaspersky Endpoint Security でエラーメッセージが表示されない可能性があります。

- ポータブルファイルマネージャーインターフェイスでは、その操作中に発生したエラーに関するメッセージは表示されません。

- Kaspersky Endpoint Security for Windows は、ファイルレベルの暗号化機能がインストールされたコンピューター上でポータブルファイルマネージャーを開始しません。

- 次の条件を同時に満たす場合、ポータブルファイルマネージャーを使ってリムーバブルドライブにアクセスすることはできません：

  - Kaspersky Security Center に接続されていない。

  - Kaspersky Endpoint Security for Windows がコンピューターにインストールされている。

  - コンピューターでデータ暗号化（FDE または FLE）が実行されていない。

  ポータブルファイルマネージャーのパスワードが分かっていてもアクセスできません。

- 暗号化が使用されると、アプリケーションは Sylpheed メールクライアントとの互換性がなくなります。

- Kaspersky Endpoint Security for Windows では、特定のアプリケーションに対して暗号化されたファイルへのアクセスを制限するルールはサポートされません。これは、一部のファイル操作がサードパーティ製品によって実行されるためです。たとえば、ファイルのコピーは、アプリケーション自体ではなく、ファイルマネージャーによって実行されます。このようにして、暗号化されたファイルへのアクセスが Outlook メールクライアントに対し拒否された場合、ユーザーがクリップボードまたはドラッグアンドドロップ機能を使用してメールメッセージにファイルをコピーした際、Kaspersky Endpoint Security は、メールクライアントが暗号化されたファイルにアクセスできるようにします。コピー操作は、暗号化されたファイルへのアクセス制限ルールが指定されていない、つまりアクセスが許可されているファイルマネージャーによって実行されました。

- リムーバブルドライブがポータブルモードのサポートで暗号化された場合、パスワードの有効期間の制御は無効にできません。

- ページファイルの設定の変更はサポートされません。オペレーティングシステムはパラメータの値で指定されたものの代わりに既定値を使用します。

- 暗号化されたリムーバブルドライブの操作には安全な取り外しを使用してください。安全に取り外されていないリムーバブルドライブのデータ整合性は保証できません。

- ファイルが暗号化された後、暗号化されていない元のファイルは安全に削除されます。

- Client-Side Caching（CSC）を使用したオフラインファイルの同期はサポートされません。オフラインファイルの暗号化も、サーバー用の SMB を経由する Branch Caching の技術もサポートされていません。共有リソースのオフライン管理はグループポリシーのレベルで禁止することを推奨します。オフラインモードのファイルは編集可能です。同期後、オフラインファイルへの変更は失われます。

- システムハードドライブのルートでの暗号化されたアーカイブの作成はサポートされません。

- ネットワーク越しでの暗号化されたファイルへのアクセスでは問題が発生する可能性があります。このようなファイルは別の場所に移動するか、ファイルサーバーとして使用されているコンピューターが同じ Kaspersky Security Center 管理サーバーで管理されているか確認してください。

- キーボードのレイアウトの変更は自己解凍アーカイブのパスワード入力画面のフリーズの原因になる可能性があります。問題を解決するには、パスワード入力画面を閉じて、オペレーティングシステムのキーボードレイアウトに切り替え、再度暗号化されたアーカイブのパスワードを入力します。

- 1つのディスク上に複数のパーティションを持つシステムでファイルの暗号化が使用された際には、pagefile.sys ファイルのサイズを自動的に決定されるオプションを使用してください。コンピューターの再起動後、pagefile.sys ファイルはディスクパーティション間で移動される可能性があります。

- *マイ ドキュメント*フォルダー内のファイルを含むファイルの暗号化ルールの適用後、暗号化が適用されたユーザーが問題なく暗号化されたファイルにアクセスできることを確認してください。Kaspersky Security Center への接続が利用可能な時に、各ユーザーにシステムへのサインインを依頼してください。Kaspersky Security Center への接続がない状態で暗号化されたファイルにアクセスした場合、システムがフリーズすることがあります。

- ファイルレベルの暗号化の範囲にシステムファイルが含まれていた場合、これらのファイルの暗号化の際のエラーについてのイベントがレポートに表示されることがあります。これらのイベント内で指定されたファイルは実際には暗号化されていません。

- ピコプロセスはサポートされません。

- パスの大文字小文字の区別はサポートされません。暗号化ルールまたは復号化ルールが適用された際、製品イベントのパスはすべて小文字で表示されます。

- スタートアップ時にシステムが使用するファイルの暗号化はお勧めしません。これらのファイルが暗号化されると、Kaspersky Security Center への接続がないときに暗号化されたファイルにアクセスすると、システムのフリーズが起きたり、暗号化されていないファイルへのアクセスを促されたりします。

- ユーザーが WordPad または FAR のようなメモリマップファイル方式を使用したアプリケーションまたは Notepad ++ などの大きなファイルで作業するために設計されたアプリケーションを介して FLE ルールが適用されたネットワークを介してファイルで作業する場合、暗号化されていない形式のファイルはファイルのあるコンピューターからのアクセスが無制限にブロックされる可能性があります。

- Kaspersky Endpoint Security は OneDrive クラウドストレージまたは OneDrive を名前にしているその他のフォルダーを暗号化しません。ファイルが暗号化ルールに追加されていない場合、暗号化されたファイルの OneDrive フォルダーへのコピーはブロックされます。

- ファイルレベルの暗号化機能がインストールされていると、WSL（Windows Subsystem for Linux）モードではユーザーおよびグループの管理は機能しません。

- ファイルレベルの暗号化機能がインストールされている際にはファイルの名前変更および削除の POSIX (Portable Operating System Interface) はサポートされません。

- データが消失する可能性があるため、一時ファイルの暗号化は推奨されません。たとえば、Microsoft Word は文書の処理中に一時ファイルを作成します。一時ファイルが暗号化されて、元のファイルが暗号化されていない場合、文書を保存する際に「*アクセスが拒否されました*」というエラーが表示される可能性があります。さらに、Microsoft Word がファイルを保存することはできても、データが消失して次回文書を開くことができなくなる問題が発生する可能性があります。このようなデータの消失を防ぐには、暗号化ルールから一時ファイルフォルダーを除外する必要があります。

Detection and Response (EDR、NDR、MDR、XDR、Sandbox)

- *ファイルの隔離*タスクの結果として隔離されたオブジェクトをスキャンすることはできません。

- 4 MB より大きい代替データストリーム（Alternate Data Stream、ADS）を隔離することはできません。Kaspersky Endpoint Security はこのような ADS をユーザーに通知せずスキップします。

- Kaspersky Endpoint Security はタスクのプロパティ内のフォルダーのパスがドライブ文字から始まるネットワークドライブに対して *IOC スキャン*タスクを実行しません。Kaspersky Endpoint Security はネットワークドライブの *IOC スキャン*タスクでは UNC パスのみサポートしています。例：「`\\server\shared_folder`」。

- Web コンソールを使用して作成された Email/* タームを含む *IOC スキャン*タスクを正常に動作させるには、Kaspersky Endpoint Security Web プラグインを最新のバージョンにアップデートする必要があります。

- Kaspersky Sandbox との連携設定が設定ファイルで有効になっている場合、製品設定ファイルのインポートはエラーが発生して終了します。製品設定をエクスポートする前に、Kaspersky Sandbox を無効にしてください。それからエクスポートまたはインポートの手順を実行してください。設定ファイルのインポート後に、Kaspersky Sandbox を有効にします。

- KLP ファイルからポリシーをインポートする場合、Kaspersky Detection and Response Expert 契約の諸条件への同意を決定するパラメータ値は適用されません。その結果、ポリシーのインポート後、Kaspersky Endpoint Security は EDR Agent の機能を実行しません。EDR Agent を動作させるには、ポリシーを開き、任意のパラメータを変更して、ポリシー設定を保存します。

- *IOC スキャン*タスクの実行中に侵害インジケーターが検知された場合、本製品は FileItem タームでのみファイルを隠します。その他のタームでの隔離はサポートされません。

- アラートの詳細を管理するには、Kaspersky Endpoint Security for Windows の Web プラグインのバージョン 11.7.0 以降が必要です。アラートの詳細は Endpoint Detection and Response ソリューション（EDR Optimum および EDR Expert）と連携する際に必要になります。アラートの詳細 は Kaspersky Security Center Web コンソール および Kaspersky Security Center Cloud コンソールでのみ使用可能です。

- [KES + KEA］構成からの［KES + 組み込みエージェント］構成への移行は、Kaspersky Endpoint Agent の削除エラーが発生して完了することがあります。アプリケーションの削除エラーは、最新版の Kaspersky Endpoint Agent では解消されています。Kaspersky Endpoint Agent を削除するには、コンピューターを再起動してアプリケーションの削除タスクを作成してください。

- [KES + KEA + 組み込みエージェント] の構成はサポートされません。このような構成は、本製品と組織内で導入されている Detection and Response ソリューションとの連携を阻害します。さらに、同じコンピューター上で Kaspersky Endpoint Agent と組み込みエージェントを使用すると、テレメトリの重複を招く可能性があり、コンピューターとネットワークの負荷を増大させることになります。[KES + 組み込みエージェント] 構成に移行した後は、Kaspersky Endpoint Agent がコンピューターから削除されたことを確認してください。移行後も Kaspersky Endpoint Agent が動作を続けている場合は、*アプリケーションのリモートアンインストール*タスクを使用するなどして、手動で製品を削除してください。

  インストーラーでは Kaspersky Endpoint Agent を Kaspersky Endpoint Security と組み込みエージェントがインストールされているコンピューターに導入することが許可されています。Kaspersky Endpoint Agent と組み込みエージェントは、*コンポーネントの変更*タスクの結果として 1 台のコンピューターにインストールすることも可能です。動作は Kaspersky Endpoint Security と Kaspersky Endpoint Agent のバージョンにより異なります。

- 警告の詳細を生成する際に、本製品から、変更されたファイルのハッシュなど、検知された脅威に関する情報が提供されます。Kaspersky Endpoint Security は、警告の詳細を生成しながらファイルのハッシュを計算します。ファイルの変更イベントが生成された際のファイルの元のハッシュは、警告の詳細が生成された際に計算されたハッシュと同じではない可能性があることに注意してください。

- EDR Optimum コンポーネントおよび Kaspersky Sandbox コンポーネントを管理するには、Kaspersky Endpoint Security for Windows の Web プラグインのバージョン 11.7.0 以降が必要です。EDR Expert コンポーネントを管理するには、Kaspersky Endpoint Security for Windows の Web プラグインのバージョン 11.8.0 以降が必要です。これらのコンポーネントの操作をサポートしない Web プラグインを使用して、*コンポーネントの変更*タスクを作成した場合、インストーラーは、EDR Optimum、EDR Expert、または Kaspersky Sandbox がインストールされているコンピューターでこれらのコンポーネントを削除します。

- 組み込みエージェント、EDR (KATA) は、コンピューターの再起動後、ネットワーク分離の有効期間が終了した後でもコンピューターの分離を再開します。コンピューターが繰り返し分離されないようにするには、Kaspersky Anti Targeted Attack Platform コンソールでネットワーク分離をオフにする必要があります。

- 本製品のアップグレードは、ネットワーク分離が完了してから実行することをお勧めします。Kaspersky Endpoint Security のアップグレード後、ネットワーク分離を停止できます。

- EDR (KATA)、EDR Optimum および EDR Expert の組み込みエージェントはそれぞれに対する互換性がありません。そのため、異なる EDR 機能を持つ Kaspersky Endpoint Security をアクティベートしている場合、スタンドアロンの Kaspersky Endpoint Detection and Response のアドオンライセンスを持つ EDR の組み込みエージェントのアクティベートはスキップすることができます。例えば、KES + EDR Optimum のライセンスが含まれる Kaspersky Endpoint Security をアクティベートしている場合は、スタンドアロンのライセンスを持つ EDR (KATA) の組み込みエージェントのアクティベートはスキップできます。

- Kaspersky Endpoint Security のバージョン 12.1 では、組み込みの EDR（KATA）エージェントは *Get NTFS metafiles* タスクでは次のメタファイルをサポートしません：$Secure:$SDH:$INDEX_ROOT、$Secure:$SDH:$INDEX_ALLOCATION、$Secure:$SDH:$BITMAP、$Secure:$SII:$INDEX_ROOT、$Secure:$SII:$INDEX_ALLOCATION、$Secure:$SII:$BITMAP、$Extend\$UsnJrnl:$J:$DATA、$Extend\$UsnJrnl:$Max:$DATA。これらのメタファイルのサポートが、Kaspersky Endpoint Security バージョン 12.2 で追加されました。

- Kaspersky Endpoint Agent から Kaspersky Anti Targeted Attack Platform (EDR) ソリューションの Kaspersky Endpoint Security に移行する際、Central Node サーバーにコンピューターを接続するときにエラーが発生することがあります。これは、Web コンソールの移行ウィザードが次のポリシー設定をスキップして移行しないために発生します。

  - 設定の変更の禁止（[**接続設定**] が鍵のかかったアイコンの状態）。

    既定では、設定は編集可能です（鍵が開いたアイコン）。このため、コンピューターに設定が適用されません。設定の変更を禁止して、アイコンは鍵がかかった状態にする必要があります。

  - 暗号化コンテナー。

    Central Node サーバーとの接続に相互認証を使用している場合は、暗号化コンテナーを再度追加する必要があります。移行ウィザードはサーバーの TLS 証明書を正常に移行します。

  管理コンソール（MMC）のポリシーとタスクの移行ウィザードは Kaspersky Anti Targeted Attack Platform (EDR) ソリューションのすべての設定を移行します。

- Kaspersky Security Center と接続されていない Kaspersky Managed Detection and Response ソリューションをサポートするために Endpoint Detection and Response Agent モードで製品をインストールした場合、製品のアクティベーションステータスが正しく表示されません。BLOB ファイルのダウンロード後、Windows タスクバーの通知領域に「*アクティベートされていません*」という誤ったステータスが表示されます。ただし、製品のインターフェイスには、アクティベーションステータスが正しく表示されます。製品を正しく動作させるには、コンピューターを再起動してください。

- Kaspersky Endpoint Security では、EDR (KATA) コンポーネントまたは Endpoint Sensor（サポート対象外）を使用して、Kaspersky Anti Targeted Attack Platform ソリューションと連携できます。Kaspersky Anti Targeted Attack Platform と連携するには、1 つのコンポーネントしか使用できないことに注意してください。コンポーネントのステータスを表示するには、管理コンソール（MMC）でコンピューターのプロパティを開き、[**アプリケーション**] セクションで Kaspersky Endpoint Security for Windows のプロパティを開いて［**コンポーネント**］セクションに移動します。Kaspersky Anti Targeted Attack Platform との連携に関するコンポーネントのステータスを表示するには、次の特別な考慮事項が適用されます。

  - 管理プラグイン 12.0 以前のバージョンでは、アプリケーションは［**Endpoint Sensor**］の現在のステータスを表示します。Kaspersky Endpoint Security 12.0 以前では、EDR (KATA) コンポーネントは使用できません。EDR (KATA) コンポーネントはバージョン 12.1 で導入されました。

  - 管理プラグイン 12.1 以降のバージョンでは、アプリケーションは、**Endpoint Detection and Response (KATA)** の全体のステータスを表示します。これは、Endpoint Sensor のステータス、または EDR (KATA) コンポーネントのステータスのいずれかを意味します。これは、ユーザーのコンピューターにインストールされているアプリケーションのバージョンと、Kaspersky Anti Targeted Attack Platform との連携に使用できるコンポーネントによって異なります。

- Kaspersky Endpoint Security バージョン 12.6 以降では、Kaspersky Security Center Web コンソールのバージョン 14.2 以前のバージョンでは、コンピューターのプロパティで **Endpoint Detection and Response (KATA)** の名前が正しく表示されないことがあります。**Endpoint Detection and Response (KATA)** コンポーネントの代わりに、**Endpoint Detection and Response Expert (KATA EDR)** コンポーネントの名前が表示されます。コンポーネントのリストを表示するには、Web コンソールでコンピューターのプロパティを開き、[**アプリケーション**] セクションで Kaspersky Endpoint Security for Windows のプロパティを開いて［**コンポーネント**］セクションに移動します。Kaspersky Security Center Web コンソールのバージョン 15.1 以降では、コンポーネント名が正しく表示されます。

- Web コンソールバージョン 14.0 ～ 14.2 にインストールされている Kaspersky Endpoint Detection and Response 管理プラグインをバージョン 15.3 にアップデートすると、警告の詳細が正しく表示されません。警告の詳細を正しく機能させるには、Kaspersky Security Center 管理サーバーを再起動してください。

- Kaspersky Endpoint Detection and Response 管理プラグインバージョン 15.4 以降は、Kaspersky Security Center バージョン 14.0 をサポートしていません。管理プラグインをアップデートすると、警告の詳細が正しく表示されません。

- Kaspersky Extended Detection and Response (XDR) バージョン 1.4 クラスのソリューションは、Kaspersky Endpoint Security for Windows Web プラグインのバージョン 12.12 以降をサポートしていません。現在の Web プラグインのバージョンをそのままにするか、XDR ソリューションをバージョン 2.0 以降にアップデートすることができます。

その他の制限事項

- Windows オペレーティングシステムのバージョン 11 24H2 以降では、UDP Receive Segment Coalescing Offload（URO）テクノロジーがサポートされます。互換性のあるネットワークカードとドライバーがコンピューターにインストールされている場合、この技術は既定で有効になります。ユーザーのコンピューターで URO を無効にすると、アプリケーションのパフォーマンスが大幅に低下する可能性があります。

- Kaspersky Endpoint Security は WSL サブシステム（Windows Subsystem for Linux）を制限付きでサポートしています：

  - WSL 1製品はネットワーク トラフィックを監視し、HTTP / HTTPS 経由で脅威を検知します。Kaspersky Endpoint Security は独自の証明書を使用して安全な HTTPS 接続をスキャンするため、一部のサードパーティ製品の動作が中断される可能性があります。

  - WSL 2WSL 2 はサポートされていません。

- 製品がエラーを返す場合や、操作中にフリーズする場合、自動的に再起動することがあります。クラッシュを引き起こすエラーが繰り返し発生する場合、製品は以下の動作を行います：

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

  2. 機能が無効になったことをユーザーに通知します。

  3. 定義データベースをアップデートしたり、製品機能のアップデートを適用したりした後で、製品を動作する状態に復元しようとします。

- 信頼リストに追加された Wen アドレスが誤って処理されることがあります。

- Kaspersky Security Center コンソールでは、［**詳細**］→［**リポジトリ**］→［**アクティブな脅威**］フォルダーからファイルをディスクに保存することはできません。ファイルを保存するには、感染したファイルを駆除する必要があります。駆除時に、ファイルのコピーがバックアップに保存されます。これで、［**詳細**］→［**リポジトリ**］→［**バックアップ**］フォルダーからファイルをディスクに保存できるようになります。

- 管理サーバーへのデータ転送の設定の継承（［**全般設定**］→［**レポートと保管領域**］→［**管理サーバーへのデータ転送**）は、その他の設定の継承とは異なります。ポリシーでデータ転送設定の変更を許可している場合（鍵が開いたアイコン）、コンソールでこれらの設定はローカルコンピューターのプロパティの既定値にリセットされます（事前に定義されていない場合）。これらの設定が以前に定義されていた場合は、その値が復元されます。ポリシーを削除すると、設定は同様の方法で継承されます。このような場合、ローカルコンピューターのプロパティのその他の設定がポリシーから継承されます。

- Kaspersky Endpoint Security は RFC 2616、RFC 7540、RFC 7541、RFC 7301 に適合する HTTP トラフィックを監視します。HTTP トラフィックに別のデータ交換形式を検知すると、Kaspersky Endpoint Security はインターネットからの悪意のあるファイルのダウンロードを防止するため、接続をブロックします。

- Kaspersky Endpoint Security は QUIC プロトコル経由の通信をブロックします。ブラウザーでは QUIC サポートがブラウザーで有効にされているかどうかにかかわらず、標準の転送プロトコル（TLS または SSL）が使用されます。

- サードパーティ製ソフトウェアが Libcurl ライブラリと連携した場合、TLS 接続エラーが発生する場合があります。これは、Kaspersky Endpoint Security が暗号化された接続をスキャンするために使用するカスペルスキー証明書に関連している可能性があります。作業を継続するには、サードパーティ製ソフトウェアの証明書検証を無効にするか（推奨しません）、またはカスペルスキー証明書本体を cURL 証明書ストレージに追加してください。詳細な情報については、カスペルスキーナレッジベースを参照してください。

- Kaspersky Endpoint Security for Windows の疎開起動時、デジタル署名されたアプリケーションは一時的に正しくないグループに配置されることがあります。デジタル署名されたアプリケーションはのちに正しいグループに配置されます。

- サードパーティのソフトウェアによりブロックされた悪意のあるオブジェクトの再スキャン中に、その脅威が再度検知されたことはユーザーには通知されません。脅威の再検知イベントは製品レポートおよび Kaspersky Security Center のレポートに表示されます。

- デバイスの暗号化に関する Kaspersky Security Center のレポートには、デバイスコントロール機能がインストールされていないサーバープラットフォームまたはワークステーション上にある Microsoft BitLocker を使用して暗号化されたデバイスに関する情報は含まれません。

- Kaspersky Security Center Web コンソールでは、すべてのレポート項目の表示を有効にすることはできません。Web コンソールでは、レポート内で表示される項目の数のみ変更できます。既定では、Kaspersky Security Center Web コンソールは 1000 個のレポート項目を表示します。管理コンソール（MMC）ではすべてのレポート項目の表示を有効にできます。

- Kaspersky Security Center コンソールでは、1000 以上のレポート項目の表示を設定することはできません。1000 以上の値を設定すると、Kaspersky Security Center コンソールは 1000 項目のみ表示します。

- ポリシー階層を使用している際、親ポリシーがこれらの設定を禁止している場合に、子ポリシーのリムーバブルドライブの暗号化セクションの設定は、編集のためのアクセスが可能です。

- 外部からの暗号化の試みに対して共有フォルダーを保護するための除外設定が正常に動作するためにオペレーティングシステムの設定内で監査ログオンを有効にする必要があります。

- 共有フォルダーの保護が有効になっていると、Kaspersky Endpoint Security for Windows は、リモートアクセスセッションが開始されたコンピューターが除外リストに追加されている場合も含め、Kaspersky Endpoint Security for Windows の開始前に開始されたリモートアクセスセッションが共有フォルダーを暗号化しようとする動作を監視します。Kaspersky Endpoint Security for Windows の開始より前に開始された、除外リストに追加されたコンピューターから開始されたリモートアクセスセッションからの共有フォルダーの暗号化の操作の監視を有効にしない場合はリモートアクセスセッションを遮断して再度確立するか、Kaspersky Endpoint Security for Windows がインストールされたコンピューターを再起動してください。

- アップデートタスクが特定のユーザーアカウントの権限で実行されている場合、認証が必要なダウンロード元からアップデートする場合製品パッチはダウンロードされません。

- システムのパフォーマンスが十分でない場合アプリケーションの開始が失敗することがあります。この問題を解決するには、Ready Boot オプションを使用するか、サービスの開始のためのオペレーティングシステムのタイムアウトを増やしてください。

- 本製品は、Safe Mode では動作しません。

- 本製品のインストール後、初回の再起動までオーディオコントロールの正常な動作は保証しません。

- 管理コンソール（MMC）では、アプリケーションの権限の設定ウィンドウの侵入防止設定の［**削除**］ボタンは使用できません。本製品のコンテキストメニューを使用してアプリケーションを信頼グループから削除することができます。

- コンピューターがポリシーによって管理されている場合、本製品のローカルインターフェイスでは侵入防止設定のアプリケーションと保護対象のリソースは表示できません。スクロール、検索、フィルターおよびその他のウィンドウコントロールは利用できません。アプリケーションの権限は Kaspersky Security Center コンソールのポリシーのプロパティで表示できます。

- トレースのローテーションが有効になっていると、AMSI コンポーネントおよび Outlook アドインにはトレースファイルは作成されません。

- パフォーマンスのトレースは Windows Server 2008 では手動で収集できません。

- 「再起動」トレース種別のパフォーマンスのトレースはサポートされていません。

- ピコプロセスについてログのダンプはサポートされていません。

- ［**システムサービスの外部からの管理を無効にする(D)**］のオプションをオフにすると、パラメータ「`AMPPL=1`」（既定ではパラメータの値は `1` に設定されており、Windows 10RS2 オペレーティングシステムバージョンから開始されます）でインストールされた本製品のサービスの停止ができなくなります。パラメータ「`AMPPL`」の値を `1` にすると、保護プロセス技術を製品サービスに対して使用できるようになります。

- フォルダーに対してオブジェクトスキャンを実行するには、スキャンを実行するユーザーがそのフォルダーの読み取り権限を持っている必要があります。そうでない場合はスキャンは実行できず、エラーで終了します。

- ポリシーで定義されるスキャンルールに、行末に文字「`\`」がついていないパスが含まれる場合（例：`C:\folder1\folder2`）、スキャンは `C:\folder1\` に対して実行されます。

- ソフトウェアの制限のポリシー（Software Restriction Policies、SRP）を使用している場合、コンピューターが読み込みに失敗することがあります（真っ黒な画面）。誤動作を防ぐには、SRP プロパティでアプリケーションライブラリの使用を許可する必要があります。SRP プロパティで、khkum.dll ファイルに対し、セキュリティレベル［**制限しない**］を追加します（［**新しいハッシュルール**］メニュー項目）。ファイルは `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.12.12\klhk\klhk_x64\` フォルダーにあります。この方法を選択した場合は、Kaspersky Endpoint Security のアップデートタスク設定で、さらに［**製品機能のアップデートをダウンロード**］チェックボックスをオフにする必要があります。SRP の使用について詳しくは、Microsoft 社の資料を参照してください。

  SRP を無効にして、Kaspersky Endpoint Security のアプリケーションコントロールコンポーネントを使用してアプリケーションの使用を制御できます。

- Windows のグループポリシーオブジェクト（Group Policy Object、GPO）で、DriverLoadPolicy パラメータが 8（Good only、良いのみ）に設定されているコンピュータがドメインに属している場合、Kaspersky Endpoint Security がインストールされたコンピューターを再起動すると、BSOD が発生します。失敗を防ぐには、グループポリシーの起動時マルウェア対策（Early Launch Antimalware、ELAM）パラメータを 1（Good and unknown、良いおよび不明）に設定する必要があります。ELAM の設定は、［**Computer Configuration**］→［**Administrative Templates**］→［**System**］→［**Early Launch Antimalware**］のポリシーに保存されています。

- Rest API 経由での Outlook プラグインの管理はサポートされません。

- 特定のユーザーのタスク実行設定は、設定ファイルを介してデバイス間で転送することはできません。設定ファイルから設定を適用した後、ユーザー名およびパスワードを手動で指定してください。

- アップデートのインストール後、整合性チェックタスクはシステムが再起動してアップデートが適用されるまで動作しません。

- リモート診断ユーティリティを介してトレースのローテーションレベルが変更された場合、Kaspersky Endpoint Security for Windows はトレースレベルに空白の値を表示します。しかし、トレースファイルは正しいトレースレベルに基づいて書き込まれます。トレースレベルが本製品音ローカルインターフェイスを介して変更された場合、トレースレベルは正しく編集されますが、リモート診断ユーティリティは、ユーティリティが最後に定義した正しくないトレースレベルを表示します。これにより、ユーザーがローカルの製品インターフェイスでトレースレベルを手動で編集すると、管理者が現在のトレースレベルに関する最新情報がを把握できず、関連する情報が欠如することがあります。

- ローカルのインターフェイスでは、パスワードによる保護の設定で、管理者アカウント（既定では KLAdmin）の名前の変更は許可されていません。管理者アカウントの名前を変更するには、パスワードによる保護を一度無効にしてから有効にし、管理者アカウントの新しい名前を指定してください。

- Windows Server 2019 サーバー上に Kaspersky Endpoint Security をインストールした場合、Docker とは互換性がありません。Kaspersky Endpoint Security がインストールされたコンピューターに Docker コンテナーを導入するとクラッシュ（BSOD）が発生します。

- Kaspersky Endpoint Security が SQL Server DBMS のサーバーにインストールされている場合、本製品からサーバーのインスタンスに要求が送信されます。これは、SQL Server エージェントのジョブをスキャンして、悪意のあるジョブの実行を防止するために必要です。Kaspersky Endpoint Security は、SQL Server ユーザーアカウントを使用して、ジョブをスキャンします。本製品は、システムメモリのスキャン時、および定義データベースのアップデート後に、サーバーに要求を送信します。

- Kaspersky Endpoint Security と Secret Net Studio ソフトウェアとの互換性には制限があります：

  - Kaspersky Endpoint Security は Secret Net Studio ソフトウェアのウイルス対策機能と互換性がありません。

    ウイルス対策機能を備えた Secret Net Studio が導入されたコンピューターには本製品をインストールすることはできません。連携を可能にするには、Secret Net Studio からウイルス対策機能を削除する必要があります。

  - Kaspersky Endpoint Security は Secret Net Studio ソフトウェアのディスク保護およびデータ暗号化コンポーネントと互換性がありません。

    ディスク保護およびデータ暗号化コンポーネントを備えた Secret Net Studio が導入されたコンピューターには本製品をインストールすることはできません。連携を可能にするには、Secret Net Studio からディスク保護およびデータ暗号化コンポーネントを削除する必要があります。

  - Secret Net Studio は Kaspersky Endpoint Security のファイルレベルの暗号化機能（FLE）と互換性がありません。

    ファイルレベルの暗号化（FLE）コンポーネントを持つ Kaspersky Endpoint Security をインストールする場合、Secret Net Studio でエラーが発生する可能性があります。確実に相互運用するには、Kaspersky Endpoint Security からファイルレベルの暗号化（FLE）コンポーネントを削除する必要があります。

- システム変更監視ルールをインポートする際に、製品によってルールの ID と名前がチェックされます。ルール ID が同じ場合、Kaspersky Endpoint Security は既存のルールを新しいルールで上書きします。ルールをエクスポートする際に、製品によって ID が自動的に割り当てられます。エクスポートされたルールの XML ファイルを手動で編集した場合などには、同一の ID を持つルールが存在する可能性があります。ルール ID が一意でルール名は同じである場合、Kaspersky Endpoint Security はルール名に `(1)` などを追加します。

- Kaspersky Endpoint Security for Windows のバージョン 12.11 から、 Web コンソールでは、子グループで開かれている親ポリシーの設定を表示することはできなくなりました。Web コンソールには警告［*これは継承したポリシーです。ポリシーを作成した管理グループでのみ、ポリシーの設定を編集できます*］が表示されます。

- 256 文字を超えるポップアップ通知は、管理コンソール（MMC）に表示されません。

用語解説

Cloud Discovery

Cloud Discovery はクラウドサービスへのユーザーアクセスを管理します。クラウドサービスには、Microsoft Teams、Salesforce、Microsoft Office 365 などがあります。クラウドサービスは、*ファイル共有*、*メッセンジャー*、*メール*などのカテゴリに分類されます。

Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent コンポーネント。Kaspersky Endpoint Security コンポーネントと仮想インフラストラクチャの間で対話します。

IOC

侵害インジケーター。悪意のあるオブジェクトまたは活動に関するデータ一式。

IOC ファイル

侵害インジケーター（IOC）を含むファイルで、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。スキャンの結果として複数の IOC ファイル内の項目と一致した場合は、検知の可能性がより高くなります。

Kerberos 認証

クライアントとサーバー間の接続を確立する前に両者が相互認証を行うメカニズム。これにより、安全でないネットワーク上での通信が可能になります。このメカニズムは、ユーザーが信頼できる認証センターから取得するチケットに基づいています。

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent コンポーネント。保護する必要があるすべての仮想マシンにインストールします。

OLE オブジェクト

別のファイルに埋め込まれた添付ファイルまたはファイル。カスペルスキー製品は、OLE オブジェクトにウイルスがあるかどうかスキャンします。たとえば、Microsoft Office Excel® のテーブルを Microsoft Office Word 文書に挿入する場合、テーブルは OLE オブジェクトとしてスキャンされます。

OpenIOC

公開されている侵害インジケーター（IOC）の規格で、XML に基づいて記述されており、500 を超える侵害インジケーターが含まれています。

SVM

セキュア仮想マシン – スキャンサーバーサービス（Protection Server、Kaspersky Endpoint Security for Virtualization Light Agent のコンポーネント）がインストールされた特別な仮想マシン。

Trusted Platform Module

セキュリティに関連する基本的な機能（暗号鍵の保存など）を提供するために開発されたマイクロチップ。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。

Web リソースアドレスの正規化された形式

Web リソースの正規化された形式のアドレスは Web リソースアドレスのテキスト表記で、正規化によって取得されます。*正規化*は、Web リソースアドレスのテキスト表記を特定のルール（ユーザーログインの除外、パスワード、Web リソースアドレスのテキスト表記の接続ポート、Web リソースアドレスを大文字から小文字に変更するかなど）に従って変更するプロセスです。

保護機能では、Web リソースアドレスの正規化は、物理的には同じでも構文上は異なる可能性がある Web サイトのアドレスが何度もスキャンされるのを回避することを目的としています。

例：
正規化されていない形式のアドレス：www.Example.com\
正規化された形式のアドレス：www.example.com

アーカイブ

1つの圧縮ファイルにまとめられた1つまたは複数のファイル。データの圧縮および回答には、アーカイバと呼ばれる専用のアプリケーションが必要です。

悪意のある URL のデータベース

危険とみなされるコンテンツを含む Web アドレスのリスト。このリストは、カスペルスキーによって作成されます。このリストは定期的にアップデートされ、カスペルスキー製品の配信キットに含まれます。

感染可能なファイル

ファイルの構造または形式により、侵入者が悪意のあるコードを保存して拡散させるための「入れ物」として使用できるファイル。一般的には、com、exe、dll などの拡張子を持つ実行ファイルです。このようなファイルには、悪意のあるコードが含まれるリスクが非常に高いです。

感染したファイル

悪意のあるコードを含むファイル（ファイルのスキャンにより、既知のマルウェアのコードが検知された）。このようなファイルは、コンピューターを感染させる可能性があるため、使用しないでください。

管理グループ

共通の機能を共有し、インストールされている一連のカスペルスキー製品を共有する一連のデバイス。デバイスは、便宜上1つのユニットとして管理できるようにグループ化されます。グループには他のグループを含めることができます。グループポリシーを作成したり、グループにインストールされている各アプリケーションに対してグループタスクを作成したりすることができます。

駆除

感染しているオブジェクトの処理方法の1つ。駆除の結果、データが完全に復元するかまたは部分的に復元します。感染したすべてのオブジェクトを駆除できるわけではありません。

現在のライセンス

製品によって現在使用されているライセンス。

誤検知

ファイルの署名がウイルスの署名に似ているため、カスペルスキー製品が未感染のファイルを感染していると報告すると、誤報が発生します。

証明書の発行元

証明書を発行した認証局。

スキャン範囲

スキャンタスクの実行時に、Kaspersky Endpoint Security によってスキャンされるオブジェクト。

タスク

カスペルスキー製品によってタスクとして実行される機能：たとえば、リアルタイムファイル保護、フルデバイススキャン、データベースのアップデート。

定義データベース

カスペルスキーが把握しているコンピューターセキュリティ上の脅威の情報が含まれるデータベース。データベースの公開時点までの情報が含まれています。定義データベースの署名は、スキャン対象のオブジェクト内の悪意のあるコードの検知に役立ちます。定義データベースは、カスペルスキーのエキスパートによって作成され、1時間ごとにアップデートされます。

認証エージェント

起動可能なハードディスクが暗号化された後で、暗号化されたハードディスクにアクセスしオペレーティングシステムを読み込むための認証を実行するインターフェイス。

ネットワークエージェント

特定のネットワークノード（ワークステーションまたはサーバー）にインストールされている管理サーバーとカスペルスキー製品の相互作用を可能にする Kaspersky Security Center のコンポーネント。このコンポーネントは、Windows で実行されるすべてのカスペルスキー製品に標準装備されています。その他のオペレーティングシステムで実行される製品については、専用バージョンのネットワークエージェントを用意しています。

フィッシングサイトの URL のデータベース

カスペルスキーがフィッシング関連であると判断した Web アドレスのリスト。定義データベースは定期的にアップデートされ、カスペルスキー製品の配信キットの一部となっています。

ポータブルファイルマネージャー

リムーバブルドライブ上の暗号化ファイルを使用するためのインターフェイスを提供するアプリケーション。暗号化機能がコンピューターにない場合に使用できます。

保護範囲

脅威対策の実行中に常にスキャンされているオブジェクト。各コンポーネントの保護範囲には、それぞれ異なる特性があります。

マスク

ワイルドカードを使用したファイル名および拡張子の表示。

ファイルマスクには、ワイルドカードを含む、ファイル名に使用可能な文字をすべて含めることができます：

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。「**」というマスクは、スキャンからの除外リストの作成でのみ使用できます。

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

ライセンス証明書

カスペルスキーが、ライセンス情報ファイルまたはアクティベーションコードと合わせてユーザーに転送するドキュメント。ユーザーに許諾されたライセンスに関する情報が記載されています。

補足資料

このセクションには、本ドキュメントの内容を補足する内容が含まれています。

補足資料1：製品設定

ポリシー、タスク、製品インターフェイスを使用して Kaspersky Endpoint Security を設定します。製品の各機能に関して詳しくは、それぞれの機能の該当セクションを参照してください。

ファイル脅威対策

ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターの RAM に常駐し、開いたファイル、保存したファイル、実行されたファイルのすべてをリアルタイムでスキャンします。このコンポーネントは、接続されているドライブを含むすべてのコンピュータードライブ上のファイルをスキャンします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

コンポーネントは、ユーザーまたはアプリケーションがアクセスしたファイルをスキャンします。悪意のあるファイルが検知された場合、Kaspersky Endpoint Security はファイル操作をブロックします。その後、ファイル脅威対策の設定に応じて、悪意のあるファイルを駆除または削除します。

コンテンツが OneDrive クラウドストレージ上にあるファイルにアクセスしようとすると、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードしてスキャンします。

ファイル脅威対策の設定

パラメータ	説明
セキュリティレベル *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	ファイル脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます： • **高**：このファイルセキュリティレベルを選択すると、ファイル脅威対策は開いたファイル、保存したファイル、実行されたファイルのすべてに対して最も厳しいコントロールを適用します。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているすべてのファイルの種類をスキャンします。また、アーカイブ、インストールパッケージ、OLE 埋め込みオブジェクトもスキャンします。 • **推奨**：このセキュリティレベルはカスペルスキーが推奨するセキュリティレベルです。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されているファイルのうち、特定の形式のファイル、OLE 埋め込みオブジェクトをスキャンします。アーカイブまたはインストールパッケージはスキャンしません。 • **低**：このファイルセキュリティレベル設定では、スキャンの速度が最大になります。ファイル脅威対策は、コンピューターに接続しているすべてのハードディスク、リムーバブルドライブ、ネットワークドライブに格納されている、指定した拡張子のファイルのみをスキャンします。複合ファイルはスキャンしません。
ファイル種別 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	**すべてのファイル**：この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。 **ファイル形式でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。 **拡張子でファイルをスキャン**：この設定を有効にすると、感染する可能性のあるファイルのみがスキャンされます。ファイル形式はファイルの拡張子に基づいて識別されます。

パラメータ	説明
スキャン範囲	ファイル脅威対策によってスキャンされるオブジェクトが含まれています。スキャンオブジェクトには、ハードディスク、リムーバブルドライブ、ネットワークドライブ、フォルダー、ファイル、またはファイル名マスク（複数のファイルを対象に含む）を指定できます。 既定では、ファイル脅威対策はすべてのハードディスク、リムーバブルドライブ、ネットワークドライブで起動したファイルをスキャンします。これらのオブジェクトの保護範囲は変更したり削除することはできません。それぞれのオブジェクト（リムーバブルドライブなど）をスキャンから除外することのみ可能です。
機械学習とシグネチャ分析 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	機械学習とシグネチャ分析では、既知の脅威の説明と脅威を無効化する方法が登録された Kaspersky Endpoint Security の定義データベースを使用します。この方法を使用する保護では、許容できる最低限のセキュリティレベルが提供されます。 カスペルスキーのエキスパートの推奨に基づき、機械学習とシグネチャ分析は常に有効になっています。
ヒューリスティック分析 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**：このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 **駆除する。駆除できない場合はブロックする**：このオプションをオンにすると、Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、Kaspersky Endpoint Security はファイルをブロックします（読み取り / 書き込み）。 **ブロック**：このオプションをオンにすると、ファイル脅威対策は、感染したファイルを駆除することなく、自動的にブロックします。 感染したファイルを駆除または削除する前に、本製品はファイルを復元する場合、またはのちに駆除できた場合に必要になった場合に備えてバックアップファイルを作成します。
新規作成または変更されたファイルのみスキャン	新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。
アーカイブをスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配布パッケージをスキャン	サードパーティ製品の配布パッケージをスキャンします。
Microsoft Office形式のファイルをスキャン	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
メール形式のファイルをスキャン	メール形式のファイルをスキャンします。本製品は MSG および EML ファイルをスキャンします。メール形式のファイルには OLE オブジェクトおよび MHT ファイルが含まれます。チェックボックスのオンオフにかかわらず、Kaspersky Endpoint Security は 1 MB より小さいサイズのメール形式のファイルをスキャンします。
大きな複合ファイルをスキャンしない	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。

パラメータ	説明
複合ファイルをバックグラウンドで展開する	このチェックボックスをオンにすると、指定された値よりも大きいサイズの複合ファイルには、これらのファイルをスキャンする前にアクセスできます。この場合、複合ファイルの解凍とスキャンはバックグラウンドで実行されます。 指定された値より小さいサイズの複合ファイルには、これらのファイルを解凍してスキャンした後にのみアクセスできます。 このチェックボックスをオフにすると、すべてのサイズのファイルを解凍してスキャンした後にのみ複合ファイルにアクセスできます。
スキャンモード *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	Kaspersky Endpoint Security はユーザー、オペレーティングシステム、ユーザーのアカウントで実行されているアプリケーションがアクセスしたファイルをスキャンします。 **スマートモードでスキャン**：オブジェクトに対する処理の分析に基づいて、オブジェクトをスキャンします。たとえば、Microsoft Office ドキュメントで作業する場合は、ファイルを最初に開くときと最後に閉じるときに、Kaspersky Endpoint Security によってファイルがスキャンされます。ファイルを上書きする中間作業を実行しても、ファイルはスキャンされません。 **ファイルのアクセス時と更新時にスキャン**：オブジェクトを開こうとするときまたは修正しようとするときにオブジェクトをスキャンします。 **ファイルのアクセス時にスキャン**：オブジェクトを開こうとする際にのみオブジェクトをスキャンします。 **ファイルの実行時にスキャン**：オブジェクトを実行しようとする際にのみオブジェクトをスキャンします。
iSwift を使用する *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iSwift テクノロジーは、NTFS ファイルシステム用の iChecker テクノロジーの進化形です。
iChecker を使用する *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	特定のファイルをスキャン対象から除外することで、スキャンの高速化を可能にします。ファイルは、Kaspersky Endpoint Security の定義データベースの公開日時、ファイルの前回のスキャン日、およびスキャン設定に加えられた変更を考慮した特別なアルゴリズムによって、スキャンから除外されます。iChecker には制限があります。大容量のファイルには向かない点と、本製品が認識する構造を持ったファイル（EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP、RAR）にのみ適用する点です。
ファイル脅威対策の一時停止 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	指定した時間または特定のアプリケーションと一緒に動作しているときに一時的または自動的にファイル脅威対策の動作を停止します。
Windows コンテナー内で実行されたファイル操作のスキャン	コンテナー内で脅威が検知された場合、ファイル脅威対策に対して選択された処理が適用されます。 **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する十分な読み取りおよび書き込み権限がない可能性があります。その場合、検知したオブジェクトを駆除したり削除したりすることはできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナーを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。 **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナーをリアルタイムで継続的にスキャンします。

ウェブ脅威対策

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

Kaspersky Endpoint Security では、HTTP、HTTPS、FTP のトラフィック、URL、IP アドレスがスキャンされます。

ウェブ脅威対策を使用するには、本製品の初期設定を完了する必要があります。

- HTTPS トラフィックを監視するには、暗号化された接続のスキャンを有効にします（既定では有効になっています）。
- Kaspersky Endpoint Security が監視する必要があるポートを選択します（既定では、本製品はすべてのポートを監視します）。
- Kaspersky Endpoint Security がトラフィックを監視するアプリケーションを選択します。ほとんどのブラウザーは、カスペルスキーが推奨するアプリケーションのリストに含まれています。ブラウザーがリストにない場合は、手動で追加してください。
- Web トラフィックに Web ページとの連携スクリプトを埋め込むことを推奨します（既定では、スクリプトの挿入は無効になっています）。このスクリプトにより、ウェブ脅威対策のイベントをアプリケーションイベントログ、OS イベントログ、レポートに登録できるようになります。

ユーザーが、悪意のある Web サイトやフィッシングサイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックし、警告を表示します（下の図を参照）。



Web サイトへのアクセスが拒否されたことを示すメッセージ

ウェブ脅威対策の設定

パラメータ	説明
セキュリティレベル *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	ウェブ脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます： • **高**：HTTP や FTP 経由でコンピューターが受信する Web トラフィックをウェブ脅威対策が最大限にスキャンするときのセキュリティレベル。ウェブ脅威対策は、あらゆる定義データベースを使用してすべての Web トラフィックオブジェクトを詳細にスキャンし、最も徹底的なヒューリスティック分析を実行します。 • **推奨**：本製品のパフォーマンスと Web トラフィックのセキュリティの間で最適なバランスが取れたセキュリティレベル。ウェブ脅威対策は中スキャンレベルでヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、この Web トラフィックセキュリティレベルを推奨しています。 • **低**：この Web トラフィックセキュリティレベルの設定により、Web トラフィックのスキャンの速度が最大になります。ウェブ脅威対策は低スキャンレベルでヒューリスティック分析を実行します。
脅威の検知時の処理	**ブロックする**：このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。 **通知する**：このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。

パラメータ	説明
悪意のあるWebサイトのデータベースでWebアドレスをチェックする *（管理コンソール（MMC）およびKaspersky Endpoint Securityのインターフェイスでのみ利用可能）*	Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
ヒューリスティック分析を使用する *（管理コンソール（MMC）およびKaspersky Endpoint Securityのインターフェイスでのみ利用可能）*	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 ウイルスやその他の脅威を持つアプリケーションがないか Web トラフィックをスキャンしている間、ヒューリスティック分析は実行ファイルの命令を処理します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
フィッシングサイトのデータベースでWebアドレスをチェックする *（管理コンソール（MMC）およびKaspersky Endpoint Securityのインターフェイスでのみ利用可能）*	フィッシングサイトの URL のデータベースには、現時点で、フィッシング攻撃を実行するために使用されていることがわかっている Web サイトのアドレスが登録されています。カスペルスキーは、国際的な組織である Anti-Phishing Working Group から得たアドレスでこのリストを補完しています。カスペルスキーが作成するフィッシングアドレスのデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。
信頼する Web アドレスの Web トラフィックをスキャンしない	このオプションをオンにすると、ウェブ脅威対策は、信頼する Web サイトにアドレスが含まれている Web ページ / Web サイトのコンテンツをスキャンしません。信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。 また、暗号化された接続の全般的な除外リストを作成することもできます。この場合 Kaspersky Endpoint Security は、ウェブ脅威対策、メール脅威対策、ウェブコントロールが動作している間は信頼する URL の HTTPS トラフィックはスキャンしません。

メール脅威対策

メール脅威対策は、受信メールメッセージと送信メールメッセージの添付ファイルをスキャンして、ウイルスやその他の脅威を探します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

メール脅威対策は、受信メッセージと送信メッセージの両方をスキャンすることができます。製品は、以下のメールクライアントの POP3、SMTP、IMAP、NNTP をサポートしています。

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird、MyOffice Mail、R7-Office Organizer の各メールクライアントでトラフィックをスキャンするには、証明書ストアにカスペルスキーの証明書を追加し、独自の証明書ストアを選択する必要があります。

メール脅威対策は、他のプロトコルやメールクライアントをサポートしていません。

メール脅威対策は、メッセージに*プロトコルレベル*でアクセスできるとは限りません（たとえば、Microsoft Exchange ソリューションを使用する場合）。このため、メール脅威対策には、Microsoft Office Outlook 用の機能拡張が含まれています。この機能拡張により、*メールクライアントレベル*でメッセージをスキャンすることができます。メール脅威対策の機能拡張は Outlook 2010、2013、2016、2019 および 2021 の操作をサポートします。

メールクライアントがブラウザーで開いている場合、メール脅威対策はメッセージをスキャンしません。

添付ファイルに悪意のあるファイルが検知されると、Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。

メール脅威対策の設定

パラメータ	説明
セキュリティレベル *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	メール脅威対策では、異なる設定の組み合わせを適用できます。本製品に保存されているこれらの設定のグループは*セキュリティレベル*と呼ばれます： • **高**：このメールセキュリティレベルを選択すると、メール脅威対策は最も厳格にメールをスキャンします。メール脅威対策は送受信されたメールメッセージをスキャンし、徹底的なヒューリスティック分析を実行します。リスクの高い環境で作業している場合には［高］メールセキュリティレベルが推奨されます。このような環境の例としては、一元化されたメールアンチウイルスで守られていない家庭用ネットワークからのフリーメールサービスへの接続などがあります。 • **推奨**：本製品のパフォーマンスとメールのセキュリティの間で最適なバランスが取れたメールセキュリティレベル。メール脅威対策は送受信メールをスキャンし、中レベルのヒューリスティック分析を実行します。カスペルスキーのスペシャリストは、このメールセキュリティレベルを推奨しています。 • **低**：このメールセキュリティレベルを選択すると、メール脅威対策は受信メールのみをスキャンし、簡易ヒューリスティック分析を実行します。メールに添付されている圧縮ファイルはスキャンしません。このメールセキュリティレベルでは、オペレーティングシステムのリソースの使用を最小限に抑えながら、メールのスキャン速度が最大化します。「低」メールセキュリティレベルは、十分に保護された環境で作業している場合に推奨されます。このような環境の例としては、一元化されたメールセキュリティが適用された企業 LAN などがあります。
脅威の検知時の処理	**駆除する。駆除できない場合は削除する**：感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品は感染したオブジェクトを削除します。本製品は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed] <メッセージの元の件名>*」のように変更します。 **駆除する。駆除できない場合はブロックする**：感染したオブジェクトが受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。ユーザーはメッセージと安全な添付ファイルにアクセスできます。オブジェクトを駆除できなかった場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。 **ブロック**：感染したオブジェクトが受信メッセージで検知された場合、本製品はメッセージの件名に警告を追加します。ユーザーはメッセージと元の添付ファイルにアクセスできます。感染したオブジェクトが送信メッセージで検知された場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。
保護範囲 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	*保護範囲*には、機能の実行中にチェックするオブジェクトが含まれます： 送受信メッセージまたは受信メッセージ。 お使いのコンピューターを保護するためであれば、受信メッセージだけをスキャンする必要があります。送信メッセージのスキャンを有効にすると、感染ファイルが圧縮ファイルで送信されることを防ぐことができます。また、オーディオやビデオなど、特定の形式のファイルが送信されることを防ぐ必要がある場合は、送信メッセージのスキャンを有効にします。
POP3、SMTP、NNTP、IMAP トラフィックをスキャンする	POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメールをメール脅威対策でスキャンします。
Microsoft Outlook アドインに接続	このチェックボックスをオンにすると、POP3、SMTP、NNTP、IMAP プロトコルで送信されるメールのスキャンは、Microsoft Outlook に組み込まれた拡張機能側で有効になります。 メールのスキャンに Microsoft Outlook 用機能拡張を使用している場合は、Cached Exchange Modeを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、マイクロソフトサポート技術情報を参照してください。

パラメータ	説明
ヒューリスティック分析 *（管理コンソール（MMC）および Kaspersky Endpoint Security のインターフェイスでのみ利用可能）*	この技術は、カスペルスキー製品の最新バージョンの定義データベースを使用しても検知できない脅威を検知するために開発されました。この技術により、未知のウイルスや既知のウイルスの新しい亜種に感染している可能性があるファイルが検知されます。 悪意のあるコードをスキャン中に、ヒューリスティック分析機能は実行ファイル内の命令を実行します。ヒューリスティック分析が実行する命令の数は、ヒューリスティック分析内で指定されたレベルに準じます。ヒューリスティック分析のレベルは、新しい脅威を検索する際の完全性レベル、オペレーティングシステムリソースへの負荷、ヒューリスティック分析時間の間のバランスを設定します。
添付のアーカイブのスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。 スキャン中にメッセージ本文に圧縮ファイルのパスワードを検出した場合は、このパスワードを使用して圧縮ファイルの内容に対して悪意のあるアプリケーションのスキャンを実行します。この場合、パスワードは保存されません。圧縮ファイルはスキャン中に解凍されます。圧縮ファイルの解凍中にアプリケーションでエラーが発生した場合、次のパスに保存されたファイルを手動で削除できます：%systemroot%\temp。このファイルには接頭辞 PR が付いています。
添付のMicrosoft Office形式のファイルをスキャン	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
次のサイズより大きいアーカイブをスキャンしない	このチェックボックスをオンにすると、メール脅威対策が指定したサイズを超える、メールメッセージに添付されたアーカイブをスキャンしません。このチェックボックスをオフにすると、添付オブジェクトのサイズに関係なく、メール脅威対策がメール添付のアーカイブをスキャンします。
アーカイブのチェックを次の時間制限する	このチェックボックスを選択すると、メールメッセージに添付されたアーカイブのスキャンに割り当てられる時間が指定の時間に制限されます。
添付ファイル	添付ファイルのフィルター機能は、送信されるメールには適用されません。 **フィルタリングをオフにする**：このオプションをオンにした場合、メール脅威対策は、メールに添付されているファイルをフィルター処理しません。 **選択した種別の添付ファイルの名前を変更する**：このオプションを選択すると、指定した種別の添付ファイルの拡張子の末尾の文字をアンダースコアに置き換えます（たとえば、「attachment.doc_」など）。このため、ファイルを開くには、ユーザーがファイルの名前を変更する必要があります。 **選択した種別の添付ファイルを削除する**：このオプションをオンにした場合、メール脅威対策は特定の種類の添付ファイルをメールから削除します。 ファイルマスクのリストを使用して、メール上で名前を変更あるいはファイル自体を削除する添付ファイル種別を指定できます。

ネットワーク脅威対策

*ネットワーク脅威対策*コンポーネント（侵入検知システム、IDS とも呼ばれます）は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視します。本製品は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、定義データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、定義データベースと製品機能のアップデート時にアップデートされます。

パラメータ	説明
ポートのスキャンおよびネットワークフラッディングを攻撃として扱う	*ネットワークフラッディング*とは、Web サーバーなど、企業のネットワークリソースに対する攻撃を意味します。これは、大量のリクエストを送信し、ネットワークリソースの帯域幅をオーバーロードさせる攻撃です。攻撃されると、ユーザーは企業のネットワークリソースにアクセスできなくなります。 *ポートのスキャン*とは、コンピューターの UDP ポート、TCP ポート、ネットワークサービスをスキャンする攻撃を意味します。これにより、攻撃者がコンピューターの脆弱性を把握して、より悪質な攻撃を仕掛けることができるようになります。また、コンピューターのオペレーティングシステムを識別し、そのオペレーティングシステムに適したネットワーク攻撃を行うためにポートがスキャンされることもあります。 このチェックボックスをオンにすると、Kaspersky Endpoint Security はこれらの攻撃を検知するためネットワークトラフィックを監視します。攻撃が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。また、脅威の対応処理を迅速に行うために必要な、攻撃元のコンピューターに関する情報が提供されます。 一部の許可されるアプリケーションがこのような攻撃と似た動作を行う場合は、これらの検知機能を無効にすることができます。これにより誤検知を減らすことができます。
攻撃元の端末をブロックする時間	このオプションを有効にすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は 1 分です。最大値は 999 分です。 ブロックのリストはネットワークモニターツールウィンドウで表示できます。 Kaspersky Endpoint Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。
除外リスト	IP アドレスのリストです。ネットワーク脅威対策は、このリストに掲載される IP アドレスからのネットワーク攻撃をブロックしません。 ポートおよびプロトコルを指定した IP アドレスを追加することができます。 除外リストに含まれる IP アドレスからのネットワーク攻撃に関する情報は、ログに記録されません。
MAC スプーフィング対策	*MAC スプーフィング攻撃*では、ネットワークデバイス（ネットワークカード）の MAC アドレスを変更します。その結果、攻撃者はデバイスに送信されたデータを別のデバイスにリダイレクトし、このデータにアクセスすることができます。Kaspersky Endpoint Security で MAC スプーフィング攻撃をブロックし、攻撃に関する通知を管理者に送信できます。

ファイアウォール

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

ネットワークエージェントは Kaspersky Security Center との連携に使用されます。ファイアウォールは本製品とネットワークエージェントが正常に動作するために、自動でネットワークルールを作成します。その結果、ファイアウォールはコンピューターのいくつかのポートを開きます。どのポートが開かれるかは、ディストリビューションポイントなど、コンピューターの役割により異なります。コンピューターで開かれるポートについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

ネットワークルール

次の情報に基づいてネットワークルールを構成できます：

- *ネットワークパケットルール*：ネットワークパケットルールでは、アプリケーションに関係なく、ネットワークパケットに制限が適用されます。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。Kaspersky Endpoint Security には、カスペルスキーのエキスパートが推奨する権限を持つネットワークパケットルールが事前に定義されています。

- *アプリケーションネットワークルール*：アプリケーションネットワークルールでは、特定のアプリケーションのネットワークアクティビティに制限が適用されます。このルールでは、ネットワークパケットの特徴だけでなく、このネットワークパケットの宛先またはネットワークパケットを発行する特定のアプリケーションも考慮されます。

オペレーティングシステムのリソース、プロセス、および個人データへのアプリケーションの制御されたアクセスは、*アプリケーション権限*を使用することにより、ホスト侵入防止によって提供されます。

アプリケーションの最初の起動時に、ファイアウォールは次の動作を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。

2. Kaspersky Security Network での製品のセキュリティを確認する

   ファイアウォールがより効果的に機能するように、Kaspersky Security Network に参加することを推奨します。

3. *信頼済み*、*弱い制限付き*、*強い制限付き*、*ブロック*のうちいずれかの信頼グループにアプリケーションを配置します。

   信頼グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

   Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

   KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security は ホスト侵入防止の設定に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じて、アプリケーションのネットワーク動作をブロックします。たとえば、*強い制限付き*の信頼グループのアプリケーションは、ネットワーク接続を使用できません。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のネットワークルールをそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

ネットワークルールの優先度

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ネットワーク動作が複数のルールに追加された場合、ファイアウォールは最も優先度の高いルールに従ってネットワーク動作を制限します。

ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。同じ種類のネットワークアクティビティに、ネットワークパケットルールとアプリケーションのネットワークルールの両方が指定されている場合、そのネットワークアクティビティはネットワークパケットルールに従って処理されます。

アプリケーションのネットワークルールは特定の方法で動作します。アプリケーションのネットワークルールには、*パブリックネットワーク*、*プライベートネットワーク*、*信頼するネットワーク*のネットワークステータスに基づいたアクセスルールが含まれます。例えば、*強い制限付き*の信頼グループのアプリケーションは、既定ではすべてのステータスのネットワーク内でネットワークアクティビティが許可されません。個別のアプリケーション（親アプリケーション）にネットワークルールが指定されている場合、他のアプリケーションの子プロセスは、親アプリケーションのネットワークルールに基づいて実行されます。アプリケーションにネットワークルールが指定されていない場合は、子プロセスはアプリケーションの信頼グループのネットワークアクセスルールに基づいて実行されます。

例えば、ブラウザー X 以外のすべてのアプリケーションのすべてのステータスのネットワークアクティビティを禁止したとします。その後ブラウザー X（親アプリケーション）からブラウザー Y（子プロセス）のインストールを開始した場合、ブラウザー Y のインストーラはネットワークにアクセスし、必要なファイルをダウンロードします。インストール後、ブラウザー Y はファイアウォールの設定により、すべてのネットワーク接続を拒否します。子プロセスとしてのブラウザー Y のネットワークアクティビティを禁止するには、ブラウザー Y のインストーラに対してネットワークルールを設定する必要があります。

ネットワーク接続の種別

ファイアウォールを使用すると、ネットワーク接続の種別に応じてネットワーク動作を制御できます。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムからネットワーク接続の種別を受け取ります。オペレーティングシステムでのネットワーク接続の種別は、接続のセットアップ時にユーザーが設定します。Kaspersky Endpoint Security の設定でネットワーク接続の種別を変更できます。ファイアウォールは、オペレーティングシステムではなく Kaspersky Endpoint Security の設定に指定されたネットワーク種別に応じてネットワーク動作を監視します。

利用可能なネットワーク接続の種別は次のとおりです：

- **パブリックネットワーク**：ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されているコンピューターを操作するときに、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。

  既定では、ファイアウォールは、［*パブリックネットワーク*］種別をインターネットに割り当てます。インターネットの種別は変更できません。

- **プライベートネットワーク**：このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。

- **信頼するネットワーク**：コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワークアクティビティを許可します。

ファイアウォールの設定

パラメータ	説明
パケットルール	ネットワークパケットルールのリストのテーブル。ネットワークパケットルールはアプリケーションに関係なく、ネットワークパケットに制限を加えるために使用します。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。 このテーブルには、Microsoft Windows オペレーティングシステムで動作しているコンピューターのネットワークトラフィックを最適に保護するために、カスペルスキーが推奨する設定済みのネットワークパケットルールがリスト表示されます。 ファイアウォールでは、各ネットワークパケットルールに実行優先度が設定されます。ファイアウォールは、ネットワークパケットルールのリストに表示されているネットワークパケットルールを、上から下に順番に処理します。ネットワーク接続ごとに適用可能な最上位のネットワークパケットルールが検出され、ネットワークの動作を許可またはブロックすることによって、そのルールが適用されます。それぞれのネットワーク接続に対して、適用されたルールよりも優先度が低いネットワークパケットルールはすべてファイアウォールによって無視されます。 ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。
使用可能なネットワーク	このテーブルには、ファイアウォールによって検知されるコンピューターのネットワーク接続に関する情報が表示されます。 既定では、［*パブリックネットワーク*］ステータスがインターネットに割り当てられます。インターネットのステータスは変更できません。
アプリケーションのルール	**アプリケーション**：ファイアウォールコンポーネントによって制御されるアプリケーションのテーブル。アプリケーションは信頼グループに割り当てられます。信頼グループは、アプリケーションのネットワーク動作を制御するときに Kaspersky Endpoint Security が使用する権限を定義します。 ポリシーの影響下でコンピューターにインストールされているすべてのアプリケーションの1つのリストからアプリケーションを選択し、そのアプリケーションを信頼グループに追加できます。 **ネットワークルール**：信頼グループの一部であるアプリケーションのネットワークルールの表。これらのルールに従って、ファイアウォールは、アプリケーションのネットワークの動作を制限します。 この表には、カスペルスキーの専門家が推奨する定義済みネットワークルールが表示されます。これらのネットワークルールは、Windows オペレーティングシステムを実行しているコンピューターのネットワークトラフィックを最適に保護するために追加されました。定義済みネットワークルールを削除することはできません。

有害 USB 攻撃ブロック

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

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

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します（下の図を参照）。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID/PID、接続されたポートの番号）が認証キーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターの USB ポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、新しいコードが生成されます。数値コードの入力試行回数は指定できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合（下の図を参照）、本製品はキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックは、既定ではインストールされません。有害 USB 攻撃ブロックが必要な場合は、製品のインストール前にインストールパッケージのプロパティにコンポーネントを追加するか、製品のインストール後に利用可能なコンポーネントを変更できます。



キーボード承認

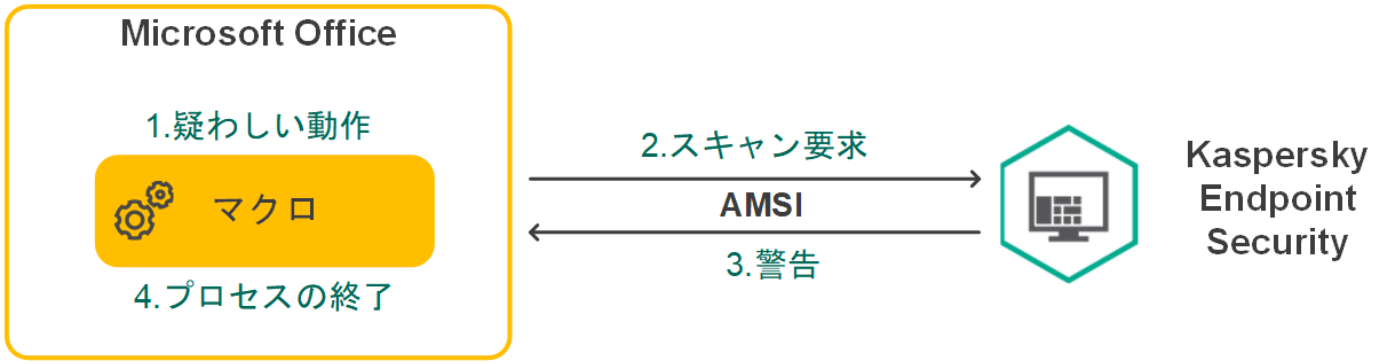
有害 USB 攻撃ブロックの設定

パラメータ	説明
USB デバイスの認証時にセキュリティキーボードの使用を禁止する	このトグルスイッチをオンにすると、認証用のコードが入力できない USB デバイスの認証時に、セキュリティキーボードの使用をブロックします。
USB デバイスの認証時にバーコードの使用を禁止する	このトグルスイッチをオンにすると、バーコードスキャナーの認証の通知にバーコードが表示されません。
USB デバイスの最大認証試行回数	認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。有効な値は 1 ～ 10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は USB デバイスをブロックする時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。
最大試行回数を超えた場合のタイムアウト	認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。有効な値は 1 ～ 180（分）です。

AMSI 保護

AMSI 保護コンポーネントは、Microsoft の Antimalware Scan Interface をサポートする目的で設計されています。*AMSI（Antimalware Scan Interface）*により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト（たとえば、PowerShell スクリプトなど）のより詳細なスキャンを実行するために Kaspersky Endpoint Security へオブジェクトを送信し、スキャン結果を取得できます。対象となるサードパーティ製品としては、たとえば Microsoft Office 製品があります。AMSI について詳しくは、Microsoft 社の資料を参照してください。

AMSI 保護機能では、脅威の検知とサードパーティ製品への検知された脅威に関する通知のみを実行できます。脅威に関する通知を受信したサードパーティ製品側では、脅威による悪意のあるふるまいを許可しません（たとえば、プロセスを終了します）。



AMSI の動作例

また、一定間隔の間に特定のサードパーティ製品から上限を超えてスキャン要求を受信した場合などにも、AMSI 保護機能でそのサードパーティ製品からのスキャン要求を拒否する場合があります。Kaspersky Endpoint Security は、拒否したサードパーティ製品のスキャン要求に関する情報を管理サーバーに送信します。AMSI 保護機能は、継続的な AMSI 保護機能との連携が有効になっているサードパーティ製品からのリクエストはブロックしません。

AMSI 保護機能は、ワークステーションおよびサーバー用の次のオペレーティングシステムで使用できます：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise マルチセッション
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2019 Essentials / Standard / Datacenter （Server Core モードを含む）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition （Server Core モードを含む）
- Windows Server 2025 Standard / Datacenter

AMSI 保護の設定

パラメータ	説明
アーカイブをスキャン	ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
配信パッケージをスキャン	サードパーティ製品の配布パッケージをスキャンします。
Microsoft Office形式のファイルをスキャン	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。チェックボックスのオンオフにかかわらず、本製品は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。
大きな複合ファイルをスキャンしない	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。

脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとすると、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。

さらに、脆弱性攻撃ブロックは、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

脆弱性攻撃ブロックの設定

パラメータ	説明
攻撃を検知したとき	**ブロックする**：この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。 **通知する**：この項目を選択した場合、攻撃が検知されると、攻撃に関する情報がログに記録され、攻撃に関する情報がアクティブな脅威のリストに追加されます。
システムプロセスのメモリ保護を有効にする	このオプションをオンにすると、システムプロセスメモリへアクセスしようとする外部プロセスをブロックします。

ふるまい検知

ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures（BSS）を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

さらに、ふるまい検知は、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

ふるまい検知の設定

パラメータ	説明
マルウェア活動の検知時の処理	**削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。 **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。 **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、アプリケーションは終了されませんが、悪意のある活動に関する情報がアクティブな脅威のリストに追加されます。

ホスト侵入防止

ホスト侵入防止は、オペレーティングシステムに危険を及ぼす可能性がある処理をアプリケーションが実行するのを防止し、オペレーティングシステムリソースや個人情報へのアクセスを管理します。このコンポーネントは、定義データベースと Kaspersky Security Network クラウドサービスを利用してコンピューターを保護します。

コンポーネントは、*アプリケーション権限*を使用してアプリケーションの動作を制御します。アプリケーション権限には、次のアクセスパラメータが含まれます：

- オペレーティングシステムリソースへのアクセス（自動起動オプション、レジストリキーなど）
- 個人データ（ファイルやアプリケーションなど）へのアクセス

アプリケーションのネットワーク動作は、*ネットワークルール*を使用してファイアウォールによって制御されます。

アプリケーションの最初の起動時に、ホスト侵入防止は次の処理を実行します：

1. ダウンロードした定義データベースを使用して、アプリケーションのセキュリティを確認します。
2. Kaspersky Security Network での製品のセキュリティを確認する

   ホスト侵入防止がより効果的に機能するように、Kaspersky Security Network に参加することを推奨します。

3. *信頼済み*、*弱い制限付き*、*強い制限付き*、*ブロック*のうちいずれかの信頼グループにアプリケーションを配置します。

   信頼グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

   Kaspersky Endpoint Security は、ファイアウォールおよびホスト侵入防止の信頼グループにアプリケーションを配置します。ファイアウォールまたはホスト侵入防止のみの信頼グループを変更することはできません。

   KSN への参加を拒否した場合、またはネットワークがない場合、Kaspersky Endpoint Security はホスト侵入防止の設定に応じて、アプリケーションを信頼グループに配置します。KSN からアプリケーションの評判を受け取った後、信頼グループを自動的に変更できます。

4. 信頼グループに応じてアプリケーション動作をブロックします。たとえば、*強い制限付き*の信頼グループのアプリケーションは、オペレーティングシステムモジュールへのアクセスを拒否されます。

次回アプリケーションが起動されると、Kaspersky Endpoint Security はアプリケーションの整合性をチェックします。アプリケーションが変更されていない場合、コンポーネントは現在のアプリケーション権限をそのアプリケーションに適用します。アプリケーションが変更されている場合、Kaspersky Endpoint Security はアプリケーションが初めて起動されたかのようにアプリケーションを分析します。

パラメータ	説明
アプリケーション権限	ホスト侵入防止によって監視されるアプリケーションのテーブル。アプリケーションは信頼グループに割り当てられます。信頼グループは、アプリケーションのアクティビティを管理する際に Kaspersky Endpoint Security によって適用される権限を定義します。 ポリシーの影響下でコンピューターにインストールされているすべてのアプリケーションの1つのリストからアプリケーションを選択し、そのアプリケーションを信頼グループに追加できます。 次の表に、アプリケーションのアクセス権を示します： • **ファイルとシステムレジストリ**：信頼グループに属するアプリケーションのオペレーティングシステムリソースと個人データへのアクセス権の表です。 • **権限**：信頼グループに属するアプリケーションのプロセスとオペレーティングシステムのリソースに対するアクセス権の表です。 • **ネットワークルール**：信頼グループの一部であるアプリケーションのネットワークルールの表。これらのルールに従って、ファイアウォールは、アプリケーションのネットワークの動作を制限します。この表には、カスペルスキーの専門家が推奨する定義済みネットワークルールが表示されます。これらのネットワークルールは、Windows オペレーティングシステムを実行しているコンピューターのネットワークトラフィックを最適に保護するために追加されました。定義済みネットワークルールを削除することはできません。
保護対象のリソース	このテーブルには、コンピューターのリソースがカテゴリ別に表示されます。ホスト侵入防止は、他のアプリケーションがテーブル内のリソースにアクセスしようとする動作を監視します。 リソースにはレジストリカテゴリ、ファイル、フォルダー、レジストリキーがあります。
本製品より前に起動したアプリケーションの信頼グループ	Kaspersky Endpoint Security が Kaspersky Endpoint Security より前に起動されるアプリケーションを配置する信頼グループ。
以前はKSNに登録されていなかったアプリケーションのルールを更新する	このチェックボックスをオンにすると、ホスト侵入防止は Kaspersky Security Network データベースを使用して以前に不明であったアプリケーションの権限をアップデートします。
デジタル署名があるアプリケーションを信頼する	このチェックボックスをオンにすると、ホスト侵入防止は信頼済みの製造元のデジタル署名付きのアプリケーションを「*信頼済み*」グループに割り当てます。 *信頼済みの製造元*とは、カスペルスキーによる信頼済みのソフトウェアベンダーです。手動で信頼済みの証明書ストアに製造元のデジタル署名を追加することも可能です。 このチェックボックスをオフにすると、ホスト侵入防止はこのようなアプリケーションを信頼するアプリケーションとみなさずに、他のパラメータを使用して信頼グループを決定します。
次の期間以上使用されなかったアプリケーションのルールを削除する	このチェックボックスをオンにすると、次の条件が満たす場合、Kaspersky Endpoint Security はアプリケーションに関する情報（信頼グループとアクセス権）を自動的に削除します： • アプリケーションを手動で信頼グループに配置したか、またはそのアクセス権を設定した • 定義された期間内にアプリケーションが開始されていない アプリケーションの信頼グループと権限が自動的に決定された場合は、Kaspersky Endpoint Security は 30 日後にこのアプリケーションに関する情報を削除します。アプリケーション情報の保管期間を変更したり、自動削除をオフにしたりすることはできません。 次回、このアプリケーションを起動すると、Kaspersky Endpoint Security は初めて起動した場合と同様に、アプリケーションを検証します。
他のグループに追加できなかったアプリケーションの信頼グループ	このドロップダウンリストの項目は、Kaspersky Endpoint Security が不明なアプリケーションを割り当てる信頼グループを決定します。 次の項目のいずれかを選択できます： • **弱い制限付き** • **強い制限付き** • **ブロック**

修復エンジン

修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックするとき、次の種別のマルウェアの動作に対して処理を実行します：

- **ファイルの動作**

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
- マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
- マルウェアによって変更または削除されたファイルを復元します。

ファイルの修復機能にはいくつかの制限事項があります。

- **レジストリの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによって作成されたレジストリキーを削除します。
  - マルウェアによって変更または削除されたレジストリキーは復元されません。

- **システムの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによって開始されたプロセスを終了します。
  - 悪意のあるアプリケーションによって侵入されたプロセスを終了します。
  - マルウェアによって停止されたプロセスは再開しません。

- **ネットワークの動作**

  Kaspersky Endpoint Security は、次の処理を実行します：

  - マルウェアによるネットワーク動作をブロックします。
  - マルウェアが侵入したプロセスによるネットワーク動作をブロックします。

マルウェアの動作のロールバックは、ファイル脅威対策またはふるまい検知から開始するか、マルウェアのスキャン中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピューターデータの整合性に悪影響を与えません。

Kaspersky Security Network

コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

KSN 機能は、アメリカ合衆国内にある本製品ではご利用いただけなくなる可能性があります。

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

Kaspersky Security Network の使用は任意です。本製品の初期設定中に、KSN を使用するかどうか尋ねられます。KSN への参加はいつでも開始または中止できます。

KSN に参加している間に生成されたカスペルスキー統計情報の送信や、そのような情報の保存と破棄について詳しくは、KSN 声明およびカスペルスキーの Web サイトを参照してください。Kaspersky Security Network 声明のテキストが含まれたファイル ksn_<言語 ID>.txt は製品配信キットに含まれています。

カスペルスキーの評価データベースのインフラストラクチャ

Kaspersky Endpoint Security は、カスペルスキーの評価データベースと連携する、次のインフラストラクチャソリューションをサポートします：

- ほとんどのカスペルスキー製品で使用されるのが *Kaspersky Security Network (KSN)* です。KSN の参加者は、カスペルスキーから情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、評価データベースと統計情報のデータベースに追加されます。

- *Kaspersky Private Security Network (KPSN)* は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報のデータにアクセスできるようにするソリューションです。KPSN は、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：

  - コンピューターがインターネットに接続されていない。

国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

パラメータ	説明
拡張 KSN モードを有効にする	*拡張 KSN モード*は、カスペルスキーに詳細なデータを送信するモードです。Kaspersky Endpoint Security は、オプションの設定にかかわらず KSN を使用して脅威を検知します。
クラウドモードを有効にする	*クラウドモード*で動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用しての本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。 このオプションをオンにすると、Kaspersky Endpoint Security では軽量なバージョンの定義データベースを使用し、オペレーティングシステムのリソースの負荷を減少させます。 このチェックボックスをオンにした次のアップデートでは、Kaspersky Endpoint Security は軽量なバージョンの定義データベースをダウンロードします。 このオプションをオフにすると、定義データベースの完全版を使用します。 このチェックボックスをオフにした次のアップデートでは、Kaspersky Endpoint Security は定義データベースの全体をダウンロードします。
KSN サーバーが使用できないときのコンピューターのステータス *（Kaspersky Security Center コンソール内でのみ利用可能）*	このドロップダウンリストでは、KSN サーバーが使用できない場合に Kaspersky Security Center に表示するコンピューターのステータスを指定できます。
管理サーバーを KSN プロキシサーバーとして使用する *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスをオンにすると、Kaspersky Endpoint Security は KSN プロキシサービスを使用します。KSN プロキシサービスの設定は管理サーバーのプロパティで編集できます。
KSN プロキシサーバーを使用できない場合は、Kaspersky Security Network サーバーを使用する *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

Windows イベントログ監視

このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

バージョン 11.11.0 から、Kaspersky Endpoint Security for Windows には Windows イベントログ監視コンポーネントが含まれるようになりました。Windows イベントログ監視は Windows イベントログの分析に基づいて保護対象環境の整合性を監視します。通常と異なるふるまいを検知した場合、本製品は管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。

Kaspersky Endpoint Security はルールに従って Windows イベントログを分析して違反を検出します。コンポーネントには事前定義済みのルールが含まれます。事前定義済みのルールはヒューリスティック分析によって動作します。独自のルールを追加することもできます（カスタムルール）。ルールが適用されると、本製品は緊急ステータスのイベントを作成します（下図を参照）。

Windows イベントログ監視を使用する場合、監査ポリシーのセキュリティが設定されており、システムが関連するイベントを記録していることを確認してください（詳細については、Microsoft のテクニカルサポートの Web サイトを参照してください）。



Windows イベントログ監視の通知

Windows イベントログ監視の設定

パラメータ	説明
事前定義済みのルール	Windows イベントログ監視のリストです。事前定義済みのルールには、保護対象コンピューター上における正常でない活動のテンプレートが含まれます。正常でない活動は、攻撃の可能性を示している場合があります。
カスタムルール	ユーザーによって追加された Windows イベントログ監視のリストです。Windows イベントログ監視のルールトリガー条件を独自に設定することができます。そのためには、イベント ID を入力してイベントソースを選択する必要があります。 ［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。また、サードパーティ製のアプリケーションのログを指定することもできます。

アンチクリプター

アンチクリプターコンポーネントは共有フォルダ内の動作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。

NTFS ファイルシステムで、EFS システムで暗号化されていないメディア上にあるファイルのみ外部からの暗号化をブロックします。

パラメータ	説明
名前または IP アドレスによる除外リスト	**名前または IP アドレスによる除外リスト**：このリストにある、共有フォルダーの暗号化を試行したコンピューターは監視されません。 共有フォルダーの外部からの暗号からの保護で、暗号化を行う側のコンピューターの除外リストを有効にするには、Windows セキュリティポリシーでログオンの監査を有効にする必要があります。既定では、ログオンの監査は無効です。Windows での監査ポリシーを使用したセキュリティ設定の詳細については、Microsoft 社の Web サイトを参照してください。 **マスクによる除外**：保護範囲の除外リスト。組織で、共有フォルダーを使用したファイルの交換時にデータ暗号化が使用されている場合、保護範囲からフォルダーを除外することで誤検知の量を減らすことができます。例えば、ユーザーが共有フォルダーで拡張子 ENC のファイルを使用していると、ふるまい検知で誤検知の量が増えることがあります。このような操作は、外部からの暗号化攻撃に典型的な動作と一致します。データを保護するために共有フォルダーでファイルを暗号化した場合は、そのフォルダーを除外リストに追加します。 マスクを使用する • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。
脅威の検知時の処理	• **通知する**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、この試みに関する情報がアクティブな脅威のリストに追加され、ローカルの製品インターフェイスレポートに項目が追加されて、検知された悪意のある活動に関する情報が Kaspersky Security Center に送信されます。 • **接続をブロックする時間（分）**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし、変更されたファイルのバックアップコピーが作成されます。 修復エンジンが有効になっていて［**接続をブロックする時間（分）**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。
保護範囲	*保護範囲*は、Kaspersky Endpoint Security がファイルの動作を監視する共有フォルダーへのパスのリストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダー内のファイルの動作を監視します。

ウェブコントロール

ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック量を減少させるとともに、業務に関係のない Web サイトへの就業時間中のアクセスなどを防ぐことができます。ユーザーがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します（下図を参照）。

ウェブコントロールを使用するには、本製品の初期設定を完了する必要があります。

- HTTPS トラフィックを監視するには、暗号化された接続のスキャンを有効にします（既定では有効になっています）。
- Kaspersky Endpoint Security が監視する必要があるポートを選択します（既定では、本製品はすべてのポートを監視します）。

- Kaspersky Endpoint Security がトラフィックを監視するアプリケーションを選択します。ほとんどのブラウザーは、カスペルスキーが推奨するアプリケーションのリストに含まれています。ブラウザーがリストにない場合は、手動で追加してください。

- Web トラフィックに Web ページとの連携スクリプトを埋め込むことを推奨します（既定では、スクリプトの挿入は無効になっています）。このスクリプトにより、ウェブコントロールのイベントをアプリケーションイベントログ、OS イベントログ、レポートに登録できるようになります。

Web サイトへのアクセスの管理方法

ウェブコントロールでは、次の設定を使用して Web サイトへのアクセスを管理できます：

- **Web サイトのカテゴリ**：Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。たとえば、「*SNS*」カテゴリまたはその他のカテゴリのサイトに対してユーザーのアクセスを制限することができます。

- **データ種別**：Web サイトのデータへのユーザーのアクセスを制限して、画像を表示できないようにするなどの使い方ができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。

  > 圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「*アーカイブ*」として識別し、「*グラフィック*」とは識別しません。

- **個別のアドレス**：URL を入力したり、マスクを使用して Web アドレスを指定できます。

Web サイトへのアクセスを管理するために、複数の設定を同時に組み合わせて使用できます。たとえば、Web サイトのカテゴリが「*Web メール*」の場合にのみ「*Office アプリケーションのファイル*」へのアクセスを制限するような使い方ができます。

Web サイトへのアクセスルール

ウェブコントロールは、*アクセスルール*を使用して Web サイトへのユーザーアクセスを管理します。Web サイトへのアクセスルールでは、次のような詳細設定を指定できます。

- ルールを適用するユーザー：

  ブラウザーによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。

- ルールのスケジュール：

  ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

アクセスルールの優先順位：

それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。適用例として、たとえば、Kaspersky Endpoint Security によって企業ポータルが「ソーシャルネットワーク」サイトと判定されているケースを考えます。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「*SNS*」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 2 つのルールを作成します。この場合、企業ポータルへのアクセスルールには、ソーシャルネットワークカテゴリへのアクセルルールよりも高い優先順位を割り当てる必要があります。



ウェブコントロールによって表示されるメッセージ

パラメータ	説明
Web リソースへのアクセスルール	Web リソースアクセスルールのリストです。それぞれのルールには優先順位が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。
既定のルール	［*既定のルール*］は、他のルールの対象範囲に含まれない Web リソースへのアクセスルールです。次の設定方法があります： • **ルールリスト以外すべてを許可**： 禁止された Web サイトへの拒否リストモードと同様です。 • **ルールリスト以外すべてをブロック**： 許可された Web サイトへの許可リストモードと同様です。
ルール適用後にアクティブなブラウザーセッションを終了する	このチェックボックスをオンにすると、ウェブコントロールにより、ポリシーの適用直後に、ブロックされた Web リソースへの接続が終了します。ブラウザーで、Web サイトからのデータのダウンロードがすぐに停止されます。Web サイトを更新したり、禁止されている別の Web サイトに移動したりすると、警告が表示されます。 ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。 チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。
テンプレート	**警告**：この入力フィールドには、Web リソースへの不正なアクセスに対し警告のルールが適用される際に表示されるメッセージのテンプレートが含まれています。 **ブロックに関するメッセージ**：入力フィールドには、Web リソースへのアクセスをブロックするルールが適用される際に表示されるメッセージのテンプレートが含まれています。 **管理者に送信するメッセージ**：メッセージのテンプレートには、ブロックが誤検知だと考えられる場合に LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**Web ページへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。 メッセージのテンプレートの管理用に特別な変数が用意されています（例：`%USER_NAME%`）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。
許可対象のページの閲覧を記録する	Kaspersky Endpoint Security は、許可されている Web サイトも含めて、すべての Web サイトへのアクセスに関するデータをログに記録します。Kaspersky Endpoint Security は、Kaspersky Security Center、Kaspersky Endpoint Security のローカルログ、Windows イベントログのそれぞれに、イベント情報を送信できます。ユーザーが行うインターネット上での活動を監視するには、イベントの保存に関する設定を指定する必要があります。 監視機能をサポートするブラウザー：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。ユーザーの操作履歴の監視はその他のブラウザーでは動作しません。 ユーザーが行うインターネット上での活動を監視すると、HTTPS トラフィックの復号のためにより多くのコンピューターリソースを消費する可能性があります。

デバイスコントロール

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。

デバイスコントロールが有効になると、本製品は接続されているデバイスの情報を Kaspersky Security Center に渡します。接続されたデバイスのリストは Kaspersky Security Center の［**詳細**］→［**リポジトリ**］→［**ハードウェア**］フォルダーで表示できます。

デバイスへのアクセスの判定基準

デバイスコントロールは、次の情報に基づいてアクセスをコントロールできます。

- **デバイス種別**：プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。
  次のようにデバイスアクセスを設定できます：
  - 許可：
  - ブロック：
  - ルールに準拠（プリンターとポータブルデバイスのみ）：
  - 接続バスに依存（Wi-Fi 以外）：
  - 例外を除きブロック（Wi-Fi のみ）：
- **接続バス**：*接続*バスとは、コンピューターへのデバイスの接続に使用されるインターフェイスです（例：USB、FireWire）。デバイス種別に対して**接続バスに依存**モードが選択されている場合、本製品は接続インターフェイス（USB など）に応じてデバイスへのアクセスを許可または拒否します。
  次のようにデバイスアクセスを設定できます：
  - 許可：
  - ブロック：
- **信頼するデバイス**：「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。
  次のデータに基づいて信頼するデバイスを追加できます。
  - **ID によるデバイス**：各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。
  - **モデルによるデバイス**：各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：`VID_1234&PID_5678`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。
  - **ID マスクによるデバイス**：ID が類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`WDC_C*`」。
  - **モデルマスクによるデバイス**：同一の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。`*` 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「`?`」記号の使用をサポートしていません。例：「`VID_05AC&PID_*`」。

デバイスコントロールは、アクセスルールを使用してデバイスへのユーザーアクセスを管理します。デバイスコントロールでは、デバイスの接続や切断のイベントを保存することもできます。イベントを保存するには、ポリシー内でイベントの記録を設定する必要があります。

デバイスへのアクセスが接続バスに依存する場合（ステータスの場合）、Kaspersky Endpoint Security ではデバイスの接続イベントと切断イベントが保存されません。Kaspersky Endpoint Security でデバイスの接続イベントと切断イベントを保存するには、デバイスへのアクセスを許可する（ステータス）か、デバイスを信頼リストに追加します。

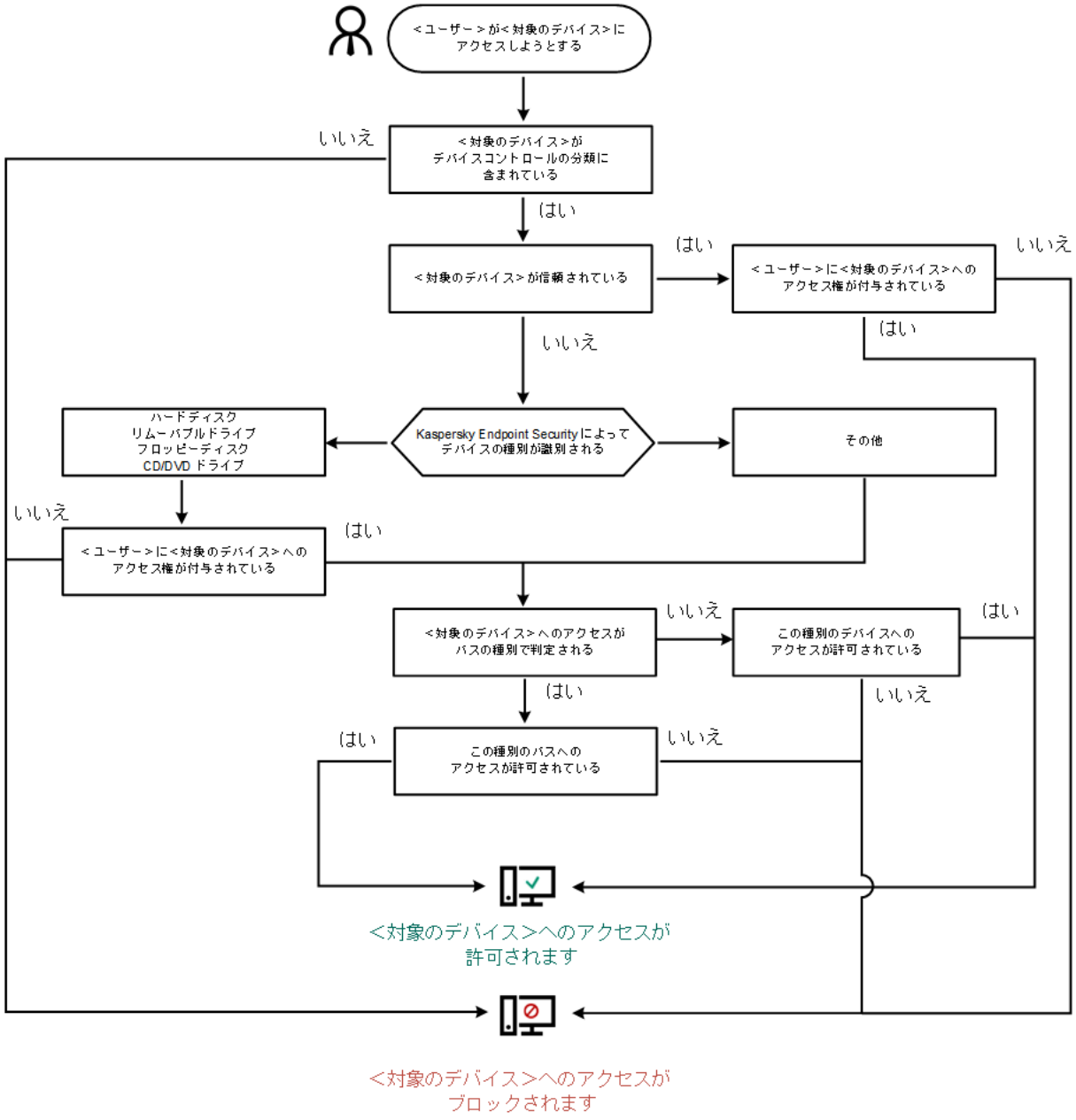
デバイスコントロールでブロックされているデバイスがコンピューターに接続された場合、Kaspersky Endpoint Security はアクセスをブロックし通知を表示します（以下の図を参照）。



デバイスコントロールの通知

デバイスコントロールの動作アルゴリズム

ユーザーがデバイスをコンピューターに接続すると、Kaspersky Endpoint Security はデバイスへのアクセスを許可するかどうかを決定します（以下の図を参照）。



デバイスコントロールの動作アルゴリズム

デバイスが接続されてアクセスが許可されている状況で、アクセスをブロックするようにアクセスルールを編集できます。この場合、（フォルダーの内容の表示や、読み取りまたは書き込みの実行など）次にデバイスへのアクセスが試行されたときに、Kaspersky Endpoint Security はアクセスをブロックします。ファイルシステムのないデバイスは、次回デバイスが接続されたときにのみブロックされます。

Kaspersky Endpoint Security がインストールされているコンピューターのユーザーが、誤ってブロックされたと考えられるデバイスへのアクセスを要求できるようにするには、アクセス要求の手順を伝えます。

パラメータ	説明
一時アクセスの要求を許可する *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスをオンにすると、Kaspersky Endpoint Security のローカルインターフェイスで［**アクセスを要求**］が有効になります。このボタンを使用して、ユーザーはブロックされたデバイスへの一時アクセスを要求できます。
デバイスと Wi-Fi ネットワーク	このテーブルには、各アクセスステータスなど、デバイスコントロールの分類に従って、考えられるすべてのデバイスの種類が表示されます。
接続バス	それぞれのアクセスルールのステータスなど、デバイスコントロールの分類に従って、すべての使用可能な接続バスのリストが表示されます。Kaspersky Endpoint Security は、**接続バスに依存**モードが選択されている場合、接続バスの種別に応じてデバイスへのアクセスを許可または拒否します。
信頼するデバイス	信頼するデバイスと、それぞれのデバイスに対してアクセス権が付与されているユーザーのリストです。
継承時に値を統合する *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Security Center の親ポリシーと子ポリシーの信頼するデバイスのリストを結合します。リストを結合するには、子ポリシーは Kaspersky Security Center の親ポリシーの設定を継承するよう設定されている必要があります。 チェックボックスがオンの場合、Kaspersky Security Center の親ポリシーのリスト項目は子ポリシー内で表示されます。このようにすることで、組織全体の信頼するデバイスのリストを作成することが可能です。 継承された子ポリシー内のリスト項目は削除または編集できません。継承時に結合された信頼するデバイスのリストの項目は親ポリシー内でのみ削除および編集可能です。リストの項目は、下位のポリシーで追加、編集、削除が可能です。 子ポリシーと親ポリシーのリスト項目が一致する場合、これらの項目は親ポリシー内の同じ項目として表示されます。 このチェックボックスをオフにすると、リストの項目は Kaspersky Security Center ポリシーの設定の継承時に結合されません。 この機能により、ポリシープロファイル内のリストを結合することもできます。リストを結合するには、最も優先度の高いプロファイルで、それよりも優先度の低いプロファイルからの設定の継承を有効にします。ポリシープロファイルのプロパティについて詳しくは、Kaspersky Security Center ヘルプ を参照してください。
アンチブリッジ	アンチブリッジは、ネットワークブリッジの作成をブロックし、コンピューターで複数のネットワーク接続が同時に確立することを防止します。この機能を使用することで、セキュリティ保護が不十分で接続が許可されていないネットワークから社内ネットワークを保護できます。 アンチブリッジは、デバイスの優先度を参照することで、複数のネットワーク接続の確立をブロックします。デバイスのリスト上の位置が高くなるほど、優先度が高くなります。 現在有効な接続と新しい接続の種別が同じ場合（たとえば、両方とも Wi-Fi など）、Kaspersky Endpoint Security は現在有効な接続をブロックし、新しい接続の確立を許可します。 現在有効な接続と新しい接続の種別が異なる場合（たとえば、1つはネットワークアダプターでもう1つは Wi-Fi など）、Kaspersky Endpoint Security は優先度が低い方の接続をブロックし、優先度が高い方の接続を許可します。 アンチブリッジの使用がサポートされるのは、次の種別のデバイスです：ネットワークアダプター、Wi-Fi、モデム。
メッセージのテンプレート	**ブロックに関するメッセージ**：ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。 **管理者に送信するメッセージ**：そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが LAN 管理者に送信するメッセージのテンプレートが含まれています。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**デバイスへのアクセスブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

アプリケーションコントロール

アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。アプリケーションコントロールは、アプリケーションへのアクセスを制限することにより、コンピューター感染のリスクも減らします。

アプリケーションコントロールの設定では、次のステップが必要です：

1. アプリケーションカテゴリの作成

   管理者は、自身が管理するアプリケーションのカテゴリを作成します。アプリケーションのカテゴリは、管理グループに関係なく、企業ネットワーク内のすべてのコンピューターを対象としています。カテゴリを作成するには、KL カテゴリ（ブラウザーなど）、ファイルのハッシュ、アプリケーションの開発元、およびその他の条件を使用できます。

2. アプリケーションコントロールルールの作成

   管理者は、管理グループのポリシーにアプリケーションコントロールルールを作成します。ルールには、アプリケーションのカテゴリと、「ブロック」または「許可」のカテゴリからのアプリケーションの起動ステータスが含まれます。管理者は複数のルールを作成できます。1つのアプリケーションが複数のルールの条件に一致する場合があります。ブロックルールの優先度は、許可ルールの優先度よりも高くなります。Kaspersky Endpoint Security は、アプリケーションが起動されるたびに、ルールに一致するかどうかをチェックします。すべてのアプリケーションコントロールルールに対して、アプリケーションが順次照合されます。

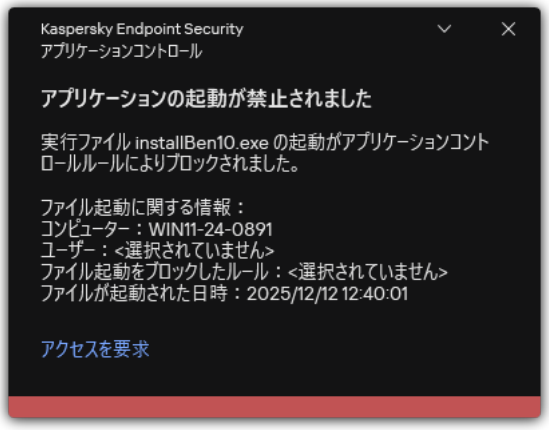
3. アプリケーションコントロールモードの選択

   管理者は、拒否リストまたは許可リストのいずれのルールにも含まれていないアプリケーションを操作するモードを選択します。

ユーザーが禁止されたアプリケーションを起動しようとすると、Kaspersky Endpoint Security はアプリケーションの起動をブロックし、通知を表示します（下の図を参照）。

Application Control の構成を確認するための *テストモード* が用意されています。このモードでは、Kaspersky Endpoint Security は次のことを行います：

- 禁止されているものも含めて、アプリケーションの起動を許可します。
- 禁止されているアプリケーションの起動に関する通知を表示し、ユーザーのコンピューターのレポートに情報を追加します。
- 禁止されたアプリケーションの起動に関するデータを Kaspersky Security Center に送信します。



アプリケーションコントロールの通知

アプリケーションコントロールの操作モード

アプリケーションコントロールは 2 つのモードで動作します。

- **拒否リスト**：このモードでは、アプリケーションコントロールルールで禁止されているアプリケーションを除くすべてのアプリケーションを、ユーザーが起動できます。

  アプリケーションコントロールのこのモードは、規定では有効になっています。

- **許可リスト**：このモードでは、アプリケーションコントロールルールで許可および禁止されていないアプリケーション以外のアプリケーションを、ユーザーが起動できないようにします。

  必要なアプリケーションコントロールの許可ルールをすべて設定すると、LAN 管理者が検証していない新しいアプリケーションの起動はブロックされますが、オペレーティングシステムとユーザーが業務で使用している信頼するアプリケーションの動作は許可されます。

  許可リストモードでは、アプリケーションコントロールルールの設定における推奨事項を確認できます。

アプリケーションコントロールは、Kaspersky Endpoint Security のローカルインターフェイスと Kaspersky Security Center の両方で、これらのモードで動作するように設定できます。

Kaspersky Security Center が提供するツールには、Kaspersky Endpoint Security のローカルインターフェイスで使用できないものもあります。これらは次の用途で必要となります：

- アプリケーションカテゴリの作成

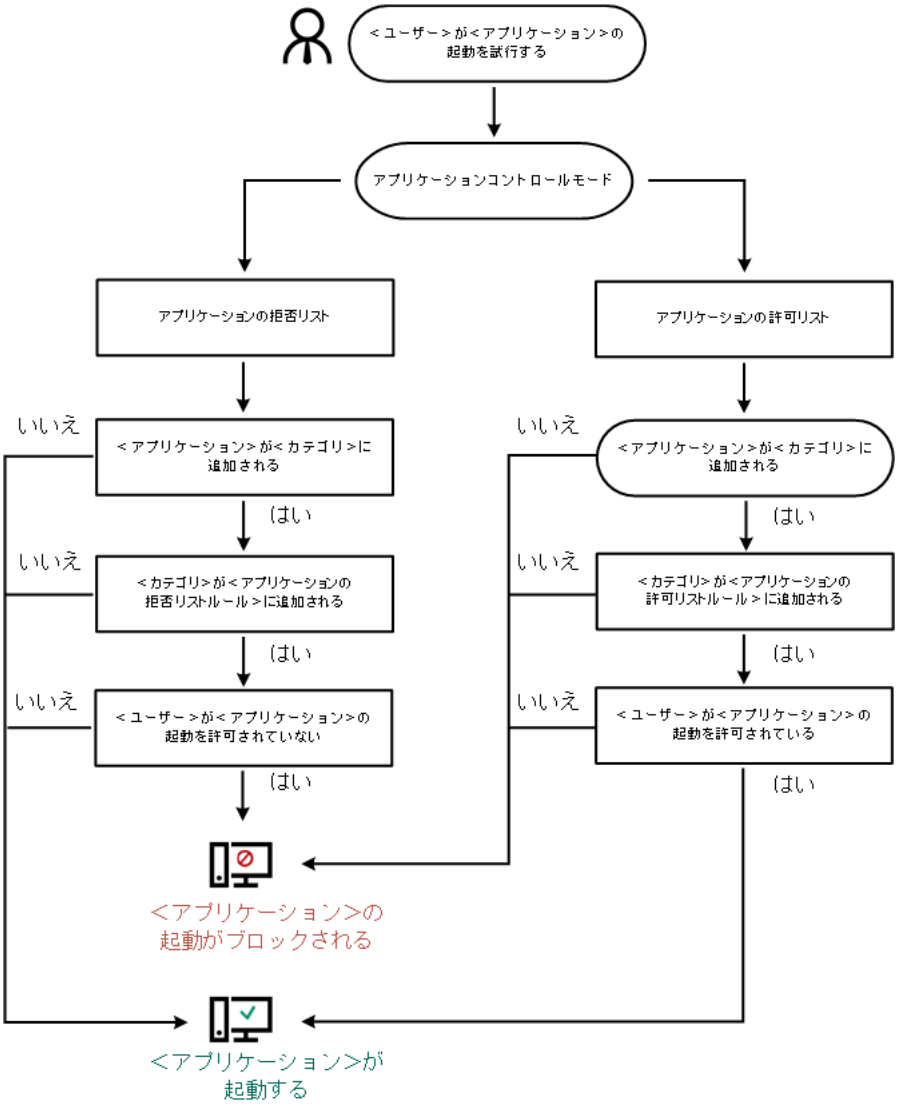
  Kaspersky Security Center の管理コンソールで作成するアプリケーションコントロールルールは、カスタマイズされたアプリケーションカテゴリに基づき、Kaspersky Endpoint Security のローカルインターフェイスでの対象条件や除外条件には基づきません。

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

そのため、アプリケーションコントロールの動作設定には Kaspersky Security Center の使用を推奨します。

アプリケーションコントロールの動作アルゴリズム

Kaspersky Endpoint Security は、アルゴリズムを使用して、アプリケーションの起動に関する決定を下します（下の図を参照）。



アプリケーションコントロールの動作アルゴリズム

パラメータ	説明
ルールによりブロックされたアプリケーションの開始時の操作	**ルールを適用**：Kaspersky Endpoint Security は選択したモードに従ってアプリケーションの開始を管理します。 **ルールをテスト運用**：アプリケーションコントロールの現在のモードでブロックされているアプリケーションの起動は許可されますが、起動に関する情報がレポートに記録されます。
アプリケーション起動コントロールモード	次のいずれかのオプションを選択できます： • **拒否リスト**：このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールの条件を満たす場合は除きます。 • **許可リスト**：このオプションを選択すると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールの条件を満たす場合は除きます。 **許可リスト**モードを選択すると、次の 2 つのアプリケーションコントロールルールが自動で作成されます： • **ゴールデンイメージ** • **信頼するアップデーター** 自動的に作成されたルールは、削除または編集することはできません。ルールを有効または無効にすることができます。
DLL モジュールの読み込みを監視する	このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。 どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、［アプリケーションコントロール］で、既定の［**ゴールデンイメージ**］ルールまたは［**ゴールデンイメージ\信頼済み証明書**］KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。［**ゴールデンイメージ**］ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。 Kaspersky Endpoint Security は、［DLL とドライバーを管理］をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。
厳密なデジタル署名検証を使用する	アプリケーションコントロールルールの適用条件として証明書を選択できます。 このチェックボックスをオンにすると、Kaspersky Endpoint Security は、信頼するシステム証明書ストアの証明書で署名されたアプリケーションにのみルールを適用します。このような証明書で署名されたアプリケーションは、さらに、マルウェアのスキャンタスクなどの保護機能によって信頼されていると判断されます。ただし、アプリケーションコントロールルールで別のストアの証明書を指定した場合、そのルールは適用されません。 チェックボックスをオフにすると、Kaspersky Endpoint Security は、Windows の信頼するルート証明書ストアの証明書で署名されたアプリケーションにルールを適用します。このようなアプリケーションは信頼ゾーンに含まれません。保護機能により、このようなアプリケーションの動作が監視されます。
アプリケーションのブロックに関するメッセージのテンプレートです	**ブロックに関するメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。 **管理者に送信するメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの起動ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

アダプティブアノマリーコントロール

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

アダプティブアノマリーコントロールは、企業のネットワーク内にあるコンピューターで一般的には発生しないはずの動作の監視とブロックを行います。アダプティブアノマリーコントロールでは、一般的には発生しないはずの異常な動作を監視するための複数のルール（「*Office アプリケーションによる Microsoft PowerShell の起動*」ルールなど）を使用します。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。アダプティブアノマリーコントロールの設定で、それぞれのルールで実行する処理を指定できます。たとえば、業務プロセスの自動化で使用されている PowerShell スクリプトはルールの適用対象から除外するように設定することができます。Kaspersky Endpoint Security は、定義データベースをアップデートするのと同様に、アダプティブアノマリーコントロールルールも Kaspersky から提供されている最新のルールにアップデートします。ルールのアップデートの適用は手動で承認する必要があります。

アダプティブアノマリーコントロールの設定

アダプティブアノマリーコントロールの設定では、次のステップが必要です：

1. アダプティブアノマリーコントロールのトレーニング

   アダプティブアノマリーコントロールを有効にすると、アダプティブアノマリーコントロールルールが*トレーニングモード*で動作します。トレーニング期間中、アダプティブアノマリーコントロールはルールを適用可能な動作が発生するかどうかを監視し、ルールを適用可能な動作が発生したらそのイベントを Kaspersky Security Center に送信します。ルールごとに、設定されているトレーニング期間は異なります。トレーニングモードの継続期間はカスペルスキーのエキスパートが設定しています。通常は、トレーニングモードの継続期間は 2 週間です。

   特定のルールを適用可能な動作がトレーニング期間中に 1 回も発生しなかった場合、アダプティブアノマリーコントロールは、そのルールの対象となる動作は平常時には発生しない動作だと判断します。そのため、トレーニング終了後、該当するルールの適用対象となる動作はすべて Kaspersky Endpoint Security でブロックされるようになります。

   特定のルールを適用可能な動作がトレーニング期間中に発生した場合、Kaspersky Endpoint Security は「ルールの適用のレポート」と［**「スマートトレーニング」ステータスのルール適用条件**］リポジトリにイベントのログ記録を保存します。

2. 「ルールの適用のレポート」の分析

   管理者は「ルールの適用のレポート」または［**「スマートトレーニング」ステータスのルール適用条件**］リポジトリの内容を分析する必要があります。分析結果に基づき、管理者はそれぞれのルールが適用されたときのアダプティブアノマリーコントロールによる処理を、「ブロック」または「許可」から選択します。管理者は、ルールの適用状況に関する情報をさらに収集した上で判断を行うために、トレーニングモードの期間を延長することもできます。また、管理者がルールの適用状況のレポートに対する対応を行わなかった場合も、アダプティブアノマリーコントロールは引き続きトレーニングモードで動作します。トレーニングモードの残り期間もリセットされます。

アダプティブアノマリーコントロールの設定は、リアルタイムで次の方法で設定されます：

- トレーニングモードの期間中に1回も適用可能な動作が発生しなかったルールについては、該当するルールが適用可能な動作をすべてブロックする設定が自動的に行われる。
- 新しいルールの追加や古くなったルールの削除が Kaspersky Endpoint Security によって行われる。
- 管理者がルール適用のレポートまたは**「スマートトレーニング」ステータスのルール適用条件**リポジトリの内容を確認した後、アダプティブアノマリーコントロールによる処理を設定します。ルールの適用に関するレポートと、[**「スマートトレーニング」ステータスのルール適用条件**] ストレージの内容をチェックすることをお勧めします。

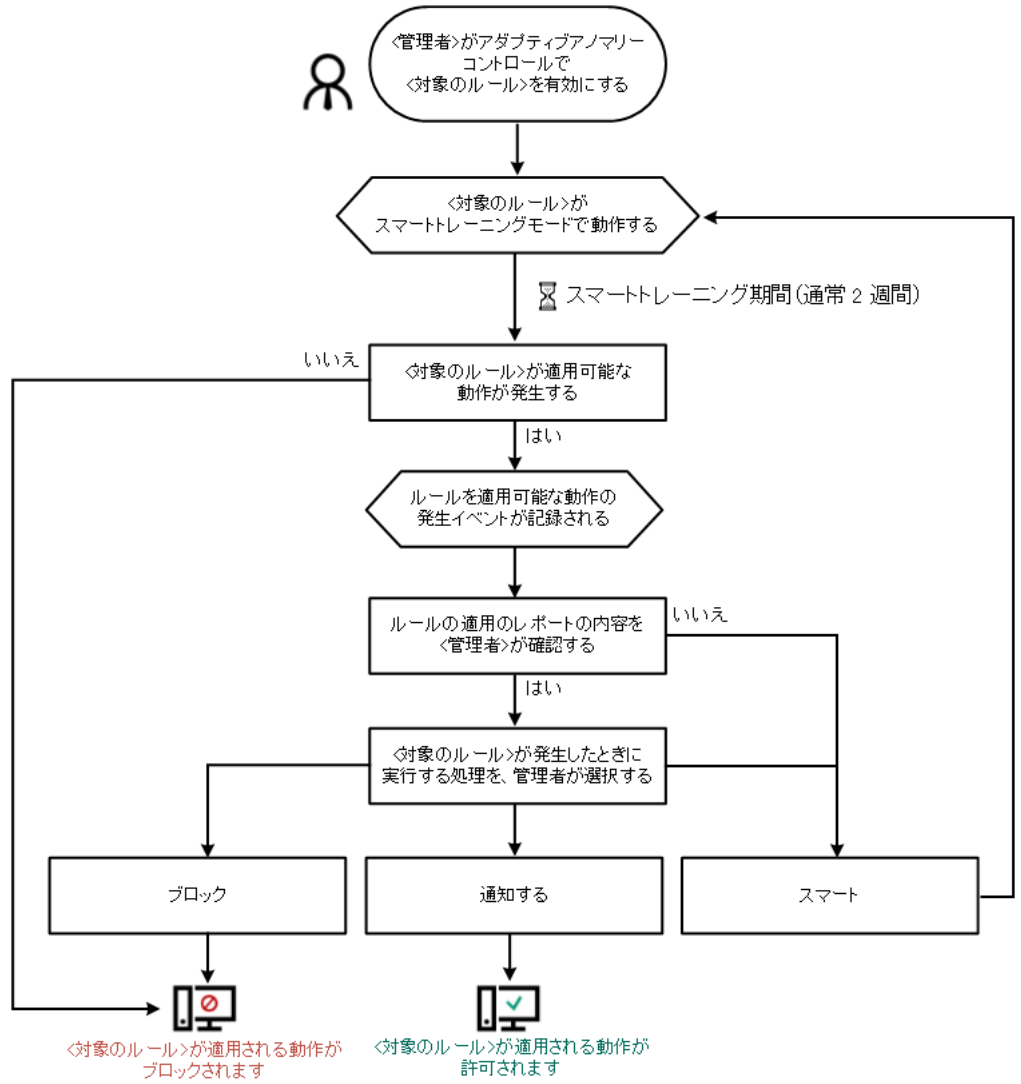
悪意のあるアプリケーションによる動作が検知された場合、Kaspersky Endpoint Security はその動作をブロックし通知を表示します（以下の図を参照）。



アダプティブアノマリーコントロールの通知

アダプティブアノマリーコントロールの動作アルゴリズム

Kaspersky Endpoint Security は次の図のアルゴリズムに従って、ルールの適用対象となる動作の実行を許可するかブロックするかを判定します。



アダプティブアノマリーコントロールの動作アルゴリズム

アダプティブアノマリーコントロールの設定

パラメータ	説明
アダプティブアノマリーコントロールルールのステータスに関するレポート *（Kaspersky Security Center コンソール内でのみ利用可能）*	このレポートにはアダプティブアノマリーコントロールの検知ルールの状態に関する情報が表示されます（ルールの状態が「*無効*」または「*ブロック*」など）。このレポートはすべての管理グループを対象に生成されます。
アダプティブアノマリーコントロールルールの適用に関するレポート *（Kaspersky Security Center コンソール内でのみ利用可能）*	このレポートには、アダプティブアノマリーコントロールを使用して検知された典型的でない動作に関する情報が含まれています。このレポートはすべての管理グループを対象に生成されます。

パラメータ	説明
ルール	アダプティブアノマリーコントロールのルールのリスト。これらのルールは、カスペルスキーのスペシャリストによって、悪意のあるソフトウェアが示す典型的な動作に基づいて作成されています。
テンプレート	**ブロックに関するメッセージ**：典型的でない動作をブロックするアダプティブアノマリーコントロールルールが適用された際に表示されるメッセージのテンプレート。 **管理者に送信するメッセージ**：ブロックが誤検知だと考えられる場合に、社内のローカルネットワークの管理者に送信できるメッセージのテンプレート。ユーザーがアクセス権を要求した後、Kaspersky Endpoint Security は Kaspersky Security Center にイベントを送信します：**アプリケーションの動作ブロックに関するメッセージが管理者に送信されました**。このイベントの説明には、代用変数を含む管理者へのメッセージが含まれます。これらのイベントは、事前定義されたイベント抽出［**ユーザー要求**］を使用して Kaspersky Security Center コンソールで確認できます。組織で Kaspersky Security Center が導入されていない、または管理サーバーに接続されていない場合は、本製品は指定されたメールアドレスの管理者にメッセージを送信します。

システム変更監視

このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

バージョン 12.6 から、Kaspersky Endpoint Security for Windows には、ファイル変更監視コンポーネントの代わりにシステム変更監視コンポーネントが含まれるようになりました。システム変更監視コンポーネントには、ファイル変更監視のすべての機能が含まれており、さらにレジストリの変更や外部デバイスの接続を監視することもできます。

システム変更監視コンポーネントは、コンピューターのセキュリティ侵害を示す可能性のあるオペレーティングシステムの変更を監視します。そのような変更を検知すると、Kaspersky Endpoint Security は対応するイベントを生成し、管理者に警告します。システム変更監視はリアルタイムモードで動作しますが、オンデマンドでシステム変更チェックを実行することもできます。

リアルタイムシステム変更監視

リアルタイムモードで、システム変更監視は、コンポーネントの範囲（*監視範囲*）に含めたオブジェクトへの変更を追跡します。システム変更監視では、このようなオブジェクトへの不正アクセスをリアルタイムでブロックすることもできます。

オンデマンドのシステム変更チェック

オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。*システム変更チェック*タスクを実行するには、コンポーネントの範囲（*監視範囲*）を設定して、ベースラインを作成します。ベースラインとは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。

システム変更監視設定の設定

パラメータ	説明
ブロックルールの操作モード	• **ブロックする**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成します。 • **通知する**：このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作を許可し、対応するイベントを生成します。

パラメータ	説明
リアルタイムシステム変更監視	リアルタイムモードで、システム変更監視は、コンポーネントの範囲（*監視範囲*）に含めたオブジェクトへの変更を追跡します。システム変更監視では、このようなオブジェクトへの不正アクセスをリアルタイムでブロックすることもできます。
デバイスを監視する	システム変更監視は、外部デバイスの接続と接続解除を監視します。
ファイルとレジストリを監視する	システム変更監視は、ファイル、フォルダー、レジストリへの変更を監視します。
システム変更チェック	オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。*システム変更チェック*タスクを実行するには、コンポーネントの範囲（*監視範囲*）を設定して、ベースラインを作成します。ベースラインとは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。

Endpoint Sensor

Kaspersky Endpoint Security 11.4.0 には Endpoint Sensor は含まれていません。

Kaspersky Security Center Web コンソールおよび Kaspersky Security Center 管理コンソールで Endpoint Sensor を管理できます。Kaspersky Security Center Cloud コンソールでは Endpoint Sensor を管理できません。

Endpoint Sensor は、Kaspersky Anti Targeted Attack Platform と連携するよう設計されています。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Endpoint Sensor の管理には次の制限事項があります：

- Kaspersky Endpoint Security のバージョン 11.0.0 から 11.3.0 がコンピューターにインストールされている場合は Endpoint Sensor の設定をポリシー内で設定できます。ポリシーを使用した Endpoint Sensor の設定について詳しくは、以前のバージョンの Kaspersky Endpoint Security のヘルプの記事 を参照してください。
- Kaspersky Endpoint Security のバージョン 11.4.0 以降のバージョンがインストールされていると、ポリシー内で Endpoint Sensor を設定することはできません。

Endpoint Sensor は、クライアントコンピューターにインストールされます。これらのコンピューターで、コンポーネントはプロセス、有効なネットワーク接続、変更されたファイルを継続的に監視し、その情報を KATA サーバーに渡します。

このコンポーネントは、以下のオペレーティングシステムで動作します：

- Windows 7 Service Pack 1 Home / Professional / Enterprise
- Windows 8.1.1 Professional / Enterprise
- Windows 10 RS3 Home / Professional / Education / Enterprise
- Windows 10 RS4 Home / Professional / Education / Enterprise
- Windows 10 RS5 Home / Professional / Education / Enterprise
- Windows 10 RS6 Home / Professional / Education / Enterprise
- Windows Server 2008 R2 Foundation / Standard / Enterprise （64 ビット）
- Windows Server 2012 Foundation / Standard / Enterprise （64 ビット）
- Windows Server 2012 R2 Foundation / Standard / Enterprise （64 ビット）
- Windows Server 2016 Essentials / Standard （64 ビット）

KATA の動作について詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Sandbox

Kaspersky Endpoint Security for Windows には Kaspersky Sandbox ソリューションとの連携用の組み込みエージェントが含まれるようになりました。*Sandbox* コンポーネントはコンピューター上の高度な脅威を検知し、自動的にブロックします。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。ソリューションについて詳しくは、Kaspersky Sandbox のヘルプおよび Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

バージョン 12.7 以降、Kaspersky Endpoint Security for Windows は、Kaspersky Anti Targeted Attack Platform ソリューションの一部である Sandbox コンポーネントをサポートします。Kaspersky Sandbox ソリューションとは対照的に、KATA Sandbox コンポーネントでは、自動でファイルをスキャンできるだけでなく、ファイルコンテキストメニューから手動でスキャンすることもできます。

KATA Sandbox を使用するには、Kaspersky Anti Targeted Attack Platform 7.0 以降を導入する必要があります。

この機能は Kaspersky Security Center Web コンソールを使用した場合のみ管理できます。管理コンソール（MMC）を使用してこの機能を管理することはできません。

Sandbox コンポーネントの設定

パラメータ	説明
連携モード	**Kaspersky Sandbox**：Kaspersky Sandbox ソリューションとの連携本製品によって Kaspersky Sandbox でスキャンするファイルが送信されるのは、自動モードの場合のみです。 **KATA Sandbox**：Kaspersky Anti Targeted Attack Platform ソリューションの Sandbox コンポーネントとの連携スキャン用ファイルの送信モードを選択できます： • **手動**：ユーザーはコンテキストメニューから手動でスキャン用ファイルを送信します（[**Sandbox に送る**]）。 • **自動**：本製品はオブジェクトを自動的に検知し、スキャンのために Sandbox に送信します。 • **複合**
サーバーの接続設定	**タイムアウト（ミリ秒）**：Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）の接続タイムアウト。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、サーバーの接続タイムアウトの時間を長くすることができます。要求のタイムアウトは 0.5 秒以下を推奨します。 **要求のキュー**：要求のキューフォルダーのサイズです。Sandbox でスキャンするために複数のオブジェクトを送信する場合、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは 100 MB に制限されています。最大サイズに到達すると、Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。 **サーバー TLS 証明書**：Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）との信頼済みの接続を設定するには、TLS 証明書を準備する必要があります。次に、ポリシーを使用してこの証明書をコンピューターに追加する必要があります。また、証明書を Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）に追加する必要があります。 **相互認証を使用する**：（KATA Sandbox のみ）。Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。
Sandbox サーバーへの接続	**Kaspersky Sandbox**Sandbox サーバーの接続設定です。サーバーは配備された Microsoft Windows オペレーティングシステムの仮想イメージを使用してスキャンする必要のあるオブジェクトを実行します。IP アドレス（IPv4 または IPv6）、または完全修飾ドメイン名を入力できます。 **KATA Sandbox**Central Node サーバーの接続設定。Central Node によって、スキャンの最適な設定が選択されて、Sandbox サーバー間の負荷が分散されます。
脅威の検知時の処理	**コピーを隔離に移動し、オブジェクトを削除する**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。 **簡易スキャンを実行する**：このオプションを選択した場合、Kaspersky Endpoint Security は*簡易スキャン*タスクを実行します。既定では、カーネルメモリ、実行中のプロセスおよびスタートアップオブジェクト、ディスクブートセクターをスキャンします。 **IOC スキャンタスクを作成する**：このオプションを選択した場合、Kaspersky Endpoint Security は自動的に *IOC スキャン*（*自動 IOC スキャンタスク*）を作成します。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、簡易スキャンタスクの実行）を設定できます。このタスクに対して、実行モード、スキャン範囲、また IOC の検知時の動作（オブジェクトの削除、*簡易スキャンタスク*の実行）を設定できます。その他の *IOC スキャンタスク*の設定を変更するには、タスクの設定に移動してください。
IOC スキャン範囲	**重要なファイル領域**：このオプションを選択した場合、Kaspersky Endpoint Security はカーネルメモリやブートセクターのような、コンピューター上の重要なファイル領域にのみ IOC スキャンを実行します。 **コンピューターのシステムドライブのファイル領域**：このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターのシステムドライブで IOC スキャンを実行します。
IOC スキャンタスクを実行する	**手動**：都合の良いときに手動で *IOC スキャンタスク*を開始できる実行方法です。 **自動**：脅威が検知されたときに自動で Kaspersky Endpoint Security が *IOC スキャンタスク*を実行する実行モードです。 **コンピューターを使用していないときにのみ実行する**：スクリーンセーバーが動作しているまたは画面がロックされているときに Kaspersky Endpoint Security が *IOC スキャンタスク*を実行する実行モードです。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はタスクを一時停止します。このため、タスクの完了まで数日かかることがあります。

Managed Detection and Response

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

Managed Detection and Response の設定

パラメータ	説明
MDR 設定情報ファイル	BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows には Kaspersky Endpoint Detection and Response Optimum ソリューション（以降、「EDR Optimum」とも表記）向けの組み込みエージェントが含まれるようになりました。バージョン 11.8.0 から、Kaspersky Endpoint Security for Windows には Kaspersky Endpoint Detection and Response Expert ソリューション（以降、「EDR Expert」とも表記）向けの組み込みエージェントが含まれるようになりました。*Kaspersky Endpoint Detection and Response* は、高度なサイバー脅威から企業の IT インフラストラクチャを保護する幅広いソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。EDR Expert は EDR Optimum に比べ、より多くの脅威監視および応答機能を備えています。ソリューションについて詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

Kaspersky Endpoint Detection and Response Optimum は脅威の活動を確認して分析し、迅速な対応に必要となる攻撃の可能性に関する情報を*セキュリティの担当者*または*管理者*に提供します。Kaspersky Endpoint Detection and Response は別のウィンドウでアラートの詳細を表示します。*アラート*とは、本製品によって異常または疑わしいと識別され、企業の IT インフラストラクチャにセキュリティ上の脅威をもたらす可能性がある、企業の IT インフラストラクチャ内のイベントです。*アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

Web コンソールおよび Cloud コンソールで EDR Optimum を設定できます。EDR Expert のコンポーネントの設定は Cloud コンソールのみで使用可能です。

パラメータ	説明
詳細なシステム動作の記録を有効にする	拡張テレメトリにより IOC 検知の精度は向上しますが、コンピューターのリソースの消費量も増加します。遡及的 IOC スキャンを行う場合、コンピューターで拡張テレメトリを有効にすることを推奨します。*遡及的 IOC スキャン*は、Kaspersky Endpoint Security が一定期間のデータを使用してセキュリティ侵害インジケーターをスキャンする *IOC スキャンタスク*のモードです。このモードは、コンピューターのネットワーク動作のデータ内のセキュリティ侵害インジケーターを検知することを目的としています。 拡張テレメトリが無効になっている場合、Kaspersky Endpoint Security は検知されたセキュリティ侵害インジケーターに関する情報を置き換えることがあります。
ネットワーク分離	検知された脅威への対応として、ネットワークからコンピューターを自動的に分離します。 ネットワーク分離がオンになると、本製品はすべてのアクティブな接続を切断し、コンピューターのすべての新規 TCP/IP 接続をブロックします。次の接続のみ有効にします： • ネットワーク分離の除外リストに追加されている接続。 • Kaspersky Endpoint Security サービスによって開始された接続。 • Kaspersky Security Center ネットワークエージェントによって開始された接続。
次の時間の経過後、分離されたデバイスを自動的にロック解除する（時間）	ネットワーク分離は、指定した時間の経過後に自動で、または手動で解除することができます。既定では、Kaspersky Endpoint Security は分離の開始から 5 時間が経過するとネットワーク分離を解除します。
ネットワーク分離の除外リスト	ネットワーク分離から除外されるルールのリストです。ネットワーク分離がオンになっても、ルールに一致するネットワーク接続はブロックされません。 *標準のネットワークプロファイル*のリストを使用してネットワーク分離の除外リストを設定できます。既定では、除外リストには DNS/DHCP サーバーおよび DNS/DHCP クライアントロールを持つデバイスの動作が妨げられないようにするルールを含むネットワークプロファイルが含まれています。標準のネットワークプロファイルまたは除外リストの設定は手動で変更できます。 ポリシーのプロパティで指定された除外リストは、脅威の検知時の対応としてネットワーク分離が自動的にオンになった場合にのみ適用されます。コンピューターのプロパティで指定された除外リストは、Kaspersky Security Center のコンソールのコンピューターのプロパティまたはアラートの詳細から手動でネットワーク分離をオンにした場合にのみ適用されます。
実行防止	実行ファイルやスクリプトを実行したり、Office 形式のファイルを開いたりする動作をコントロールします。たとえば、選択したコンピューター上で安全でないと判断されたアプリケーションの実行を防止することができます。実行防止は、Office ファイルの拡張子のセットおよびスクリプトインタープリターのセットをサポートしています。 実行防止機能を使用するには、実行防止ルールを追加する必要があります。*実行防止ルール*とは、オブジェクトの実行のブロックなど、製品がオブジェクトの実行時への対応時に適用する一連の条件です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。
禁止されたオブジェクトを実行、または開いたときの処理	**ブロックしイベントログへ追加する**：このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントを Windows イベントログおよび Kaspersky Security Center のイベントログに記録します。 **イベントログに追加する**：このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベント Windows イベントログと Kaspersky Security Center のイベントログに記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。
実行防止のルール	*実行防止ルール*とは、オブジェクトの実行のブロックなど、製品がオブジェクトの実行時への対応時に適用する一連の条件です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。

パラメータ	説明
Cloud Sandbox	*Cloud Sandbox* はコンピューター上のより高度な脅威を検知する技術です。Kaspersky Endpoint Security は、検知したファイルを自動的に Cloud Sandbox に送って分析します。Cloud Sandbox はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してそのファイルの評価を決定します。これらのファイルのデータは Kaspersky Security Network に送られます。このため、Cloud Sandbox が悪意のあるファイルを検知すると、Kaspersky Endpoint Security はこのファイルが検出されたすべてのコンピューター上でこの脅威を除去するための適切な操作を実行します。 Cloud Sandbox 技術は、使用しているライセンス種別にかかわらずすべての Kaspersky Security Network ユーザーに対して有効で使用可能です。 このチェックボックスをオンにすると、Kaspersky Endpoint Security は［**脅威検知技術**］の下のメインウィンドウで Cloud Sandbox を使用して検知された脅威向けのカウンターを有効にします。また、Kaspersky Endpoint Security では製品イベントおよび Kaspersky Security Center コンソールの *脅威レポート* で Cloud Sandbox 脅威検知技術が表示されます。

Endpoint Detection and Response Expert（オンプレミス）

Endpoint Detection and Response Expert（オンプレミス）

Kaspersky Endpoint Security for Windows は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションとの連携をサポートしています。*Kaspersky Endpoint Detection and Response Expert（オンプレミス）*は、組織がほとんどの種別のサイバーリスクを防ぎ、最も重要な脅威の拡散シナリオに対応できるようにするカスペルスキー製品を含むエンタープライズ向けのサイバーセキュリティソリューションです。EDR Expert（オンプレミス）コンポーネントは、Open Single Management Platform (OSMP) に配備されます。このプラットフォームは、単一のインターフェイスでクロスプラットフォームのシナリオを実行し、カスペルスキー製品とサードパーティ製品を包括的なセキュリティシステムに統合することを可能にします。

ソリューションの中心的な要素の 1 つは *SIEM* です。SIEM は、すべてのコンポーネントからのイベントを追跡し、ベンダーおよびユーザー定義のルールを使用してこれらのイベントを相互に関連付けます。EDR Expert（オンプレミス）は、企業インフラストラクチャから受信したログとテレメトリを調べて攻撃を自動的に検出し、 カスペルスキー製品やサードパーティの情報セキュリティ製品からのイベントを含む、EDR Expert（オンプレミス）で収集されたすべてのイベントを組み合わせた統合調査グラフを使用してインシデントの調査を可能にします。

高度なインシデントに対応するために、EDR Expert（オンプレミス）は、事前設定されたシナリオとユーザー定義のシナリオを使用します。サードパーティ製品からの対応処理や、複数のアプリケーションが関係する対応シナリオを使用することもできます。

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows は、Kaspersky Anti Targeted Attack Platform (EDR (KATA))ソリューションの一部である Kaspersky Endpoint Detection and Response コンポーネントとの連携をサポートします。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリデータ）は Kaspersky Anti Targeted Attack Platform サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検出した脅威に関する情報およびその脅威の処理結果についての情報を Kaspersky Anti Targeted Attack Platform サーバーに 送信します。

EDR (KATA) および NDR (KATA) 連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Kaspersky Anti Targeted Attack Platform コンソールを使用して管理されるようになります。

Endpoint Detection and Response Expert（オンプレミス）の設定

パラメータ	説明
テレメトリ収集サーバーへの接続	*テレメトリの収集サーバー*は、コンピューター上で発生するイベントに関する情報を収集、正規化、関連付け、分析、保存する SIEM ソリューションの一部であるサーバーです。 テレメトリ収集サーバー（KUMA）に接続するには、次を設定します： • **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。 • **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。 • **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。
アドレス：および**ポート**（テレメトリ収集サーバー）	テレメトリ収集サーバーに接続するための設定。IP アドレス（IPv4 または IPv6）を入力できます。 複数のテレメトリ収集サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
テレメトリ収集サーバーにテレメトリを送信する	この機能を使用して KATA サーバーへのテレメトリの送信を完全にオフにすることができます。例えば、テレメトリを使用する別のソリューションとあわせて Kaspersky Anti Targeted Attack Platform を使用している場合は、KATA (EDR) 向けのテレメトリ送信をオフにすることができます。これにより、これらのソリューションのサーバー負荷を最適化することができます。Managed Detection and Response ソリューションと KATA (EDR) を導入している場合、MDR テレメトリを使用して KATA (EDR) で脅威応答タスクを作成することができます。 • **IOA のあるテレメトリのみ送信する**：これにより、テレメトリを最適化し、IOA のあるテレメトリのみを送信できるようになります。*攻撃の痕跡（IOA）*は、標的型攻撃を示す可能性のあるシステム内の疑わしい動作の説明を含むルールです。本製品は、システム内で進行中の動作をこれらのルールと比較し、標的型攻撃を示唆するイベントをログに記録します。本製品は、このようなイベントをリアルタイムで追跡できる*ストリーミングスキャン*の技術を採用しています。 • **最大イベント転送遅延時間（秒）**：指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。 • **転送ごとのイベントパケット数を制限する**：バッファがイベントでいっぱいになると、本製品はサーバーと同期します。既定値は 1024 イベントです。この機能を使用すると、サーバーとの同期の前のイベントのバッファリングを無効にすることができます。
リクエストの調整を有効にする	これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。 テレメトリを設定します： • **1 時間ごとのイベントの最大数**：本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1 時間後にイベントの送信は再開されます。1 時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を 1 時間あたり 60,000 イベントに増やすことを推奨します。 • **イベントの制限超過のパーセンテージ**：本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。
サーバーに同期リクエストを送信する間隔（分）	サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。

パラメータ	説明
応答サーバーへの接続	*応答サーバー*は、データを受信してスキャンし、オブジェクトのふるまいを調査し、そのような調査結果を公開するためのサーバーです。 応答サーバーの接続用に以下を設定します： • **タイムアウト（秒）**：サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。 • **サーバー証明書**：サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。 • **相互認証を使用する**：Kaspersky Endpoint Security とサーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナは Open Single Management Platform で取得できます（Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください）。サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。
アドレス：および**ポート**（応答サーバー）	応答サーバーに接続するための設定。IP アドレス（IPv4 または IPv6）を入力できます。 複数のテレメトリ収集サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

Endpoint Detection and Response (KATA) の設定

パラメータ	説明
サーバーに同期リクエストを送信する間隔（分）	サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。
KATA サーバーへの接続	Central Node サーバー接続用に以下を設定します： • **タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。 • **サーバー証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。 • **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。
アドレス：および**ポート**（KATA サーバー）	Kaspersky Anti Targeted Attack Platform サーバーへの接続を設定します。Central Node サーバーの IP アドレス（IPv4、IPv6）とサーバーに接続するポートを指定します。 複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
KATA にテレメトリを送信する	この機能を使用して KATA サーバーへのテレメトリの送信を完全にオフにすることができます。例えば、テレメトリを使用する別のソリューションとあわせて Kaspersky Anti Targeted Attack Platform を使用している場合は、KATA (EDR) 向けのテレメトリ送信をオフにすることができます。これにより、これらのソリューションのサーバー負荷を最適化することができます。Managed Detection and Response ソリューションと KATA (EDR) を導入している場合、MDR テレメトリを使用して KATA (EDR) で脅威応答タスクを作成することができます。 テレメトリを設定します： • **最大イベント転送遅延時間（秒）**：指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。 • イベントパッケージの最大数バッファがイベントでいっぱいになると、本製品はサーバーと同期します。既定値は 1024 イベントです。

パラメータ	説明
リクエストの調整を有効にする	これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。 テレメトリを設定します： • **1時間ごとのイベントの最大数**：本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1時間後にイベントの送信は再開されます。1時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を1時間あたり 60,000 イベントに増やすことを推奨します。 • **イベントの制限超過のパーセンテージ**：本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows は、Kaspersky Anti Targeted Attack Platform (EDR (KATA))ソリューションの一部である Kaspersky Network Detection and Response コンポーネントとの連携をサポートします。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリデータ）は Kaspersky Anti Targeted Attack Platform サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検出した脅威に関する情報およびその脅威の処理結果についての情報を Kaspersky Anti Targeted Attack Platform サーバーに 送信します。

EDR (KATA) および NDR (KATA) 連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Kaspersky Anti Targeted Attack Platform コンソールを使用して管理されるようになります。

Network Detection and Response (KATA) のパラメータ

パラメータ	説明
サーバーの接続設定	**タイムアウト（秒）**：Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。 **サーバー TLS 証明書**：Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。 **相互認証を使用する**：Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。

パラメータ	説明
アドレスおよび**ポート**	Kaspersky Anti Targeted Attack Platform サーバーへの接続を設定します。Central Node サーバーの IP アドレス（IPv4、IPv6）とサーバーに接続するポートを指定します。 複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
NDR サーバーに同期リクエストを送信する間隔（分）	サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。
最大イベント転送遅延時間（秒）	指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。
リクエストの調整を有効にする	これは、サーバーの負荷の最適化に役立ちます。このチェックボックスがオンになっていると、本製品はイベントの転送を制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。
1 時間ごとのイベントの最大数	本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1 時間後にイベントの送信は再開されます。1 時間あたりの既定値は 3000 イベントです。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を 1 時間あたり 60,000 イベントに増やすことを推奨します。
イベントの制限超過のパーセンテージ	本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。既定値は 15 % です。

KUMA との連携

Kaspersky Endpoint Security for Windows は、Kaspersky Unified Monitoring and Analysis Platform ソリューションをサポートしています。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* は、組織の IT インフラストラクチャ向けの SIEM (Security Information and Event Management) ソリューションです。KUMA を使用すると、セキュリティ上の脅威が被害をもたらす前にそれを検知、分析し、緩和することができます。

KUMA 連携設定

パラメータ	説明
イベント送信時の最大遅延（秒）	指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。既定値は 30 秒です。
KUMA サーバーへの接続	**タイムアウト（秒）**：KUMA サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の KUMA サーバーに接続を試みます。 **サーバー証明書**：KUMA サーバーと信頼済みの接続を確立するための TLS 証明書。Kaspersky Unifield Monitoring and Analysis Platform コンソールで TLS 証明書を取得できます（Kaspersky Unified Monitoring and Analysis Platform の手順を参照してください）。 信頼済みの接続を確立するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**With verification**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプ を参照してください）。 **相互認証を使用する**：Kaspersky Endpoint Security と KUMA 間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**Custom PFX**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプ を参照してください）。次に、暗号化コンテナーを取得し、暗号コンテナーを保護するためのパスワードを設定する必要があります。*暗号化コンテナー*とは、証明書と秘密鍵が含まれた PFX アーカイブです。KUMA を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナーはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナーを追加することはできません。
KUMA サーバー	Kaspersky Unified Monitoring and Analysis Platform サーバーへの接続設定。IP アドレス（IPv4 または IPv6）を入力できます。 複数の KUMA サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスでサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスで接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。

ディスク全体の暗号化

次の暗号化技術を選択できます：Kaspersky Disk Encryption、BitLocker ドライブ暗号化（単に BitLocker とも）。

Kaspersky Disk Encryption

システムハードディスクが暗号化されると、次回のコンピューターの起動時、ユーザーはハードディスクにアクセスしてオペレーティングシステムを読み込む前に認証エージェントによる認証を完了する必要があります。それには、コンピューターに接続されているトークンまたはスマートカードのパスワードを入力するか、*認証エージェントアカウントの管理*タスクを使用して LAN 管理者により作成される認証エージェントアカウントのユーザー名とパスワードを入力します。これらのアカウントは、ユーザーがオペレーティングシステムにログインする際にログインアカウントとして使用する Microsoft Windows アカウントに基づいています。また、認証エージェントアカウントのユーザー名とパスワードを使用してオペレーティングシステムに自動的にログインできるSingle Sign-On（シングルサインオン、SSO）技術を使用することもできます。

認証エージェントでのユーザー認証は 2 通りの方法で実行できます：

- LAN 管理者が Kaspersky Security Center ツールを使用して作成した認証エージェントアカウントの名前とパスワードを入力する。
- コンピューターに接続されたトークンまたはスマートカードのパスワードを入力する。

> トークンやスマートカードは、コンピューターのハードディスクが AES256 アルゴリズムを使用して暗号化されている場合にのみ使用できます。コンピューターのハードディスクが AES56 アルゴリズムで暗号化された場合、コマンドへの電子署名ファイルの追加は拒否されます。

BitLocker ドライブ暗号化

BitLocker は、Windows オペレーティングシステムに組み込まれた暗号化技術です。Kaspersky Endpoint Security では、Kaspersky Next のインフラストラクチャを使用して BitLocker を制御および管理できます。BitLocker は論理ボリュームを暗号化します。BitLocker はリムーバブルドライブの暗号化には使用できません。BitLocker について詳しくは、Microsoft 社の資料を参照してください。

> BitLocker は、ディスクを暗号化する際に、ブートローダーとその他の補助ファイルを system partition に配置します。このパーティションは暗号化されません。Windows のインストール中に、オペレーティングシステムによって、システムパーティションが自動的に作成されます。Windows をインストールする前にディスクが完全にパーティション分割されている場合、オペレーティングシステムはシステムパーティションを作成できません。この場合、BitLocker のディスク暗号化を開始すると、オペレーティングシステムは、ディスクを再パーティション化してシステムパーティションを作成するよう要求します。システムパーティションが作成されると、オペレーティングシステムによって BitLocker 暗号化が開始されます。

BitLocker 信頼済みプラットフォームモジュールを使用して、安全なアクセスキーの保管領域を提供します。*Trusted Platform Module*（TPM）は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。TPM は起動前のシステム整合性検証を行うため、TPM を使用すると最も安全に BitLocker アクセスキーを保管できます。TPM なしでもコンピューター上のドライブを暗号化することは可能です。この場合は、アクセスキーはパスワードで暗号化されます。BitLocker は次の暗号化の方法を使用します：

- TPM。
- TPM と PIN。
- パスワード。

システムの暗号化後、ユーザーはオペレーティングシステムを起動するために BitLocker 認証の手順を完了する必要があります。認証後、 BitLocker はユーザーのログインを許可します。BitLocker はシングルサインオン（SSO）をサポートしていません。

ドライブを暗号化した後、BitLocker はマスター鍵を作成します。Kaspersky Endpoint Security はこのマスター鍵を Kaspersky Security Center に送るため、ユーザーがパスワードを忘れた場合などにディスクへのアクセスを復元することができます。

ユーザーが BitLocker を使用してディスクを暗号化すると、Kaspersky Endpoint Security は Kaspersky Security Center にディスク暗号化に関する情報 を送ります。一方、Kaspersky Endpoint Security はマスター鍵を Kaspersky Security Center に送らないため、Kaspersky Security Center を使用してディスクへのアクセスを復元することはできません。Kaspersky Security Center と BitLocker が正しく動作するために、ドライブの復号化および再暗号化にはポリシーを使用してください。ローカルで、またはポリシーを使用してドライブを復号化できます。

Windows のグループポリシーを使用している場合、ポリシーで BitLocker の管理をオフにしてください。Windows のポリシー設定は Kaspersky Endpoint Security のポリシー設定と競合する可能性があります。ドライブの暗号化の際にエラーが発生する可能性があります。

Kaspersky Disk Encryption の設定

パラメータ	説明
暗号化モード	**すべてのハードディスクを暗号化する**：このオプションをオンにすると、ポリシーが適用された時点ですべてのハードディスクが暗号化されます。 コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。 **すべてのハードディスクを復号化する**：このオプションをオンにすると、ポリシーの適用時、それ以前に暗号化されていたすべてのハードディスクが復号化されます。 **変更しない**：このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。
暗号化中に Windows ユーザー向けの認証エージェントアカウントを自動的に作成する	このチェックボックスをオンにすると、コンピューター上の Windows ユーザーアカウントのリストに基づいて認証エージェントアカウントを作成します。既定では、Kaspersky Endpoint Security は、過去 30 日間にユーザーがオペレーティングシステムにログインしたすべてのローカルアカウントとドメインアカウントを使用します。

パラメータ	説明
認証エージェントアカウント作成の設定	**コンピューター上のすべてのアカウント**：常時有効なコンピューター上のすべてのアカウント。 **コンピューター上のすべてのドメインアカウント**：いずれかのドメインに属しており、常時有効なコンピューター上のすべてのアカウント。 **コンピューター上のすべてのローカルアカウント**：常時有効なコンピューター上のすべてのローカルアカウント。 **ワンタイムパスワードが設定されたサービスアカウント**：サービスアカウントは、ユーザーがパスワードを忘れたときなどにコンピューターへのアクセス権を取得するために必要です。このサービスアカウントは予備のアカウントとして使用することもできます。アカウントの名前を入力する必要があります（既定では `ServiceAccount` です）。Kaspersky Endpoint Security はパスワードを自動で作成します。Kaspersky Security Center コンソールでパスワードを確認できます。 **ローカル管理者**：Kaspersky Endpoint Security は、コンピューターのローカル管理者に認証エージェントのユーザーアカウントを作成します。 **コンピューター管理者**：Kaspersky Endpoint Security は、コンピューター管理者に認証エージェントのユーザーアカウントを作成します。Active Directory のコンピューターのプロパティで、どのアカウントがコンピューター管理者ロールを持っているか確認できます。既定では、コンピューター管理者ロールは定義されておらず、どのアカウントにも紐づけられていません。 **アクティブなアカウント**：Kaspersky Endpoint Security は、ディスクの暗号化時に有効になっているアカウントに対して自動的に認証エージェントアカウントを作成します。
このコンピューターのすべてのユーザーの初回ログイン時に認証エージェントアカウントを自動で作成する	このチェックボックスをオンにすると、認証エージェントの開始前にコンピューター上の Windows ユーザーアカウントに関する情報をチェックします。認証エージェントアカウントを持たない Windows ユーザーアカウントを検知すると、Kaspersky Endpoint Security は暗号化ドライブにアクセスするための新規アカウントを作成します。認証エージェントアカウントには次の既定の設定（パスワードで保護されているログインのみ、初回認証時のパスワード変更を要求）が適用されています。そのため、すでに暗号化されたドライブを持つコンピューター用に*認証エージェントアカウントの管理*タスクを使用して認証エージェントを手動で追加する必要はありません。
認証エージェントに入力したユーザー名を保存する	チェックボックスをオンにすると、認証エージェントアカウントの名前が保存されます。次回、認証エージェントで同じアカウントを使用して認証を完了しようとした場合、アカウント名の入力は要求されません。
使用されているディスク領域のみを暗号化（暗号化時間を短縮）	このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。 暗号化の開始後に［**使用されているディスク領域のみを暗号化（暗号化時間を短縮）**］を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。 このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。 チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。 データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。既に使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。 既定では、このチェックボックスはオフです。
レガシー USB サポートを使用する（推奨されません）	このチェックボックスでは、Legacy USB Support 機能を有効または無効にします。*レガシー USB サポート*は BIOS / UEFI 機能であり、オペレーティングシステム（BIOS モード）を起動する前のコンピューターのブートフェーズ中に USB デバイス（セキュリティトークンなど）を使用することができます。レガシー USB サポートは、オペレーティングシステムが起動した後の USB デバイスのサポートには影響しません。 このチェックボックスをオンにすると、コンピューター起動中の USB デバイスのサポートが有効になります。 レガシー USB サポート（Legacy USB Support）が有効になっている場合、BIOS モードの認証エージェントでは USB を介してトークンを操作することはできません。ハードウェアの互換性の問題が発生しているコンピューターでのみ、このオプションをオンにしてください。
パスワードの設定	認証エージェントアカウントのパスワード強度設定。シングルサインオン技術を使用する場合、認証エージェントは Kaspersky Security Center で指定されたパスワードの強度の要件を無視します。パスワードの強度の要件は、オペレーティングシステムの設定で設定できます。

パラメータ	説明
シングルサインオン（SSO）技術を使用する	SSO 技術を使用すると、暗号化されたハードディスクにアクセスする際やオペレーティングシステムにサインインする際に、同一のアカウント認証情報を使用できます。 このチェックボックスをオンにすると、アカウントの資格情報を入力してから暗号化されたハードディスクにアクセスすればオペレーティングシステムに自動的にログインできます。 このチェックボックスをオフにすると、暗号化されたハードディスクにアクセスしてからオペレーティングシステムにログインする場合に、暗号化されたハードディスクへのアクセスに必要な資格情報と、オペレーティングシステムのユーザーアカウントの資格情報を個別に入力する必要があります。
サードパーティの資格情報プロバイダーをラップする	Kaspersky Endpoint Security では、サードパーティの資格情報プロバイダー ADSelfService Plus がサポートされます。 サードパーティの資格情報プロバイダーと連携する際には、認証エージェントはオペレーティングシステムが読み込まれる前にパスワードを読み取ります。つまり、ユーザーがパスワードを入力する必要があるのは、Windows にログインするときの1度のみということです。Windows にログインした後、ユーザーは企業のサービスの認証などにサードパーティの資格情報プロバイダーを使用することができます。サードパーティの資格情報プロバイダーを使用して、ユーザーは個別に自身のパスワードをリセットすることが可能です。この場合、Kaspersky Endpoint Security は認証エージェントのパスワードを自動的に更新します。 本製品がサポートしていないサードパーティの資格情報プロバイダーを使用している場合は、シングルサインオン技術の操作に制限がある可能性があります。
ヘルプ	**認証**：アカウントの認証情報を入力するときに認証エージェントウィンドウに表示されるヘルプテキスト。 **パスワードの変更**：認証エージェントアカウントのパスワードを変更するときに、認証エージェントウィンドウに表示されるヘルプテキスト。 **パスワードの復元**：認証エージェントアカウントのパスワードを復元するときに、認証エージェントウィンドウに表示されるヘルプテキスト。

BitLocker ドライブ暗号化の設定

パラメータ	説明
暗号化モード	**すべてのハードディスクを暗号化する**：このオプションをオンにすると、ポリシーが適用された時点ですべてのハードディスクが暗号化されます。 コンピューターに複数のオペレーティングシステムがインストールされている場合、暗号化が完了すると、本製品がインストールされているオペレーティングシステムしか読み込めなくなります。 **すべてのハードディスクを復号化する**：このオプションをオンにすると、ポリシーの適用時、それ以前に暗号化されていたすべてのハードディスクが復号化されます。 **変更しない**：このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。
タブレットでプリブート キーボード入力が必要な BitLocker 認証を使用できるようにする	起動前の環境でデータ入力を必要とする認証を使用します。この設定は、起動前に入力できる機能がないプラットフォームに対しても適用されます（例：タブレットのタッチスクリーンキーボード）。 タブレットコンピューターのタッチスクリーンは起動前環境では利用できません。タブレットコンピューターで BitLocker 認証を完了するには、ユーザーは USB キーボードなどを接続する必要があります。 このチェックボックスをオンにすると、起動前の入力を必要とする認証の使用が許可されます。この設定は、起動前の環境でデータ入力ができるツールがあるデバイスに対してのみ使用してください（例：タッチスクリーンキーボードだけでなく USB キーボードも付いているデバイスなど）。 チェックボックスをオフにすると、タブレットコンピューターで BitLocker ドライブ暗号化が使用できなくなります。
ハードウェア暗号化を使用（Windows 8 以降）	このチェックボックスをオンにすると、ハードウェア暗号化が適用されます。ハードウェア暗号化を使用すると、より少ないコンピューターリソースで、より速く暗号化することができます。

パラメータ	説明
使用されているディスク領域のみを暗号化（Windows 8 以降）	このチェックボックスでは、暗号化の対象をハードディスクの使用中のセクターのみに限定する設定を有効または無効にします。限定することにより、暗号化にかかる時間を短縮できます。 暗号化の開始後に［**使用されているディスク領域のみを暗号化（暗号化時間を短縮）**］を有効または無効にしても、ハードドライブが復号化されるまでこの設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。 このチェックボックスをオンにすると、ハードディスク内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。 チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ハードディスク全体が暗号化されます。 データが変更されたり削除されていない新しいハードディスクでは、このオプションをオンにしてください。既に使用されているハードディスクに暗号化を適用する場合、ハードディスク全体を暗号化してください。それにより、削除されているが回復の可能性があるデータを含め、すべてのデータが保護されます。 既定では、このチェックボックスはオフです。
認証方法	**パスワードのみ（OS が Windows 8 以降のバージョンの場合）** このオプションを選択すると、暗号化されたドライブにアクセスしようとした際に、パスワードの入力が要求されます。 このオプションは、Trusted Platform Module（TPM）が使用されていない場合に選択できます。 **トラステッド プラットフォーム モジュール（TPM）** このオプションを選択すると、BitLocker は Trusted Platform Module（TPM）を使用します。 *Trusted Platform Module*（TPM）は、セキュリティ関連の基本機能（暗号化鍵の保存など）を提供するために開発されたマイクロチップです。Trusted Platform Module は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと連携します。 Windows 7 と Windows 2008 R2 では、TPM モジュールを使用した暗号化のみを利用できます。TPM モジュールがインストールされていない場合、BitLocker 暗号化は実行できません。これらのオペレーティングシステムを使用しているコンピューターでは、パスワードを使用した暗号化はサポートされません。 Trusted Platform Module を搭載したデバイスで作成された暗号鍵は、そのデバイスでしか復号化できません。Trusted Platform Module は、各 TPM が保持するストレージルートキーを使って暗号鍵を暗号化します。ストレージルートキーは Trusted Platform Module 内部に格納されています。そのため、暗号鍵を盗もうとする試みに対して、より強固な保護を提供することができます。 既定では、この処理が選択されています。 暗号化鍵およびパスワードまたは PIN で保護された暗号化鍵へのアクセスに、より強固な保護を提供することが可能です。 • **TPM の PIN を使用する**：このチェックボックスをオンにすると、Trusted Platform Module（TPM）内に格納されている暗号鍵にアクセスする際に暗証番号を使用できます。このチェックボックスをオフにすると、PIN コードの使用が禁止されます。暗号鍵へのアクセスには、パスワードの入力が必要となります。 • **トラステッド プラットフォーム モジュール（TPM）、TPM が使用できない場合はパスワード**：このオプションをオンにすると、Trusted Platform Module（TPM）が使用できない場合、パスワードを使用して暗号鍵にアクセスできます。チェックボックスがオフの場合は TPM は使用できず、ディスク全体の暗号化は開始されません。 パスワードまたは PIN の要件を指定して、選択した認証方法を設定する必要があります： • **PIN の最小文字数** • **パスワードの最小文字数** • **TPM のパスワード / PIN の有効期間を設定する（日）** • **拡張 PIN を使用する（文字と数字）**：*拡張 PIN* を使用すると数字以外にも半角英数字の大文字小文字、特殊文字、スペースを使用できるようになります
回復キーを自動的に再生成する（日）	パスワードを自動的に更新して、BitLocker で保護されたハードドライブへのアクセスを復元します。このチェックボックスをオンにしたら、回復キーのパスワードの有効期間を指定します。これは、回復キーのパスワードの再使用を防ぐのに役立ちます。

ファイルレベルの暗号化

拡張子や拡張子グループ、ローカルコンピューターのドライブに保存されているフォルダーのリストに基づいて、ファイルのリストを作成できます。また、特定のアプリケーションで作成されたファイルを暗号化するルールを作成できます。ポリシーが適用されると、Kaspersky Endpoint Security は以下のファイルを暗号化および復号化します：

- 暗号化および復号化のリストに追加されたファイル
- 暗号化および復号化のリストに追加されたフォルダーにあるファイル
- 別々のアプリケーションによって作成されたファイル

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

ファイル暗号化には、次の特別な機能があります：

- Kaspersky Endpoint Security は、オペレーティングシステムのローカルユーザープロファイルについてのみ定義済みフォルダーのファイルの暗号化や復号化を行います。Kaspersky Endpoint Security は、移動ユーザープロファイル、固定ユーザープロファイル、一時ユーザープロファイル、またはリダイレクトされたフォルダーの、定義済みフォルダー内のファイルを暗号化または復号化しません。
- Kaspersky Endpoint Security は、暗号化が原因でオペレーティングシステムやインストールされたアプリケーションに損害を与える可能性がある場合は、ファイルを暗号化しません。たとえば、次のファイルおよびフォルダーは、入れ子になっているすべてのフォルダーとともに、暗号化しないファイルまたはフォルダーのリストに含まれます：
  - %WINDIR%
  - %PROGRAMFILES% および %PROGRAMFILES(X86)%
  - Windows のレジストリファイル

  暗号化しないファイルまたはフォルダーのリストは、表示することも編集することもできません。暗号化除外リストにあるファイルとフォルダーは暗号化リストに追加できますが、ファイルの暗号化中は暗号化されません。

ファイルレベルの暗号化の設定

パラメータ	説明
暗号化モード	**変更しない**：このオプションを選択すると、ファイルやフォルダーの状態は維持され暗号化や復号化は行われません。 **ルールに従う**：このオプションを選択すると、暗号化ルールに従ってファイルとフォルダーが暗号化され、復号化ルールに従ってファイルとフォルダーが復号化されます。また、アプリケーションのルールに従って暗号化されたファイルへのアクセスが規制されます。 **すべてを復号化する**：このオプションを選択すると、暗号化されたすべてのファイルとフォルダーが復号化されます。

パラメータ	説明
暗号化	このタブには、ローカルドライブに保存されているファイルの暗号化ルールが表示されます。次のようにファイルを追加できます： • **定義済みフォルダー**：Kaspersky Endpoint Security では、次の領域を追加できます： **ドキュメント**：オペレーティングシステムの標準の［ドキュメント］フォルダー内のファイルとそのサブフォルダー。 **お気に入り**：オペレーティングシステムの標準の［お気に入り］フォルダー内のファイルとそのサブフォルダー。 **デスクトップ**：オペレーティングシステムの標準の［デスクトップ］フォルダー内のファイルとそのサブフォルダー。 **一時ファイル**：コンピューターにインストールされたアプリケーションの動作に関連する一時ファイル。たとえば、Microsoft Office 製品ではドキュメントのバックアップコピーを含む一時ファイルが作成されます。 **Outlook ファイル**：Outlook メールクライアントの動作に関連するファイル (データファイル (PST)、オフラインデータファイル (OST)、オフラインアドレス帳ファイル (OAB)、および個人のアドレス帳ファイル (PAB))。 • **カスタムフォルダー**：フォルダーのパスを入力できます。フォルダーのパスを追加するときは、次のルールに従います： 環境変数を使用します（たとえば、`%FOLDER%\UserFolder\`）。環境変数は、パスの先頭で一度だけ使用できます。 相対パスは使用しないでください。 `*` および `?` の文字は使用しないでください。 UNC パスは使用しないでください。 区切り文字として、`;` または `,` を使用してください。 • **ファイルの拡張子による指定**：拡張グループの *アーカイブ*など、拡張グループをリストから選択できます。ファイルの拡張子を手動で追加することもできます。
復号化	このタブには、ローカルドライブに保存されているファイルの復号化ルールが表示されます。
アプリケーションのルール	このタブには、暗号化されたファイルに対するアプリケーションのアクセスルールおよび、個別のアプリケーションによって作成または変更されたファイルの暗号化ルールのテーブルが表示されます。
暗号化されたパッケージ	暗号化されたパッケージの作成時に必要なパスワードの強度。

リムーバブルドライブの暗号化

このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

Kaspersky Endpoint Security は、FAT32 および NTFS ファイルシステムのファイルの暗号化に対応しています。対応していないファイルシステムのリムーバブルドライブがコンピューターに接続されると、このリムーバブルドライブの暗号化タスクはエラーにより失敗し、リムーバブルドライブが読み取り専用になります。

リムーバブルドライブ上のデータを保護するには、次の暗号化種別を使用できます：

- Full Disk Encryption（FDE）：

  ファイルシステムを含むリムーバブルドライブ全体の暗号化。

  企業ネットワークの外部で暗号化されたデータにアクセスすることはできません。Kaspersky Security Center へ接続されていないコンピューターの場合（ゲストコンピューターなど）も、企業ネットワーク内の暗号化されたデータへアクセスできません。

- File Level Encryption（FLE）：

  リムーバブルドライブ上のファイルのみの暗号化。ファイルシステムは変更されません。

リムーバブルドライブ上のファイルの暗号化は、*ポータブルモード*と呼ばれる特別なモードを使用して、企業ネットワークの外部のデータにアクセスする機能を提供します。

暗号化中に、Kaspersky Endpoint Security はマスター鍵を作成します。Kaspersky Endpoint Security は、マスター鍵を次のリポジトリに保存します：

- Kaspersky Security Center
- ユーザーのコンピューター

  マスター鍵はユーザーの秘密鍵で暗号化されます。
- リムーバブルドライブ

  マスター鍵は、Kaspersky Security Center の公開鍵で暗号化されています。

暗号化が完了すると、従来のリムーバブルドライブを暗号化せずに使用しているかのように、企業ネットワーク内でリムーバブルドライブ上のデータにアクセスできます。

暗号化されたデータへのアクセス

暗号化されたデータのリムーバブルドライブが接続されると、Kaspersky Endpoint Security は次の処理を実行します：

1. ユーザーのコンピューターのローカル保管領域でマスター鍵を確認します。

   マスター鍵が見つかった場合、ユーザーはリムーバブルドライブ上のデータにアクセスできます。

   マスター鍵が見つからない場合、Kaspersky Endpoint Security は次の処理を実行します：

   a. Kaspersky Security Center に要求を送信します。

      要求を受け取った後、Kaspersky Security Center はマスター鍵を含む応答を送信します。

   b. Kaspersky Endpoint Security は、暗号化されたリムーバブルドライブを使用した、それ以降の操作のために、ユーザーのコンピューターのローカル保管領域にマスター鍵を保存します。

2. データを復号化します。

リムーバブルドライブ暗号化の特別な機能

リムーバブルドライブの暗号化には、次の特別な機能があります：

- リムーバブルドライブの暗号化に関する事前設定はポリシーに含まれます。このポリシーは、管理対象コンピューターの特定のグループに対して作成されています。このため、リムーバブルドライブの暗号化または復号化の設定を含む Kaspersky Security Center ポリシーの適用結果は、そのリムーバブルドライブがどのコンピューターに接続しているかによって異なります。
- Kaspersky Endpoint Security は、リムーバブルドライブに保存されている読み取り専用ステータスのファイルの暗号化や復号化は行いません。

- リムーバブルドライブとして、次のデバイス種別がサポートされています：
  - USB バス経由で接続されているリムーバブルドライブ
  - USB および FireWire バス経由で接続されているハードディスク
  - USB および FireWire バス経由で接続されている SSD ドライブ

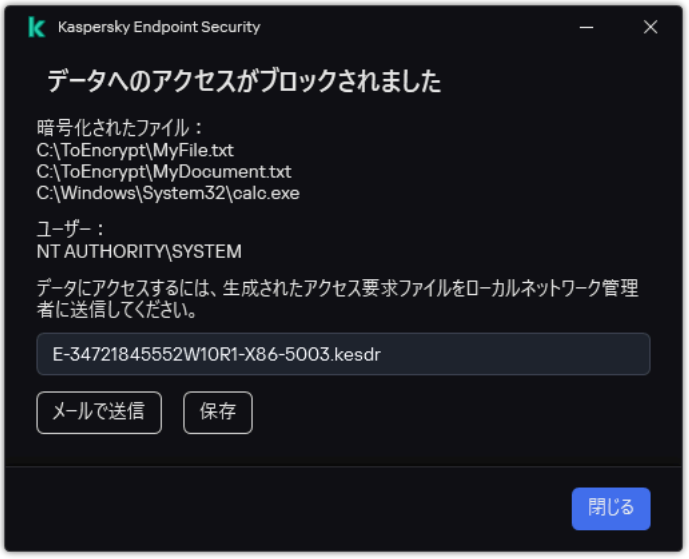
リムーバブルドライブの暗号化機能の設定

パラメータ	説明
暗号化モード	**リムーバブルドライブ全体の暗号化**：このオプションを選択した場合、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、ファイルシステムも含めて、リムーバブルドライブをセクター単位で暗号化します。 **すべてのファイルの暗号化**：このオプションをオンにすると、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、リムーバブルドライブに保存されているすべてのファイルを暗号化します。既に暗号化されたファイルの再暗号化は実行しません。暗号化されるフォルダー構造やファイルの名前を含む、リムーバブルドライブのファイルシステムの内容は暗号化されないため、引き続きアクセスできます。 **新しいファイルのみ暗号化**：このオプションをオンにすると、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、Kaspersky Security Center ポリシーが前回適用された後でリムーバブルドライブに追加されたファイル、またはポリシーの適用後にリムーバブルドライブ上で変更されたファイルのみを暗号化します。この暗号化モードは、リムーバブルドライブをプライベートと仕事の両方で使う場合に便利です。この暗号化モードでは、既存のファイルをすべて変更しないまま残し、Kaspersky Endpoint Security がインストールされ暗号化機能が有効になっている作業用コンピューター上でユーザーが作成したファイルだけを暗号化できます。このため、Kaspersky Endpoint Security がインストールされているコンピューターで暗号化機能が有効になっているかいないかにかかわらず、個人用のファイルには常にアクセスすることができます。 **リムーバブルドライブ全体の復号化**：このオプションを選択した場合、リムーバブルドライブに対して指定した暗号化設定でポリシーを適用すると、リムーバブルドライブに保存されている暗号化ファイルをすべて復号化すると共に、リムーバブルドライブのファイルシステムも以前に暗号化されている場合は復号化します。 **変更しない**：このオプションを選択すると、ポリシーの適用時、ドライブに変更を加えずそのままの状態を保持します。ドライブが暗号化されている場合は、暗号化された状態を保持します。ドライブが復号化されている場合は、復号化された状態を保持します。既定ではこのオプションが選択されます。
ポータブルモード	このチェックボックスを使用して、社内ネットワーク外にあるコンピューターのリムーバブルドライブ上に保存されたファイルにアクセスできるようにするためのリムーバブルドライブの準備を有効または無効にすることができます。 このチェックボックスをオンにした場合、ポリシーを適用すると、リムーバブルドライブにあるファイルを暗号化する前にパスワードを指定するよう要求されます。社内ネットワーク外にあるコンピューターのリムーバブルドライブ上の暗号化ファイルにアクセスするにはパスワードが必要です。パスワードの強度を設定できます。 ポータブルモードは、**すべてのファイルの暗号化**モードまたは**新しいファイルのみ暗号化**モードで使用できます。
使用されているディスク領域のみを暗号化	このチェックボックスでは、ディスクの使用されている領域のみを暗号化する暗号化モードを有効または無効にできます。データが変更されたり削除されていない新しいドライブでは、このモードを使用してください。 このチェックボックスをオンにすると、ドライブ内のファイルがある領域のみが暗号化されます。新しいデータは、追加されると自動的に暗号化されます。 チェックボックスをオフにすると、過去に削除されたファイルや変更が加えられたファイルの残存フラグメントも含め、ディスク全体が暗号化されます。 占有領域のみを暗号化する機能は、**リムーバブルドライブ全体の暗号化**モードでのみ使用できます。 暗号化の開始後に［**使用されているディスク領域のみを暗号化**］の有効または無効を切り替えても、設定は変更されません。チェックボックスのオン / オフは、暗号化が開始する前に選択してください。
カスタムルール	このテーブルには、カスタムの暗号化ルールが定義されているデバイスが表示されます。次の方法で、個々のリムーバブルドライブの暗号化ルールを作成できます： • デバイスコントロール用の信頼するデバイスのリストからリムーバブルドライブを追加します。 • リムーバブルドライブを手動で追加します： • デバイス ID を使用：Hardware ID（ハードウェア ID、または HWID） • デバイスモデルを使用：Vendor ID（製造元 ID、または VID）および Product ID（製品 ID、またはPID）

パラメータ	説明
オフラインモードでのリムーバブルドライブの暗号化を許可する	このチェックボックスがオンになっている場合、Kaspersky Endpoint Security は、Kaspersky Security Center との接続がない場合でもリムーバブルドライブを暗号化します。この場合、リムーバブルドライブの復号化に必要なデータはリムーバブルドライブが接続されているコンピューターのハードディスク上に保存され、Kaspersky Security Center には配信されません。 このチェックボックスをオフにすると、Kaspersky Security Center への接続がない場合、Kaspersky Endpoint Security はリムーバブルドライブを暗号化しません。
暗号化パスワードの設定 / ポータブルファイルマネージャー	ポータブルファイルマネージャーのパスワードの強度設定。

テンプレート（データの暗号化）

データの暗号化後、Kaspersky Endpoint Security は、たとえば組織のインフラストラクチャの変更や Kaspersky Security Center 管理サーバーの変更により、データへのアクセスを制限する場合があります。ユーザーが暗号化されたデータにアクセスできない場合、ユーザーは管理者にデータへのアクセスを依頼できます。つまり、ユーザーはアクセス要求ファイルを管理者に送信する必要があります。ユーザーは、管理者から受け取った応答ファイルを Kaspersky Endpoint Security にアップロードする必要があります。Kaspersky Endpoint Security では、管理者からのデータへのアクセスをメールで要求できます（下の図を参照）。



暗号化されたデータへのアクセス要求

暗号化されたデータへのアクセスができないことを報告するためのテンプレートが提供されます。ユーザーの利便性のため、次のフィールドに入力できます：

- **宛先**：データ暗号化機能に対する権限を持つ管理者グループのメールアドレスを入力します。
- **件名**：暗号化されたファイルへのアクセス権をリクエストするメールの件名を入力します。たとえば、タグを追加してメッセージをフィルタリングできます。
- **ユーザーのメッセージ**：必要に応じて、メッセージの内容を変更します。変数を使用して、必要なデータを取得できます（たとえば、%USER_NAME%変数）。

除外リスト

*信頼ゾーン*は Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。

管理者は処理されるオブジェクトとコンピューターにインストールされるアプリケーションの特徴を考慮しながら、信頼ゾーンを個別に定義します。Kaspersky Endpoint Security がアクセスをブロックする特定のオブジェクトやアプリケーションが無害であることが確実なときには、オブジェクトやアプリケーションを信頼ゾーンに含めなければならない場合があります。管理者が、ユーザーが特定のコンピューターに対してローカルの信頼するゾーンを作成するよう許可することも可能です。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。

Kaspersky Endpoint Security 12.5 for Windows から、EDR テレメトリを信頼ゾーンに追加できるようになりました。これにより、アプリケーションが Kaspersky Anti Targeted Attack Platform (EDR) ソリューション向けにテレメトリの収集サーバーに送信するデータを最適化できます。

Kaspersky Endpoint Security 12.6 for Windows から、信頼するオブジェクトとアプリケーションは信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、SQL サーバー、Microsoft Exchange サーバー、System Center Configuration Manager 上で Kaspersky Endpoint Security を迅速に設定できます。つまり、サーバーでの本製品の信頼ゾーンを手動で設定する必要はありません。

Kaspersky Endpoint Security 12.8 for Windows 以降では、本製品を仮想環境保護用 Light Agent モードでインストールできます。設定済みの信頼するオブジェクトとアプリケーションにより、Citrix と VMware の仮想環境で Kaspersky Endpoint Security を迅速に設定できます。

信頼するオブジェクト

*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。信頼するオブジェクトにより、ユーザーに損害を与える目的で悪用される可能性がある合法的なソフトウェアを安全に使用できるようになります。悪意のある機能はありませんが、このようなアプリケーションは侵入者によって悪用される可能性があります。ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェアについて詳しくは、カスペルスキーのウイルス百科事典を参照してください。

このようなアプリケーションは Kaspersky Endpoint Security によってブロックされる場合があります。ブロックしないようにするには、使用している製品を信頼するオブジェクトに設定できます。これを行うには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクを信頼ゾーンに追加します。たとえば、ユーザーがコンピューターのリモート管理用に Radmin アプリケーションを使用しているとします。Kaspersky Endpoint Security はこの処理を疑わしいものとみなして、ブロックする可能性があります。アプリケーションがブロックされないようにするには、カスペルスキーのウイルス百科事典に登録されている名前または名前マスクによって信頼するオブジェクトを作成します。

情報を収集し、それを処理するために送信するアプリケーションがコンピューターにインストールされていると、Kaspersky Endpoint Security がそのアプリケーションをマルウェアに分類する可能性があります。それを防ぐために、ヘルプ内で説明する方法で Kaspersky Endpoint Security を設定することで、そのアプリケーションをスキャン対象から除外できます。

システム管理者が設定した以下のコンポーネントとタスクによって信頼するオブジェクトを使用できます：

- ふるまい検知
- 脆弱性攻撃ブロック
- ホスト侵入防止
- ファイル脅威対策
- ウェブ脅威対策
- メール脅威対策
- マルウェアのスキャンタスク

信頼するアプリケーションのリスト

*信頼するアプリケーションのリスト*は、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Endpoint Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Endpoint Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトを監視し、すべてのアプリケーションとこのようなアプリケーションが生成するネットワークトラフィックの処理を管理します。アプリケーションが信頼するアプリケーションのリストに追加されると、Kaspersky Endpoint Security はアプリケーションのアクティビティの監視を停止します。

信頼するオブジェクトと信頼するアプリケーションの違いは、信頼するオブジェクトの場合、Kaspersky Endpoint Security はファイルをスキャンしないのに対し、信頼するアプリケーションの場合は、開始されたプロセスを制御しないことです。信頼するアプリケーションが信頼するオブジェクトに含まれていないフォルダーに悪意のあるファイルを作成した場合、Kaspersky Endpoint Security はそのファイルを検知して脅威を排除します。フォルダーが除外リストに追加されている場合、Kaspersky Endpoint Security はこのファイルをスキップします。

たとえば、Microsoft Windows 標準のメモ帳アプリケーションで使用するオブジェクトが安全であり信頼できると考える場合は、Microsoft Windows メモ帳を信頼するアプリケーションのリストに追加し、このアプリケーションが使用するオブジェクトが監視されないようにすることができます。これにより、サーバーアプリケーションで特に重要となるコンピューターのパフォーマンスを高めることができます。

また、特定の処理が Kaspersky Endpoint Security によって疑わしい処理に分類されたとしても、多数のアプリケーションの機能を考慮すると安全な場合があります。たとえば、キーボードで入力したテキストの取得は、自動キーボードレイアウト切り替えプログラム（Punto Switcher など）では通常の処理です。このようなアプリケーションの特性を考慮して、アプリケーション処理を監視対象から除外するために、このようなアプリケーションを信頼するアプリケーションのリストに追加してください。

信頼するアプリケーションは、Kaspersky Endpoint Security と他のアプリケーションとの間の互換性の問題（たとえば、Kaspersky Endpoint Security と他のアンチウイルス製品によるサードパーティ製コンピューターのネットワークトラフィックの二重スキャンなど）を回避するのに役立ちます。

ただし、信頼するアプリケーションの実行ファイルとプロセスのウイルスおよびその他のマルウェアスキャンは実行されます。アプリケーションを Kaspersky Endpoint Security のスキャンから完全に除外するには、信頼するオブジェクトを設定します。

除外リストの設定

パラメータ	説明

検知するオブジェクトの種別

製品設定にかかわらず、Kaspersky Endpoint Security は常にウイルスやワーム、トロイの木馬を検知してブロックします。これらのプログラムはコンピューターに重大な損害を与える可能性があります。

- **ウイルス、ワーム**

  サブカテゴリ：ウイルスやワーム（Viruses_and_Worms）

  危険度：高

  古典的なウイルスやワームは、ユーザーが許可していない処理を実行します。このようなウイルスやワームは、自己複製が可能な自身のコピーを作成することができます。

  古典的ウイルス

  古典的ウイルスがコンピューターに侵入すると、ファイルに感染して活動を開始し、悪意のある処理を実行し、それ自体のコピーを他のファイルに追加します。

  古典的ウイルスは、コンピューターのローカルリソースでしか増殖しないため、自力で他のコンピューターに侵入できません。このウイルスが別のコンピューターに感染するのは、ウイルス自身のコピーを共有フォルダーに保管されているファイルまたは挿入された CD に追加したときや、ユーザーが感染したファイルを添付したメールを転送したときです。

  古典的ウイルスのコードはコンピューター、オペレーティングシステム、アプリケーションの各種領域に侵入する可能性があります。環境により、ウイルスは、*ファイルウイルス*、*ブートウイルス*、*スクリプトウイルス*、および *マクロウイルス*に分けられます。

  ウイルスはさまざまな技法を駆使してファイルを感染させます。上書き（*Overwriting*）ウイルスは、そのコードを、感染したファイルのコードに上書きして、そのファイルの内容を消去します。感染したファイルは機能しなくなり、復元できません。寄生（*Parasitic*）ウイルスは、ファイルを変更しますが、ファイルが完全にまたは部分的に機能する状態を維持します。コンパニオンウイルス（*Companion*）は、ファイルを変更しませんが、代わりに複製を作成します。感染したファイルが開かれると、ウイルスの複製（実際にはこれがウイルス）が起動します。他にも、次のような種別のウイルスが見つかっています：*Link* ウイルス、*OBJ ウイルス*、*LIB ウイルス*、*ソースコード*ウイルスなど多数。

  ワーム

  古典的ウイルスのコードと同様に、ワームのコードは、コンピューターに侵入してから活動を開始し、悪意のある処理を実行します。ワームは、コンピューターから別のコンピューターに「這うように移動」し、ユーザーの許可なく多数のデータチャネルを経由してコピーを拡散させることから、この名が付けられました。

  さまざまなワームの種類を区別する主な特徴は、その拡散方法です。次のテーブルに、拡散方法によって分類される各種ワームの概要を示します：

  ワームの拡散方法

種別	Name	説明
メールワーム	メールワーム	これらのワームはメールを介して広がります。 感染したメールには、ワームのコピーを含んだ添付ファイル、あるいは感染した Web サイトまたは感染させる目的で作成された Web サイトにアップロードされるファイルへのリンクが含まれています。添付ファイルを開くと、ワームが起動します。リンクをクリックし、ファイルをダウンロードして開くと、ワームも悪意のある処理を実行し始めます。その後、ワームは他のメールアドレスを検索して、これらのアドレスに感染メールを送信しながら、自身のコピーを拡散し続けます。
IM ワーム	IM クライアントワーム	インスタントメッセージ（IM）クライアント経由で拡散します。 通常、このようなワームは、ユーザーの連絡先リストを使用して、ワームのコピーに感染した Web サイト上のファイルへのリンクを含んだメールを送信します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。
IRC ワーム	インターネットチャットワーム	このワームは Internet Relay Chats（インターネット上の別のユーザーとリアルタイムで通信できるサービスシステム）を介して拡散します。 この種のワームは、インターネットチャットで自身のコピーを含むファイルまたはそのファイルへのリンクを公開します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。
インターネットワーム（Net-Worm）	ネットワークワーム	これらのワームは、コンピューターネットワークを介して広がります。 通常のネットワークワームは、他の種類のワームと異なり、ユーザーが参加していなくても拡散します。このワームはプライベートネットワークに、脆弱性のあるプログラムがインストールされたコンピューターがないか探します。この操作を行うために、このワームはワームコードまたはその一部を含む特別に形成されたネットワークパケット（エクスプロイト）を送信します。ネットワーク上に「脆弱な」コンピューターが存在すると、そのコンピューターはこのようなネットワークパケットを受信します。ワームが完全にコンピューターに侵入すると、ワームが起動します。
P2P ワーム	ファイル共有ネットワークワーム	peer-to-peer のファイル共有ネットワーク経由で拡散します。 P2P ネットワークに潜入するために、ワームはそれ自身をファイル共有フォルダーにコピーします。このフォルダーは通常、ユーザーのコンピューター上にあります。P2P ネットワークでは、ネットワーク上の感染したファイルをユーザーが他のファイルと同様に「見つけ」、このファイルをダウンロードして開くように、このファイルに関する情報が表示されます。 さらに巧妙なワームは特定の P2P ネットワークのネットワークプロトコルを装って検索クエリに肯定応答を返し、自身のコピーをダウンロードさせます。
ワーム	他の種類のワーム	他の種類のワームには、以下のものがあります： • 自身のコピーをネットワークリソースを介して拡散するワーム。このようなワームは、オペレーティングシステムの機能を使って使用可能なネットワークフォルダーを検索し、インターネット上のコンピューターへ接続し、このコンピューターのディスクドライブへのフルアクセス権を取得しようと試みます。他の種類のワームは上記種類のワームとは異なり、自力で起動するのではなく、ユーザーがワームのコピーを含むファイルを開いたときに起動します。 • 上記のどの拡散方法も使用しないワーム（携帯電話を通じて拡散するワームなど）。

- **トロイの木馬（ランサムウェアを含む）**

  サブカテゴリ：トロイの木馬

危険度：高

ワームやウイルスとは異なり、トロイの木馬は自己複製しません。たとえば、ユーザーが感染している Web サイトにアクセスすると、トロイの木馬はメールやブラウザーからコンピューターに侵入します。トロイの木馬は、ユーザーの関与によって起動します。起動直後に、悪意のある処理を実行し始めます。

トロイの木馬は多種多様で、感染コンピューター上でのふるまいも多岐にわたります。トロイの木馬の主な機能は、情報のブロック、改変、破壊、およびコンピューターまたはネットワークの無効化です。また、トロイの木馬はファイルの送受信、ファイルの実行、画面上へのメッセージの表示、Web サイトの要求、プログラムのダウンロードとインストール、コンピューターの再起動を行うこともできます。

多くの場合、ハッカーはトロイの木馬の「セット」を使用します。

次のテーブルでは、トロイの木馬における動作の種類について説明します。

感染コンピューターにおけるトロイの木馬の動作種類

種別	Name	説明
Trojan-ArcBomb	トロイの木馬 - 「圧縮爆弾」	このアーカイブは、解凍するとコンピューターの動作に影響を与える程度のサイズにまで膨張します。 ユーザーがこのようなアーカイブを解凍しようとすると、コンピューターは処理速度が低下したりフリーズしたりすることがあります。また、ハードディスクが「空の」データで満杯になることがあります。「圧縮爆弾」は、特にファイルサーバーやメールサーバーにとって危険です。サーバーが自動システムを使用して受信情報を処理すると、「圧縮爆弾」によってサーバーが停止することがあります。
バックドア	リモート管理用のトロイの木馬	このプログラムは、トロイの木馬の中でも最も危険なものと考えられます。機能面で、コンピューターにインストールされるリモート管理アプリケーションに似ています。 これらのプログラムは、ユーザーに気付かれずにコンピューターにインストールされるので、侵入者はコンピューターを遠隔管理できます。
トロイの木馬	トロイの木馬	トロイの木馬には、次のような悪意のあるアプリケーションがあります： • **古典的なトロイの木馬**：これらのプログラムはトロイの木馬の主な機能（情報のブロック、改変または破壊、およびコンピューターまたはネットワークの無効化）のみを実行し、テーブルに示す他の種類のトロイの木馬とは異なり、高度な機能を持っていません。 • **多目的なトロイの木馬**：これらのプログラムは、数種類のトロイの木馬に特徴的な先進機能を備えています。
Trojan-Ransom	トロイの木馬型ランサムウェア	このプログラムは、ユーザーの情報を「人質」にとって改変したり、ブロックしたりします。また、ユーザーが情報を使用する能力を喪失するように、コンピューターの動作に影響を与えます。侵入者は、コンピューターのパフォーマンスと保存されていたデータを復元するアプリケーションを送るという約束と引き替えに、ユーザーから身代金を要求します。
Trojan-Clicker	トロイの木馬クリッカー	このプログラムは、ブラウザーにコマンドを送信するか、オペレーティングシステムファイルで指定されている Web アドレスを変更することによって、ユーザーのコンピューターから Web サイトにアクセスします。 侵入者はこのようなプログラムを使用することによって、ネットワーク攻撃を行って Web サイトのアクセス数を増やし、バナー広告の表示回数を増やします。
Trojan-Downloader	トロイの木馬ダウンローダー	これは侵入者の Web サイトにアクセスして、そこから他の悪意のあるアプリケーションをダウンロードし、ユーザーのコンピューターにインストールします。このプログラムには、悪意のあるアプリケーションをダウンロードまたは受信するためにアクセスした Web サイトのファイル名が含まれていることがあります。
Trojan-Dropper	トロイの木馬ドロッパー	このプログラムは他のトロイの木馬を内包しており、この内包されたプログラムがハードディスクにインストールされ、実行されます。 侵入者は、トロイの木馬ドロッパー型プログラムを次のような目的で使用することがあります： • ユーザーに気付かれずに悪意のあるプログラムをインストールする：トロイの木馬ドロッパー型プログラムは、メッセージを表示しないか、たとえば、アーカイブ中にエラーが発生したことやオペレーティングシステムが互換性のないバージョンであることを示すといった偽のメッセージを表示します。 • 既知の悪意のある別のアプリケーションが検知されないようにする：すべてのアンチウイルスのソフトウェアがトロイの木馬ドロッパー型アプリケーション内の悪意のあるアプリケーションを検知できるわけではありません。
Trojan-Notifier	トロイの木馬型ノーティファイア	このプログラムは、感染したコンピューターにアクセスできることを侵入者に教えるため、コンピューターの次のような情報を侵入者に送信します：IP アドレス、開いているポートの番号、メールアドレスなど。このプログラムはこれらの情報をメール、FTP、侵入者の Web サイトへのアクセス、あるいはこれら以外の方法で侵入者に送ります。 トロイの木馬型ノーティファイアプログラムは、多くの場合、複数のトロイの木馬からなるセットとして使用されます。また、このプログラムはトロイの木馬がユーザーのコンピューターにインストールされたことを侵入者に知らせます。
Trojan-Proxy	トロイの木馬型プロキシ	これらのトロイの木馬により、侵入者は、ユーザーのコンピューターを使って匿名で Web サイトにアクセスします。このトロイの木馬はスパムの送信によく利用されます。
Trojan-PSW	パスワード窃盗ソフトウェア	パスワード窃盗ソフトウェアは、ソフトウェア登録データなどのユーザーアカウントを盗むトロイの木馬の一種です。このトロイの木馬はシステムファイルおよびレジストリ内の機密データを見つけ、そのデータを「攻撃者」にメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって送信します。 これらのトロイの木馬のうち、いくつかがこのテーブルに示す種類に分類されます。これらは、銀行のアカウント情報（Trojan-Banker）、メッセンジャークライアントのユーザーのデータ（Trojan-IM）、およびオンラインゲームのユーザーの情報（Trojan-GameThief）を盗むトロイの木馬です。
Trojan-Spy	スパイウェア型トロイの木馬	このトロイの木馬はコンピューター上で動作しながら、ユーザーが行う処理に関する情報を収集して、ユーザーの行動を秘密裏に監視します。このトロイの木馬は、ユーザーがキーボードで入力するデータの傍受、スクリーンショットの撮影、あるいはアクティブなアプリケーションのリストの収集などを行うことがあります。このプログラムが情報を入手すると、その情報をメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。
Trojan-DDoS	トロイの木馬ネットワークアタッカー	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。ハッカーは、1 台のサーバーを多数のコンピューターから同時に攻撃できるように、このプログラムを利用して多数のコンピューターを感染させることがあります。 DoS プログラムは 1 台のコンピューターから、ユーザーに気付かれることなく攻撃を実行します。DDoS（分散 DoS）プログラムは、感染したコンピューターのユーザーに気付かれずに、複数のコンピューターから分散して攻撃を行います。
Trojan-IM	メッセンジャークライアントのユーザーから情報を盗むトロイの木馬	このトロイの木馬は、メッセンジャークライアントのユーザーのアカウント番号とパスワードを盗みます。このプログラムは、データをメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。

ルートキット	ルートキット	ルートキットは、他の悪意のあるアプリケーションやその活動を隠蔽します。そのため、このアプリケーションはオペレーティングシステムに長期間潜入します。また、ルートキットはファイル、感染しているコンピューターのメモリ内のプロセス、または悪意のあるアプリケーションを実行するレジストリキーを隠蔽することもできます。さらにルートキットは、ユーザーのコンピューターにインストールされているアプリケーションとネットワーク上の他のコンピューターにインストールされているアプリケーションの間で行われるデータ交換を隠蔽できます。
Trojan-SMS	SMS メッセージ形式のトロイの木馬	このトロイの木馬は携帯電話を感染させ、高額の通話料が発生する電話番号に SMS メッセージを送信します。
Trojan-GameThief	オンラインゲームのユーザーから情報を盗むトロイの木馬	このトロイの木馬は、オンラインゲームのユーザーのアカウント情報を盗み、このデータを侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。
Trojan-Banker	銀行のアカウント情報を盗むトロイの木馬	このトロイの木馬は、銀行のアカウント情報や電子マネーシステムのデータを盗み、このデータをメールや FTP を使用して侵入者に送信するか、侵入者の Web サイトにアクセスするなどして送信します。
Trojan-Mailfinder	メールアドレスを収集するトロイの木馬	このトロイの木馬は、コンピューターに保存されているメールアドレスを収集し、侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。侵入者が収集したアドレスにスパムを送信することがあります。

- **悪意のあるツール**

  サブカテゴリ：悪意のあるツール

  危険度：中

  悪意のあるツールは、他の種類のマルウェアとは異なり、起動した直後に処理を実行しません。このプログラムはユーザーのコンピューターに安全に侵入し、そこで起動することができます。侵入者は、多くの場合、悪意のあるツールの機能を悪用して、ウイルス、ワーム、トロイの木馬を作成したり、リモートサーバーに対してネットワーク攻撃を仕掛けたりします。

  悪意のあるツールのさまざまな機能を、次のテーブルに示す種類別に分類しています：

  悪意のあるツールの機能

種別	Name	説明
コンストラクター	コンストラクター	このツールを使用して、新しいウイルス、ワームおよびトロイの木馬を作成します。一部のコンストラクターは標準的なウィンドウベースのインターフェイスを備えています。このインターフェイスでは、悪意のあるアプリケーションの種類を選択して、デバッガを無効にする手段やその他の機能を作成できます。
Dos	ネットワーク攻撃	このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。
エクスプロイト	エクスプロイト	*エクスプロイト*は、処理されるアプリケーションの脆弱性を利用する一連のデータまたはプログラムコードで、コンピューター上で悪意のある処理を実行します。たとえば、エクスプロイトは、ファイルの書き込みまたは読み取り、あるいは「感染している」Web サイトの要求を行うことができます。 それぞれのエクスプロイトは、さまざまなアプリケーションまたはネットワークサービスの脆弱性を利用します。ネットワークパケットに偽装したエクスプロイトは、ネットワーク経由で多数のコンピューターに送信され、脆弱なネットワークサービスを備えるコンピューターを探します。DOC ファイルのエクスプロイトは、テキストエディターの脆弱性を利用します。このエクスプロイトは、ユーザーが感染したファイルを開いたときに、ハッカーが事前にプログラミングした処理を開始することがあります。メールに組み込まれたエクスプロイトは、メールクライアントの脆弱性を探します。このエクスプロイトは、ユーザーがメールクライアントの感染メールを開くとすぐに悪意のある処理を実行します。 エクスプロイトを使用してネットワーク上に拡散するのがネットワームです。ヌーカー型エクスプロイトは、コンピューターを無効にするネットワークパケットです。
FileCryptor	エンクリプター	このプログラムは、他の悪意のあるアプリケーションを暗号化してアンチウイルス製品から隠蔽します。
Flooder	ネットワークを「汚染する」ためのプログラム	このプログラムは大量のメールをネットワークチャネル上に送信します。この種のツールには、インターネットリレーチャットなどを汚染するプログラムがあります。 Flooder 型ツールには、メール、IM クライアントおよびモバイル通信システムで使用されるチャネルを「汚染する」プログラムは含まれません。これらのプログラムは、テーブルに示す別種（Email-Flooder、IM-Flooder および SMS-Flooder）として区別されます。
HackTool	ハッキングツール	このプログラムは、たとえば、ユーザーの許可なしに新しいシステムアカウントを追加したり、システムログを消去してオペレーティングシステムにおける存在の痕跡を隠蔽したりすることによって、このプログラムがインストールされたコンピューターをハッキングすることや別のコンピューターを攻撃することを可能にします。この種のツールには、パスワードの傍受などの悪意のある機能を特徴とする一部のスニファーが含まれます。スニファーは、ネットワークトラフィックの監視を可能にするプログラムです。
Hoax	デマウイルス	このプログラムはウイルスメッセージに似たメッセージでユーザーに注意を喚起します。具体的には、感染していないファイルで「ウイルスを検知した」というメッセージや、実際にはディスクのフォーマットが発生しなかったのに、ディスクがフォーマットされたというメッセージを表示します。
スプーファ	スプーフィングツール	このツールは、メッセージ要求やネットワーク要求を送信者の偽装アドレスで送信します。たとえば、侵入者はスプーファ型のツールを使用して、ツール本体をメールの実際の送信者として渡します。
VirTool	悪意のあるアプリケーションを改変するツール	このツールを使用すると、他のマルウェアを改変して、アンチウイルス製品から隠蔽することができます。
Email-Flooder	メールアドレスを「汚染する」プログラム	このプログラムはさまざまなメールアドレスに大量のメールを送信して、これらのメールアドレスを「汚染」します。大量の受信メールによって、ユーザーは必要なメールを受信ボックスで表示できなくなります。
IM-Flooder	メッセンジャークライアントのトラフィックを「汚染する」プログラム	IM クライアントのユーザーをメッセージであふれさせます。大量のメールが送られてくるため、ユーザーは必要な受信メールを表示できなくなります。
SMS-Flooder	トラフィックを SMS メッセージで「汚染する」プログラム	このプログラムは携帯電話に大量の SMS メッセージを送信します。

- **アドウェア**

サブカテゴリ：広告ソフトウェア（アドウェア）

危険度：中

アドウェアはユーザーに対して広告情報を表示します。アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。このようなプログラムには、ユーザーに関するマーケティング情報を収集し、それを開発者に送信するものがあります。この情報には、ユーザーが表示した Web サイトの名前や、ユーザーの検索の内容などが含まれます。スパイウェア型のトロイの木馬とは異なり、アドウェアは、このような情報をユーザーの同意を得てから開発者に送ります。

- **オートダイヤラー**

サブカテゴリ：ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア。

危険度：中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

種別	Name	説明
クライアント-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他のコンピューターにインストールされているアプリケーションとどのようにデータをやり取りしているかを監視する）。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理プログラム	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。 合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。
Server-FTP	FTP サーバー	このプログラムは FTP サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP 経由でコンピューターへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnet サーバー	このプログラムは Telnet サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet 経由でコンピューターへのリモートアクセスを開きます。
Server-Web	Web サーバー	このプログラムは Web サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP 経由でコンピューターへのリモートアクセスを開きます。
RiskTool	ローカルコンピューターで動作するツール	このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、コンピューターにインストールされているアプリケーションを起動することできます。
Client-P2P	P2P ネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
クライアント-SMTP	SMTP クライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Web ツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

- **ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア**

サブカテゴリ：ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア。

危険度：中

これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

種別	Name	説明
クライアント-IRC	インターネットチャットクライアント	これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。
ダウンローダー	ダウンロード用プログラム	これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。
モニター	監視用プログラム	このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他のコンピューターにインストールされているアプリケーションとどのようにデータをやり取りしているかを監視する）。
PSWTool	パスワード不正取得ツール	このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。
RemoteAdmin	リモート管理プログラム	このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。 合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。
Server-FTP	FTP サーバー	このプログラムは FTP サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP 経由でコンピューターへのリモートアクセスを開きます。
Server-Proxy	プロキシサーバー	このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
Server-Telnet	Telnet サーバー	このプログラムは Telnet サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet 経由でコンピューターへのリモートアクセスを開きます。
Server-Web	Web サーバー	このプログラムは Web サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP 経由でコンピューターへのリモートアクセスを開きます。
RiskTool	ローカルコンピューターで動作するツール	このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。
NetTool	ネットワークツール	このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、コンピューターにインストールされているアプリケーションを起動することできます。
Client-P2P	P2P ネットワーククライアント	このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。
クライアント-SMTP	SMTP クライアント	このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。
WebToolbar	Web ツールバー	このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。
FraudTool	擬似プログラム	このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。

- **悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト**

  サブカテゴリ：損害を与える可能性がある圧縮ファイル

  危険度：中

  ファイルは、マルウェア（ウイルス、ワーム、トロイの木馬）の圧縮に使用される特殊なパッカーを使用して圧縮されます。Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に解凍モジュールがないかスキャンします。

  マルウェアをアンチウイルスによる検知から隠すために、ハッカーは特殊なパッカーを使用してマルウェアを圧縮します。カスペルスキーのエキスパートは、ハッカーの間で最も使用されているパッカーを特定しています。

- **多重圧縮オブジェクト**

  サブカテゴリ：損害を与える可能性がある圧縮ファイル

  危険度：中

  ファイルは、マルウェア（ウイルス、ワーム、トロイの木馬）の圧縮に使用される特殊なパッカーを使用して圧縮されます。Kaspersky Endpoint Security は、SFX（自己解凍形式）アーカイブ内に解凍モジュールがないかスキャンします。

  マルウェアをアンチウイルスによる検知から隠すために、ハッカーは特殊なパッカーを使用してマルウェアを圧縮します。カスペルスキーのエキスパートは、ハッカーの間で最も使用されているパッカーを特定しています。

除外リスト

このテーブルには、信頼するオブジェクトに関する情報が示されます。

絶対パスではなく相対パスを指定することを推奨します。これにより、ファイルシステムのオブジェクトだけでなく、ファイルレス攻撃の対象オブジェクトも除外できるようになります。例：「`*\Program Files (x86)\Folder\Subfolder`」。

次の方法を使用して、スキャンからオブジェクトを除外できます：

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

    ファイルまたはフォルダーのパスにマスクを使用できます。たとえば、コンピューター上のすべてのユーザーアカウントを対象として［ダウンロード］フォルダーをスキャンする場合は、「`C:\Users\*\Downloads\`」と入力します。

    Kaspersky Endpoint Security は環境変数をサポートしています。

    > Kaspersky Security Center コンソールを使用して除外リストを作成する際、環境変数「`%userprofile%`」は Kaspersky Endpoint Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「*」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

- 「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（例：「`Email-Worm`」、「`Rootkit`」、「`RemoteAdmin`」）。任意の 1 文字を置き換える「`?`」と複数の文字を置き換える「`*`」を使用してマスクを使用することができます。たとえば、マスク「`Client*`」を使用すると、「`Client-IRC`」、「`Client-P2P`」および「`Client-SMTP`」がスキャンから除外されます。

> 信頼するオブジェクトの設定がコンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトが禁止されている場合（［**ローカルの除外リストの使用を許可する**］チェックボックスがオフ）は、すべての信頼するオブジェクトのリストが製品のユーザーインターフェイスで非表示になります。

信頼するアプリケーション

このテーブルには、Kaspersky Endpoint Security の動作中にアクティビティが監視されない信頼するアプリケーションのリストが表示されます。

Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

> Kaspersky Security Center コンソールで信頼するアプリケーションのリストを作成する際、環境変数 `%userprofile%` は Kaspersky Endpoint Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「*」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

アプリケーションコントロールは、それぞれのアプリケーションが信頼するアプリケーションの表に含まれているかどうかに関係なく、アプリケーションの起動を制限します。

> 信頼するアプリケーションの設定が管理者によってコンソールでブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するアプリケーションが禁止されている場合（［**ローカルの信頼するアプリケーションの使用を許可する**］チェックボックスがオフ）は、すべての信頼するアプリケーションのリストが製品のユーザーインターフェイスで非表示になります。

継承時に値を統合する *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Security Center の親ポリシーと子ポリシーのスキャンの除外リストと信頼するアプリケーションのリストを結合します。リストを結合するには、子ポリシーは Kaspersky Security Center の親ポリシーの設定を継承するよう設定されている必要があります。 チェックボックスがオンの場合、Kaspersky Security Center の親ポリシーのリスト項目は子ポリシー内で表示されます。このようにすることで、組織全体の信頼するアプリケーションのリストを作成することが可能です。 継承された子ポリシー内のリスト項目は削除または編集できません。継承時に結合されたスキャンの除外リストと信頼するアプリケーションのリストの項目は親ポリシー内でのみ削除および編集可能です。リストの項目は、下位のポリシーで追加、編集、削除が可能です。 子ポリシーと親ポリシーのリスト項目が一致する場合、これらの項目は親ポリシー内の同じ項目として表示されます。 このチェックボックスをオフにすると、リストの項目は Kaspersky Security Center ポリシーの設定の継承時に結合されません。 この機能により、ポリシープロファイル内のリストを結合することもできます。リストを結合するには、最も優先度の高いプロファイルで、それよりも優先度の低いプロファイルからの設定の継承を有効にします。ポリシープロファイルのプロパティについて詳しくは、Kaspersky Security Center ヘルプを参照してください。
ローカルの除外リストの使用を許可する / ローカルの信頼するアプリケーションの使用を許可する *（Kaspersky Security Center コンソール内でのみ利用可能）*	*ローカルの除外リストとローカルの信頼するアプリケーションのリスト（ローカルの信頼ゾーン）*とは、Kaspersky Endpoint Security で特定のコンピューターに向けてユーザーが定義したオブジェクトのリストです。Kaspersky Endpoint Security はローカルの信頼ゾーンのオブジェクトとアプリケーションを監視しません。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。 チェックボックスがオンの場合、ユーザーはスキャンの除外リストと信頼するアプリケーションのリストをローカルに作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。 チェックボックスがオフの場合、ユーザーはポリシー内で作成されたスキャンの除外リストと信頼するアプリケーションの全体的なリストのみにアクセスできます。
EDR (KATA) / NDR (KATA) のテレメトリ *（Kaspersky Security Center コンソール内でのみ利用可能）*	このテーブルには、EDR テレメトリの除外リストに関する情報が示されます。
KUMA テレメトリ *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Unified Monitoring and Analysis Platform (KUMA) に送信されるイベントのリスト。Kaspersky Endpoint Security は次のモードで動作します： • **すべてのイベントを送信する**：このモードでは、本製品は除外ルールに追加されたイベントを除くすべてのイベントを Windows ログから送信します。 • **選択したイベントのみ送信する**：このモードでは、本製品は包含ルールに追加されたイベントのみを送信します。
信頼するシステム証明書ストア	信頼するシステム証明書ストアの1つが選択されている場合、Kaspersky Endpoint Security は信頼するデジタル署名を持つアプリケーションをスキャンから除外します。Kaspersky Endpoint Security はこのようなアプリケーションを**信頼済み**グループに割り当てます。 ［**使用しない**］が選択されている場合、Kaspersky Endpoint Security はアプリケーションが署名されているかどうかにかかわらずスキャンします。Kaspersky Endpoint Security は、このアプリケーションがコンピューターに与える危険のレベルに応じて、アプリケーションを信頼グループに配置します。

製品設定

製品の全般設定について次の設定を指定できます：

- ブロックモード
- セルフディフェンス
- パフォーマンス
- デバッグ情報
- 設定が適用された際のコンピューターの状態

パラメータ	説明
コンピューターの開始時に本製品を開始する（推奨）	このオプションをオンにすると、オペレーティングシステムの読み込み後に Kaspersky Endpoint Security が起動し、セッション中にコンピューターを保護します。 このオプションをオフにすると、オペレーティングシステムの読み込み後、ユーザーが手動で起動するまでは Kaspersky Endpoint Security が起動しません。コンピューター保護が無効になるため、ユーザーデータが脅威にさらされる可能性があります。
特別な駆除技術を使用する（システムリソースを大量に消費します）	通常、Kaspersky Endpoint Security は、コンピューターが感染する前に検知したマルウェアを終了します。特別な駆除は、すでに活動を開始したマルウェア (アクティブな感染) からコンピューターを保護し、データ損失や脅威の拡散のリスクを最小限に抑えます。 特別な駆除をオンにすると、Kaspersky Endpoint Security は悪意のある活動を検知するとポップアップ通知を表示します。この通知で、Kaspersky Endpoint Security は特別な駆除を実行するようユーザーに通知します。ユーザーがこの方法に同意すると、Kaspersky Endpoint Security はこれらの脅威を無効にして、コンピューターを再起動します。特別な駆除には大量のコンピューターリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。 本製品がアクティブな感染の検知を処理している際、オペレーティングシステムの一部が利用できなくなることがあります。特別な駆除が完了し、コンピューターが再起動すると復元されます。 サーバー向けの Windows を実行しているコンピューターに Kaspersky Endpoint Security がインストールされている場合、Kaspersky Endpoint Security は通知を表示しません。そのため、アクティブな脅威を駆除する操作を選択することはできません。脅威を駆除するには、製品設定で特別な駆除を有効にして、*マルウェアのスキャンタスク*の設定ですぐに特別な駆除を実行するよう設定する必要があります。その後 *マルウェアのスキャンタスク*を開始します。
アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する *（Kaspersky Security Center コンソール内でのみ利用可能）*	このチェックボックスをオンにすると、本製品は Kaspersky Security Center 管理サーバーをアクティベーションサーバーへの接続用のプロキシサーバーとして使用します。これは、アクティベーションコードを使用して、インターネットに接続できない分離されたネットワークセグメントにある製品をアクティベートする場合に必要です。ライセンス情報ファイルを使用して製品をアクティベートする場合、インターネット接続は必要ありません。
セルフディフェンスをオンにする	この機能ンをオンにすると、Kaspersky Endpoint Security によってハードディスクのアプリケーションファイル、メモリプロセス、システムレジストリエントリの改竄や削除が防止されます。
外部からのアプリケーションサービスの管理をブロックする	この機能をオンにすると、サードパーティ製アプリケーション（CMD など）を使用してアプリケーションサービスを管理できなくなります。サードパーティ製アプリケーションを使用してアプリケーションサービスを管理しようとすると、Microsoft Windows タスクバーのアプリケーションアイコン上に通知が表示されます（通知サービスが無効になっている場合を除く）。 外部からのアプリケーションサービスの管理は、AM-PPL 技術をサポートしていないコンピューター、または AM-PPL 技術が無効になっているコンピューターでのみ許可できます。
バッテリー使用中はスケジュールタスクを延期する	このチェックボックスをオンにすると、コンピューターがバッテリー電源で動作しているときに省電力モードが有効になります。Kaspersky Endpoint Security がスケジュールされているタスクを延期します。必要に応じて、スキャンタスクとアップデートタスクを手動で実行できます。 省エネモードが有効のときは、コンピューターがバッテリーの電力で動作している場合、以下のタスクがスケジュールされていても実行されません。 • *定義データベースと製品機能のアップデート* • *完全スキャン* • *簡易スキャン* • *オブジェクトスキャン* • *アプリケーション整合性チェック* • *IOC スキャン*
他のアプリケーションにシステムリソースを優先的に割り当てる	Kaspersky Endpoint Security がコンピューターをスキャンする際にコンピューターのリソースを消費するため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。これにより、他のアプリケーションの動作が遅くなることがあります。パフォーマンスを最適化するために、Kaspersky Endpoint Security には、*他のアプリケーションにリソースを振り分けるモード*が用意されています。このモードでは、CPU の負荷が高い場合に、オペレーティングシステムが Kaspersky Endpoint Security のスキャンタスクスレッドの優先度を下げることができます。これにより、オペレーティングシステムのリソースを他のアプリケーションに再分配することが可能になり、スキャンタスクの CPU 時間が減ります。その結果、Kaspersky Endpoint Security のスキャンに時間がかかるようになります。既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。

パラメータ	説明
スキャンタスクのCPU使用率を制限する	Kaspersky Endpoint Security のパフォーマンスを最適化するには、*マルウェアのスキャンタスク*による CPU 使用率を制限できます。 チェックボックスをオンにした場合、すべての CPU コアにかかる*マルウェアのスキャンタスク*からの平均負荷が、指定された値に近づきます。 既定では、このチェックボックスはオフです。
ダンプへの書き込みを有効にする	このチェックボックスをオンにすると、Kaspersky Endpoint Security はクラッシュ時にダンプを書き出します。 このチェックボックスをオフにすると、Kaspersky Endpoint Security はダンプを書き出しません。また、コンピューターのハードディスクから既存のダンプファイルを削除します。
ダンプおよびトレースファイルの保護を有効にする	このチェックボックスをオンにすると、ダンプファイルまたはトレースファイルの書き込みを有効にしたユーザーの他に、システム管理者およびローカル管理者にもダンプファイルへのアクセス権が付与されます。トレースファイルには、システムおよびローカルの管理者のみがアクセスできます。 このチェックボックスをオフにすると、すべてのユーザーがダンプファイルとトレースファイルにアクセスできるようになります。
設定が適用された際のコンピューターの状態 *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Endpoint Security がインストールされたクライアントコンピューターについて、ポリシーの適用またはタスクの実行時にエラーが発生した場合に、Web コンソールで表示されるステータスの設定です。*OK*、*警告*および*緊急*のステータスが利用可能です。
コンピューターを再起動せずにアップデートをインストールする	コンピューターを再起動せずにアプリケーションをアップグレードすることで、サーバーの動作が中断されることがありません。 バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。これより前のバージョンのアプリケーションをアップグレードする場合は、コンピューターを再起動する必要があります。 バージョン 11.11.0 以降、コンピューターを再起動せずに次の操作を実行できます： • パッチをインストールする • 製品コンポーネントのセットを変更する • Kaspersky Security for Windows Server に Kaspersky Endpoint Security をインストールする パラメータの既定値は、オペレーティングシステムの種類によって異なります。本製品がワークステーションにインストールされている場合、再起動せずに本製品をアップグレードするオプションは無効になります。本製品がサーバーにインストールされている場合、再起動せずに本製品をアップグレードするオプションは有効になります。
リモート管理ソフトウェアとの互換性 *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Endpoint Security をリモート管理ツール（RAT）と一緒に使用すると問題が発生する場合は、互換性モードを有効にすることができます。この問題は、RAT と製品のセキュアデスクトップ（Secure Desktop）機能に互換性がないことに関連して生じる可能性があります。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。 このオプションをオンにすると、RAT 互換性モードが有効になります。この機能を使用しない場合、アプリケーションは確認ダイアログを表示します。これは、コンピューターのセキュリティレベルを低下させる可能性があります。Kaspersky Endpoint Security と RAT で問題が発生していない場合、互換性モードを有効にすることは推奨しません。 このオプションをオフにすると、RAT 互換性モードは無効になります。既定では、このチェックボックスはオフです。 例：ブラウザーを RemoteApp モードで使用している場合、信頼されていない証明書を使用する Web サイトにアクセスしたときに確認ウィンドウが表示されないことがあります。これは、RemoteApp が本製品のセキュアデスクトップ機能をサポートしていないためです。これにより、ブラウザーが応答しなくなることがあります。RemoteApp モードでブラウザーを正しく動作させるには、互換性モードを有効にする必要があります。他のサードパーティ製ソフトウェアを使用しているときにセキュアデスクトップ機能に問題が発生した場合にも、互換性モードを有効にしてみることができます。

レポートと保管領域

レポート

レポートには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

レポートは、フォルダー「`C:\ProgramData\Kaspersky Lab\KES.12.12\Report`」に保存されます。

バックアップ

*バックアップ保管領域*には、*脅威*の駆除で削除または修正されたファイルのバックアップコピーが保存されています。*バックアップコピー*は、ファイルが駆除または削除される前に作成されるファイルのコピーです。ファイルのバックアップコピーは特別な形式で保存され、*脅威*となることはありません。

ファイルのバックアップコピーは、フォルダー `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` に保存されます。

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

Kaspersky Endpoint Security では、ファイルのバックアップコピーへのアクセス権を編集できません。

隔離

*隔離*はコンピューター上にある特別なローカル保管領域です。ユーザーがコンピューターに対して危険だと判断したファイルを隔離することができます。隔離されたファイルは暗号化された状態で保管され、端末のセキュリティに影響はありません。Kaspersky Endpoint Security は、Detection and Response ソリューション (EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox) と連携する際にのみ隔離を使用します。その他のケースにおいては、Kaspersky Endpoint Security は関連するファイルをバックアップに保管します。ソリューションの一部として隔離を管理するには、Kaspersky Sandbox のヘルプ、Kaspersky Endpoint Detection and Response Optimum のヘルプ、および Kaspersky Endpoint Detection and Response Expert のヘルプ、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

隔離は Web コンソールを使用しないと設定できません。Web コンソールを使用して、隔離されたオブジェクトを管理（復元、削除、追加など）できます。コマンドラインを使用してオブジェクトをローカルコンピューター上に復元できます。

Kaspersky Endpoint Security はシステムアカウント（SYSTEM）を使用してファイルを隔離します。

パラメータ	説明
レポートを削除するまでの期間（日）	このチェックボックスをオンにすると、レポートの最長保管期間は指定した期間に制限されます。既定の最長レポート保管期間は 30 日です。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
レポートファイルのサイズを制限する（MB）	このチェックボックスをオンにすると、最大レポートファイルサイズは指定した値に制限されます。既定では、最大ファイルサイズは 1024 MB です。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
オブジェクトを削除するまでの期間（日）	このチェックボックスをオンにすると、ファイルの最長保管期間は指定した期間に制限されます。既定の最長ファイル保管期間は 30 日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。
バックアップのサイズを制限する（MB）	このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。既定では、最大サイズは 1024 MB です。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Endpoint Security は最も古いファイルを保管領域から自動的に削除します。
隔離のサイズを制限する	このチェックボックスをオンにすると、隔離の最大サイズは指定した値に制限されます。既定では、最大サイズは 1024 MB です。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security は*隔離の保管領域に十分な空き容量がありません*のイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を停止します。隔離の中身を手動で空にしてください。
隔離の容量が次の割合に到達した際に通知する（%）	隔離のしきい値です。たとえば、「50%」のように隔離のしきい値を設定できます。隔離のサイズのしきい値に到達すると、Kaspersky Endpoint Security は対応するイベントを Kaspersky Security Center に送信し、イベントを Windows イベントログに公開します。その間本製品は新しいオブジェクトの隔離を継続します。
管理サーバーへのデータ転送 *（Kaspersky Security Center でのみ利用可能）*	管理サーバーへ情報を転送する必要のあるイベントのカテゴリです。管理サーバーのディスク領域を最適化するために、一部のデータの転送を無効にすることができます。 本製品は次のカテゴリのイベントを送信します： • **隔離ファイルの情報**：隔離されたファイルのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**リポジトリ**］→［**隔離**］フォルダーで確認できます。Kaspersky Endpoint Security は、Kaspersky Detection and Response ソリューションに統合されている場合にのみ隔離を使用します。 • **バックアップ内のファイルの情報**：バックアップファイルのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**リポジトリ**］→［**バックアップ**］フォルダーで確認できます。 • **未処理のファイルの情報**：未処理のファイルのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**リポジトリ**］→［**アクティブな脅威**］フォルダーで確認できます。 • **インストールされたデバイスの情報**：接続されたデバイスのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**リポジトリ**］→［**ハードウェア**］フォルダーで確認できます。デバイスのリストは、コンピューターのプロパティと Kaspersky Endpoint Security for Windows のポリシー（［**デバイスコントロール**］セクション）でも確認できます。 • **起動されたアプリケーションの情報**：実行ファイルのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**アプリケーションの管理**］→［**実行ファイル**］フォルダーで確認できます。実行ファイルのリストは、コンピューターのプロパティでも確認できます。 • **ファイル暗号化エラーの情報**：ファイル暗号化エラーのリストは、Kaspersky Security Center コンソールの［**詳細**］→［**データ暗号化と保護機能**］→［**暗号化イベント**］フォルダーで確認できます。エラーのリストは、コンピューターのプロパティでも確認できます。 • **アダプティブアノマリーコントロールルールのステータスに関するレポート**：レポートは、Kaspersky Security Center コンソールの［**レポート**］タブの［**管理サーバー**］フォルダーで確認できます。このレポートは、Kaspersky Endpoint Security for Windows のポリシーのプロパティ（［**アダプティブアノマリーコントロール**］セクション）でも確認できます。 • **アダプティブアノマリーコントロールルールの適用に関するレポート**：レポートは、Kaspersky Security Center コンソールの［**レポート**］タブの［**管理サーバー**］フォルダーで確認できます。このレポートは、Kaspersky Endpoint Security for Windows のポリシーのプロパティ（［**アダプティブアノマリーコントロール**］セクション）でも確認できます。 • **脅威の活動連鎖の情報**：検知の詳細は、Kaspersky Security Center Web コンソールの［**監視とレポート**］→［**アラート**］セクションで確認できます。脅威の活動連鎖に関する情報は、Kaspersky Endpoint Detection and Response ソリューションで使用されます。

ネットワークの設定

インターネットへの接続と定義データベースのアップデートで使用するプロキシサーバーの設定、ネットワークポートの監視モードの選択、暗号化された接続のスキャンの設定を行えます。

パラメータ	説明
従量制接続時に本製品によるデータ通信量を抑制する	このチェックボックスをオンにすると、インターネット接続が制限されているときに本製品のネットワークトラフィックを制限します。高速モバイルインターネット接続は制限するネットワークとして、Wi-Fi 接続は無制限のネットワークとして判断されます。 ネットワークにかかる費用の対策は、Windows 8 以降を実行中のコンピューターで動作します。
Webページと連携するためWebトラフィック内にスクリプトを埋め込む	このチェックボックスをオンにすると、Kaspersky Endpoint Security は Web ページと連携するためのスクリプトを Web トラフィック内に埋め込みます。このスクリプトはウェブコントロール機能が正常に動作するために必要です。スクリプトはウェブントロールのイベントの登録を有効にします。このスクリプトがない場合は、ユーザーのインターネット上の活動の監視を有効にできません。 Web ページと連携するスクリプトのトラフィックへの埋め込みは、ウェブコントロールの正常な動作のためカスペルスキーにより推奨されています。
プロキシサーバーの設定	クライアントコンピューターのユーザーによるインターネット接続で使用されるプロキシサーバーの設定です。Kaspersky Endpoint Security では、定義データベースや製品機能のアップデートに使用するものを含む、特定の保護機能にこの設定が使用されます。 プロキシサーバーの自動設定のために、Kaspersky Endpoint Security では WPAD プロトコル（Web Proxy Auto-Discovery Protocol）が使用されます。このプロトコルを使用してプロキシサーバーの IP アドレスを判別できない場合、Microsoft Internet Explorer のブラウザー設定で指定されているプロキシサーバーアドレスを使用します。
ローカルアドレスにはプロキシサーバーを使用しない	このチェックボックスをオンにすると、共有フォルダーからアップデートを行う際に、プロキシサーバーは使用されません。
プロキシサーバーの認証設定	インターネットアクセス用のプロキシサーバーで本製品を認証するには、ユーザーの資格情報を入力する必要があります。Kaspersky Endpoint Security は、プロキシサーバーでの自動認証をサポートしています。自動認証に失敗した場合は、資格情報を入力する必要があります。 **認証を使用しない** **NTLM認証**：現在のユーザーアカウントによる NTLM 認証（既定）。 **ユーザー名とパスワードを指定してNTLM認証を使用する**：手動で指定された資格情報による NTLM 認証。 **ユーザー名とパスワード**：手動で指定された資格情報による認証。 **自動認証** **Kerberos 認証**：現在のユーザーアカウントによる Kerberos 認証。 **ユーザー名とパスワードを指定して Kerberos 認証を使用する**：手動で指定された資格情報による Kerberos 認証。 Kerberos 認証を選択すると、Kaspersky Endpoint Security はプロキシサーバーの設定に応じて、Kerberos または NTLM プロトコルのいずれかを使用して認証を実行できます。
監視対象のポート	**すべてのネットワークポートを監視する**：このネットワークポート監視モードでは、保護機能（ファイル脅威対策、ウェブ脅威対策、メール脅威対策）はコンピューターで開いているすべてのネットワークポート経由で送信されるデータストリームを監視します。 **選択したネットワークポートを監視する**：このネットワークポートの監視モードでは、コンピューターの選択したポートおよび選択したアプリケーションのネットワークの動作を監視します。メールの送信とネットワークトラフィックで通常使用されるネットワークポートのリストは、カスペルスキーの専門家の推奨に従って構成されます。 **カスペルスキー推奨のリストに登録されているアプリケーションのすべてのポートを監視する**：Kaspersky Endpoint Security によってポートが監視されるアプリケーションの事前定義済みのリストを使用します。このリストには例えば、Google Chrome、Adobe Reader、Java やその他のアプリケーションが含まれます。 **選択したアプリケーションのすべてのポートを監視する**：Kaspersky Endpoint Security によってポートが監視されるアプリケーションのリストを使用します。

パラメータ	説明
暗号化された接続のスキャン	Kaspersky Endpoint Security は次のプロトコルを介して通信される暗号化されたネットワークトラフィックをスキャンします： • SSL 3.0 • TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3 Kaspersky Endpoint Security は次の暗号化された接続のスキャンモードをサポートします： • **暗号化された接続をスキャンしない**：Kaspersky Endpoint Security は「`https://`」で始まるアドレスの Web サイトのコンテンツにアクセスしません。 • **保護機能の要求に応じて暗号化された接続をスキャンする**：Kaspersky Endpoint Security はウェブ脅威対策、メール脅威対策、ウェブコントロールからの要求があった際にのみ暗号化された接続をスキャンします。 • **常に暗号化された接続をスキャンする**：Kaspersky Endpoint Security は保護機能が無効にされている場合でも暗号化されたネットワークトラフィックをスキャンします。 トラフィックのスキャンが無効にされている信頼するアプリケーションにより確立された暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストからの暗号化された接続はスキャンされません。事前設定された信頼する Web サイトのリストは、カスペルスキーによって作成されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。信頼する Web サイトのリストは Kaspersky Endpoint Security のインターフェイス内でのみ内容を表示できます。Kaspersky Security Center コンソールではリストを表示できません。
信頼するルート証明書	信頼するルート証明書のリストです。新しい認証局を導入する場合などに、Kaspersky Endpoint Security を使用してユーザーのコンピューターに信頼済みのルート証明書をインストールすることができます。本製品を使用して、Kaspersky Endpoint Security の証明書ストアに証明書を追加できます。この場合、証明書は Kaspersky Endpoint Security に対してのみ信頼済みと認識されます。言い換えると、ユーザーは新しい証明書を持つ Web サイトにブラウザーでアクセスできます。別のアプリケーションが Web サイトにアクセスしようとすると、証明書の問題により接続エラーが発生します。システムの証明書ストアに追加するには、Active Directory のグループポリシーを使用できます。
信頼されない証明書を持つドメインへのアクセス	• **許可する**：信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続を許可します。 信頼されていない証明書を持つドメインをブラウザーで開こうとすると、Kaspersky Endpoint Security は、警告とそのドメインにアクセスすることが推奨されない理由が記載された HTML ページを表示します。ユーザーは HTML 警告ページのリンクをクリックすることで、要求された Web リソースにアクセスできます。 サードパーティの製品またはサービスが信頼されていない証明書を持つドメインと接続を確立した場合、Kaspersky Endpoint Security はトラフィックをスキャンするために固有の証明書を作成します。新しい証明書のステータスは *ブロック* になっています。HTML ページはこの場合表示できず、接続はバックグラウンドモードで確立可能であるため、サードパーティの製品に信頼されていない接続に関して通知するためにこのようになっています。 • **ブロックする**：信頼されていない証明書を持つドメインにアクセスするときに Kaspersky Endpoint Security はネットワーク接続をブロックします。信頼されていない証明書を持つドメインをブラウザーで開こうとすると、Kaspersky Endpoint Security は、そのドメインがブロックされる理由が記載された HTML ページを表示します。
暗号化された接続のスキャンでエラーが発生するドメインへのアクセス	• **ブロックする**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はネットワーク接続をブロックします。 • **許可して除外リストにドメインを追加する**：このオプションを選択した場合、暗号化された接続のスキャンでエラーが発生したときに Kaspersky Endpoint Security はエラーが発生したドメインを［スキャンエラーの発生したドメイン］リストに追加し、このドメインへのアクセスでの暗号化されたネットワークトラフィックを監視しません。暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。リストに含まれる内容を消去して空にするには、［**ブロックする**］を選択する必要があります。Kaspersky Endpoint Security は、暗号化された接続のスキャンエラーのイベントを生成します。
SSL 2.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、SSL 2.0 プロトコルで確立されたネットワーク接続が監視されてブロックされます。 このチェックボックスをオフにすると、SSL 2.0 プロトコルで確立されたネットワーク接続はブロックされません。ただし、このプロトコル経由のネットワークトラフィックが監視されなくなります。
SSL 3.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、SSL 3.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、SSL 3.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。
TLS 1.0プロトコルでの接続をブロックする	このチェックボックスをオンにすると、TLS 1.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、TLS 1.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。

パラメータ	説明
EV証明書を使用したWebサイトへの暗号化された接続を復号化する	EV 証明書（Extended Validation Certificate）は、Web サイトの信頼性を示すためのもので、接続のセキュリティを向上させます。Web サイトで EV 証明書が使用されている場合、ブラウザーのアドレスバーの鍵アイコンでそのことが示されます。また、アドレスバーの全体や一部の色が緑色に変わるブラウザーもあります。 このチェックボックスをオンにすると、EV 証明書を使用している Web サイトの暗号化された接続を復号化して監視します。 このチェックボックスをオフにすると、本製品は HTTPS トラフィックの通信内容にアクセスできません。そのため、HTTPS トラフィックは「`https://bing.com`」などの URL のみに基づいて監視されます。 EV 証明書を使用している Web サイトに最初にアクセスするときには、チェックボックスがオンかオフかにかかわらず、接続が復号されます。
信頼するアドレスを設定	Kaspersky Endpoint Security でネットワーク接続をスキャンしない Web アドレスのリストを使用します。この場合 Kaspersky Endpoint Security は、ウェブ脅威対策、メール脅威対策、ウェブコントロールが動作している間は信頼する URL の HTTPS トラフィックはスキャンしません。 ドメイン名または IP アドレスを入力できます。Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「`*`」をサポートします。 Kaspersky Endpoint Security は IP アドレスで記号「`*`」をサポートしません。サブネットマスクを使用して IP アドレス範囲を選択することができます（例：198.51.100.0/24）。 例： • 「`domain.com`」と入力すると次のアドレスが含まれます：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。サブドメイン（例：`subdomain.domain.com`）は含まれません。 • 「`subdomain.domain.com`」と入力すると次のアドレスが含まれます：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。「`domain.com`」ドメインは含まれません。 • 「`*.domain.com`」と入力すると次のアドレスが含まれます：`https://movies.domain.com`、`https://images.domain.com/page123`。「`domain.com`」ドメインは含まれません。
信頼するアプリケーションを設定	Kaspersky Endpoint Security の動作中にアクティビティが監視されない信頼するアプリケーションのリストが表示されます。アプリケーションによるどの種別のアクティビティを監視しないかを選択できます（例：ネットワークトラフィックはスキャンしない、など）。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
固有の証明書ストアを使用してMozilla製品内で暗号化された接続をスキャンする場合、次を使用する *（Kaspersky Endpoint Security のインターフェイス内でのみ利用可能）*	このチェックボックスがオンの場合、Mozilla Firefox ブラウザーおよび Thunderbird メールクライアントでの暗号化されたトラフィックをスキャンします。Web サイトによっては、HTTPS プロトコルでアクセスする際にブロックされる可能性があります。 Mozilla Firefox のブラウザーおよび Thunderbird メールクライアントでトラフィックをスキャンするには、暗号化された接続のスキャンを有効にする必要があります。暗号化された接続のスキャンが無効になっている場合、Mozilla Firefox ブラウザーおよび Thunderbird メールクライアントでのトラフィックはスキャンされません。 本製品はカスペルスキーのルート証明書を使用して復号化したり暗号化したトラフィックを分析します。カスペルスキーのルート証明書を含む証明書ストアを選択することができます。 • **Windowsの証明書ストア（推奨）**：カスペルスキーのルート証明書は Kaspersky Endpoint Security のインストール中にこのストアに追加されます。 • **固有の証明書ストア**：Mozilla Firefox および Thunderbird は独自の証明書ストアを使用します。Mozilla 証明書ストアが選択されている場合、カスペルスキーのルート証明書をブラウザーのプロパティを使用してこのストアに手動で追加する必要があります。

インターフェイス

製品インターフェイスの設定を編集できます。

パラメータ	説明
ユーザーインターフェイス *（Kaspersky Security Center コンソール内でのみ利用可能）*	**簡略化したインターフェイスを表示する**：クライアントコンピューター上で、本製品のメインウィンドウにアクセスできなくなり、Windows の通知領域のアイコンだけが利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の一定範囲に限定された操作を実行できます。製品アイコンの上の通知も表示されます。 **ユーザーインターフェイスを表示する**：クライアントコンピューター上で、Kaspersky Endpoint Security のメインウィンドウと Windows の通知領域のアイコンが利用できます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。 **アプリケーション動作モニターセクションを非表示**：クライアントコンピューターの Kaspersky Endpoint Security のメインウィンドウで［**アプリケーション動作モニター**］を使用できなくなります。*アプリケーション動作モニター*は、ユーザーのコンピューターのアプリケーションの動作に関する情報をリアルタイムで表示するように設計されたツールです。 **ユーザーインターフェイスを表示しない**：クライアントコンピューター上で、Kaspersky Endpoint Security の動作に関するメニューなどが表示されません。Windows の通知領域のアイコンと通知も表示されません。
通知の設定	コンポーネントやタスク、アプリケーション全体の動作中に発生する可能性がある、さまざまな重要度のイベントに関する通知の設定を含むテーブル。Kaspersky Endpoint Security では、これらのイベントに関する通知を画面に表示したり、メールで送信したり、ログを取ったりします。
メール通知の設定	本製品の動作中に登録されたイベントに関する通知を配信するための SMTP サーバー設定。 既定では、Kaspersky Endpoint Security は Kaspersky Security Center からのメール通知設定を使用します。メール通知設定の詳細については、Kaspersky Security Center ヘルプを参照してください。 個別のメール通知の設定が必要な場合は、以下の設定を編集することができます。 • **送信者のアドレス**：送信者のメールアドレス。存在しないアドレスを使用することは推奨されません。 • **SMTP サーバー**：組織内のメールサーバーのアドレス1つ以上（たとえば、`mail.company.com`）。IP アドレス（IPv4 または IPv6）を入力できます。 SMTP サーバーでユーザーを認証するには、対応するフィールドに送信者の認証情報を入力します。メール通知をテストするために、テストメッセージを送信することができます。 • **受信者のアドレス**：アプリケーションが通知を送信する受信者のメールアドレス。 • **送信方法**：メール通知の送信モード。Kaspersky Endpoint Security は、イベント発生時に即座にメッセージを送信することも、またはあらかじめ設定したスケジュールに従って送信することも可能です。
通知領域に製品のステータスを表示する	該当するカテゴリのイベントが発生した場合、Windows タスクバーの通知領域の Kaspersky Endpoint Security アイコンが変化し（ または ）、ポップアップ通知が表示されます。
ローカルのマルウェア対策データベースのステータスに関する通知	製品で使用されている定義データベースが長期間アップデートされていない場合の通知設定です。
パスワードによる保護	切り替えスイッチがオンの場合、パスワードによる保護の範囲内でユーザーが操作を実行しようとしたときに Kaspersky Endpoint Security によってパスワードの入力が要求されます。パスワードによる保護の対象範囲は、ブロックされる操作（例：保護機能の停止）とパスワードによる保護が適用されるユーザーアカウントとを組み合わせて指定されます。 パスワードによる保護を有効にすると、Kaspersky Endpoint Security では KLAdmin アカウントのパスワードの設定が要求されます。
ユーザーサポート / Web リソースへのリンク *（Kaspersky Security Center コンソール内でのみ利用可能）*	このウィンドウでは、Kaspersky Endpoint Security のサポート関連情報が記載されている Web リソースへのリンクです。標準のリンクに代わって、追加されたリンクが Kaspersky Endpoint Security のローカルインターフェイスの［**サポート**］ウィンドウに表示されます。
ユーザーサポート / 説明 *（Kaspersky Security Center コンソール内でのみ利用可能）*	Kaspersky Endpoint Security のローカルインターフェイスの［**サポート**］ウィンドウに表示されるメッセージ。

設定の管理

現在の Kaspersky Endpoint Security の設定をファイルに保存して、これを使用して別のコンピューターにアプリケーションを簡単にインストールすることができます。また Kaspersky Security Center を介してインストールパッケージを使用したアプリケーションの配布時にこの設定ファイルを使用することができます。既定の設定をいつでも復元することができます。

製品設定の管理設定は Kaspersky Endpoint Security のインターフェイス内でのみ利用可能です。

製品設定の管理設定

設定	説明
インポート	CFG 形式のファイルから設定を抽出し、適用します。
エクスポート	CFG 形式のファイルに現在の設定を保存します。
復元	カスペルスキーが推奨する製品設定はいつでも復元することができます。この設定が復元されると、すべての保護機能のセキュリティレベルが［**推奨**］に設定されます。

定義データベースとソフトウェアモジュールのアップデート

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

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

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

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

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

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

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

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

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

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

定義データベースが長期間アップデートされていない場合、アップデートパッケージのサイズが大きくなり、インターネットトラフィックが最大で数十 MB まで増加することがあります。

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

アップデート結果、およびアップデートタスクの実行中に発生するイベントに関する情報が Kaspersky Endpoint Security のレポートに記録されます。

本製品が Light Agent モードで動作している場合、定義データベースとモジュールのアップデート時に特別な考慮事項が適用されます。

製品機能と定義データベースのアップデートの設定

パラメータ	説明
定義データベースのアップデートのスケジュール	**自動で開始**：このモードでは、新しいアップデートパッケージが使用可能であるかどうかがアップデート元に特定の頻度で確認されます。アップデートパッケージを確認する頻度は、ウイルスの発生中には高くなり、ウイルスがないときは低くなります。新しいアップデートパッケージが検知されると、Kaspersky Endpoint Security によってそのパッケージがコンピューターにダウンロードされアップデートがインストールされます。 **手動**：このアップデートタスク実行方法を使用して、アップデートタスクを手動で開始することができます。 **スケジュールで指定**：このアップデートタスク実行方法では、アップデートタスクは指定したスケジュールに従って実行されます。このアップデートタスク実行方法を選択した場合でも、Kaspersky Endpoint Security のアップデートタスクを手動で開始することができます。
未実行のタスクを実行する	このチェックボックスをオンにすると、スキップされたタスクは実行可能になると同時に開始されます。タスクの開始時間にコンピューターの電源がオフになっていた場合などに、タスクがスキップされることがあります。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。 このチェックボックスをオフにすると、スキップされたタスクは開始されません。代わりに、現在のスケジュールに従って、次のタスクが実行されます。
アップデート元	「*アップデート元*」は、Kaspersky Endpoint Security の定義データベースと機能のアップデートを含むリソースです。 アップデート元には、Kaspersky Security Center サーバーやカスペルスキーのアップデートサーバー、ネットワークフォルダーまたはローカルフォルダーが含まれます。 アップデート元の既定のリストには Kaspersky Security Center とカスペルスキーのアップデートサーバーが含まれています。リストに他のアップデート元を追加できます。アップデート元には、HTTP/FTP サーバーと共有フォルダーを指定できます。 Kaspersky Endpoint Security は、カスペルスキーのアップデートサーバーである場合を除き、HTTPS サーバーからのアップデートをサポートしません。 複数のリソースがアップデート元として選択されている場合は、リスト上位のリソースから次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。 既定では、Kaspersky Endpoint Security は Kaspersky Security Center サーバーを最初のアップデート元として使用します。これにより、アップデート時のトラフィックを節約することができます。ポリシーがコンピューターに適用されていない場合、製品が Kaspersky Security Center サーバーにアクセスできない可能性があるため、ローカルタスクの *定義データベースと製品機能のアップデート* 設定でカスペルスキーサーバーが最初のアップデート元として選択されます。 本製品が Light Agent モードで実行されている場合、SVM 上のフォルダーがアップデート元として選択されます。

パラメータ	説明
定義データベースをアップデートするユーザー	既定では、Kaspersky Endpoint Security のアップデートタスクは、オペレーティングシステムへのログインに使用したアカウントを持つユーザーの代わりに開始されます。ただし、Kaspersky Endpoint Security は、必要な権利がないことが原因でユーザーがアクセスできないアップデート元（アップデートパッケージを含む共有フォルダーからアップデートを実行する場合など）やプロキシサーバーの認証が設定されていないアップデート元からアップデートされる場合があります。製品設定でアップデートの権限を持つユーザーを指定して、そのユーザーアカウントで Kaspersky Endpoint Security のアップデートタスクを開始できます。
製品機能のアップデートをダウンロード	製品のデータベースのアップデートと製品機能のアップデートをダウンロードします。 このチェックボックスをオンにすると、Kaspersky Endpoint Security によって適用可能な製品機能のアップデートについてユーザーに通知され、アップデートタスクの実行中に、アップデートパッケージに製品機能のアップデートが含まれます。製品機能のアップデートを適用する方法は次の設定によって決定されます： • **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Endpoint Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。 • **承認済みのアップデートのみをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Endpoint Security によりアップデートがインストールされます。既定ではこのオプションが選択されます。 このチェックボックスをオフにすると、Kaspersky Endpoint Security から適用可能な製品機能のアップデートについてユーザーに通知されず、アップデートタスクの実行中に、アップデートパッケージに製品機能のアップデートは含まれません。 製品機能のアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。 既定では、このチェックボックスはオンです。
アップデートをフォルダーにコピー	このチェックボックスをオンにすると、チェックボックス下部で指定されている共有フォルダーにアップデートパッケージをコピーします。これで、LAN 上のその他のコンピューターは、アップデートパッケージを共有フォルダーから受け取ることができます。この設定を行うと、アップデートパッケージのダウンロードは一度だけ実行されるようになります。このため、インターネットトラフィックが減少します。既定では、次のフォルダーが指定されます：`C:\ProgramData\Kaspersky Lab\KES.12.12\Update distribution\`。
アップデート対象のプロキシサーバー *（Kaspersky Endpoint Security のインターフェイス内でのみ利用可能）*	製品機能と定義データベースのアップデート用のクライアントコンピューターのユーザーのインターネットアクセスのプロキシサーバー設定です。 プロキシサーバーの自動設定のために、Kaspersky Endpoint Security では WPAD プロトコル（Web Proxy Auto-Discovery Protocol）が使用されます。このプロトコルを使用してプロキシサーバーの IP アドレスを判別できない場合、Kaspersky Endpoint Security は、Microsoft Internet Explorer のブラウザー設定で指定されているプロキシサーバーアドレスを使用します。
ローカルアドレスにはプロキシサーバーを使用しない *（Kaspersky Endpoint Security のインターフェイス内でのみ利用可能）*	このチェックボックスをオンにすると、共有フォルダーからアップデートを行う際に、プロキシサーバーは使用されません。

補足資料 2：アプリケーションの信頼グループ

Kaspersky Endpoint Security は、コンピューターで起動したすべてのアプリケーションを信頼グループに分類します。アプリケーションがオペレーティングシステムに及ぼす脅威レベルに応じて、アプリケーションはいずれかの信頼グループに分類されます。

信頼グループは次の通りです：

- **信頼済み**：このグループには次の条件の1つ以上を満たすアプリケーションが含まれます：
  - 信頼できる開発元によってデジタル署名されたアプリケーション。
  - Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されたアプリケーション。
  - ユーザーがアプリケーションを「*信頼済み*」グループに配置した。

  これらのアプリケーションでは、ブロックされる操作はありません。
- **弱い制限付き**：このグループには次の条件を満たすアプリケーションが含まれます：
  - 信頼できる開発元によってデジタル署名されていないアプリケーション。
  - Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
  - ユーザーがアプリケーションを「*弱い制限付き*」グループに配置した。

  これらのアプリケーションはオペレーティングシステムリソースへのアクセスに最小限の制限が付けられます。
- **強い制限付き**：このグループには次の条件を満たすアプリケーションが含まれます：
  - 信頼できる開発元によってデジタル署名されていないアプリケーション。
  - Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
  - ユーザーがアプリケーションを「*強い制限付き*」グループに配置した。

  これらのアプリケーションはオペレーティングシステムリソースへのアクセスに強い制限が付けられます。
- **ブロック**：このグループには次の条件を満たすアプリケーションが含まれます：
  - 信頼できる開発元によってデジタル署名されていないアプリケーション。
  - Kaspersky Security Network の信頼するアプリケーションのデータベースに記録されていないアプリケーション。
  - ユーザーがアプリケーションを「*ブロック*」グループに配置した。

  これらのアプリケーションでは、すべての操作がブロックされます。

補足資料3：リムーバブルドライブの簡易スキャンのファイル拡張子

com – アプリケーションの実行ファイル（64 KB 以下）

exe – 実行ファイルまたは自己解凍型アーカイブ

sys – Microsoft Windows システムファイル

prg – dBase™、Clipper または Microsoft Visual FoxPro® のプログラムテキスト、または WAVmaker プログラム

bin – バイナリファイル

bat – バッチファイル

cmd – Microsoft Windows NT（DOS のバッチファイルに類似）、OS/2 のコマンドファイル

dpl – Borland Delphi の圧縮ライブラリ

dll – ダイナミックリンクライブラリ

scr – Microsoft Windows スプラッシュスクリーン

cpl – Microsoft Windows コントロールパネルモジュール

ocx – Microsoft OLE（オブジェクトのリンクと埋め込み）オブジェクト

tsp – スプリットタイムモードで実行されているプログラム

drv – デバイスドライバー

vxd – Microsoft Windows 仮想デバイスドライバー

pif – プログラム情報ファイル

lnk – Microsoft Windows リンクファイル

reg – Microsoft Windows システムレジストリキーファイル

ini – Microsoft Windows、Windows NT、および一部のアプリケーションの構成データを含む設定ファイル

cla – Java クラス

vbs – Visual Basic® スクリプト

vbe – BIOS Video Extension

js、jse – JavaScript ソーステキスト

htm – ハイパーテキストドキュメント

htt – Microsoft Windows ハイパーテキストヘッダー

hta – Microsoft Internet Explorer® のハイパーテキストプログラム

asp – Active Server Pages スクリプト

chm – コンパイル済み HTML ファイル

pht – 統合 PHP スクリプトを含む HTML ファイル

php – HTML ファイルに組み込まれたスクリプト

wsh – Microsoft Windows スクリプトホストファイル

wsf – Microsoft Windows スクリプト

the – Microsoft Windows 95 デスクトップ壁紙ファイル

hlp – Windows ヘルプファイル

msg – Microsoft Mail メール

plg – メール

mbx – 保存されている Microsoft Office Outlook メールメッセージ

doc* – Microsoft Office Word ドキュメント（doc – Microsoft Office Word ドキュメント、docx – XML のサポートを含む Microsoft Office Word 2007 ドキュメント、docm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメント）

dot* – Microsoft Office Word ドキュメントテンプレート（dot – Microsoft Office Word ドキュメントテンプレート、dotx – Microsoft Office Word 2007 ドキュメントテンプレート、dotm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメントテンプレート）

fpm – データベースプログラム、Microsoft Visual FoxPro 開始ファイル

rtf – リッチテキストフォーマットドキュメント

shs – Shell Scrap Object Handler フラグメント

dwg – AutoCAD® 図面データベース

msi – Microsoft Windows インストールパッケージ

otm – Microsoft Office Outlook 用 VBA プロジェクト

pdf – Adobe Acrobat ドキュメント

swf – Shockwave® Flash パッケージオブジェクト

jpg、jpeg – 圧縮イメージグラフィック形式

emf – Enhanced Metafile 形式のファイル

ico – オブジェクトアイコンファイル

ov? – Microsoft Office Word 実行ファイル

xl* – Microsoft Office Excel ドキュメントおよびファイル（xla – Microsoft Office Excel の拡張子、xlc – ダイアグラム、xlt – ドキュメントテンプレート、xlsx – Microsoft Office Excel 2007 ブック、xltm – マクロのサポートを含む Microsoft Office Excel 2007 ブック、xlsb – バイナリ（非 XML）形式の Microsoft Office Excel 2007 ブック、xltx – Microsoft Office Excel 2007 テンプレート、xlsm – マクロのサポートを含む Microsoft Office Excel 2007 テンプレート、xlam – マクロのサポートを含む Microsoft Office Excel 2007 プラグイン）

pp* – Microsoft Office PowerPoint® ドキュメントおよびファイル（pps – Microsoft Office PowerPoint スライド、ppt – プレゼンテーション、pptx – Microsoft Office PowerPoint 2007 プレゼンテーション、pptm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーション、potx – Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、potm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、ppsx – Microsoft Office PowerPoint 2007 スライドショー、ppsm – マクロのサポートを含む Microsoft Office PowerPoint 2007 スライドショー、ppam – マクロのサポートを含む Microsoft Office PowerPoint 2007 プラグイン）

md* – Microsoft Office Access® ドキュメントおよびファイル（mda – Microsoft Office Access ワークグループ、mdb – データベース）

sldx – Microsoft PowerPoint 2007 スライド

sldm – マクロのサポートを含む Microsoft PowerPoint 2007 スライド

thmx – Microsoft Office 2007 テーマ

補足資料 4：メール脅威対策用の添付ファイルフィルターのファイル種別

注意：実際のファイル形式は、そのファイル名の拡張子と一致しないことがあります。

添付ファイルのフィルタリングを有効にした場合、メール脅威対策によって、次の拡張子をもつファイルの名前が変更されたり、ファイルが削除されることがあります：

com – アプリケーションの実行ファイル（64 KB 以下）

exe – 実行ファイルまたは自己解凍型アーカイブ

sys – Microsoft Windows システムファイル

prg – dBase™、Clipper または Microsoft Visual FoxPro® のプログラムテキスト、または WAVmaker プログラム

bin – バイナリファイル

bat – バッチファイル

cmd – Microsoft Windows NT（DOS のバッチファイルに類似）、OS/2 のコマンドファイル

dpl – Borland Delphi の圧縮ライブラリ

dll – ダイナミックリンクライブラリ

scr – Microsoft Windows スプラッシュスクリーン

cpl – Microsoft Windows コントロールパネルモジュール

ocx – Microsoft OLE（オブジェクトのリンクと埋め込み）オブジェクト

tsp – スプリットタイムモードで実行されているプログラム

drv – デバイスドライバー

vxd – Microsoft Windows 仮想デバイスドライバー

pif – プログラム情報ファイル

lnk – Microsoft Windows リンクファイル

reg – Microsoft Windows システムレジストリキーファイル

ini – Microsoft Windows、Windows NT、および一部のアプリケーションの構成データを含む設定ファイル

cla – Java クラス

vbs – Visual Basic® スクリプト

vbe – BIOS Video Extension

js、jse – JavaScript ソーステキスト

htm – ハイパーテキストドキュメント

htt – Microsoft Windows ハイパーテキストヘッダー

hta – Microsoft Internet Explorer® のハイパーテキストプログラム

asp – Active Server Pages スクリプト

chm – コンパイル済み HTML ファイル

pht – 統合 PHP スクリプトを含む HTML ファイル

php – HTML ファイルに組み込まれたスクリプト

wsh – Microsoft Windows スクリプトホストファイル

wsf – Microsoft Windows スクリプト

the – Microsoft Windows 95 デスクトップ壁紙ファイル

hlp – Windows ヘルプファイル

msg – Microsoft Mail メール

plg – メール

mbx – 保存されている Microsoft Office Outlook メールメッセージ

doc* – Microsoft Office Word ドキュメント（doc – Microsoft Office Word ドキュメント、docx – XML のサポートを含む Microsoft Office Word 2007 ドキュメント、docm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメント）

dot* – Microsoft Office Word ドキュメントテンプレート（dot – Microsoft Office Word ドキュメントテンプレート、dotx – Microsoft Office Word 2007 ドキュメントテンプレート、dotm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメントテンプレート）

fpm – データベースプログラム、Microsoft Visual FoxPro 開始ファイル

rtf – リッチテキストフォーマットドキュメント

shs – Shell Scrap Object Handler フラグメント

dwg – AutoCAD® 図面データベース

msi – Microsoft Windows インストールパッケージ

otm – Microsoft Office Outlook 用 VBA プロジェクト

pdf – Adobe Acrobat ドキュメント

swf – Shockwave® Flash パッケージオブジェクト

jpg、jpeg – 圧縮イメージグラフィック形式

emf – Enhanced Metafile 形式のファイル

ico – オブジェクトアイコンファイル

ov? – Microsoft Office Word 実行ファイル

xl* – Microsoft Office Excel ドキュメントおよびファイル（xla – Microsoft Office Excel の拡張子、xlc – ダイアグラム、xlt – ドキュメントテンプレート、xlsx – Microsoft Office Excel 2007 ブック、xltm – マクロのサポートを含む Microsoft Office Excel 2007 ブック、xlsb – バイナリ（非 XML）形式の Microsoft Office Excel 2007 ブック、xltx – Microsoft Office Excel 2007 テンプレート、xlsm – マクロのサポートを含む Microsoft Office Excel 2007 テンプレート、xlam – マクロのサポートを含む Microsoft Office Excel 2007 プラグイン）

pp* – Microsoft Office PowerPoint® ドキュメントおよびファイル（pps – Microsoft Office PowerPoint スライド、ppt – プレゼンテーション、pptx – Microsoft Office PowerPoint 2007 プレゼンテーション、pptm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーション、potx – Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、potm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、ppsx – Microsoft Office PowerPoint 2007 スライドショー、ppsm – マクロのサポートを含む Microsoft Office PowerPoint 2007 スライドショー、ppam – マクロのサポートを含む Microsoft Office PowerPoint 2007 プラグイン）

md* – Microsoft Office Access® ドキュメントおよびファイル（mda – Microsoft Office Access ワークグループ、mdb – データベース）

sldx – Microsoft PowerPoint 2007 スライド

sldm – マクロのサポートを含む Microsoft PowerPoint 2007 スライド

補足資料 5：外部サービスとの相互作用のためのネットワーク設定

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

Kaspersky Endpoint Security は以下のネットワーク設定を使用して外部サービスと相互に作用します。

ネットワークの設定

アドレス	説明
`activation-v2.kaspersky.com/activationservice/activationservice.svc` プロトコル：`HTTPS` ポート：`443`	製品のアクティベーション。

アドレス	説明

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
プロトコル：`HTTPS`
ポート：`443`
	定義データベースとソフトウェアモジュールのアップデート。

`downloads.upd.kaspersky.com` プロトコル：`HTTPS` ポート：`443`	• 定義データベースとソフトウェアモジュールのアップデート。 • カスペルスキーのサーバーへのアクセスの検証。システム DNS を使用してサーバーにアクセスできない場合は、パブリック DNS を使用します。これは、確実に定義データベースをアップデートし、コンピューターのセキュリティレベルを維持するために必要です。Kaspersky Endpoint Security は一連のパブリック DNS サーバーを次の順番で使用します。 1. Google Public DNS (8.8.8.8) 2. Cloudflare DNS (1.1.1.1) 3. Alibaba Cloud DNS (223.6.6.6) 4. Quad9 DNS (9.9.9.9) 5. CleanBrowsing (185.228.168.168) 本製品は DNS サーバーを使用して TCP/UDP 接続を確立するため、本製品の要求にはドメインのアドレスと予備ユーザーのパブリック IP アドレスが含まれることがあります。この情報は、HTTPS を使用している場合に Web リソースの証明書を検証するためなどに必要になります。Kaspersky Endpoint Security がパブリック DNS サーバーを使用している場合、データは対応するサービスのプライバシーポリシーに従って処理されます。Kaspersky Endpoint Security がパブリック DNS サーバーを使用しないようにする場合は、テクニカルサポートに連絡してプライベートパッチを依頼してください。
`touch.kaspersky.com` プロトコル：`HTTP`	• 証明書の有効期間確認の信頼できる時刻の受信（TLS 接続） • ウェブ脅威対策の実行中にブラウザーで Web リソースへのアクセスが拒否されたことに関する警告

アドレス	説明
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com プロトコル：`HTTP` ポート：`80`	定義データベースとソフトウェアモジュールのアップデート。
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com プロトコル：`HTTPS` ポート：`443`	Kaspersky Security Network を使用する
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com プロトコル：`KSN` ポート：`443`、`1443`	Kaspersky Security Network を使用する
click.kaspersky.com redirect.kaspersky.com プロトコル：`HTTPS` ポート：`443`	インターフェイスからのリンクを使用。

暗号化に使用される設定

アドレス	説明
crl.kaspersky.com ocsp.kaspersky.com プロトコル：`HTTP` ポート：`80`	公開鍵基盤（PKI）。

補足資料 6：アプリケーションイベント

Kaspersky Security Center イベントログおよび Windows イベントログには、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各マルウェアのスキャンタスク、アップデートタスクおよび変更チェックタスクの完了状況、ならびに製品全体の操作に関する情報が記録されます。

Kaspersky Endpoint Security は次の種別のイベントを生成します：一般的なイベントおよび特定のイベント。特定のイベントは Kaspersky Endpoint Security for Windows によってのみ作成されます。特定のイベントは `000000cb` のように単純な識別子を持ちます。特定のイベントには次の必須設定が含まれます：

- `GNRL_EA_DESCRIPTION` はイベントの内容です。
- `GNRL_EA_ID` はイベントのサービス ID です。
- `GNRL_EA_SEVERITY` はイベントのステータスです。`1` – *情報*、 `2` – *警告*、 `3` – *機能エラー*、 `4` – *緊急*。
- `EVENT_TYPE_DISPLAY_NAME` はイベントのタイトルです。
- `TASK_DISPLAY_NAME` はイベントが発生した製品コンポーネントの名前です。

一般的なイベントは Kaspersky Endpoint Security for Windows とその他のカスペルスキー製品（Kaspersky Security for Windows Server など）によって作成されます。一般的なイベントは `GNRL_EV_VIRUS_FOUND` のような複雑な識別子を持ちます。必要な設定に加えて、一般的なイベントには詳細設定が含まれます。

イベントがサーバーに保存される期間

緊急

ライセンスの有効期間が終了しています

ステータス	!
コンポーネント	システム監査
Windows イベント ID	201
Kaspersky Security Center イベント ID	GNRL_EV_LICENSE_EXPIRATION
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ライセンスの有効期間が終了します

ステータス	!
コンポーネント	システム監査
Windows イベント ID	203
Kaspersky Security Center イベント ID	000000cb

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

定義データベースが存在しないか、破損しています

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	206
Kaspersky Security Center イベント ID	000000ce
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

定義データベースが長期間アップデートされていません

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	207
Kaspersky Security Center イベント ID	000000cf
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

コンピューター起動時の自動実行が無効です

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	209
Kaspersky Security Center イベント ID	000000d1
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アクティベーションエラー

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	229
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アクティブな脅威が検知されました。特別な駆除を開始してください

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	231
Kaspersky Security Center イベント ID	000000e7

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

KSN サーバーが使用できません

ステータス	!
コンポーネント	システム監査
Windows イベント ID	2023
Kaspersky Security Center イベント ID	000007e7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

隔離の保管領域に十分な空き容量がありません

ステータス	!
コンポーネント	システム監査
Windows イベント ID	343
Kaspersky Security Center イベント ID	00000157
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは隔離から復元されませんでした

ステータス	!
コンポーネント	システム監査
Windows イベント ID	346
Kaspersky Security Center イベント ID	0000015a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは隔離から削除されませんでした

ステータス	!
コンポーネント	システム監査
Windows イベント ID	348
Kaspersky Security Center イベント ID	0000015c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションが信頼されない証明書を持つ Web サイトとの接続を確立しました

ステータス	!
コンポーネント	システム監査
Windows イベント ID	57
Kaspersky Security Center イベント ID	00000039

Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

暗号化された接続を検証できませんでした。ドメインを除外リストに追加しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	60
Kaspersky Security Center イベント ID	0000003c
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

悪意のあるオブジェクトが検知されました（ローカルの設定に基づく）

ステータス	ⓘ
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 ふるまい検知 アンチクリプター 脆弱性攻撃ブロック マルウェアのスキャン
Windows イベント ID	302
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 外部からの共有フォルダーの暗号化が検知された場合、本製品は対象ファイルのパスを表示します。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

悪意のあるオブジェクトが検知されました（KSN）

ステータス	!
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 ふるまい検知 アンチクリプター 脆弱性攻撃ブロック マルウェアのスキャン
Windows イベント ID	302
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND_BY_KSN
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

駆除できません

ステータス	!
コンポーネント	ファイル脅威対策 メール脅威対策 ホスト侵入防止 ふるまい検知 アンチクリプター マルウェアのスキャン
Windows イベント ID	312
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_NOTCURED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

削除できません

ステータス	!
コンポーネント	ファイル脅威対策 ホスト侵入防止 ふるまい検知 アンチクリプター マルウェアのスキャン
Windows イベント ID	313
Kaspersky Security Center イベント ID	00000139
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

処理エラー

ステータス	!
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 ホスト侵入防止 AMSI 保護 マルウェアのスキャン
Windows イベント ID	317
Kaspersky Security Center イベント ID	0000013d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスが終了しました

ステータス	!
コンポーネント	ファイル脅威対策 ホスト侵入防止 ふるまい検知 マルウェアのスキャン
Windows イベント ID	452
Kaspersky Security Center イベント ID	000001c4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

プロセスを終了できません

ステータス	!
コンポーネント	ファイル脅威対策 ホスト侵入防止 ふるまい検知 マルウェアのスキャン
Windows イベント ID	453
Kaspersky Security Center イベント ID	000001c5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

危険なリンクをブロックしました

ステータス	!
コンポーネント	ウェブ脅威対策
Windows イベント ID	362
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
イベントパラメータ	• GNRL_EA_PARAM_2 はオブジェクトのパスです。 • GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Private KSN によって検知された脅威（blacklist）：true または false。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

危険なリンクを開きました

ステータス	!
コンポーネント	ウェブ脅威対策
Windows イベント ID	363
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND_AND_REPORTED
イベントパラメータ	• GNRL_EA_PARAM_2 はオブジェクトのパスです。 • GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Private KSN によって検知された脅威（blacklist）：true または false。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

以前開いた危険なリンクを検知しました

ステータス	!
コンポーネント	ウェブ脅威対策
Windows イベント ID	1201
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND_AND_PASSED
イベントパラメータ	• GNRL_EA_PARAM_2 はオブジェクトのパスです。 • GNRL_EA_PARAM_5 はカスペルスキーの分類によるオブジェクトの名前です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Private KSN によって検知された脅威（blacklist）：true または false。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスの処理がブロックされました

ステータス	!
コンポーネント	アダプティブアノマリーコントロール
Windows イベント ID	2200
Kaspersky Security Center イベント ID	GNRL_EV_ADSEC_DETECT
イベントパラメータ	• GNRL_EA_PARAM_1 はアダプティブアノマリーコントロールルールの名前です。 • GNRL_EA_PARAM_2 はヒューリスティックルールの ID です。 • GNRL_EA_PARAM_3 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_4 はソースプロセスです。 • GNRL_EA_PARAM_5 はソースオブジェクトです。 • GNRL_EA_PARAM_6 はターゲットプロセスです。 • GNRL_EA_PARAM_7 はターゲットオブジェクトです。 • GNRL_EA_PARAM_8 は検知されたオブジェクトに関する追加の情報です： ソースプロセス / オブジェクトおよびターゲットプロセス / オブジェクトのチェックサムです。 ブロックされたプロセス（verdict_type）：true または false。 ユーザーセキュリティ ID（SID）。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

キーボードが認証されませんでした

ステータス	!
コンポーネント	有害 USB 攻撃ブロック
Windows イベント ID	2051
Kaspersky Security Center イベント ID	00000803
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

AMSI リクエストはブロックされました

ステータス	!
コンポーネント	AMSI 保護
Windows イベント ID	2200
Kaspersky Security Center イベント ID	00000898
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク動作がブロックされました

ステータス	!
コンポーネント	ファイアウォール
Windows イベント ID	602
Kaspersky Security Center イベント ID	00000329
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク攻撃が検知されました

ステータス	⚠
コンポーネント	ネットワーク脅威対策
Windows イベント ID	651
Kaspersky Security Center イベント ID	GNRL_EV_ATTACK_DETECTED
イベントパラメータ	• GNRL_EA_PARAM_1 は攻撃の名前です。 • GNRL_EA_PARAM_2 はプロトコルです。 • GNRL_EA_PARAM_3 はネットワーク攻撃の攻撃元として動作しているコンピューターの IP アドレスです。IP アドレスはホストのバイト順で示されます。たとえば、172.16.0.201 は 2886729929 となります。 • GNRL_EA_PARAM_4 はポート番号です。 • GNRL_EA_PARAM_5 は IPv6 アドレス（例：12B012B012B012B012B012B012B012B0）です。 • GNRL_EA_PARAM_6 はネットワーク攻撃の対象となったコンピューターの IP アドレスです。IP アドレスはホストのバイト順で示されます。たとえば、172.16.0.201 は 2886729929 となります。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動が禁止されました

ステータス	⚠
コンポーネント	アプリケーションコントロール
Windows イベント ID	702
Kaspersky Security Center イベント ID	GNRL_EV_APPLICATION_LAUNCH_DENIED
イベントパラメータ	• GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。 • GNRL_EA_PARAM_4 アプリケーションのカテゴリ ID です。 • GNRL_EA_PARAM_5 はアプリケーションのデジタル署名に関する情報です。 • GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。 • GNRL_EA_PARAM_7 は実行ファイルのパスです。 • GNRL_EA_PARAM_8 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Endpoint Security の起動前にブロック対象のプロセスが開始されました

ステータス	⚠
コンポーネント	アプリケーションコントロール
Windows イベント ID	710
Kaspersky Security Center イベント ID	000002c6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アクセスが拒否されました（ローカルの設定に基づく）

ステータス	⚠
コンポーネント	ウェブコントロール

Windows イベント ID	752
Kaspersky Security Center イベント ID	GNRL_EV_WEB_URL_BLOCKED
イベントパラメータ	• GNRL_EA_PARAM_1 は URL です。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 ウェブコントロールルールの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アクセスが拒否されました（KSN）

ステータス	!
コンポーネント	ウェブコントロール
Windows イベント ID	752
Kaspersky Security Center イベント ID	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
イベントパラメータ	• GNRL_EA_PARAM_1 は URL です。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 ウェブコントロールルールの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスを使用した操作がブロックされました

ステータス	!
コンポーネント	デバイスコントロール
Windows イベント ID	802
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
イベントパラメータ	• GNRL_EA_PARAM_1 はハードウェアの ID です（HWID）。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク接続がブロックされました

ステータス	!
コンポーネント	デバイスコントロール
Windows イベント ID	809
Kaspersky Security Center イベント ID	00000329
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

コンポーネントのアップデートエラー

ステータス	!
コンポーネント	アップデート
Windows イベント ID	1011
Kaspersky Security Center イベント ID	000003f3

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

コンポーネントのアップデートの配信エラー

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1012
Kaspersky Security Center イベント ID	000003f4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

ローカルのアップデートエラー

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1014
Kaspersky Security Center イベント ID	000003f6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

ネットワークアップデートエラー

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1015
Kaspersky Security Center イベント ID	000003f7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

2 つのタスクを同時に開始できません

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1017
Kaspersky Security Center イベント ID	000003f9
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの定義データベースおよびモジュールの検証中にエラーが発生しました

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1018
Kaspersky Security Center イベント ID	000003fa

Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Security Center との通信中にエラーが発生しました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1019
Kaspersky Security Center イベント ID	000003fb
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

アップデートされていないコンポーネントがあります

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1021
Kaspersky Security Center イベント ID	000003fd
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

アップデートは正常に完了しましたが、アップデートの配信に失敗しました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1023
Kaspersky Security Center イベント ID	000003ff
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	-

内部タスクエラー

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	101
Kaspersky Security Center イベント ID	00000065
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	-

パッチをインストールできませんでした

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2153
Kaspersky Security Center イベント ID	00000869

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

パッチをロールバックできませんでした

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	2156
Kaspersky Security Center イベント ID	0000086c
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	904
Kaspersky Security Center イベント ID	00000388
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルの暗号化 / 復号化中にエラーが発生しました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	912
Kaspersky Security Center イベント ID	GNRL_EV_ENCRYPTION_ERROR
イベントパラメータ	• GNRL_EA_PARAM_1 はファイルのパスです。 • GNRL_EA_PARAM_2 はエラーの原因です。 • GNRL_EA_PARAM_3 はデバイスの種別です。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルへのアクセスがブロックされました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	940
Kaspersky Security Center イベント ID	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
イベントパラメータ	• GNRL_EA_PARAM_1 はターゲットオブジェクトです。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 は、ファイルへのアクセスを取得しようとしているアプリケーションの実行ファイルの名前です（chrome.exe など）。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ポータブルモードの有効化中にエラーが発生しました

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	951
Kaspersky Security Center イベント ID	000003b7
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ポータブルモードの無効化中にエラーが発生しました

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	953
Kaspersky Security Center イベント ID	000003b9
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

暗号化されたパッケージの作成でエラーが発生しました

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	931
Kaspersky Security Center イベント ID	000003a3
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

デバイスの暗号化 / 復号化中にエラーが発生しました

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	1305
Kaspersky Security Center イベント ID	00000519
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

暗号化モジュールを読み込めません

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	1311
Kaspersky Security Center イベント ID	0000051f
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

認証エージェントアカウントの管理タスクでエラーが発生しました

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	1340
Kaspersky Security Center イベント ID	0000053c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ポリシーを適用できません

ステータス	!
コンポーネント	システム監査
Windows イベント ID	1312
Kaspersky Security Center イベント ID	00000520
Windows イベントログ（既定）	-
Kaspersky Security Center イベントログ（既定）	✓

FDE をアップグレードできませんでした

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	1342
Kaspersky Security Center イベント ID	0000053e
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

FDE のアップグレードをロールバックできませんでした（詳細については、Kaspersky Endpoint Security for Windows のオンラインヘルプを参照してください）

ステータス	!
コンポーネント	データ暗号化
Windows イベント ID	1344
Kaspersky Security Center イベント ID	00000540
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Anti Targeted Attack Platform サーバーが使用できません

ステータス	!
コンポーネント	Endpoint Sensor
Windows イベント ID	2100
Kaspersky Security Center イベント ID	00000834
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトを削除できませんでした

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2252
Kaspersky Security Center イベント ID	000008cc
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが隔離されませんでした（Sandbox）

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2603
Kaspersky Security Center イベント ID	00000a2b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

内部エラーが発生しました

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2607
Kaspersky Security Center イベント ID	00000a2f
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox サーバー証明書が無効です

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2613
Kaspersky Security Center イベント ID	00000a35
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox ノードが使用できません

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2614
Kaspersky Security Center イベント ID	00000a36
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox のオブジェクトを処理できませんでした

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2617
Kaspersky Security Center イベント ID	00000a39
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox の負荷が最大値を超えました

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2618
Kaspersky Security Center イベント ID	00000a3a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

IOC が見つかりました

ステータス	!
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2651
Kaspersky Security Center イベント ID	00000a5b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox のライセンスが確認できませんでした

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2620
Kaspersky Security Center イベント ID	00000a3c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ユーザーによる Sandbox へのスキャンタスクの送信に失敗しました

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2623
Kaspersky Security Center イベント ID	00000a3e
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Sandbox タスクの作成中にエラーが発生しました

ステータス	!
コンポーネント	Sandbox
Windows イベント ID	2621
Kaspersky Security Center イベント ID	00000a3d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトの開始がブロックされました

ステータス	!
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2553
Kaspersky Security Center イベント ID	000009f9
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスの開始がブロックされました

ステータス	!
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2551
Kaspersky Security Center イベント ID	000009f7
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

スクリプトの実行がブロックされました

ステータス	!
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2559
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが隔離されませんでした（Endpoint Detection and Response）

ステータス	!
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2556
Kaspersky Security Center イベント ID	000009fc
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスの開始はブロックされていません

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2561
Kaspersky Security Center イベント ID	00000a01
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトはブロックされていません

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2562
Kaspersky Security Center イベント ID	00000a02
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

スクリプトの実行はブロックされていません

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2563
Kaspersky Security Center イベント ID	00000a03
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションコンポーネントの変更中にエラーが発生しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	1401
Kaspersky Security Center イベント ID	00000579
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

システムにブルートフォース攻撃の可能性を示すパターンがあります

ステータス	ⓘ
コンポーネント	Windows イベントログ監視
Windows イベント ID	2800
Kaspersky Security Center イベント ID	00000af0
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Windows イベントログの悪用の可能性を示すパターンがあります

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2801
Kaspersky Security Center イベント ID	00000af1
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

新しくインストールしたサービスに通常と異なる活動が検出されました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2802
Kaspersky Security Center イベント ID	00000af2
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

明示的な資格情報を使用した通常と異なるログオンが検出されました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2803
Kaspersky Security Center イベント ID	00000af3
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2804
Kaspersky Security Center イベント ID	00000af4
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

特権付きの組み込み管理者グループ内で疑わしい変更を検知しました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2805
Kaspersky Security Center イベント ID	00000af5
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワークログオンセッション中に通常と異なる活動を検知しました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2806
Kaspersky Security Center イベント ID	00000af6
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Windows イベントログ監視ルールが適用されました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2807
Kaspersky Security Center イベント ID	00000af7
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

通常と異なるイベントが頻発しています。イベントの集計を開始しました

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2808
Kaspersky Security Center イベント ID	00000af8
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

集計期間の通常と異なるイベントのレポート

ステータス	!
コンポーネント	Windows イベントログ監視
Windows イベント ID	2809
Kaspersky Security Center イベント ID	00000af9
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert サーバーへの接続エラー

ステータス	!
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2850
Kaspersky Security Center イベント ID	00000b22
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert サーバーの証明書が無効です

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2851
Kaspersky Security Center イベント ID	00000b23
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert サーバーのエージェントの証明書が無効です

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2852
Kaspersky Security Center イベント ID	00000b24
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert 応答サーバーへの接続中にエラーが発生しました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2858
Kaspersky Security Center イベント ID	00000b22
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert 応答サーバーの証明書が無効です

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2859
Kaspersky Security Center イベント ID	00000b23
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert 応答サーバーのエージェントの証明書が無効です

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2860
Kaspersky Security Center イベント ID	00000b24
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expertテレメトリ収集サーバーの接続エラー

ステータス	⊗
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2854
Kaspersky Security Center イベント ID	00000b22
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expertテレメトリ収集サーバーの証明書が無効です

ステータス	⊗
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2855
Kaspersky Security Center イベント ID	00000b23
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expertテレメトリ収集サーバーのエージェントの証明書が無効です

ステータス	⊗
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2856
Kaspersky Security Center イベント ID	00000b24
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

NDR サーバーへの接続中にエラーが発生しました

ステータス	⊗
コンポーネント	Network Detection and Response (KATA)
Windows イベント ID	3080
Kaspersky Security Center イベント ID	00000c08
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

NDR サーバーの証明書が無効です

ステータス	⊗
コンポーネント	Network Detection and Response (KATA)
Windows イベント ID	3081
Kaspersky Security Center イベント ID	00000c09
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

NDR サーバーのエージェントの証明書が無効です

ステータス	!
コンポーネント	Network Detection and Response (KATA)
Windows イベント ID	3082
Kaspersky Security Center イベント ID	00000c0a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

デバイスは信頼済みでない管理サーバーに接続されています。管理者にお問い合わせください。

ステータス	!
コンポーネント	管理サーバーの接続の保護
Windows イベント ID	3301
Kaspersky Security Center イベント ID	00000ce5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイルまたはフォルダーの変更が検知されました

ステータス	i / ⚠ / !
コンポーネント	システム変更監視
Windows イベント ID	2950
Kaspersky Security Center イベント ID	00000b86
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

オブジェクトの変更が多すぎます。イベントの集計を開始しました

ステータス	i / ⚠ / !
コンポーネント	システム変更監視
Windows イベント ID	2955
Kaspersky Security Center イベント ID	00000b8b
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

集計期間のオブジェクト変更のレポート

ステータス	i / ⚠ / !
コンポーネント	システム変更監視
Windows イベント ID	2956
Kaspersky Security Center イベント ID	00000b8c

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

監視範囲に正しくないオブジェクトが含まれています

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2953
Kaspersky Security Center イベント ID	00000b89
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

レジストリの変更が検知されました

ステータス	ⓘ / ⚠ / ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2951
Kaspersky Security Center イベント ID	00000b87
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

デバイスの接続または接続解除が検出されました

ステータス	ⓘ / ⚠ / ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2952
Kaspersky Security Center イベント ID	00000b88
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

監視範囲に正しくないオブジェクトが含まれています

ステータス	ⓘ / ⚠ / ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2903

Kaspersky Security Center イベント ID	00000b89
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

オブジェクトに対する制限された操作の試行回数が多すぎます。イベントの集計を開始しました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2963
Kaspersky Security Center イベント ID	00000b93
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

監視範囲のファイルに対する操作がブロックされました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2959
Kaspersky Security Center イベント ID	00000b8f
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

レジストリ変更がブロックされました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2960
Kaspersky Security Center イベント ID	00000b90
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

処理エラー

ステータス	ⓘ
コンポーネント	システム変更監視

Windows イベント ID	2954
Kaspersky Security Center イベント ID	00000b8a
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

システム変更監視：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	システム変更監視
Windows イベント ID	2964
Kaspersky Security Center イベント ID	00000b94
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションコントロール：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	アプリケーションコントロール
Windows イベント ID	711
Kaspersky Security Center イベント ID	000002c7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスコントロール：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	デバイスコントロール
Windows イベント ID	810
Kaspersky Security Center イベント ID	0000032a
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ウェブコントロール：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	ウェブコントロール
Windows イベント ID	757
Kaspersky Security Center イベント ID	000002f5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アダプティブアノマリーコントロール：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	アダプティブアノマリーコントロール
Windows イベント ID	504
Kaspersky Security Center イベント ID	000001f8
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Windows イベントログ監視：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています

ステータス	⚠
コンポーネント	Windows イベントログ監視
Windows イベント ID	2810
Kaspersky Security Center イベント ID	00000afa
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

6 時間以上 Integration Server に接続できませんでした。Integration Server の状態とネットワーク設定を確認してください。

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3103
Kaspersky Security Center イベント ID	00000c1f
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

SVM が使用できません

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3151
Kaspersky Security Center イベント ID	00000c4f
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

悪意のあるオブジェクトが検知されました。仮想マシンテンプレートで特別な駆除を開始してください。

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3182
Kaspersky Security Center イベント ID	00000c6e
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

非推奨プロトコル経由で確立されたネットワーク接続がブロックされました

ステータス	⚠
コンポーネント	プロテクション
Windows イベント ID	75
Kaspersky Security Center イベント ID	0000004b
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

KUMA サーバー接続エラー

ステータス	⚠
コンポーネント	KUMA 連携
Windows イベント ID	2854
Kaspersky Security Center イベント ID	00000b26
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

KUMA サーバーの証明書が無効です

ステータス	⚠
コンポーネント	KUMA 連携
Windows イベント ID	2855
Kaspersky Security Center イベント ID	00000b27
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

KUMA サーバーのエージェントの証明書が無効です

ステータス	⚠
コンポーネント	KUMA 連携
Windows イベント ID	2856
Kaspersky Security Center イベント ID	00000b28
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

機能エラー

タスクを実行できません

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	212
Kaspersky Security Center イベント ID	000000d4

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

タスク設定が無効です。設定は反映されていません

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	707
Kaspersky Security Center イベント ID	000002c3
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

警告

前回のセッション中に製品がクラッシュしました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	237
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ライセンスの有効期間がまもなく終了します

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	204
Kaspersky Security Center イベント ID	000000cc
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

定義データベースがアップデートされていません

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	208
Kaspersky Security Center イベント ID	000000d0
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アップデートの自動開始が無効です

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	210
Kaspersky Security Center イベント ID	000000d2
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

セルフディフェンスが無効です

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	211
Kaspersky Security Center イベント ID	000000d3
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

保護機能が無効です

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	214
Kaspersky Security Center イベント ID	000000d6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

コンピューターがセーフモードで動作しています

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	215
Kaspersky Security Center イベント ID	000000d7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

未処理のファイルがあります

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	216
Kaspersky Security Center イベント ID	000000d8
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

グループポリシーが適用されました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	219
Kaspersky Security Center イベント ID	000000db
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

タスクが停止しました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	222
Kaspersky Security Center イベント ID	000000de
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アップデートを完了するには、アプリケーションを終了して再実行してください

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	224
Kaspersky Security Center イベント ID	0000057b
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

コンピューターの再起動が必要です

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	225
Kaspersky Security Center イベント ID	000000e1
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

このライセンスは、インストールされていないコンポーネントの使用を許可します

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	226
Kaspersky Security Center イベント ID	000000e2
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

特別な駆除が開始されました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	232
Kaspersky Security Center イベント ID	000000e8
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

特別な駆除が完了しました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	233
Kaspersky Security Center イベント ID	000000e9
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

予備のライセンスが正しくありません

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	230
Kaspersky Security Center イベント ID	000000e6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

定額制サービスの有効期間がまもなく終了します

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	240
Kaspersky Security Center イベント ID	000000f0
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ブロックしました

ステータス	⚠
コンポーネント	ふるまい検知 アンチクリプター 脆弱性攻撃ブロック ウェブ脅威対策
Windows イベント ID	331

Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_BLOCKED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 外部からの共有フォルダーの暗号化が検知された場合、本製品は対象ファイルのパスを表示します。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

オペレーティングシステムの設定で、Wi-Fi ネットワークへのアクセスの制御が許可されていません。

ステータス	⚠
コンポーネント	デバイスコントロール
Windows イベント ID	249
Kaspersky Security Center イベント ID	000000f9
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

バックアップからオブジェクトが復元されませんでした

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	336
Kaspersky Security Center イベント ID	00000150
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

疑わしいネットワーク動作を検知しました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	2001
Kaspersky Security Center イベント ID	000007d1
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

暗号化された接続が終了しました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	250
Kaspersky Security Center イベント ID	000007d3
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

KSN への参加が無効になっています

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	2021
Kaspersky Security Center イベント ID	000007e5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

OS の一部の機能の処理が無効になっています

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	245
Kaspersky Security Center イベント ID	000000f5
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

隔離の保管領域の容量がまもなく上限に達します

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	344
Kaspersky Security Center イベント ID	00000158
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク接続がブロックされました

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	809
Kaspersky Security Center イベント ID	00000abe
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

バックアップを作成できません

ステータス	⚠
コンポーネント	ファイル脅威対策 メール脅威対策 ホスト侵入防止 AMSI 保護 マルウェアのスキャン
Windows イベント ID	314
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_REPORTED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ステータス	⚠
コンポーネント	ファイル脅威対策 ふるまい検知 アンチクリプター ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	310
Kaspersky Security Center イベント ID	00000136
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが暗号化されました

ステータス	⚠
コンポーネント	ホスト侵入防止
Windows イベント ID	320
Kaspersky Security Center イベント ID	00000140
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

オブジェクトが破損しています

ステータス	⚠
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	321
Kaspersky Security Center イベント ID	00000141
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェアを検知しました（ローカルの設定に基づく）

ステータス	⚠
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 ホスト侵入防止 AMSI 保護 ふるまい検知 アンチクリプター アンチクリプター マルウェアのスキャン
Windows イベント ID	303
Kaspersky Security Center イベント ID	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェアを検知しました（KSN）

ステータス	⚠
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 ホスト侵入防止 AMSI 保護 ふるまい検知 アンチクリプター アンチクリプター マルウェアのスキャン
Windows イベント ID	303

Kaspersky Security Center イベント ID	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが削除されました

ステータス	⚠
コンポーネント	ファイル脅威対策 メール脅威対策 ホスト侵入防止 脆弱性攻撃ブロック ふるまい検知 アンチクリプター マルウェアのスキャン
Windows イベント ID	307
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_DELETED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが駆除されました

ステータス	⚠
コンポーネント	ファイル脅威対策 メール脅威対策 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	306

Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_CURED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが再起動時に駆除されます

ステータス	⚠
コンポーネント	ホスト侵入防止 ファイル脅威対策 マルウェアのスキャン
Windows イベント ID	324
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

オブジェクトが再起動時に削除されます

ステータス	⚠
コンポーネント	ふるまい検知 アンチクリプター 脆弱性攻撃ブロック ホスト侵入防止 ファイル脅威対策 マルウェアのスキャン
Windows イベント ID	323
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

設定によりオブジェクトが削除されました

ステータス	⚠
コンポーネント	メール脅威対策
Windows イベント ID	342
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ロールバックが完了しました

ステータス	⚠
コンポーネント	ファイル脅威対策 ふるまい検知 アンチクリプター 脆弱性攻撃ブロック マルウェアのスキャン
Windows イベント ID	455
Kaspersky Security Center イベント ID	000001c7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトのダウンロードがブロックされました

ステータス	⚠
コンポーネント	ウェブ脅威対策
Windows イベント ID	341
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_BLOCKED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

キーボード認証エラー

ステータス	⚠
コンポーネント	有害 USB 攻撃ブロック
Windows イベント ID	2052
Kaspersky Security Center イベント ID	00000804
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトのスキャン結果はサードパーティ製品に送信されました

ステータス	⚠
コンポーネント	AMSI 保護
Windows イベント ID	1512

Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_REPORTED
イベントパラメータ	• GNRL_EA_PARAM_1 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_5 は EICAR-Test-File など、カスペルスキーの分類に基づく脅威の種別です。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_8 は脅威の種別です（type）。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 Kaspersky Private Security Network によって検知された脅威（blacklist）：true または false。 EDR のバージョン。 EDR の脅威識別子。 オブジェクトの MD5 ハッシュ。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

タスク設定が正常に適用されました

ステータス	⚠
コンポーネント	アプリケーションコントロール
Windows イベント ID	708
Kaspersky Security Center イベント ID	000002c4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

望ましくないコンテンツに関する警告（ローカルの設定に基づく）

ステータス	⚠
コンポーネント	ウェブコントロール
Windows イベント ID	708
Kaspersky Security Center イベント ID	GNRL_EV_WEB_URL_WARNING
イベントパラメータ	• GNRL_EA_PARAM_1 は URL です。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 ウェブコントロールルールの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

望ましくないコンテンツに関する警告（KSN）

ステータス	⚠
コンポーネント	ウェブコントロール
Windows イベント ID	708
Kaspersky Security Center イベント ID	GNRL_EV_WEB_URL_WARNING
イベントパラメータ	• GNRL_EA_PARAM_1 は URL です。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 ウェブコントロールルールの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

望ましくないコンテンツの警告後にアクセスが試行されました

ステータス	⚠
コンポーネント	ウェブコントロール
Windows イベント ID	754
Kaspersky Security Center イベント ID	000002f2
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

デバイスへの一時的なアクセスが有効になりました

ステータス	⚠
コンポーネント	デバイスコントロール
Windows イベント ID	803
Kaspersky Security Center イベント ID	000002f2
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ユーザーによりキャンセルされました

ステータス	⚠
コンポーネント	アップデート
Windows イベント ID	1016
Kaspersky Security Center イベント ID	000003f8
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ユーザーが暗号化ポリシーを拒否しました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	1306
Kaspersky Security Center イベント ID	0000051a
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイル暗号化 / 復号化ルールの適用が中断されました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	903
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルの暗号化 / 復号化が中断されました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	914
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスの暗号化 / 復号化が中断されました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	1303
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

WinRE イメージへの Kaspersky Disk Encryption ドライバーのインストール、またはイメージ内のドライバーのアップグレードが失敗しました

ステータス	⚠
コンポーネント	データ暗号化
Windows イベント ID	1345
Kaspersky Security Center イベント ID	00000541
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

モジュールの署名をチェックできませんでした

ステータス	⚠
コンポーネント	システム変更チェック
Windows イベント ID	2002
Kaspersky Security Center イベント ID	000007d2
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動がブロックされました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2105
Kaspersky Security Center イベント ID	00000839
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

文書を開く操作がブロックされました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2106
Kaspersky Security Center イベント ID	0000083a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスが Kaspersky Anti Targeted Attack Platform サーバーの管理者によって終了されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2112
Kaspersky Security Center イベント ID	00000840
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションは Kaspersky Anti Targeted Attack Platform サーバーの管理者によって終了されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2113
Kaspersky Security Center イベント ID	00000841
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルまたはストリームは Kaspersky Anti Targeted Attack Platform サーバーの管理者によって削除されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2111
Kaspersky Security Center イベント ID	0000083f
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバーの隔離から復元されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2110
Kaspersky Security Center イベント ID	0000083e
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバーに隔離されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2109
Kaspersky Security Center イベント ID	0000083d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

すべてのサードパーティ製品のネットワーク動作がブロックされました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2107
Kaspersky Security Center イベント ID	0000083b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

すべてのサードパーティ製品のネットワーク動作のブロックが解除されました

ステータス	⚠
コンポーネント	Endpoint Sensor
Windows イベント ID	2108
Kaspersky Security Center イベント ID	0000083c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは再起動後に削除されます（Sandbox）

ステータス	⚠
コンポーネント	Sandbox
Windows イベント ID	2605
Kaspersky Security Center イベント ID	00000a2d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

スキャンタスクのサイズの合計が上限を超えています

ステータス	⚠
コンポーネント	Sandbox
Windows イベント ID	2612
Kaspersky Security Center イベント ID	00000a34
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトの開始が許可されました。イベントが記録されました

ステータス	⚠
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2553
Kaspersky Security Center イベント ID	000009fa
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

プロセスの開始が許可されました。イベントが記録されました

ステータス	⚠
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2554
Kaspersky Security Center イベント ID	000009f8
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは再起動後に削除されます（Endpoint Detection and Response）

ステータス	⚠
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2558
Kaspersky Security Center イベント ID	000009fe
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク分離

ステータス	⚠
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2700
Kaspersky Security Center イベント ID	00000a8c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク分離の終了

ステータス	⚠
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2701
Kaspersky Security Center イベント ID	00000a8d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

タスクを完了するには、再起動する必要があります

ステータス	⚠
コンポーネント	システム監査
Windows イベント ID	225
Kaspersky Security Center イベント ID	0000057b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動ブロックに関するメッセージが管理者に送信されました

ステータス	⚠
コンポーネント	アプリケーションコントロール
Windows イベント ID	503
Kaspersky Security Center イベント ID	GNRL_EV_AC_USER_REQUEST
イベントパラメータ	• GNRL_EA_DESCRIPTION はユーザーへのメッセージです。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。 • GNRL_EA_PARAM_7 は実行ファイルのパスです。 • GNRL_EA_PARAM_8 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスへのアクセスブロックに関するメッセージが管理者に送信されました

ステータス	⚠
コンポーネント	デバイスコントロール
Windows イベント ID	804
Kaspersky Security Center イベント ID	GNRL_EV_DC_USER_REQUEST
イベントパラメータ	• c_er_descr はユーザーへのメッセージです。 • GNRL_EA_PARAM_1 はハードウェアの ID です（HWID）。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Web ページへのアクセスブロックに関するメッセージが管理者に送信されました

ステータス	⚠
コンポーネント	ウェブコントロール
Windows イベント ID	755
Kaspersky Security Center イベント ID	GNRL_EV_WC_USER_REQUEST
イベントパラメータ	• GNRL_EA_DESCRIPTION はユーザーへのメッセージです。 • GNRL_EA_PARAM_1 は URL です。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスの接続がブロックされました

ステータス	⚠
コンポーネント	デバイスコントロール
Windows イベント ID	807
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
イベントパラメータ	• GNRL_EA_PARAM_1 はハードウェアの ID です（HWID）。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの動作ブロックに関するメッセージが管理者に送信されました

ステータス	⚠
コンポーネント	ファイル変更監視
Windows イベント ID	2901
Kaspersky Security Center イベント ID	00000b55
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ステータス	⚠
コンポーネント	ファイル変更監視
Windows イベント ID	2900
Kaspersky Security Center イベント ID	00000b54
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ステータス	⚠
コンポーネント	アダプティブアノマリーコントロール
Windows イベント ID	503
Kaspersky Security Center イベント ID	GNRL_EV_ADSEC_USER_REQUEST
イベントパラメータ	• GNRL_EA_DESCRIPTION はユーザーへのメッセージです。 • GNRL_EA_PARAM_1 はアダプティブアノマリーコントロールルールの名前です。 • GNRL_EA_PARAM_2 はヒューリスティックルールの ID です。 • GNRL_EA_PARAM_3 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_4 はソースプロセスです。 • GNRL_EA_PARAM_5 はソースオブジェクトです。 • GNRL_EA_PARAM_6 はターゲットプロセスです。 • GNRL_EA_PARAM_7 はターゲットオブジェクトです。 • GNRL_EA_PARAM_8 は検知されたオブジェクトに関する追加の情報です： ソースプロセス / オブジェクトおよびターゲットプロセス / オブジェクトのハッシュです。 ブロックされたプロセス（verdict_type）：true または false。 ユーザーセキュリティ ID（SID）。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

クラウドサービスのクライアントアプリケーションの起動がブロックされました

ステータス	⚠
コンポーネント	Cloud Discovery
Windows イベント ID	2212
Kaspersky Security Center イベント ID	000008a4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

クラウドサービスへのアクセスがブロックされました

ステータス	⚠
コンポーネント	Cloud Discovery
Windows イベント ID	2213
Kaspersky Security Center イベント ID	000008a5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイルまたはフォルダーの変更が検知されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2950
Kaspersky Security Center イベント ID	00000b86
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

オブジェクトの変更が多すぎます。イベントの集計を開始しました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2955
Kaspersky Security Center イベント ID	00000b8b
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

集計期間のオブジェクト変更のレポート

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2956
Kaspersky Security Center イベント ID	00000b8c
Windows イベントログ（既定）	–

Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

レジストリの変更が検知されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2951
Kaspersky Security Center イベント ID	00000b87
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

デバイスの接続または接続解除が検出されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2952
Kaspersky Security Center イベント ID	00000b88
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

監視範囲に正しくないオブジェクトが含まれています

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2903
Kaspersky Security Center イベント ID	00000b89
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

テストモードで禁止された操作が許可されました

ステータス	⚠
コンポーネント	システム変更監視
Windows イベント ID	2961
Kaspersky Security Center イベント ID	00000b91
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

30 分以上 Integration Server に接続できませんでした。Integration Server の状態とネットワーク設定を確認してください。

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3102
Kaspersky Security Center イベント ID	00000c1e
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Integration Server に接続できませんでした。Integration Server の状態とネットワーク設定を確認してください。

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3101
Kaspersky Security Center イベント ID	00000c1d
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

仮想マシンテンプレートをアップデートする必要があります

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3181
Kaspersky Security Center イベント ID	00000c6d
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Standard ライセンスの有効期間が終了しました。本製品は Enterprise ライセンスで動作しています

ステータス	⚠
コンポーネント	Light Agent
Windows イベント ID	3171
Kaspersky Security Center イベント ID	00000c64
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

情報メッセージ

製品が起動しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	235
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

製品が停止しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	236
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

セルフディフェンスは保護されたリソースへのアクセスを制限しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	213
Kaspersky Security Center イベント ID	000000d5
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

レポートが消去されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	217
Kaspersky Security Center イベント ID	000000d9
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

グループポリシーが無効化されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	220

Kaspersky Security Center イベント ID	000000dc
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アプリケーションの設定が変更されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	218
Kaspersky Security Center イベント ID	000000da
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

タスクを開始しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	221
Kaspersky Security Center イベント ID	000000dd
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

タスクが完了しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	223
Kaspersky Security Center イベント ID	000000df
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ライセンスによって定義されているすべてのコンポーネントがインストールされ、通常モードで動作しています

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	227
Kaspersky Security Center イベント ID	000000e3
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

定額制サービスの設定が変更されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	238

Kaspersky Security Center イベント ID	000000ee
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

定額制サービスが更新されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	239
Kaspersky Security Center イベント ID	000000ef
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

バックアップからオブジェクトが復元されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	335
Kaspersky Security Center イベント ID	0000014f
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ユーザー名とパスワードが入力されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	2000
Kaspersky Security Center イベント ID	000007d0
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

KSN への参加が有効になっています

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	2020
Kaspersky Security Center イベント ID	000007e4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

KSN サーバーが使用可能です

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	2022

Kaspersky Security Center イベント ID	000007e6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

本製品は、関連する法律に従って動作およびデータの処理を行い、適切なインフラを使用します

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	2024
Kaspersky Security Center イベント ID	000007e8
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

隔離からオブジェクトが復元されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	345
Kaspersky Security Center イベント ID	00000159
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは隔離から削除されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	347
Kaspersky Security Center イベント ID	0000015b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトのバックアップが作成されました

ステータス	ⓘ
コンポーネント	ファイル脅威対策 メール脅威対策 ふるまい検知 アンチクリプター ホスト侵入防止 Sandbox マルウェアのスキャン
Windows イベント ID	308
Kaspersky Security Center イベント ID	00000134
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

以前駆除したファイルのコピーで上書きしました

ステータス	ⓘ
コンポーネント	ファイル脅威対策 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	327
Kaspersky Security Center イベント ID	00000147
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

パスワードで保護されているアーカイブが検知されました

ステータス	ⓘ
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	322
Kaspersky Security Center イベント ID	GNRL_EV_PASSWD_ARCHIVE_FOUND
イベントパラメータ	• GNRL_EA_PARAM_2 はオブジェクトの名前です。 • GNRL_EA_PARAM_3 はオブジェクトの作成日です（省略可能）。 • GNRL_EA_PARAM_7 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_9 は検知されたオブジェクトに関する追加の情報です： 製品コンポーネント（engine）。 脅威検知技術（method）。 プライベート KSN により検知された脅威（denylist）：true または false。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

検知したオブジェクトに関する情報

ステータス	ⓘ
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	332
Kaspersky Security Center イベント ID	0000014c
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトは Kaspersky Private Security Network の許可リストに登録されています

ステータス	ⓘ
コンポーネント	ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 ホスト侵入防止 マルウェアのスキャン
Windows イベント ID	340

Kaspersky Security Center イベント ID	00000154
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトの名前が変更されました

ステータス	ⓘ
コンポーネント	メール脅威対策 脆弱性攻撃ブロック ふるまい検知 アンチクリプター マルウェアのスキャン
Windows イベント ID	329
Kaspersky Security Center イベント ID	00000149
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが処理されました

ステータス	ⓘ
コンポーネント	ホスト侵入防止 ファイル脅威対策 ウェブ脅威対策 メール脅威対策 マルウェアのスキャン
Windows イベント ID	301
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

オブジェクトがスキップされました

ステータス	ⓘ
コンポーネント	ホスト侵入防止 ファイル脅威対策 AMSI 保護 マルウェアのスキャン
Windows イベント ID	315
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

アーカイブが検知されました

ステータス	ⓘ
コンポーネント	ホスト侵入防止 ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 マルウェアのスキャン
Windows イベント ID	318

Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

圧縮オブジェクトが検知されました

ステータス	ⓘ
コンポーネント	ホスト侵入防止 ファイル脅威対策 ウェブ脅威対策 メール脅威対策 AMSI 保護 マルウェアのスキャン
Windows イベント ID	319
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

リンクを処理しました

ステータス	ⓘ
コンポーネント	ウェブ脅威対策
Windows イベント ID	361
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

アプリケーションの起動が許可されました

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
Windows イベント ID	701
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

アップデート元が選択されています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1001
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

プロキシサーバーが選択されています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1002
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

リンクは Kaspersky Private Security Network の許可リストに登録されています

ステータス	ⓘ
コンポーネント	ウェブ脅威対策
Windows イベント ID	370
Kaspersky Security Center イベント ID	00000172
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションが「許可」グループに割り当てられました

ステータス	ⓘ
コンポーネント	ホスト侵入防止
Windows イベント ID	401
Kaspersky Security Center イベント ID	00000191
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションが「制限付き」グループに割り当てられました

ステータス	ⓘ
コンポーネント	ホスト侵入防止
Windows イベント ID	402
Kaspersky Security Center イベント ID	00000192
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ホスト侵入防止が適用されました

ステータス	ⓘ
コンポーネント	ホスト侵入防止
Windows イベント ID	403
Kaspersky Security Center イベント ID	00000193
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイルが復元されました

ステータス	ⓘ
コンポーネント	ふるまい検知 アンチクリプター 脆弱性攻撃ブロック ホスト侵入防止
Windows イベント ID	457
Kaspersky Security Center イベント ID	000001c9
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

レジストリ値が復元されました

ステータス	ⓘ
コンポーネント	ふるまい検知 脆弱性攻撃ブロック
Windows イベント ID	458
Kaspersky Security Center イベント ID	000001ca
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

レジストリ値が削除されました

ステータス	ⓘ
コンポーネント	ふるまい検知 脆弱性攻撃ブロック
Windows イベント ID	459
Kaspersky Security Center イベント ID	000001cb
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

プロセスの処理がスキップされました

ステータス	ⓘ
コンポーネント	アダプティブアノマリーコントロール
Windows イベント ID	2201
Kaspersky Security Center イベント ID	GNRL_EV_ADSEC_DETECT
イベントパラメータ	• GNRL_EA_PARAM_1 はアダプティブアノマリーコントロールルールの名前です。 • GNRL_EA_PARAM_2 はヒューリスティックルールの ID です。 • GNRL_EA_PARAM_3 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_4 はソースプロセスです。 • GNRL_EA_PARAM_5 はソースオブジェクトです。 • GNRL_EA_PARAM_6 はターゲットプロセスです。 • GNRL_EA_PARAM_7 はターゲットオブジェクトです。 • GNRL_EA_PARAM_8 は検知されたオブジェクトに関する追加の情報です： ソースプロセス / オブジェクトおよびターゲットプロセス / オブジェクトのハッシュです。 ブロックされたプロセス（verdict_type）：true または false。 ユーザーセキュリティ ID（SID）。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

キーボードが認証されました

ステータス	ⓘ
コンポーネント	有害 USB 攻撃ブロック
Windows イベント ID	2050
Kaspersky Security Center イベント ID	00000802
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク動作が許可されました

ステータス	ⓘ
コンポーネント	ファイアウォール
Windows イベント ID	601
Kaspersky Security Center イベント ID	00000259
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アプリケーションの起動がテストモードでブロックされています

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
Windows イベント ID	703
Kaspersky Security Center イベント ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
イベントパラメータ	• GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。 • GNRL_EA_PARAM_4 はアカウントセキュリティ識別子（SID）です。 • GNRL_EA_PARAM_5 はアプリケーションのデジタル署名に関する情報です。 • GNRL_EA_PARAM_6 は chrome.exe など、アプリケーションの実行ファイルの名前です。 • GNRL_EA_PARAM_7 は実行ファイルのパスです。 • GNRL_EA_PARAM_8 はオブジェクトのハッシュ（SHA256）です。 • GNRL_EA_PARAM_9 はユーザーが実行しようとしているアプリケーションのバージョンです。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動がテストモードで許可されています

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
Windows イベント ID	704
Kaspersky Security Center イベント ID	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
イベントパラメータ	• GNRL_EA_PARAM_2 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_3 は手動で作成されたカテゴリ ID です。 • GNRL_EA_PARAM_4 はアカウントセキュリティ識別子（SID）です。 • GNRL_EA_PARAM_5 はアプリケーションのデジタル署名に関する情報です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

許可対象のページが開かれました

ステータス	ⓘ
コンポーネント	ウェブコントロール
Windows イベント ID	751
Kaspersky Security Center イベント ID	000002f4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

デバイスを使用した操作が許可されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
Windows イベント ID	801
Kaspersky Security Center イベント ID	00000321
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

ファイル操作が実行されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
Windows イベント ID	808
Kaspersky Security Center イベント ID	GNRL_EV_USB_FILE_OPERATION
イベントパラメータ	• GNRL_EA_PARAM_1 はファイルの操作です（書き込みまたは削除）。 • GNRL_EA_PARAM_2 はファイルのパスです。 • GNRL_EA_PARAM_3 はデバイスの名前です。 • GNRL_EA_PARAM_4 はセッションのユーザーの名前です。 • GNRL_EA_PARAM_5 はハードウェアの ID です（HWID）。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

適用可能なアップデートはありません

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1020
Kaspersky Security Center イベント ID	000003fc
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アップデートの配信が正常に完了しました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1022
Kaspersky Security Center イベント ID	000003fe

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

ファイルをダウンロードしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1003
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルをダウンロードしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1004
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルをインストールしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1005
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルをアップデートしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1006
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

アップデートエラーのためファイルをロールバックしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1007
Kaspersky Security Center イベント ID	–

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルをアップデートしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1008
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

アップデートを配信しています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1009
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルをロールバックしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1010
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ダウンロードするファイルのリストを作成しています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	1013
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

パッチをダウンロードしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2150
Kaspersky Security Center イベント ID	–

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

パッチをインストールしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2151
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

パッチをインストールしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2152
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

パッチをロールバックしています

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2154
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

パッチをロールバックしました

ステータス	ⓘ
コンポーネント	アップデート
Windows イベント ID	2155
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイル暗号化 / 復号化ルールの適用が開始されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	901
Kaspersky Security Center イベント ID	00000385

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイル暗号化 / 復号化ルールの適用が完了しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	902
Kaspersky Security Center イベント ID	00000386
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ファイル暗号化 / 復号化ルールの適用が再開されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	905
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルの暗号化 / 復号化を開始しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	910
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルの暗号化 / 復号化が完了しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	911
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ファイルは除外対象であるため暗号化されていません

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	913
Kaspersky Security Center イベント ID	–

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ポータブルモードが有効になりました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	950
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ポータブルモードが無効になりました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	952
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスの暗号化 / 復号化が開始されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1301
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスの暗号化 / 復号化が完了しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1302
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスの暗号化 / 復号化が再開されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1304
Kaspersky Security Center イベント ID	–

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスが暗号化されていません

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1307
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイス暗号化 / 復号化プロセスがアクティブモードに移行しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1308
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイス暗号化 / 復号化プロセスがパッシブモードに移行しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1309
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

暗号化モジュールが読み込まれました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1310
Kaspersky Security Center イベント ID	0000051e
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

新しい認証エージェントアカウントが作成されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1330
Kaspersky Security Center イベント ID	00000532

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

認証エージェントアカウントが削除されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1331
Kaspersky Security Center イベント ID	00000533
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

認証エージェントアカウントのパスワードが変更されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1332
Kaspersky Security Center イベント ID	00000534
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

認証エージェントに正常にログインしました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1333
Kaspersky Security Center イベント ID	00000535
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

認証エージェントへのログインに失敗しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1334
Kaspersky Security Center イベント ID	00000536
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

暗号化済みデバイスへのアクセスを要求する手順によってハードディスクにアクセスしました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1335
Kaspersky Security Center イベント ID	00000537

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

暗号化済みデバイスへのアクセスを要求する手順によるハードディスクへのアクセスに失敗しました

ステータス	
コンポーネント	データ暗号化
Windows イベント ID	1336
Kaspersky Security Center イベント ID	00000538
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アカウントが追加できません。このアカウントは既に存在しています

ステータス	
コンポーネント	データ暗号化
Windows イベント ID	1337
Kaspersky Security Center イベント ID	00000539
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アカウントが変更できません。このアカウントは存在しません

ステータス	
コンポーネント	データ暗号化
Windows イベント ID	1338
Kaspersky Security Center イベント ID	0000053a
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

アカウントが削除できません。このアカウントは存在しません

ステータス	
コンポーネント	データ暗号化
Windows イベント ID	1339
Kaspersky Security Center イベント ID	0000053b
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

FDE をアップグレードしました

ステータス	
コンポーネント	データ暗号化
Windows イベント ID	1341
Kaspersky Security Center イベント ID	0000053d

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

FDE のアップグレードをロールバックしました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1343
Kaspersky Security Center イベント ID	0000053f
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

WinRE イメージからの Kaspersky Disk Encryption ドライバーのアンインストールが失敗しました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1346
Kaspersky Security Center イベント ID	00000542
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

BitLocker 回復キーが変更されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1370
Kaspersky Security Center イベント ID	0000055a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

BitLocker のパスワード / PIN が変更されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1371
Kaspersky Security Center イベント ID	0000055b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

BitLocker 回復キーがリムーバブルドライブに保存されました

ステータス	ⓘ
コンポーネント	データ暗号化
Windows イベント ID	1372
Kaspersky Security Center イベント ID	0000055c

Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Anti Targeted Attack Platform サーバーからのタスクの処理は無効です

ステータス	ⓘ
コンポーネント	Endpoint Sensor
Windows イベント ID	2103
Kaspersky Security Center イベント ID	00000837
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Endpoint Sensor がサーバーに接続しました

ステータス	ⓘ
コンポーネント	Endpoint Sensor
Windows イベント ID	2101
Kaspersky Security Center イベント ID	00000835
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Anti Targeted Attack Platform サーバーへの接続が復元されました

ステータス	ⓘ
コンポーネント	Endpoint Sensor
Windows イベント ID	2102
Kaspersky Security Center イベント ID	00000836
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Kaspersky Anti Targeted Attack Platform サーバーからのタスクは処理中です

ステータス	ⓘ
コンポーネント	Endpoint Sensor
Windows イベント ID	2104
Kaspersky Security Center イベント ID	00000838
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが削除されました

ステータス	ⓘ
コンポーネント	データの消去
Windows イベント ID	2251
Kaspersky Security Center イベント ID	000008cb

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	–

データ消去タスクの統計

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2853
Kaspersky Security Center イベント ID	00000b25
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ステータス	ⓘ
コンポーネント	データの消去
Windows イベント ID	2253
Kaspersky Security Center イベント ID	000008cd
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが隔離されました（Sandbox）

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2602
Kaspersky Security Center イベント ID	00000a2a
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが削除されました（Sandbox）

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2604
Kaspersky Security Center イベント ID	00000a2c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

IOC スキャンが開始されました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2652
Kaspersky Security Center イベント ID	00000a5c
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

IOC スキャンが完了しました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2653
Kaspersky Security Center イベント ID	00000a5d
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが隔離されました（Endpoint Detection and Response）

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2555
Kaspersky Security Center イベント ID	000009fb
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが削除されました（Endpoint Detection and Response）

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response
Windows イベント ID	2557
Kaspersky Security Center イベント ID	000009fd
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションコンポーネントが正常に変更されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	1402
Kaspersky Security Center イベント ID	0000057a
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2606
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2609
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2610
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2616
Kaspersky Security Center イベント ID	–
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	–

デバイスが接続している管理サーバーは信頼済みに設定されました。

ステータス	ⓘ
コンポーネント	管理サーバーの接続の保護
Windows イベント ID	3300
Kaspersky Security Center イベント ID	00000ce4
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスは新しい信頼済みの管理サーバーに接続されました。

ステータス	ⓘ
コンポーネント	管理サーバーの接続の保護
Windows イベント ID	3302
Kaspersky Security Center イベント ID	00000ce6
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスが接続している管理サーバーは信頼済みとして設定されていません。

ステータス	ⓘ
コンポーネント	管理サーバーの接続の保護
Windows イベント ID	3303

Kaspersky Security Center イベント ID	00000ce7
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

非同期の Sandbox 検知

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2619
Kaspersky Security Center イベント ID	GNRL_EV_APP_INCIDENT_OCCURED
イベントパラメータ	• GNRL_EA_PARAM_1 は Sandbox コンポーネントのパラメータです。 • GNRL_EA_PARAM_2 はオブジェクトのパスです。 • GNRL_EA_PARAM_3 はインシデント ID です。 • GNRL_EA_PARAM_4 はオブジェクトのハッシュ（SHA256）です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

スキャンタスクはユーザーにより正常に Sandbox に送信されました

ステータス	ⓘ
コンポーネント	Sandbox
Windows イベント ID	2622
Kaspersky Security Center イベント ID	00000a3e
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスが接続されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
Windows イベント ID	805
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_PLUGGED
イベントパラメータ	• GNRL_EA_PARAM_1 はハードウェアの ID です（HWID）。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスの接続が切断されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
Windows イベント ID	806
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
イベントパラメータ	• GNRL_EA_PARAM_1 はハードウェアの ID です（HWID）。 • GNRL_EA_PARAM_2 はセッションのユーザーの名前です。
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

本製品の以前のバージョンを削除する際にエラーが発生しました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	246
Kaspersky Security Center イベント ID	000000f6
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert サーバーに正常に接続しました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2853
Kaspersky Security Center イベント ID	00000b25
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert 応答サーバーに正常に接続しました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2853
Kaspersky Security Center イベント ID	00000b25
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

EDR Expert テレメトリ収集サーバーに正常に接続されました

ステータス	ⓘ
コンポーネント	Endpoint Detection and Response Expert（オンプレミス）
Windows イベント ID	2857
Kaspersky Security Center イベント ID	00000b26
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

NDR サーバーに正常に接続されました

ステータス	ⓘ
コンポーネント	Network Detection and Response (KATA)
Windows イベント ID	3083
Kaspersky Security Center イベント ID	00000c0b
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

クラウドサービスのクライアントアプリケーションの起動が許可されました

ステータス	ⓘ
コンポーネント	Cloud Discovery
Windows イベント ID	2210
Kaspersky Security Center イベント ID	000008a2
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

クラウドサービスへのアクセスが許可されました

ステータス	ⓘ
コンポーネント	Cloud Discovery
Windows イベント ID	2211
Kaspersky Security Center イベント ID	000008a3
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

保護された領域にアクセスしました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	2004
Kaspersky Security Center イベント ID	000007d4
Windows イベントログ（既定）	✓
Kaspersky Security Center イベントログ（既定）	✓

ファイルまたはフォルダーの変更が検知されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2950
Kaspersky Security Center イベント ID	00000b86
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

オブジェクトの変更が多すぎます。イベントの集計を開始しました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2955
Kaspersky Security Center イベント ID	00000b8b

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

集計期間のオブジェクト変更のレポート

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2956
Kaspersky Security Center イベント ID	00000b8c
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

レジストリの変更が検知されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2951
Kaspersky Security Center イベント ID	00000b87
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

デバイスの接続または接続解除が検出されました

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2952
Kaspersky Security Center イベント ID	00000b88
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

監視範囲に正しくないオブジェクトが含まれています

ステータス	ⓘ / ⚠ / ⓔ
コンポーネント	システム変更監視
Windows イベント ID	2903

Kaspersky Security Center イベント ID	00000b89
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

ベースラインが作成されました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2957
Kaspersky Security Center イベント ID	00000b8d
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ベースラインが更新されました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2958
Kaspersky Security Center イベント ID	00000b8e
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

操作は信頼するユーザーにより実行されました

ステータス	ⓘ
コンポーネント	システム変更監視
Windows イベント ID	2962
Kaspersky Security Center イベント ID	00000b92
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

このイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションに移動して、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の保管期間を設定します。

SVM に接続しました

ステータス	ⓘ
コンポーネント	Light Agent
Windows イベント ID	3152
Kaspersky Security Center イベント ID	00000c50

Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

新しい一時パスワードが作成されました

ステータス	ⓘ
コンポーネント	システム監査
Windows イベント ID	265
Kaspersky Security Center イベント ID	00000109
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Integration Server に正常に接続しました

ステータス	ⓘ
コンポーネント	Light Agent
Windows イベント ID	3105
Kaspersky Security Center イベント ID	00000c21
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Integration Server への接続を復元しています

ステータス	ⓘ
コンポーネント	Light Agent
Windows イベント ID	3104
Kaspersky Security Center イベント ID	00000c20
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

KUMA サーバーに正常に接続されました

ステータス	ⓘ
コンポーネント	KUMA 連携
Windows イベント ID	2857
Kaspersky Security Center イベント ID	00000b29
Windows イベントログ（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

補足資料 7：実行防止でサポートされるファイルの拡張子

Kaspersky Endpoint Security は特定のアプリケーションで開かれる Office 形式のファイルを開く動作を防止します。サポートされるファイルの拡張子に関する情報は次の表を参照してください。

実行防止でサポートされるファイルの拡張子

アプリケーション名	実行ファイル	ファイルの拡張子
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
ワードパッド	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

補足資料 8：実行防止でサポートされるスクリプトインタープリター

実行防止は次のスクリプトインタープリターをサポートしています：

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe

- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

実行防止は Java Runtime Environment （java.exe および javaw.exe のプロセス）で動作する Java アプリケーションの動作をサポートします。

補足資料 9：レジストリ内の IOC スキャン範囲（RegistryItem）

IOC スキャン範囲に データ種別 **Windows レジストリ - RegistryItem** を追加すると、Kaspersky Endpoint Security は次のレジストリキーをスキャンします：

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile
```

```
HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

補足資料 10：IOC ファイルの要件

IOC スキャンタスクを作成する際は、次の IOC ファイルの要件および制限を考慮してください：

- 本製品は侵害インジケーターの記述に OpenIOC のバージョン 1.0 および 1.1 の IOC および XML が含まれる IOC ファイルをサポートしています。
- IOC ファイルをアップロードしたら、タスクのプロパティで直接、組み込みエディターを使用してファイルを手動で編集できます。Kaspersky Endpoint Security は、OpenIOC 1.1 標準に準拠した IOC ファイルの編集をサポートしています。OpenIOC バージョン 1.0 に準拠した IOC ファイルの内容を変更することはできません。
- コマンドラインで *IOC* スキャンタスクの作成中にサポートされない IOC ファイルをアップロードした場合、本製品はタスクが実行されたときにサポートされる IOC ファイルのみを使用します。コマンドラインで *IOC* スキャンタスクの作成中、すべてのアップロードされた IOC ファイルがサポートされないファイルだった場合は、タスクは実行されますが侵害インジケーターは検知されません。Web コンソールまたは Cloud コンソールを使用してサポートされない ＩＯＣ ファイルをアップロードすることはできません。
- IOC ファイルの構文エラーおよびサポートされない IOC タームおよびタグがあってもタスクの実行は失敗しません。IOC ファイルのこのようなセクションでは、本製品は一致なしとして判断します。
- 単一の IOC スキャンタスクで使用されるすべての IOC ファイルの識別子は一意である必要があります。同じ識別子を持つ IOC ファイルが存在した場合、タスクの実行結果に影響を与えることがあります。
- 単一の IOC ファイルのサイズは 2 MB を超えることはできません。サイズの大きいファイルを使用すると IOC スキャンタスクはエラーで終了します。IOC コレクションに追加されるすべてのファイルの合計サイズが 10MB を超えることはできません。すべてのファイルの合計サイズが 10 MB を超える場合は、IOC コレクションを分割して複数の *IOC* スキャンタスクを作成する必要があります。

- 脅威ごとに1つのIOCファイルを作成することを推奨します。*IOC*スキャンタスクの結果の解析がしやすくなるためです。

以下のリンクをクリックしてダウンロードできるファイルには、すべてのOpenIOC標準のIOCタームの一覧が含まれています。

こちらのリンクからIOC_TERMS.XLSXファイルをダウンロードできます

本製品のOpenIOC標準をサポートする機能および制限を次の表に示します。

OpenIOCバージョン1.0および1.1をサポートする機能および制限

サポートされる条件	OpenIOC 1.0：
	
	`is`
	`isnot`（セットからの例外として）
	`contains`
	`containsnot`（セットからの例外として）
	OpenIOC 1.1：
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Email/*タームについては、条件`contains`と`is`のみがサポートされています。遡及的IOCスキャンが正しく動作するため、条件`is`を使用する際には、IOCファイル内のメールアドレスは次の形式で指定する必要があります：`"name@example.org" <SMTP:name@example.org>`通常の*IOC*スキャンタスクを実行する場合は、次の形式でメールアドレスを指定すれば問題ありません：`name@example.org`。

サポートされる条件の属性値	OpenIOC 1.1：
	
	`preserve-case`
	`negate`

サポートされる演算子	`AND` `OR`
サポートされるデータ種別	`"date"`：日付（適用可能な条件：`is`、`greater-than`、`less-than`） `"int"`：整数（適用可能な条件：`is`、`greater-than`、`less-than`） `"string"`：文字列（適用可能な条件：`is`、`contains`、`matches`、`starts-with`、`ends-with`） `"duration"`：期間（秒）（適用可能な条件：`is`、`greater-than`、`less-than`）

データ種別の解釈機能	`"boolean string"`、`"restricted string"`、`"md5"`、`"IP"`、`"sha256"`および`"base64Binary"`データ種別は文字列として解釈されます。
	
	本製品はインターバルのフォームに設定されている場合は`Content`および`date`データ種別の`int`設定の解釈をサポートします：
	
	OpenIOC 1.0：
	`Content`フィールドの`TO`演算子の使用：
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1：
	条件`greater-than`および`less-than`の使用
	`Content`フィールドでの演算子`TO`の使用
	本製品は、インジケーターが`ISO 8601, Zulu time zone, UTC`形式に設定されている場合に、データ種別`date`および`duration`の解釈をサポートします。

補足資料 11：アプリケーションコンポーネントルールのユーザーアカウント

一部のアプリケーションコンポーネントを設定するには、特別なルールを追加する必要があります。たとえば、ウェブコントロールの場合、本製品でブロックする Web アドレスのリストを含むルールを追加する必要があります。アプリケーションコンポーネントルールでは、コンポーネントのスケジュールを設定することや、本製品によりルールを適用する必要があるユーザーを選択することもできます。

次のアプリケーションコンポーネントを構成するには、ルールを追加する必要があります：

- アプリケーションコントロール
- ウェブコントロール
- デバイスコントロール
- Windows イベントログ監視
- アダプティブアノマリーコントロール
- システム変更監視

Kaspersky Endpoint Security for Windows 12.5 から、Active Directory のユーザーだけでなく、Kaspersky Security Center のユーザーリストのユーザーも選択できるようになりました。また、ローカルユーザーアカウントデータを手入力することもできます。つまり、ユーザーの追加には次の方法があります：

- Active Directory（推奨）
- Kaspersky Security Center のユーザーリスト
- ローカルユーザーアカウント

すべてのユーザー選択方法を正しく使用するには、 Kaspersky Endpoint Security と管理プラグインをバージョン 12.5 以上にアップデートする必要があります。

ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。ローカルアカウントを使用する際のセキュリティリスクについて詳しくは、マイクロソフトサポート技術情報を参照してください。ローカルユーザーアカウントを使用する場合、コンピューターのセキュリティに関する全責任はユーザーにあります。特に、Kaspersky Endpoint Security 設定へのアクセスのコントロールと制限に関する責任が含まれます。

本製品はユーザーの SID（セキュリティ識別子）を使用してユーザーを識別します。Active Directory または Kaspersky Security Center ユーザーリストのユーザーアカウントを使用する場合、本製品は管理サーバーで SID を識別します。つまり、ユーザーを識別するためにコンピューターに余分な負荷をかけることはありません。1000 人以上のローカルユーザーアカウントをアプリケーションルールに追加した場合、本製品はドメインコントローラーに接続してユーザーを識別します。つまり、コンピューターへの負荷が増加します。コンピューターのパフォーマンスへの影響を最適化するには、Active Directory または Kaspersky Security Center ユーザーリストのユーザーアカウントを使用することを推奨します。

本製品は、手動で追加されたユーザーアカウントを識別するために `<username>` と `<hostname>\<username>` の形式の NetBIOS 名を使用します。NetBIOS 名の長さは最大 16 バイト（15 文字）です。コンピューター名が 15 文字を超える場合、本製品はユーザーを識別できません。その場合、本製品はルールを無効にして、「*ウェブコントロール：一致するセキュリティ識別子（SID）のないユーザーアカウントに対するルールの適用が無効になっています*」などのエラーを生成します。ルールを機能させるには、コンピューター名を手動で短縮する必要があります。Active Directory または Kaspersky Security Center からユーザーアカウントを追加できます。この場合、本製品によって、コンピューター名が自動的に短縮されます。

Kaspersky Endpoint Security は、ルール内の組み込みのユーザーとグループ（「すべて」グループなど）もサポートします。本製品では、ユーザーの SID が決定する仕組みにより、Active Directory または Kaspersky Security Center のユーザーリストから追加された組み込みのユーザーアカウントしか使用することができません。組み込みのユーザーアカウントがローカルに追加されるルールは、機能しません。

補足資料 12：EDR Threat Response 用 API

Kaspersky Endpoint Security 12.9 for Windows では、Kaspersky Security Center OpenAPI を使用する EDR Threat Response 処理（EDR responses）のサポートが導入されています。つまり、Python を使用して、OpenAPI メソッドを呼び出して、EDR Threat Response を自動化できます。SIEM ソリューションと統合すると、これらのメソッドを呼び出すことができます。カスペルスキーの SIEM ソリューションである *Kaspersky Unified Monitoring and Analysis Platform* は、バージョン 3.4.1 以降で EDR Threat Response OpenAPI をサポートしています。サンプルスクリプトについては、KUMA のドキュメントを参照してください。

EDR Threat Response 処理を実行するには、KSC Open API（`AddIncident`）を使用してリクエストを作成して送信する必要があります。リクエストが処理されると、Kaspersky Security Center コンソールに特別なタスクが作成されます。

EDR の脅威に対応する場合にタスクを作成するには、管理サーバーと Kaspersky Security Center Web コンソールの間にバックグラウンド接続を確立する必要があります。バックグラウンド接続サービスは、Kaspersky Security Center Windows 14.2 以降および Kaspersky Security Center Linux 15.2 以降で使用できます。Kaspersky Detection and Response ソリューションのコンソールを含むその他のコンソールはサポートされていません。

EDR Threat Response に対して、基本的なリクエストパラメータを JSON などの形式で指定する必要があります：

- `task` はタスクの種別です（下記参照）。
- `targetHost` はスクリプトを実行するコンピューターの ID です。必須の引数です。スクリプトはイベントからこの引数を取得します。
- `responseEventIncidentArea` は、スクリプトを実行したアプリケーションの名前です（例：`KUMA`）。このパラメータは、作成されたタスクの名前に追加されます。

EDR Threat Response を設定するには、JSON 形式の `"KLINCDT_BODY": json.dumps(data)` パラメータでタスク設定を指定する必要があります。これにより、Kaspersky Security Center コンソールに `[Response] [KUMA] <task type> - <Date> <Time> - <ID>` が作成されます。

Kaspersky Security Center OpenAPI への接続

本製品は、EDR Threat Response の一環として、Kaspersky Security Center コンソールに特別なタスクを作成します。これらのタスクを作成するには、コンピューターと Kaspersky Security Center の間に接続を確立する必要があります。これを行うには、リクエストで Kaspersky Security Center の接続パラメータを指定する必要があります。

Kaspersky Security Center の接続パラメータ

パラメータ	種別	説明
`kscHost`	`string`	Kaspersky Security Center 管理サーバーのアドレス。必須パラメータ。
`kscPort`	`int`	管理サーバーの接続のポート。必須パラメータ。
`kscCert`	`string`	Kaspersky Security Center 管理サーバーに接続するための証明書ファイルへのパス。既定では、パラメータは `False` に設定されています。
`kscUser`	`string`	ユーザーアカウント名。必須パラメータ。
`kscPassword`	`string`	ユーザーアカウントのパスワード。必須パラメータ。

例

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)
```

```
    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

ユーザーアカウントデータは保護されないため、別のユーザーを専用のユーザーにして、これらの処理を実行するためだけにそのユーザーを使用する必要があります。

getFile：ファイルの取得

［ファイルの取得］タスクの設定

パラメータ	種別	説明
md5hash	`string`	取得するファイルの MD5 ハッシュ。
sha256hash	`string`	取得するファイルの SHA256 ハッシュ。
path	`string`	取得するファイルへのパス。

例

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

deleteFile：ファイルの削除

［ファイルの削除］タスクの設定

パラメータ	種別	説明
md5hash	`string`	削除するファイルの MD5 ハッシュ。
sha256hash	`string`	削除するファイルの SHA256 ハッシュ。
path	`string`	削除するファイルへのパス。
searchInSubfolders?	`boolean`	削除するファイルをサブフォルダー内で検索します。

例

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
```

```
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

quarantineFile：ファイルの隔離

［ファイルの隔離］タスクの設定

パラメータ	種別	説明
md5hash	string	隔離するファイルの MD5 ハッシュ。
sha256hash	string	隔離するファイルの SHA256 ハッシュ。
path	string	隔離するファイルへのパス。

例

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

iocScan：IOC スキャン

［IOC スキャン］タスクの設定

パラメータ	種別	説明
ioc	string	スキャンに使用する IOC ファイルを含む ZIP アーカイブのパス。
isolateHost	boolean	侵害インジケーターの検知時に脅威の拡散を防ぐためにコンピューターをネットワークから分離します。
scanCriticalAreas	boolean	侵害インジケーターの検知時に*簡易スキャン*タスクを実行します。
quarantineObject	boolean	侵害インジケーターの検知時に悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。

例

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
```

```
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

startProcess：プロセスの開始

［プロセスの開始］タスクの設定

パラメータ	種別	説明
executablePath	string	プロセスを開始するために使用される実行ファイルへのパス。
arguments?	string	プロセスを開始するための追加のコマンドライン引数。
workingFolder?	string	プロセスの作業フォルダーのパス。

例

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

terminateProcess：プロセスの終了

［プロセスの終了］タスクの設定

パラメータ	種別	説明
md5hash	string	プロセスを終了するファイルの MD5 ハッシュ。
sha256hash	string	プロセスを終了するファイルの SHA256 ハッシュ。
path	string	削除するファイルへのパス。
caseSensitive	boolean	ファイルを検索する際の大文字小文字の区別。

例

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

isolateHost：コンピューターのネットワーク分離

コンピューターのネットワーク分離の設定

パラメータ	種別	説明
`action`	`string`	ネットワーク分離の動作モード。

例

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

preventExecution：実行防止

実行防止の設定

パラメータ	種別	説明
hash	`string`	実行を禁止するファイルの MD5 ハッシュ。
path	`string`	実行を禁止するファイルへのパス。
caseSensitive	`boolean`	ファイルを検索する際の大文字小文字の区別。

例

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

onDemandScan：マルウェアのスキャン

［マルウェアのスキャン］タスクの設定

パラメータ	種別	説明
path	`string`	オブジェクトスキャンのファイルとフォルダーのスペース区切りリスト。
recursive	`boolean`	再帰的スキャンモード。

パラメータ	種別	説明
type	`number`	スキャン範囲。

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

例

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、本製品のインストールフォルダーにあるファイル legal_notices.txt に記載されています。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、Reader、Shockwave は Adobe のアメリカ合衆国およびその他の国における商標または登録商標です。

Amazon、Amazon Web Services、AWS は Amazon.com, Inc. およびその子会社の商標です。

Apple、FireWire、iTunes、Mac、Safari は Apple Inc. の商標です。

Arm は、米国およびその他の国における Arm Limited（またはその子会社）の登録商標です。

AutoCAD は、アメリカ合衆国およびその他の国における Autodesk, Inc. およびその子会社の商標または登録商標です。

文字商標 Bluetooth およびそのロゴは Bluetooth SIG, Inc. の所有財産です。

Borland は、Borland Software Corporation の商標または登録商標です。

Cisco、Cisco AnyConnect、IOS はアメリカ合衆国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Citrix、Citrix Provisioning、Citrix Provisioning Services、Citrix Virtual Apps and Desktop、XenDesktop、および XenServer は、米国およびその他の国における Cloud Software Group, Inc. およびその子会社の登録商標または商標です。

Cloudflare、Cloudflare Workers、および Cloudflare ロゴはアメリカ合衆国およびその他の国における Cloudflare, Inc.およびその子会社の商標または登録商標です。

Core は、Intel Corporation およびその子会社の商標です。

dBase は dataBased Intelligence, Inc. の商標です。

Dell Technologies、Dell、EMC およびその他の商標は Dell Inc. およびその子会社の商標です。

Docker および Docker ロゴはアメリカ合衆国およびその他の国における Docker, Inc. およびその子会社の商標または登録商標です。Docker, Inc.およびその他の関係者は、商標権や本文書で使用される用語の所有者である可能性があります。

ESET は ESET spol. s r.o. または ESET の各エンティティの商標または登録商標です。

Foxit は Foxit Corporation の登録商標です。

Radmin は Famatech の登録商標です。

Google、Android、Google Public DNS、Google Chrome および Chrome は、Google LLC の商標です。

HUAWEI FusionCompute、および FusionSphere は、Huawei Technologies Co., Ltd. の商標です。

ICQ は ICQ LLC の商標および/またはサービスマークです。

Intel は、Intel Corporation およびその子会社の商標です。

IBM は、International Business Machines Corporation の世界各国における登録商標です。

Lenovo および Lenovo ThinkPad are はアメリカ合衆国における Lenovo の商用です。

Linux はアメリカ合衆国およびその他の国における Linus Torvalds の登録商標です。

Logitech は Logitech のアメリカ合衆国および他の国における登録商標または商標です。

LogMeIn Pro および Remotely Anywhere は LogMeIn, Inc. の商標です。

Mail.ru は Mail.Ru, LLC の登録商標です。

McAfee はアメリカ合衆国およびその他の国における McAfee LLC およびその子会社の商標または登録商標です。

Microsoft、Access、Active Directory、ActiveSync、Bing、BitLocker、Excel、Hyper-V、Internet Explorer、JScript、LifeCam Cinema、Microsoft Edge、MSDN、MS-DOS、MultiPoint、Office 365、Outlook、PowerPoint、PowerShell、Skype、SQL Server、Surface、Visual Basic、Visual FoxPro、Windows、Windows Live、Windows PowerShell、Windows Server および Windows Store は、Microsoft グループの企業の商標です。

Mozilla、Firefox および Thunderbird はアメリカ合衆国およびその他の国における Mozilla Foundation の商標です。

NetApp は NetApp のアメリカ合衆国およびほかの国における登録商標または商標です。

OpenSSL は OpenSSL Software Foundation が所有する商標です。

OpenStack は、アメリカ合衆国およびその他の国における OpenStack Foundation の登録商標です。

Oracle、Java および JavaScript は Oracle およびその子会社の登録商標です。

Python は Python Software Foundation の商標または登録商標です。

Realtek は Realtek Semiconductor Corporation の商標です。

SAMSUNG は SAMSUNG のアメリカ合衆国およびその他の国における商標です。

Thawte は Symantec Corporation のアメリカ合衆国およびその他の国における子会社の商標または登録商標です。

Trend Micro は Trend Micro Incorporated の商標または登録商標です。

VERISIGN はアメリカ合衆国およびその他の国における VeriSign, Inc. およびその子会社の登録商標または未登録商標です。

VMware、VMware ESXi、VMware Horizon、VMware Workstation、VMware Tools、VMware vSphere はアメリカ合衆国およびその他の国における VMware, Inc. の登録商標または商標です。