kaspersky

Kaspersky Endpoint Security Cloud

Kaspersky Security for Microsoft Office 365

2023年05月23日

カスペルスキー　セールスエンジニアリング本部

本資料では、以下の3製品を紹介します。

- Kaspersky Endpoint Security Cloud
- Kaspersky Endpoint Security Cloud Plus
- Kaspersky Endpoint Security Cloud Pro
- Kaspersky Security for Microsoft Office 365

Kaspersky Endpoint Security Cloud Plus、Proには、
Kaspersky Security for Microsoft Office 365を含みます。

Kaspersky Security for Microsoft Office 365は、
単体製品として使用することが出来ます。

Kaspersky Endpoint Security Cloud
Kaspersky Security for Microsoft Office 365
概要

Kaspersky Endpoint Security Cloud（KES Cloud）

小規模～中堅規模に向けた、クラウド管理で提供するエンドポイントセキュリティ製品。
10～999ライセンスまで。

Kaspersky
Endpoint Security
Cloud

管理サーバーの準備が不要、
今すぐに高度なセキュリティで企業を保護。

クラウドで管理機能が提供されるため、
オフィス外でもセキュリティ管理が可能。

オフィス

リモートワーク

Kaspersky Endpoint Security Cloudの先進性

Windows、Mac、Androidのエンドポイントセキュリティ、iOS MDMを提供し、
KES Cloudならではの便利な付加機能を装備。

KES Cloud

脆弱性スキャン

脆弱性の一覧

アップデート可能な最新のパッチ名称の確認

クラウドディスカバリー

ソーシャルネットワーク、ファイル共有などの使用状況確認

エンドポイントベースの
Shadow IT 発見ソリューション

KES Cloud Plus

＋ パッチ管理

適用可能な最新バージョン
パッチインストール

＋ Cloud blocking

発見されたクラウド使用を
ブロック

＋ Kaspersky Security for Microsoft Office 365

＋ ルートコーズ分析
(EDRサブセット)

KES Cloud Pro

＋ 高度なWindows
セキュリティ

＋ レスポンスを兼ね
備えたEDR

kaspersky

Kaspersky Security for Microsoft Office 365（KSMO365）

Kaspersky Security for Microsoft Office 365

高度なMicrosoft 365 の保護を実現

Microsoft 365のコンポーネントを保護
- Exchange Online
- OneDrive
- SharePoint Online
- Teams

✓ 各コンポーネントでのインバウンド・アウトバウンド通信
✓ 各コンポーネントに保存されているファイル

Exchange Online　OneDrive　SharePoint Online　Microsoft Teams

kaspersky

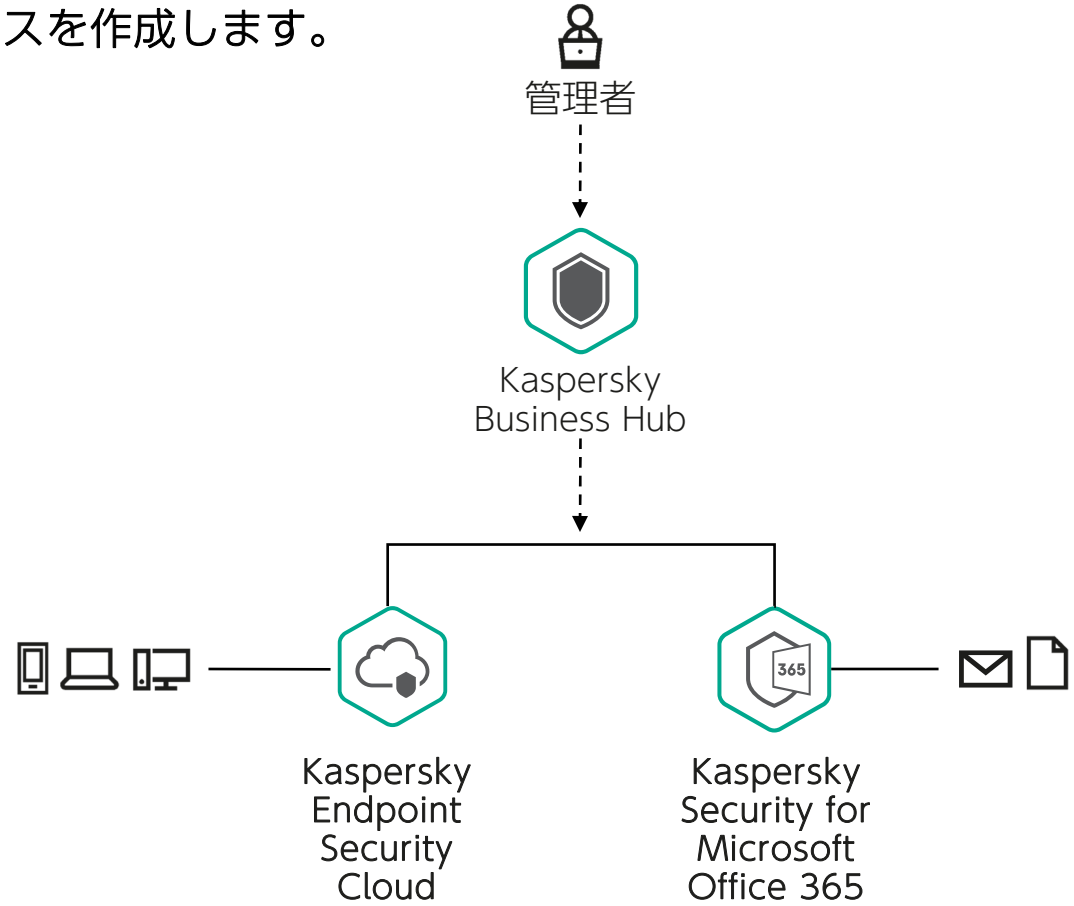
Kaspersky Business Hubによる統合管理

管理者はKaspersky Business Hubにログインし、
Kaspersky Endpoint Security Cloud ワークスペース、
Kaspersky Security for Microsoft Office 365 ワークスペースを作成します。

1企業（組織）は、ワークスペース単位で管理されます。

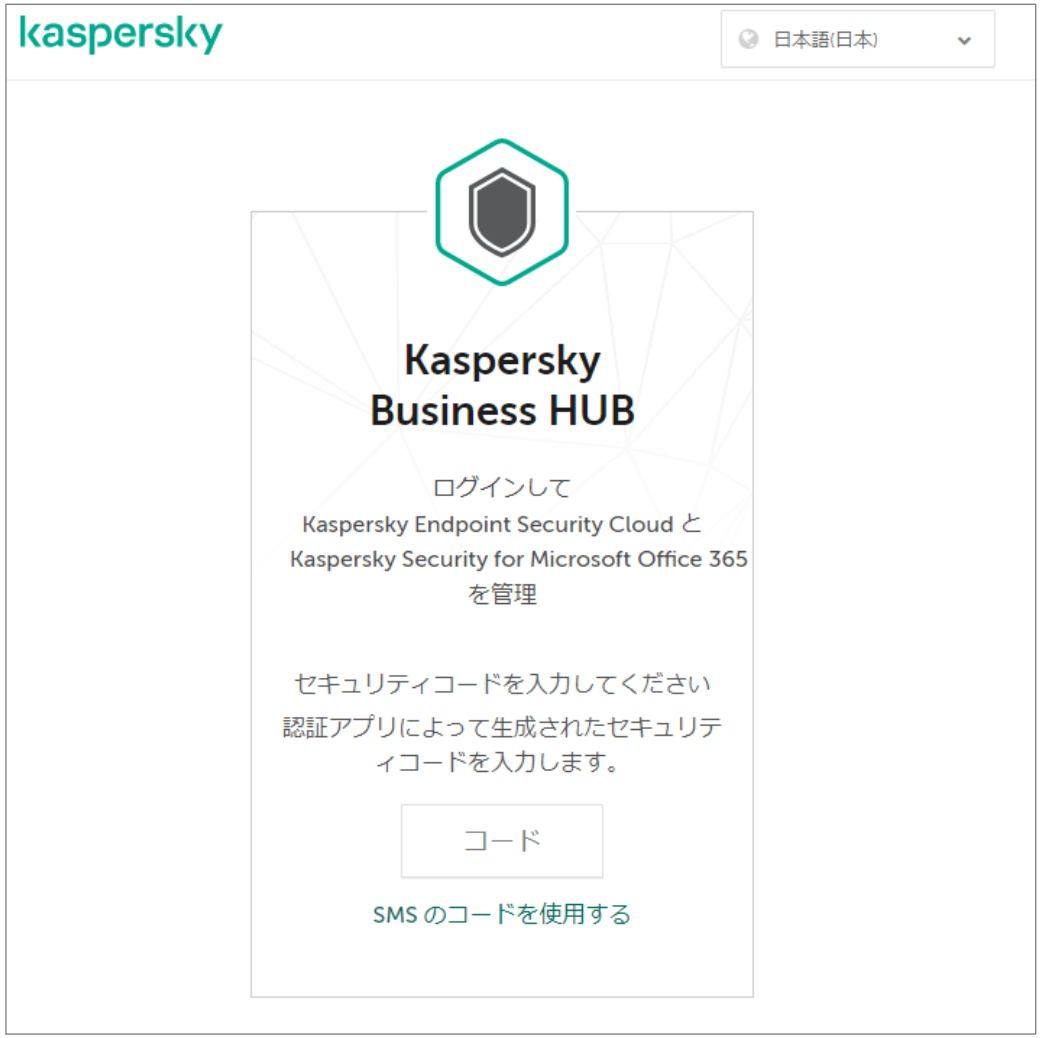
KES Cloudワークスペースでは、Windows、MAC、
Android セキュリティと、iOS MDMを管理。

KSO365ワークスペースでは、Exchange Online保護、
OneDrive保護などを管理。

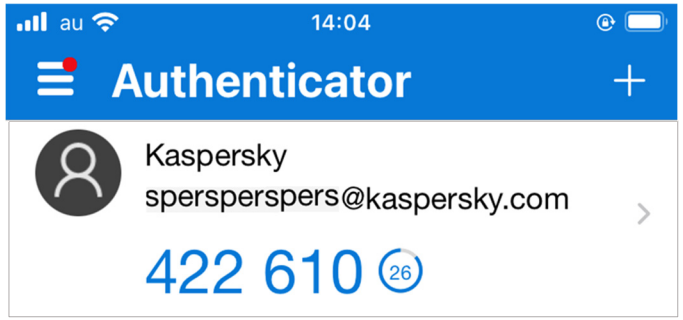


Kaspersky Business Hubによる統合管理

ワークスペースへのログインにはワンタイムパスワードを用いた
多要素認証が使用出来ます。



携帯へのSMS、Microsoft Authenticator、
Google Authenticatorなどを利用出来ます。



ライセンスのコンセプト

一人複数台を使用する時代。

1ユーザーで、コンピュータ1台、モバイル2台を使用出来るライセンス体系。

1 ユーザー

1 PC

2 モバイル端末
携帯・タブレット

KES Cloudライセンス

実際のライセンス数カウントはシンプル。

ライセンスの総数は、保護対象デバイスの数によって計算される。
次のいずれか大きい方。

- 保護対象コンピュータ（デスクトップ / ノート / サーバー）の総数。
- Android / iOS モバイルデバイスの総数の半分。

例
10 台の PC / サーバーと、12台のモバイルデバイスの場合、
10と12÷2=6の比較なので、10が大きい。
ソフトウェアを使用するライセンス数は 10。

10 台の PC / サーバーと、32台のモバイルデバイスの場合、
10と32÷2=16の比較なので、16が大きい。
ソフトウェアを使用するライセンス数は 16。

kaspersky

KES Cloudライセンス

Kaspersky Endpoint Security Cloud

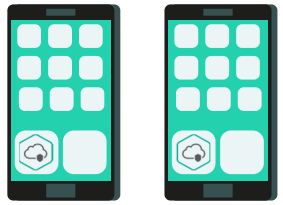
1 ライセンス

=

1 台のコンピュータ

Windows / Mac

+



2 モバイル端末

iOSデバイス+Android

Android2台の使用でもOK

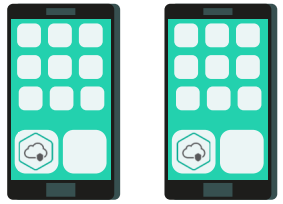
Kaspersky Endpoint Security Cloud Plus、Pro

1 ライセンス

=

1 台のコンピュータ

+



2 モバイル端末

+

Kaspersky Security for Microsoft Office 365

1.5 x Microsoft 365 ユーザー数

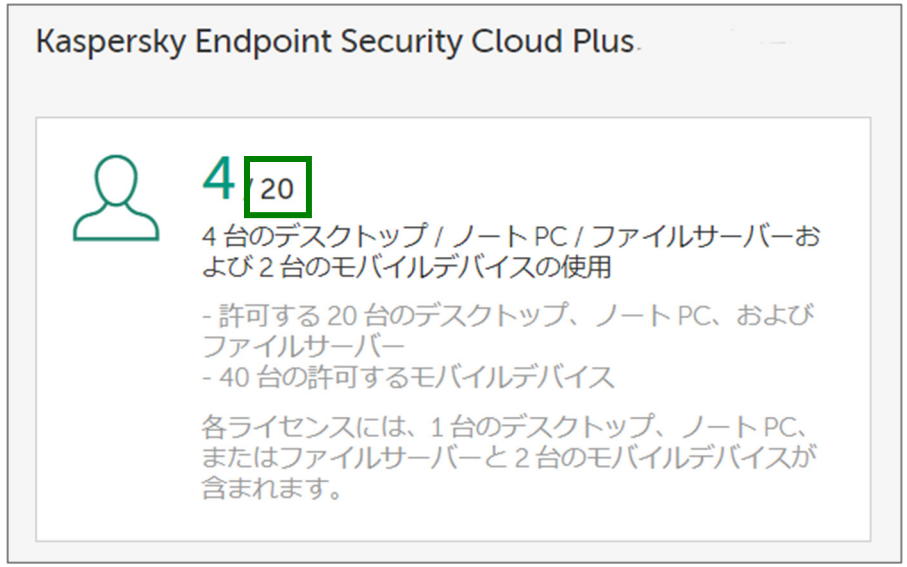
kaspersky

KES Cloud Plusにおける1.5x Microsoft 365 ユーザー数の意味

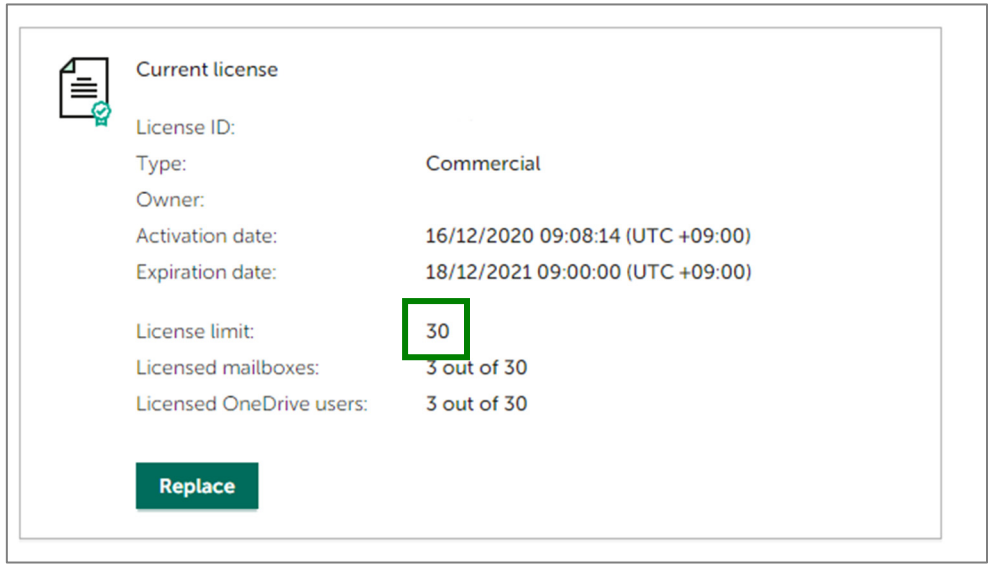
Kaspersky Security for Microsoft Office 365

1.5 x Microsoft 365 ユーザー数

KES Cloud Plusで
20ライセンス保有ならば、



KSMO365は
30ライセンス使用できる。



kaspersky

Kaspersky Endpoint Security Cloud
機能紹介

機能詳細

Kaspersky Endpoint Security for Windows 12の特徴

Kaspersky Endpoint Security Cloudのセキュリティアプリケーションは、
Kaspersky Endpoint Security for Businessと共通。
詳しくは、各アプケーションの資料もご参照ください。

脆弱性管理
エクスプロイトブロック

正規アプリケーションの
悪用を検知

ファイルレス
マルウェア防御

HTTPS通信
監視・可視化

先進的かつ高度な保護機能を持ち、多層で防御を行う。

ふるまい検知(2006年から搭載)、機械学習エンジン(2012年から搭載)
脆弱性攻撃ブロック、ホスト侵入防止

Big Dataの活用

Kaspersky Security Network
エキスパートによる分析、機械学習アルゴリズムとビッグデータ

コントロール機能

アプリケーションコントロール、デバイスコントロール、ウェブコンテンツフィルタリング、
バナー広告ブロック

kaspersky

OS別 機能一覧

	Windows(12.0ベース)			Mac	Android	iOS/iPad OS
	KES Cloud	KES Cloud Plus	KES Cloud Pro			
セキュリティ機能セット						
Kaspersky Security Network	○	○	○	○	○	○
ファイルアンチウイルス	○	○	○	○	○	―
Webアンチウイルス	○ 注1	○	○	○	○	○
メールアンチウイルス	○ 注1	○	○	―	―	―
ネットワーク攻撃防御	○	○	○	○	―	―
ファイアウォール	○	○	○	―	―	―
ホスト侵入防止	○ 注1	○ 注1	○ 注1	―	―	―
ふるまい検知、脆弱性攻撃ブロック、修復エンジン	○	○	○	―	―	―
AMSI（Antimalware Scan Interface）	○	○	○	―	―	―
有害USB攻撃ブロック	―	―	○	―	―	―
脆弱性の評価	○	○	○	―	―	―
ルートコーズ分析	―	○	○	―	―	―
Endpoint Detection and Response	―	―		―	―	―
Cloud Discovery (発見のみ)	○ 注1	○ 注1	○ 注1	―	―	―
管理機能セット						
Cloud Discoveryとブロック	―	○ 注1	○ 注1	―	―	―
ウェブコントロール	―	○	○	―	○	アダルトカテゴリーブロック＋個別URL 注3
デバイスコントロール	―	○	○	―	―	―
アプリケーションコントロール	―	―	○	―	○	―
アダプティブアノマリコントロール	―	―	○ 注1	―	―	―
リモートデータ消去	―	―	○	―	―	―
暗号化管理	―	○	○	○注2	―	―
パッチ管理	―	○	○	―	―	―

Windows版 注1 クライアントOSのみで有効。サーバーOSは未サポート。　Mac版 注2 Plus、Proのみで有効。

注3 iOS/iPad OSのウェブコントロール機能の使用は、Apple Configuratorにより監視済みになっている必要があります。

Kaspersky Endpoint Security Cloud　推し機能
その1 EDR

EDR機能　エディションによる違い

KES Cloud Plus
ルートコーズ分析(Root cause)

ブロックした脅威の、プロセス遷移、ファイルドロップ、
ネットワークアクセス、レジストリアクセスを表示。

マルウェア検知結果だけでなく、脅威状況を把握することが可能になる。

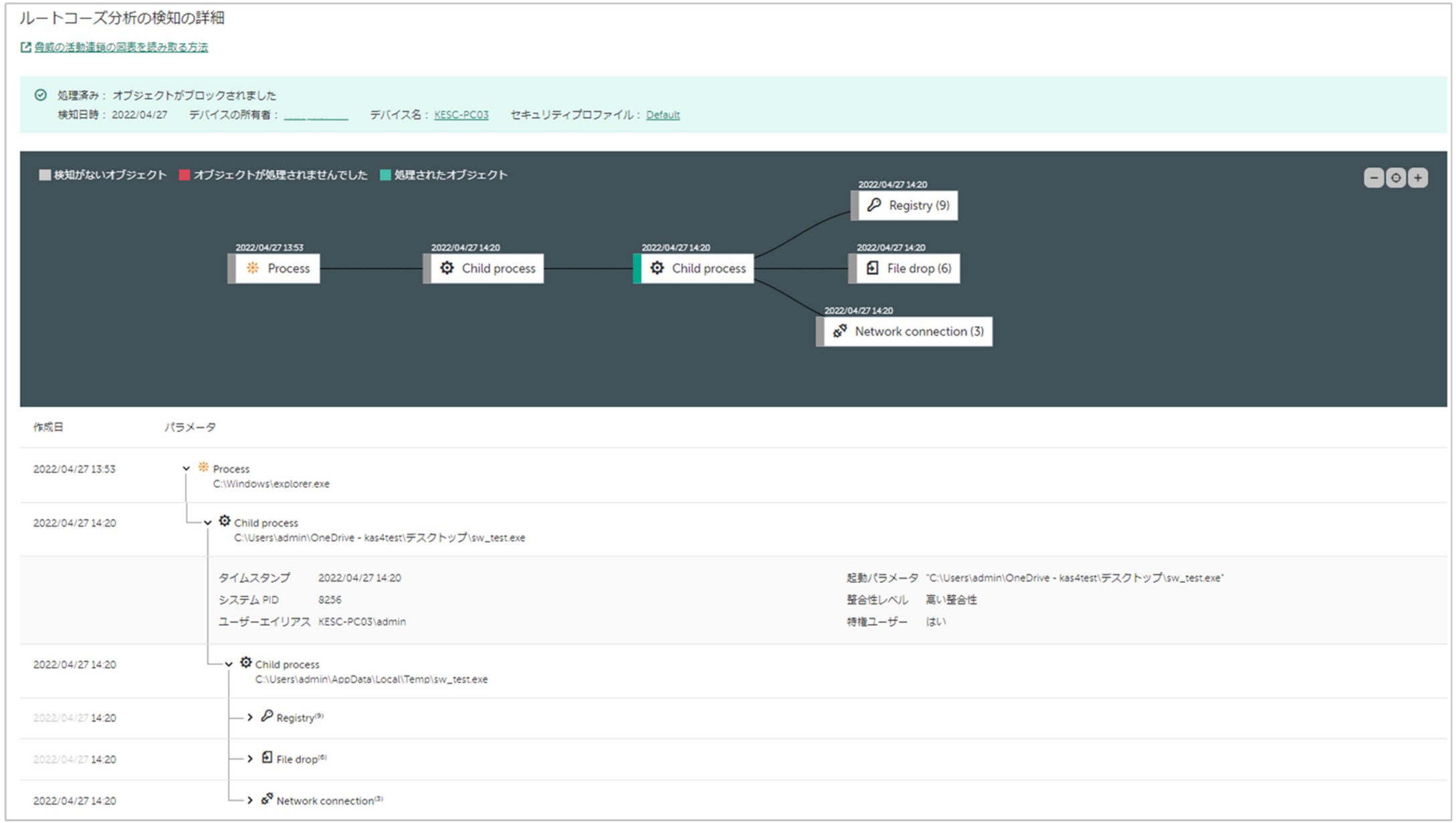
KES Cloud Pro
Endpoint Detection and Response

脅威活動の詳細分析は、ルートコーズ分析と同じ。

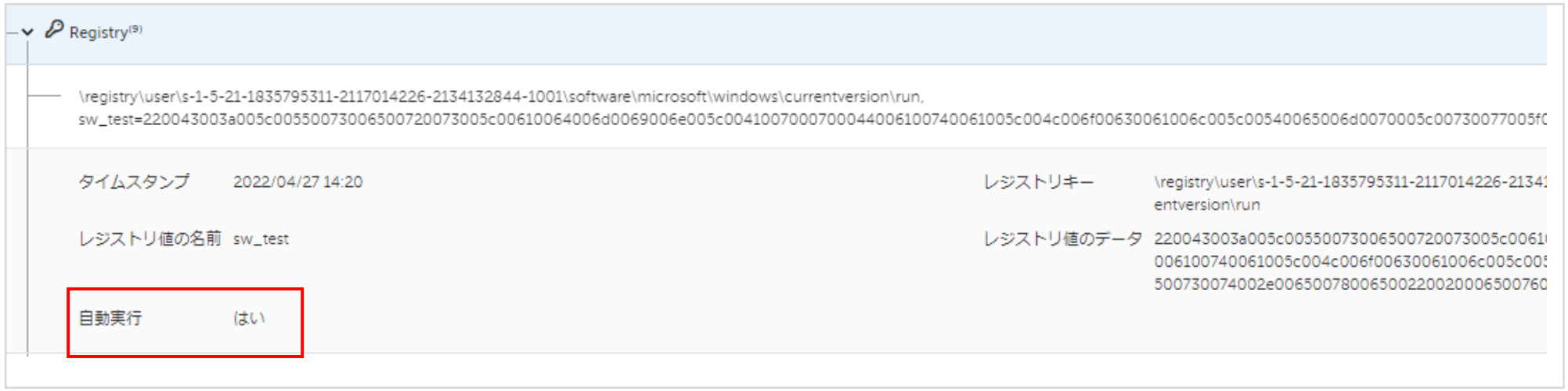
次のレスポンスが可能。
- 実行を防止（ファイル）
- 隔離に移動（ファイル）
- IOCスキャン（ファイルハッシュ、ファイルパス、リモートコンピュータのIPアドレス、レジストリ）
- デバイスのネットワーク分離

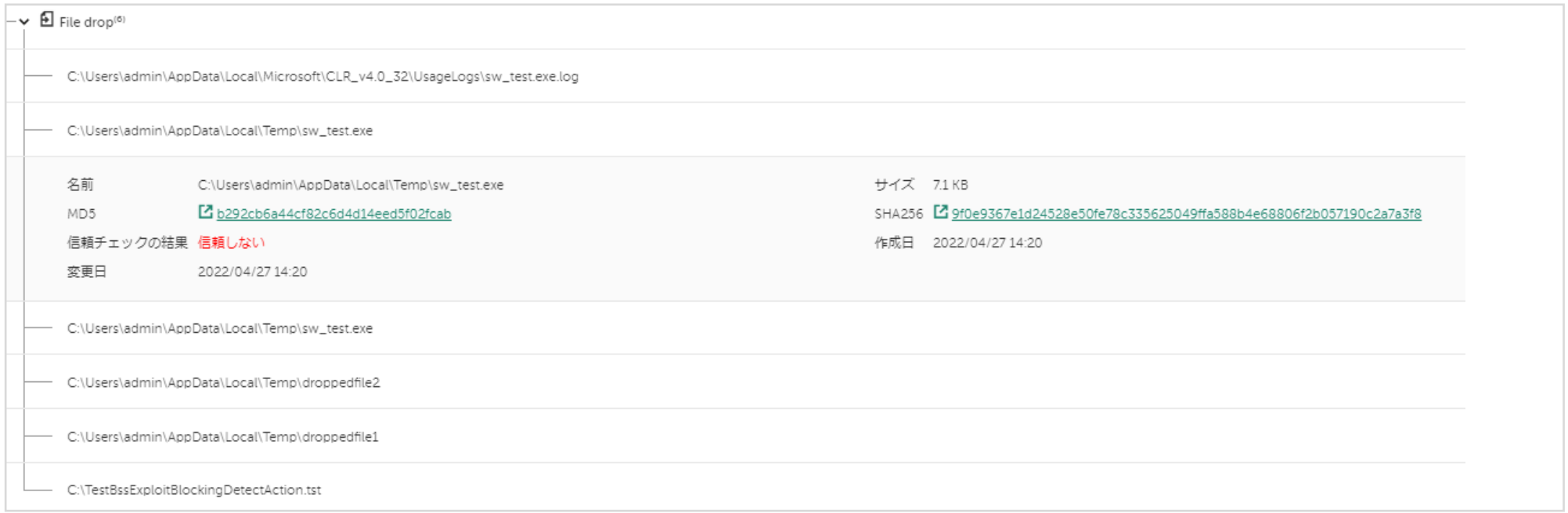
kaspersky

ルートコーズ分析(Root cause)



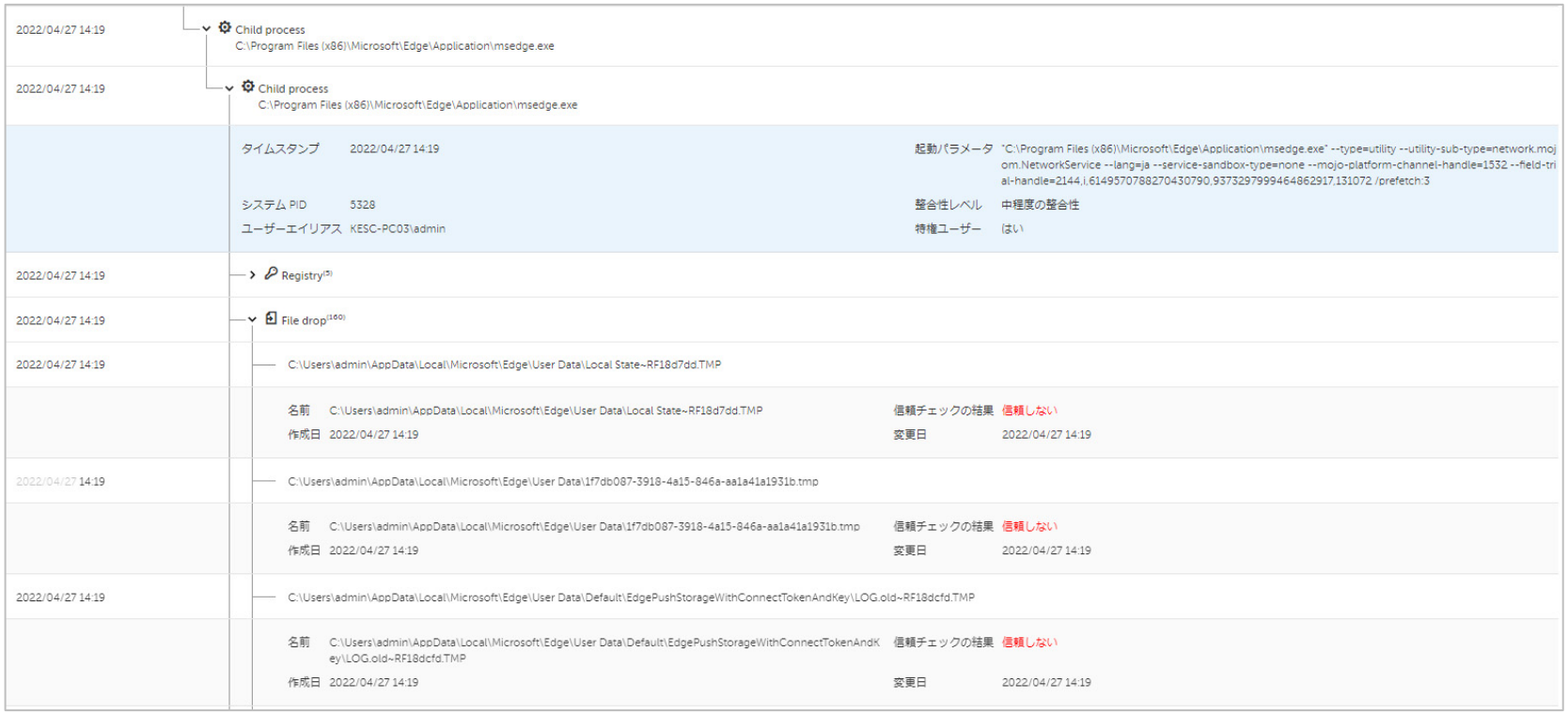
ルートコーズ分析(Root cause) 例 1



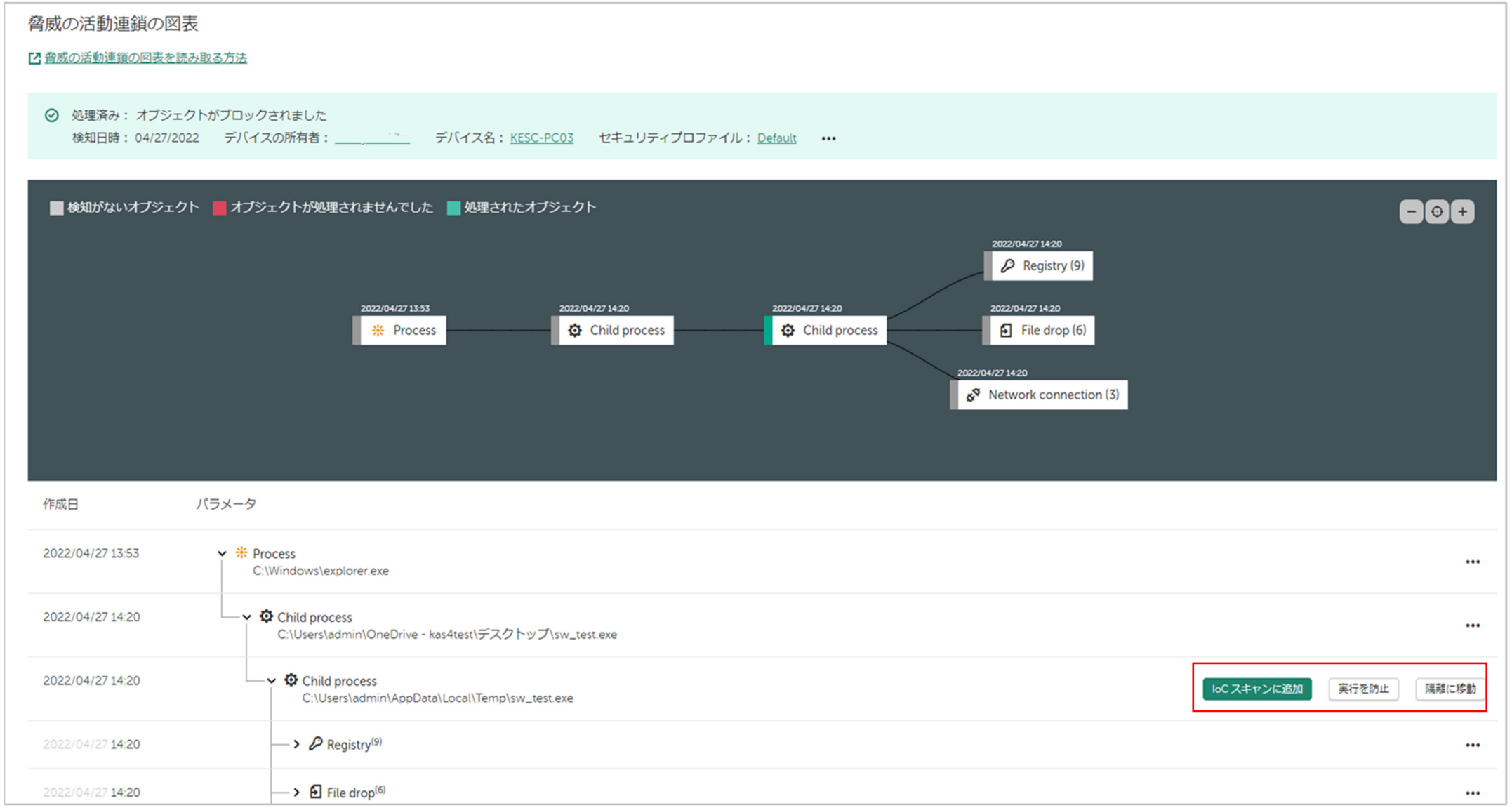


kaspersky

ルートコーズ分析(Root cause) 例2



KES Cloud Pro
Endpoint Detection and Response



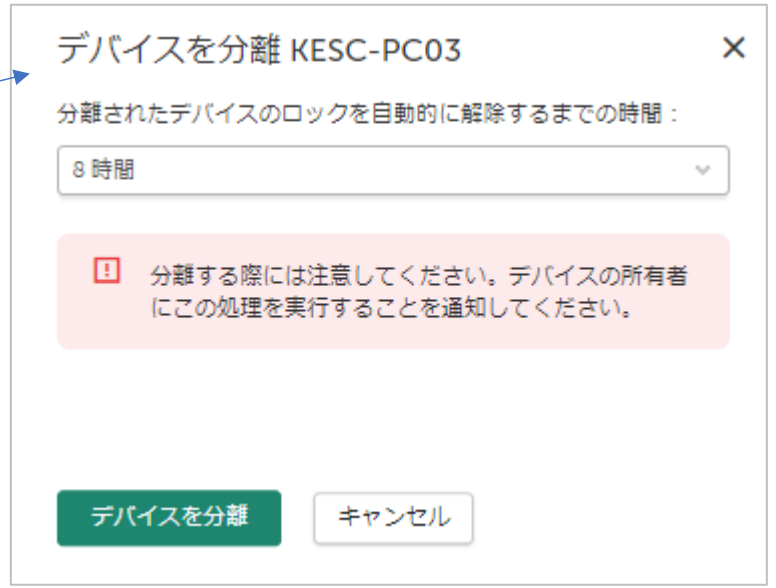
Endpoint Detection and Response
レスポンス機能

IOCスキャンに対象ファイルを追加

対象ファイルの実行を防止

対象ファイルを隔離に移動

Endpoint Detection and Response
レスポンス機能：デバイスのネットワーク分離



Kaspersky Endpoint Security Cloud　推し機能
その2 Cloud Discovery

Cloud Discovery

ブロックはKES Cloud Plus, Proのみ

管理対象の Windows デバイスでのクラウドサービスの利用を監視し、
不要と思われるクラウドサービスへのアクセスをブロック。

ブラウザーやデスクトップアプリケーションから
これらのサービスにアクセスしようとするユーザーの試行を追跡。

シャドー IT によるクラウドサービスの使用を検知して停止するのに役立ちます。

KES Cloud Plus、Proではブロックが可能

Cloud Discovery　新機能

ブロックはKES Cloud Plus, Proのみ

ウィジェットからブロックを簡単に実行

kaspersky

Cloud Discovery アクセス、ブロックのレポート

使用の開始　監視　レポート　イベントログ　ライセンス

ネットワーク攻撃 [PDF | CSV]
このレポートには、管理対象デバイスに対するネットワーク攻撃が表示されます。

脆弱性 [PDF | CSV]
このレポートには、管理対象デバイスで検知されたソフトウェアの脆弱性が表示されます。

Cloud Discovery：クラウドサービスへのアクセスの成功 [PDF | CSV]
このレポートには、Windows デバイスからクラウドサービスへの成功したアクセス試行を表示されます。

Cloud Discovery：クラウドサービスへのブロックされたアクセス試行 [PDF | CSV]
このレポートには、Windows デバイスからクラウドサービスへのアクセスのブロックされた試行が表示さ

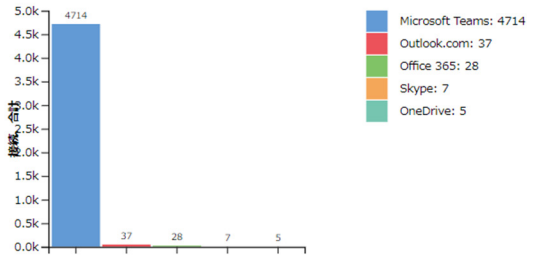
管理

デバイスコントロールによる検知 [PDF | CSV]
このレポートには、デバイスコントロールによって検知された接続デバイスが表示されます。

ウェブコントロールによる検知 [PDF | CSV]
このレポートには、ブロック対象 Web サイト（ウェブコントロールの設定にリストされている）へのアク

Cloud Discovery：クラウドサービスへのアクセスの成功

このレポートには、Windows デバイスからクラウドサービスへの成功したアクセス試行を表示されます。　CSV ファイルを作成　PDF ファイルを



詳細

生成されたレポート 2021/01/21 18:06

デバイスのオペレーティングシステムの時刻が表示されます

デバイスの所有者	デバイス	クラウドサービスのカテゴリ	クラウドサービス	ブラウザーからの接続	クライアントアプリケーションからの接続
k uki	DESKTOP-EJICQDR	その他	Office 365	28	0
t a	DESKTOP-94J4JBK	ファイル共有	OneDrive	0	1
k uki	DESKTOP-EJICQDR	ファイル共有	OneDrive	0	2
s	DESKTOP-NRHMP3E	ファイル共有	OneDrive	0	2
k uki	DESKTOP-EJICQDR	メール	Outlook.com	36	1
k uki	DESKTOP-EJICQDR	メッセンジャー	Microsoft Teams	0	2091

Kaspersky Endpoint Security Cloud　推し機能
その3 脆弱性管理と対策

脆弱性とパッチ管理

脆弱性とパッチ管理に関するインターフェースを統合

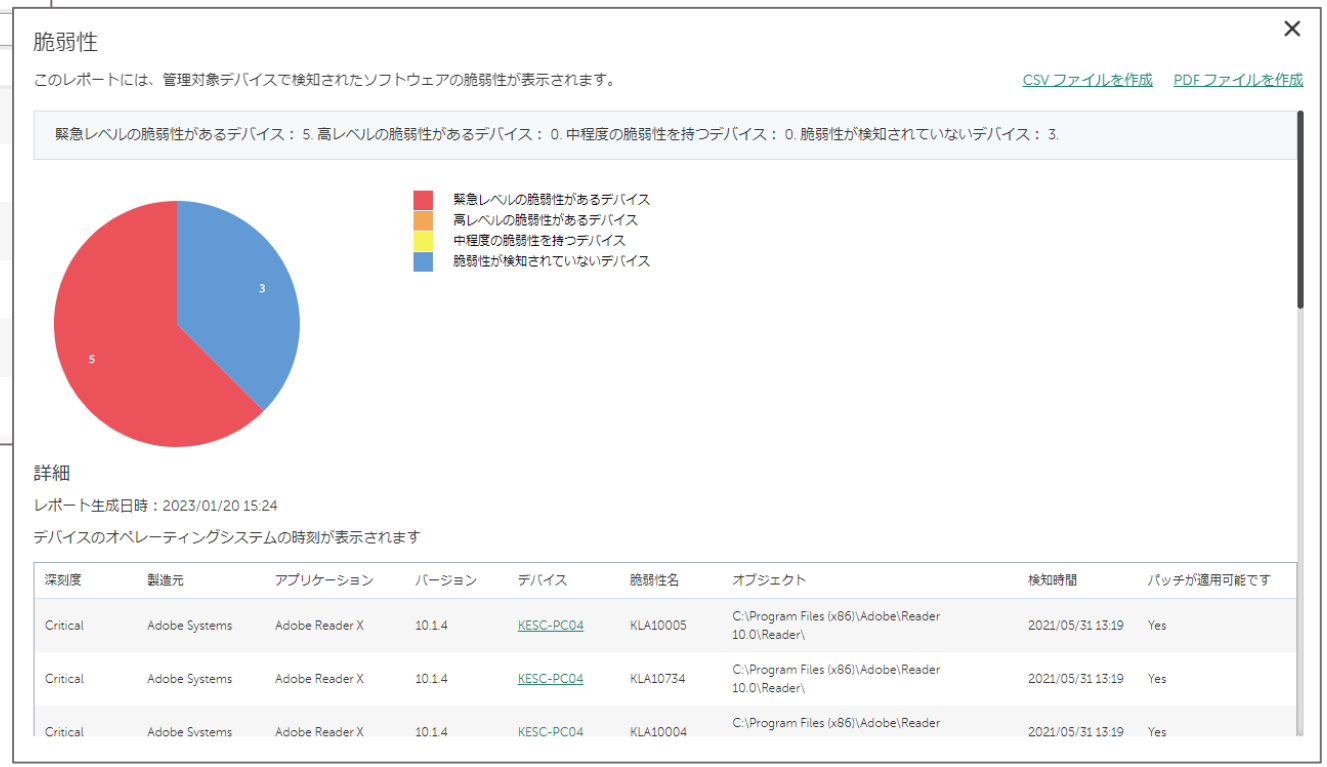
KES Cloud Plus、Proの場合

KES Cloudの場合

脆弱性の評価

Windowsデバイス対象。OS、サードパーティー製品の脆弱性をレポート。
緊急度、適用状況の把握。

レポートを管理者にメールで定期配信可能



脆弱性の評価

どの端末に脆弱性が残っているかを一覧表示。

脆弱性とパッチ管理

脆弱性に対し、パッチ適用を実行。

kaspersky

脆弱性とパッチ管理

重要度	デバイスにインストール済み
低	1 / 3

どの端末がパッチ適用済みか、適用対象かを一覧表示。

アップデートをインストール可能なデバイス（3）

デバイスを表示　すべて 3 | 計画していない (2) | 計画中 (0) | 操作が必要です (0) | 進行中 (0) | インストールエラー (0) | インストール済み (1)

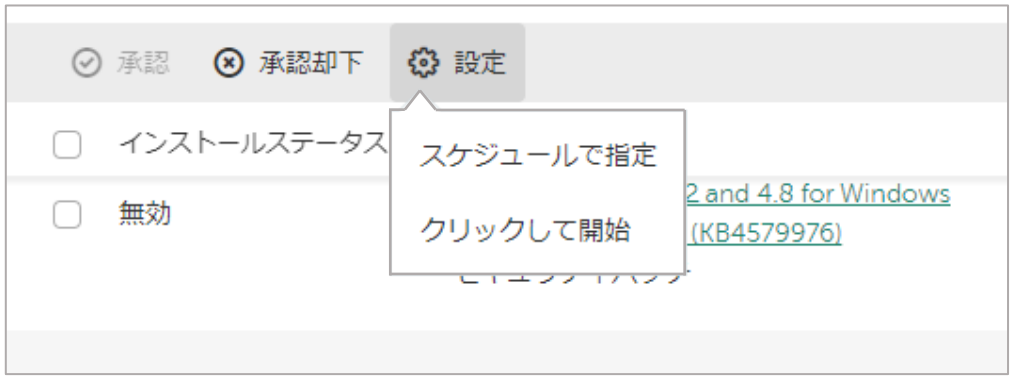
インストールステータス	デバイス名	デバイスの所有者	グループ	Recommendations
インストール済み アップデートがインストールされました	KESC-PC02	–	–	–
計画していない インストールが無効です	KESC-PC05	[redacted]@[redacted].com	–	アップデートのインストール設定へ移動
計画していない インストールが無効です	WINSRV2019-01 Microsoft Windows Server 2019	[redacted]@[redacted]	–	アップデートのインストール設定へ移動

脆弱性とパッチ管理

サードパーティーアプリケーションのパッチをダウンロードし、事前評価する支援。

kaspersky

脆弱性とパッチ管理

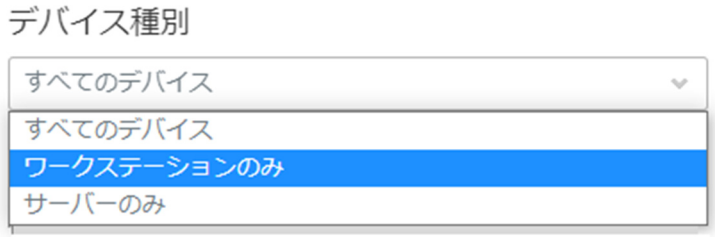


スケジュール実行だけでなく、
即時インストールが可能。

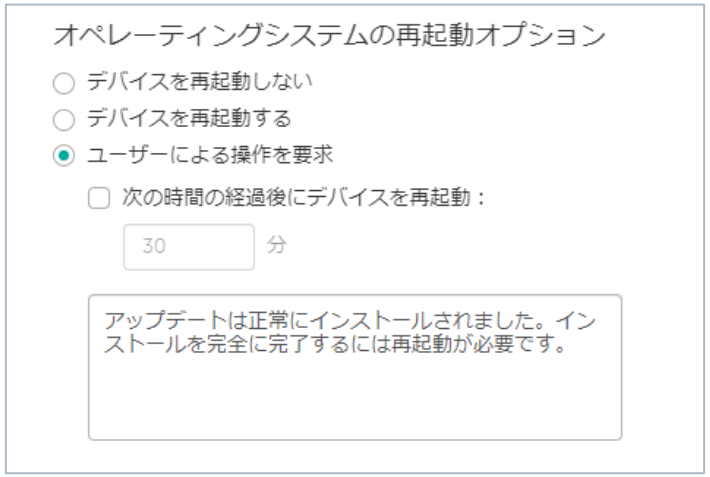
緊急度の高いパッチの適用を
柔軟に実行可能。

脆弱性の評価・パッチ管理

タイムゾーン指定など柔軟なオプションを用いてパッチをスケジュール適用。



再起動オプション



Kaspersky Endpoint Security Cloud
その他の機能

kaspersky

暗号化管理

Windows版

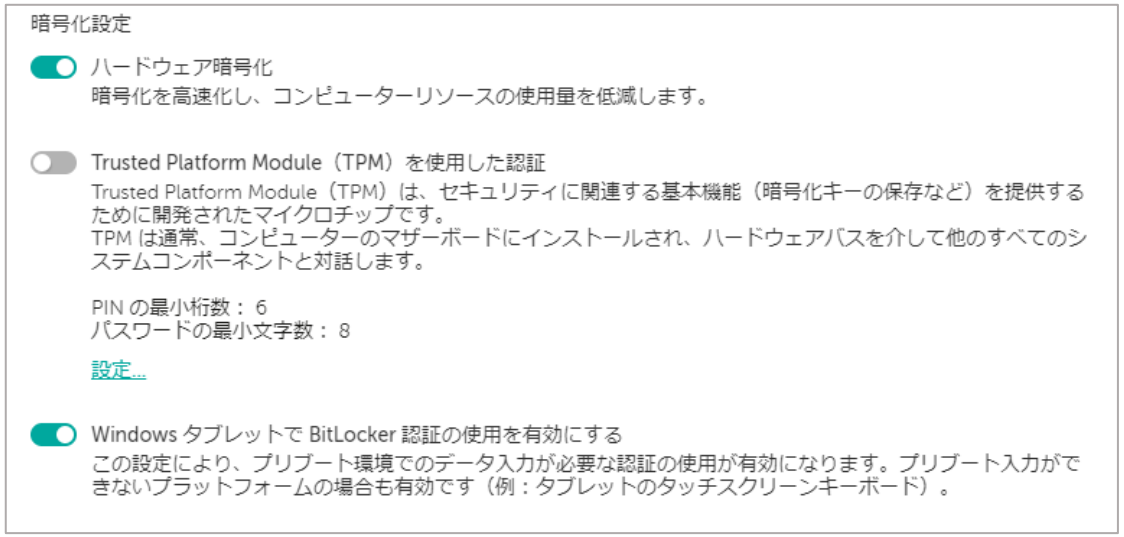
Bitlockerを強制的に有効にする。

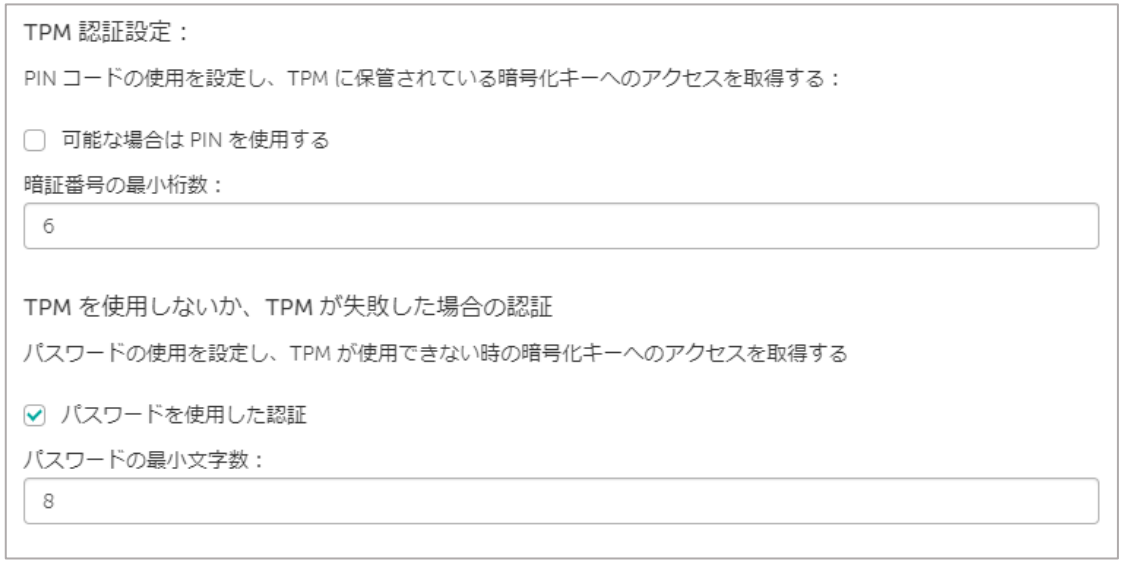
暗号化のオプション
・Trusted Platform Module（TPM）を使用。
（6 文字以上の PIN ）

・TPM認証に失敗した場合、パスワードを使用。
（ 8 文字以上の長さのパスワード）

TPM認証を設定せず、パスワード認証だけに
することも可能。

Windows Server OSで暗号化を使用するには
Bitlockerをインストールする必要があります。





暗号化管理

KES Cloud Plus, Proのみ

Windows版

・Bitlocker パスワードはエンドユーザーがそれぞれ設定。

端末側ポップアップメッセージ

・回復キーは KES Cloudに保存される。

ウェブコントロール

KES Cloud Plus, Proのみ

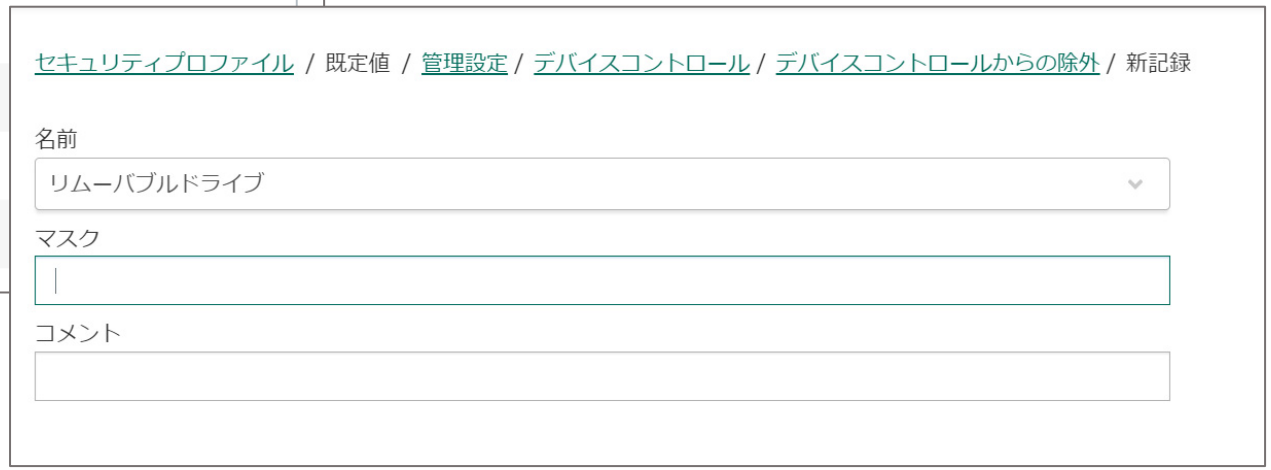
コンテンツカテゴリブロック

デバイスコントロール

KES Cloud Plus, Proのみ

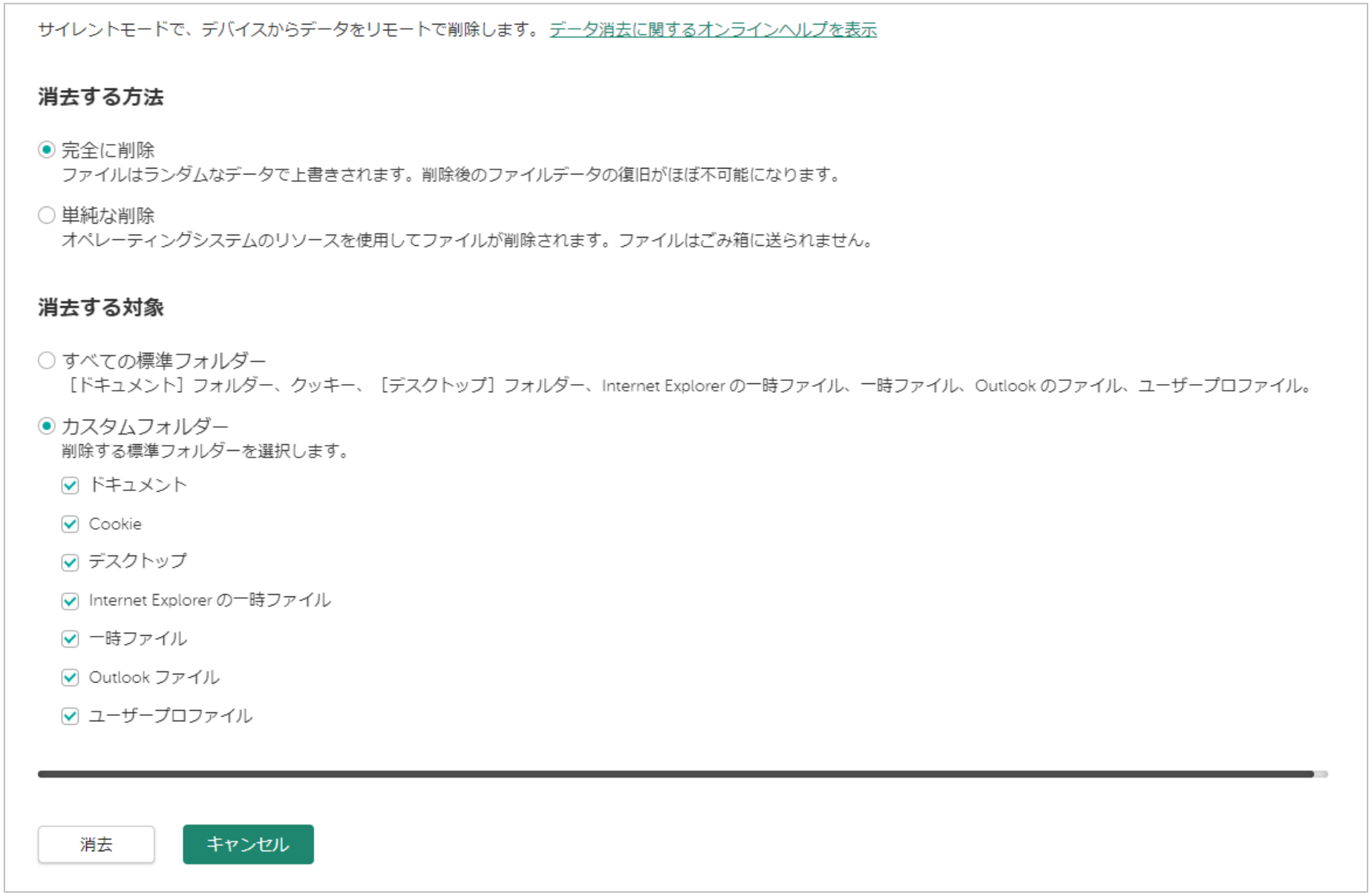
デバイス種別で許可・ブロックを設定。

モデルやシリアルNoでの除外設定可能



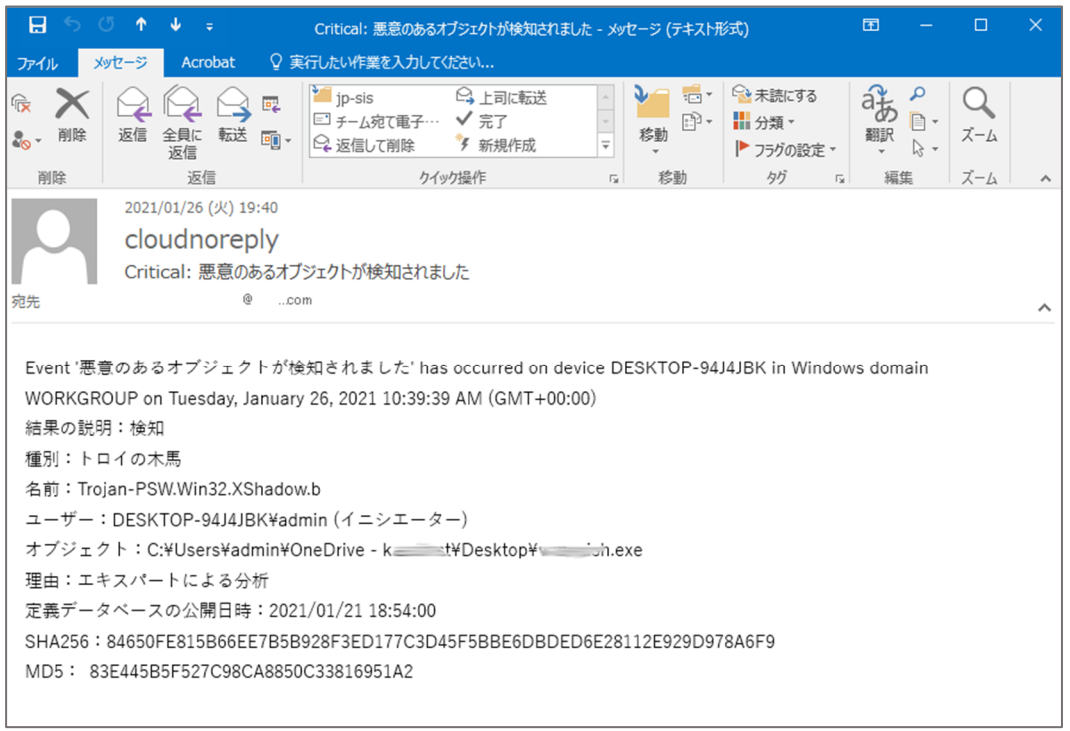
データ消去

KES Cloud Proのみ



アラートメール

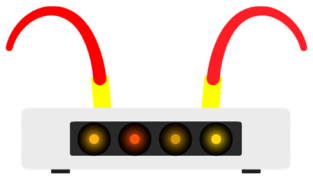
クラウドサービスなので、送信メールサーバーの準備不要。受信アドレスを登録するだけ。



Android

アンチウイルス、WebセキュリティとMDM機能を提供

使用出来るアクセスポイントの指定



GPS追跡

コマンド

日付 時間	名前	ステータス
2021/02/25 09:07	GPS 追跡 地図	実行済み
2021/02/25 09:07	GPS 追跡	送信済み

Google Map

kaspersky

Android

セキュリティプロファイル

- アンチウイルス
- フィッシングサイトブロック
- 悪意のあるサイトアクセスブロック
- Webコンテンツカテゴリ
- 画面ロック（パスワード強制）
- 使用出来るアクセスポイントの指定
- カメラ・Wi-Fi・Bluetoothの禁止
- アプリケーション
  - インストール・削除中のイベント生成
  - 許可ルール・禁止ルール（ブロック・レポートのみ）
- KES for Android削除禁止

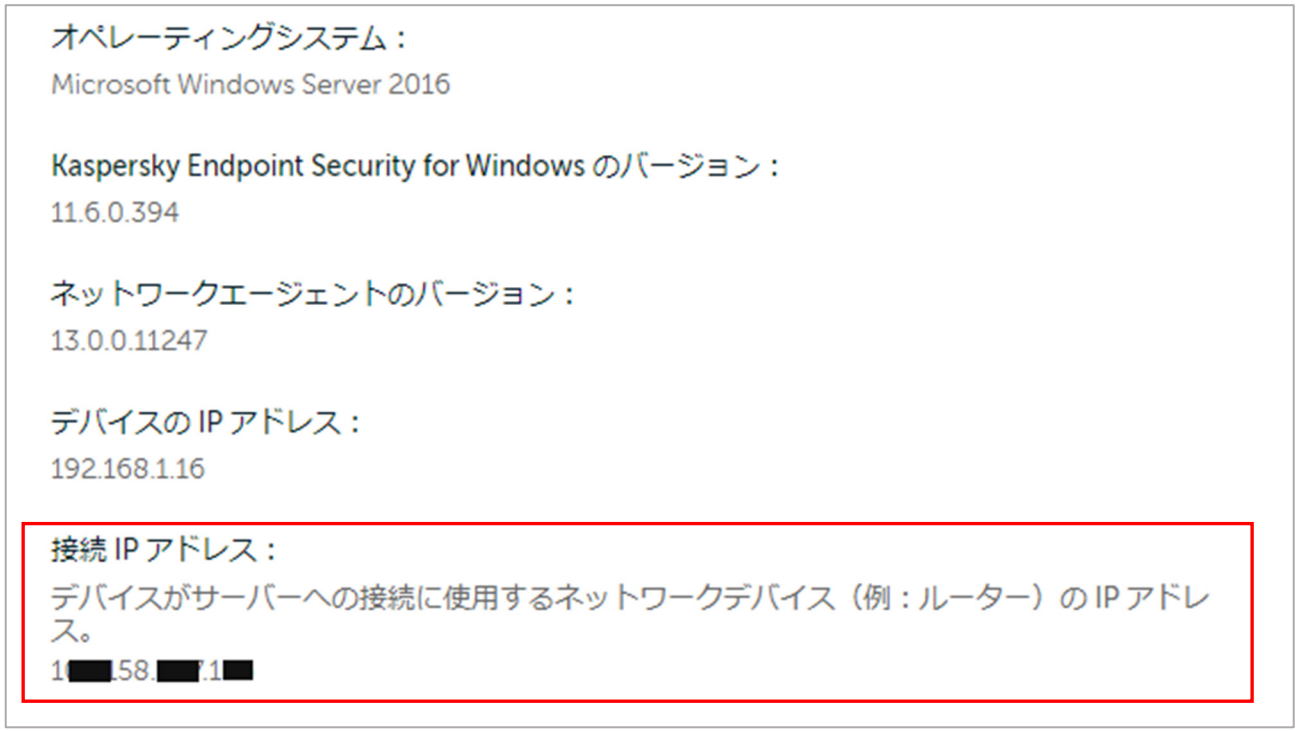
ワークスペースからの管理コマンド

- ロック・ロック解除
- 工場出荷時設定にリセット
- GPS追跡
- 遠隔アラーム
- 同期
- 管理を無効にする

kaspersky

管理コンソール 新機能

デバイスのIPアドレスだけでなく、
接続に使用されるグローバルアドレスを表示。



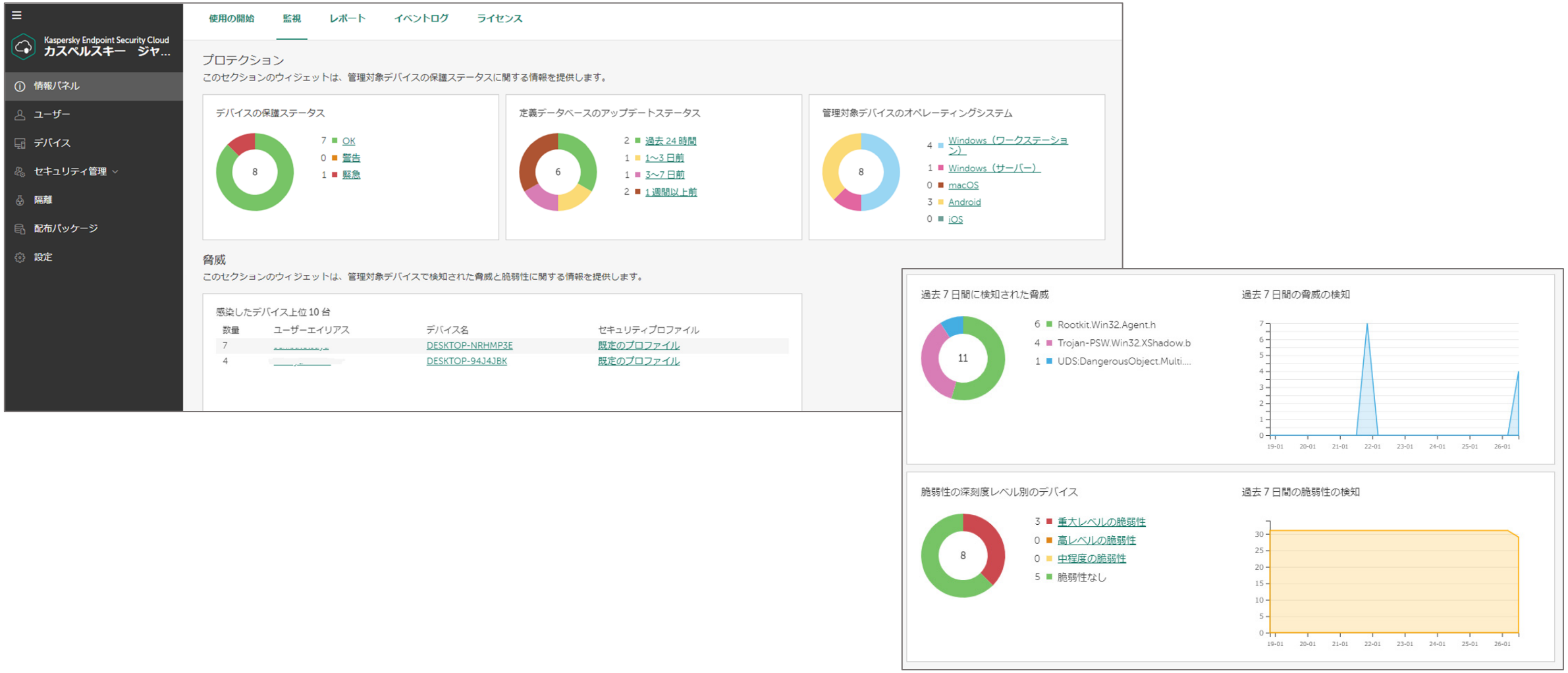
kaspersky

Kaspersky Endpoint Security Cloud
機能紹介

管理機能・インストール

情報パネル

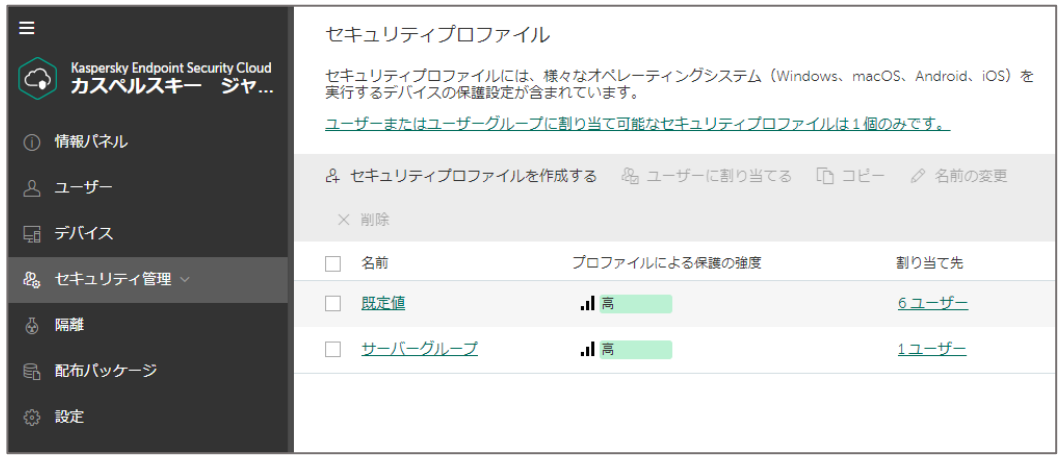
ヘルス状態を簡単に把握



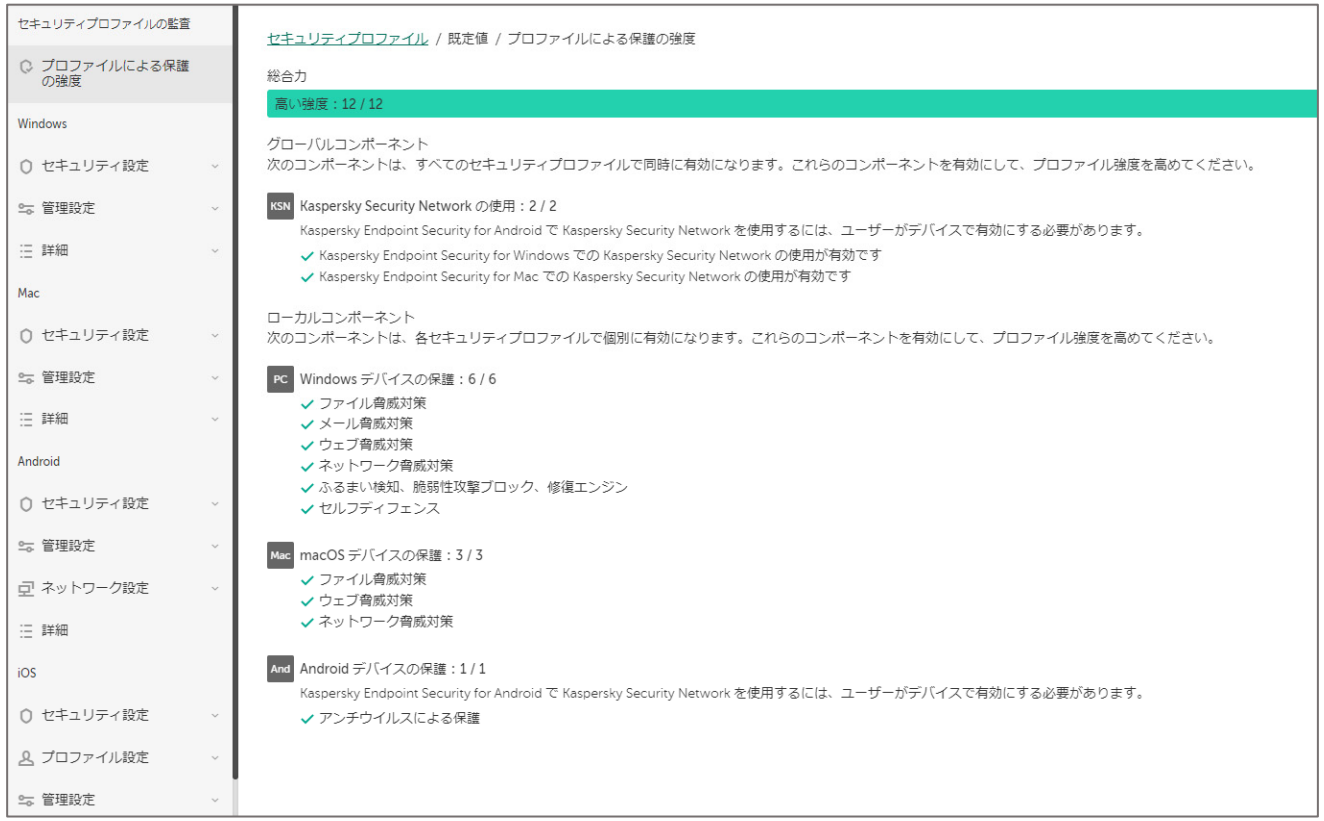
プロファイルによるセキュリティ設定

セキュリティプロファイル＝ポリシーによって、
デバイスの設定を行う。

セキュリティプロファイルはユーザーに割り当てられ、
最終的にユーザーに紐づけられたデバイスに設定が適用される。

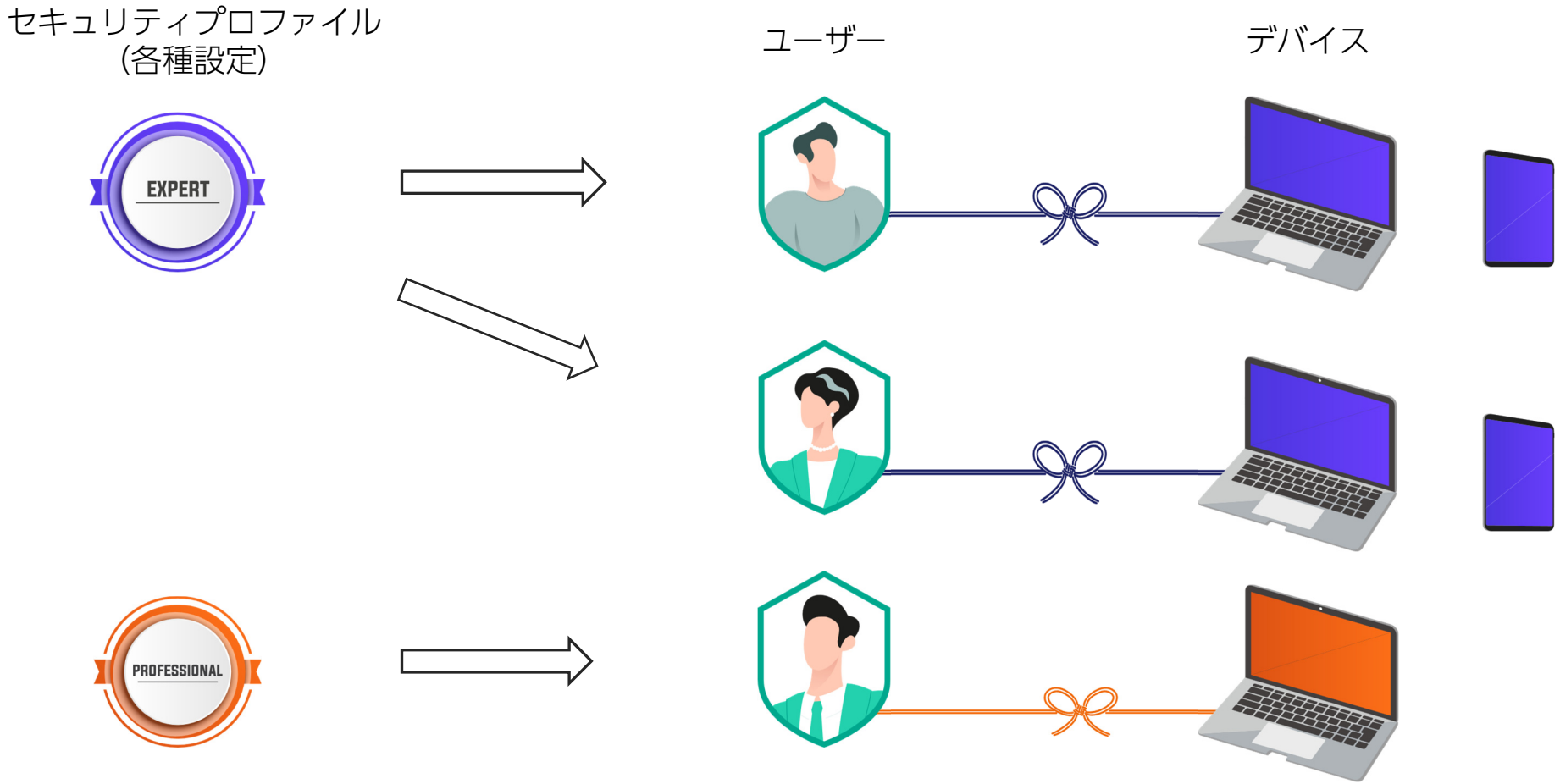


Windows、MAC、Android、iOS向け設定



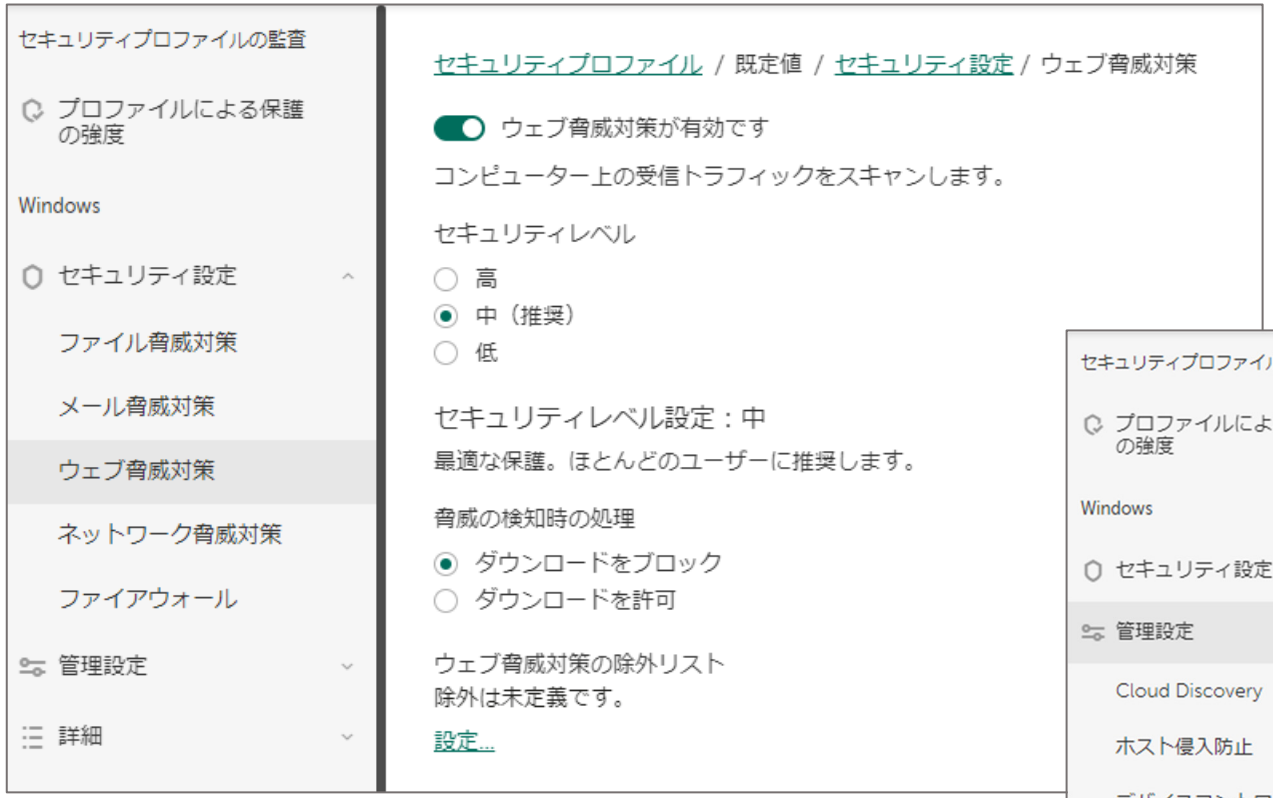
プロファイルによるセキュリティ設定

セキュリティプロファイルはユーザーに割り当てられ、
ユーザーに紐づいたデバイスに適用される。



kaspersky

プロファイルによるセキュリティ設定



プロファイルによるセキュリティ設定

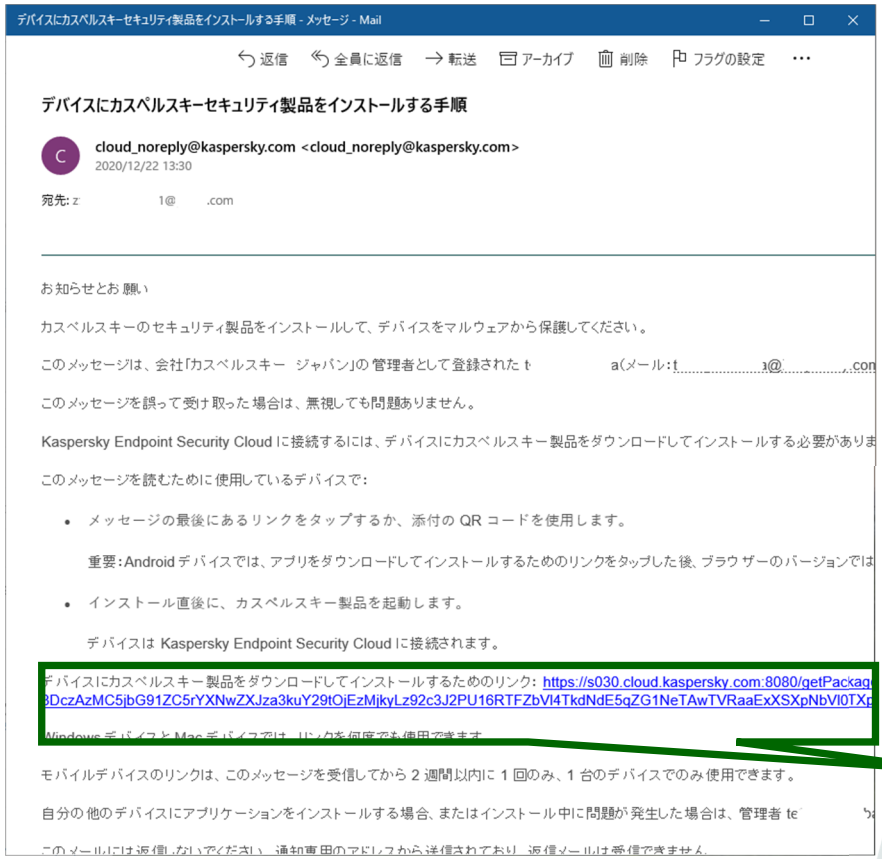
エンドポイントセキュリティ、ネットワークエージェントの両アプリケーションに
パスワード設定をすることにより、エンドユーザーによる不用意な削除、
マルウェアによるエンドポイントセキュリティ無効化の試みを防止。

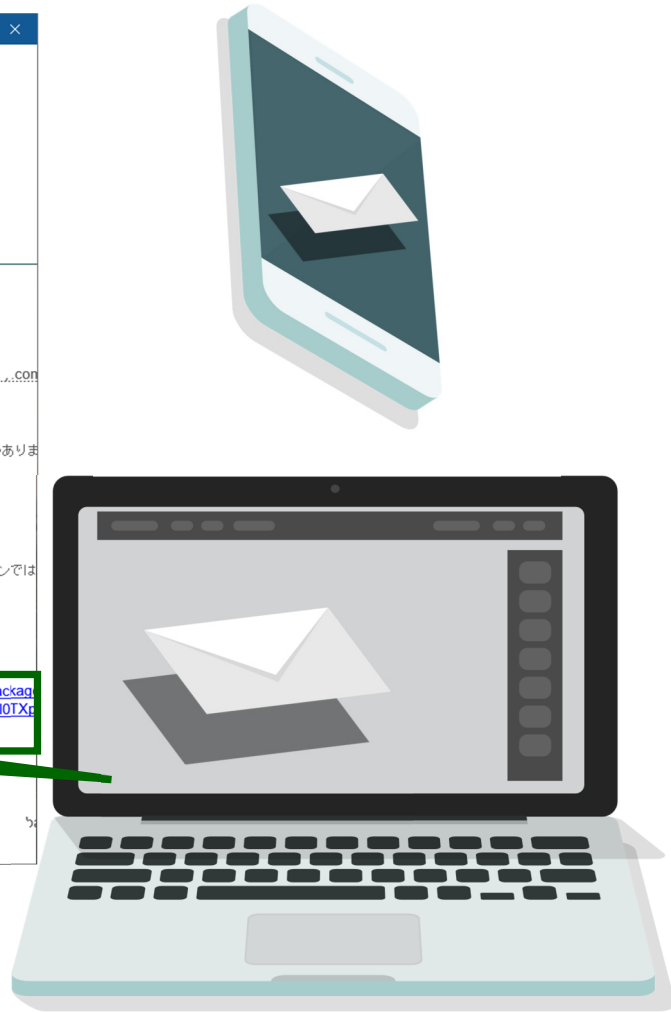
kaspersky

簡単インストール

管理コンソールでユーザーを登録。
メールでインストールリンクを送信。

受信したメールからリンククリック。
インストールは簡単に終了。





簡単インストール

Windows、Macには、そのまま利用可能なパッケージも準備。

Windows版は、Windows 設定からProxy設定を読み取り、自動でProxy経由の通信を行います。
パッケージにProxy設定を行いインストールした端末で、Proxyが使用出来ない場合は、直接通信を行います。

Active Directory グループポリシーを利用したインストール

配布パッケージを使用し、Active Directory グループポリシーを利用したインストールが可能。

インストーラーは Exe形式のため、グループポリシー スタートアップスクリプトを使用。

詳細はオンラインヘルプ参照
https://support.kaspersky.com/Cloud/1.0/ja-JP/147138.htm

Active Directory を使用したセキュリティ製品の導入

顧客のインフラストラクチャで Active Directory を使用している場合、Kaspersky Endpoint Security for Windows を複数のデバイスに同時に導入できます。

このセクションの手順には、事前に設定されたログオンスクリプトが含まれています。このスクリプトは、デバイスが起動するたびに自動的に実行され、Kaspersky Endpoint Security for Windows のインストールがデバイスで開始されているかどうかを確認します。開始されていない場合、スクリプトはサイレントモードでインストールを実行します。

Active Directory を使用して複数の *Windows* デバイスにセキュリティ製品を導入するには：

1. 必要なセキュリティ製品の配布パッケージをダウンロードし、セキュリティ製品を導入するデバイスがアクセスできる共有フォルダーにパッケージを保存します。

   完全パスにスペースが含まれていないフォルダーを選択してください。

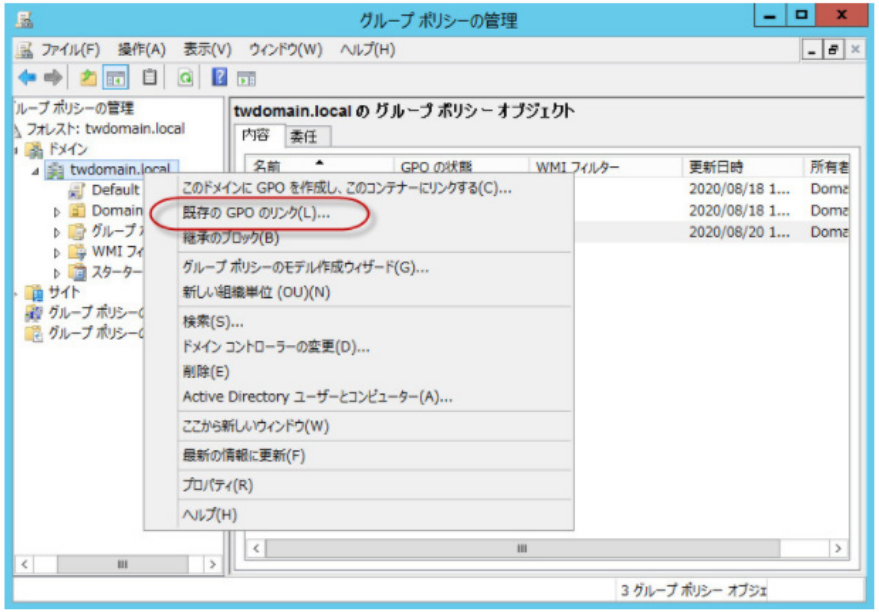
   パッケージ名にスペースが含まれている場合は、それを削除するか、アンダースコア（_）に変更します。

2. ダウンロードしたパッケージがあるフォルダーに移動し、次のスクリプトを使用して bat ファイルを作成します：

```
ECHO ON
set SHARE_PATH=<path to distribution package>
set PACKAGE_NAME=<name of distribution package>
set __KESCLOUD_ROOT_KEY="HKLM¥Software¥KasperskyLab¥KESCloud"
set __KESCLOUD_KEY_NAME="<name of registry entry>"
set __KESCLOUD_PACKAGE_FULL_PATH="%SHARE_PATH%¥%PACKAGE_NAME%"
set __KESCLOUD_PACKAGE_ARGUMENTS=-s
REG QUERY %__KESCLOUD_ROOT_KEY% /v %__KESCLOUD_KEY_NAME% | FIND "0x1"
IF %ERRORLEVEL% == 1 GOTO INSTALL
GOTO END
:INSTALL
REG ADD %__KESCLOUD_ROOT_KEY% /v %__KESCLOUD_KEY_NAME% /t REG_DWORD /f /D 1
%__KESCLOUD_PACKAGE_FULL_PATH% %__KESCLOUD_PACKAGE_ARGUMENTS%
:END
```

   説明：

   - <path to distribution package>：ダウンロードした配布パッケージが保存されている共有フォルダーへの実際のパスを記載します。引用符は使用しないでください。



Kaspersky Security for Microsoft Office 365
機能紹介

Kaspersky Security for Microsoft Office 365

Microsoft365の
コミュニケーション・コラボレーションツールを
保護するオールインワンソリューション。

スパムメール、フィッシング、マルウェア
BECからの保護。

- 柔軟な保護ポリシー:
  a) オンデマンドスキャンの任意実行
  b) 特定のユーザーグループへのスキャン
- E-Mailやファイルを消失させない – 検知したオブジェクトは隔離に移動。検索・リストアが可能。
- 単一の調査ポイント:
  Exchange Online Protection隔離と KSO365 隔離の
  統合されたビュー。

隔離されたE-Mailやファイルは、お客様のMS365に保管される。カスペルスキーには保管されない。

kaspersky

Kaspersky Security for Microsoft Office 365ライセンス

- ライセンスはメールボックスまたはOneDriveユーザー単位。
  1 メールボックスは 1 Microsoft 365 ユーザー。

- KSO365単体製品のライセンス数は上限無し。
  (KES Cloud Plus内でのKSO365ライセンス上限は1498)

Kaspersky Endpoint Security Cloud
Kaspersky Security for Microsoft Office 365

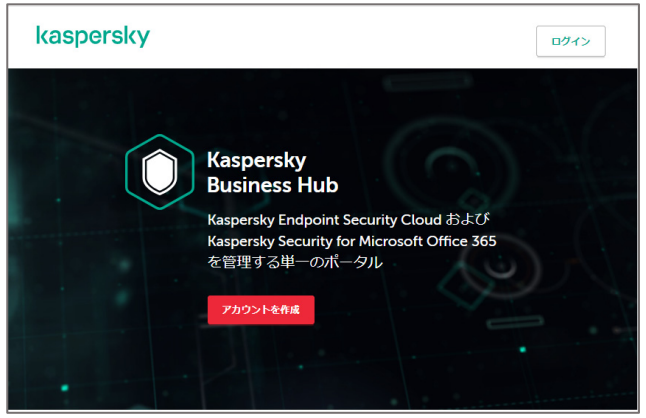
製品の評価・試用

製品の評価・試用

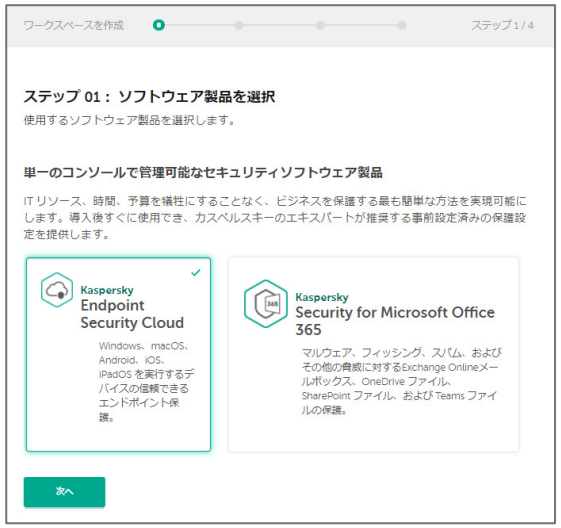
① https://cloud.kaspersky.com/ にアクセス。

② アカウントを作成し、ログイン。

③ ワークスペースを作成し、準備完了。

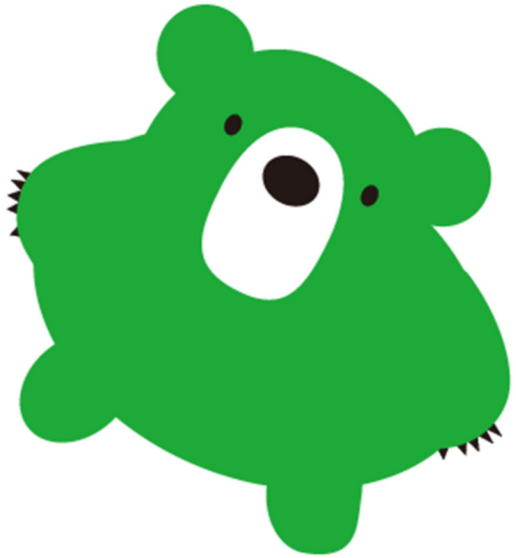


1. 評価期間は30日。
2. クレジットカード登録や契約などはありません。
3. 試用後、商用ライセンスを購入すれば、
   <u>引き続き使用することが出来ます</u>。



kaspersky

Thank you



03-3525-8530
jp-sales@kaspersky.com