

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できます。

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

クラウドディスクカバリー

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



ルートコース分析
(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 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

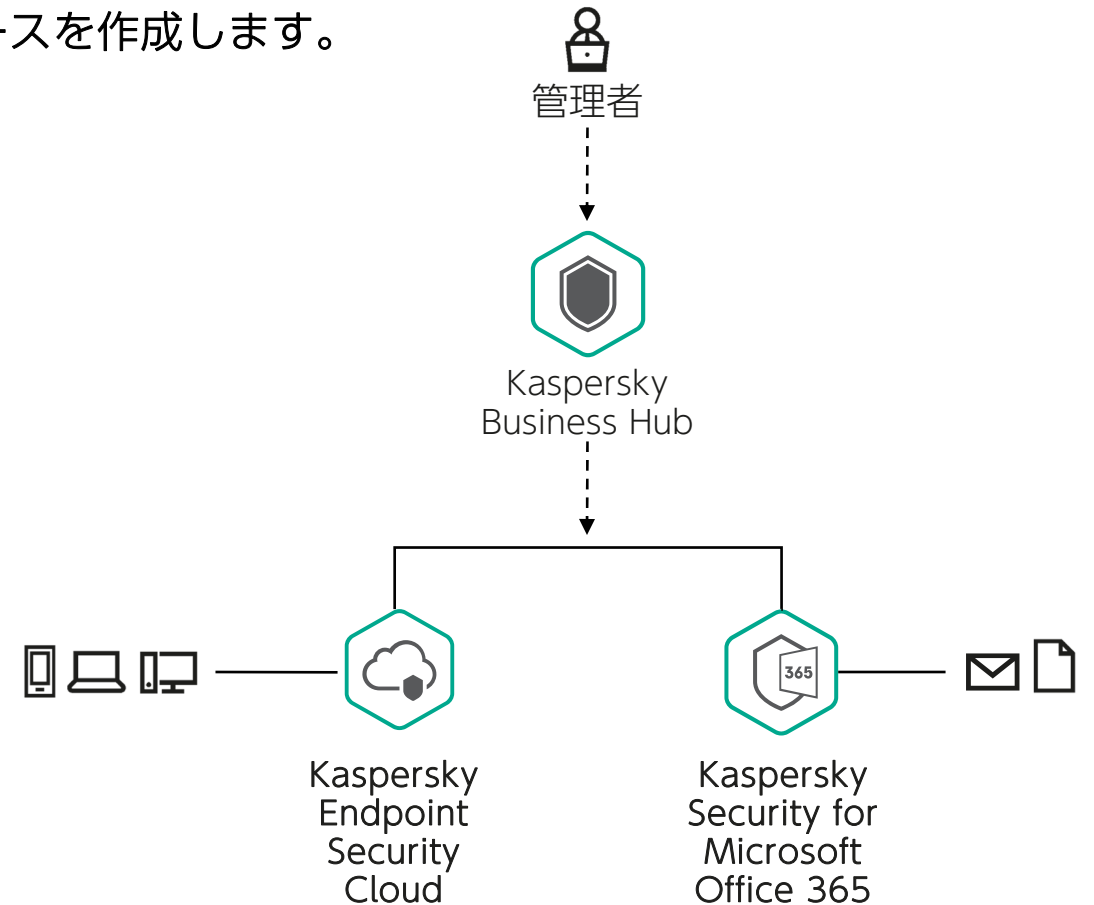
Kaspersky Business Hubによる統合管理

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。

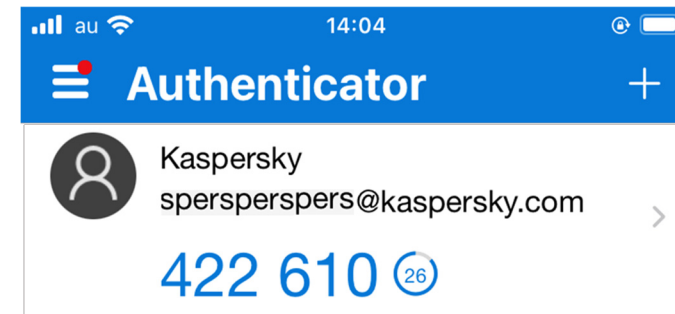


Kaspersky Business Hubによる統合管理

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。



KES Cloudライセンス

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。



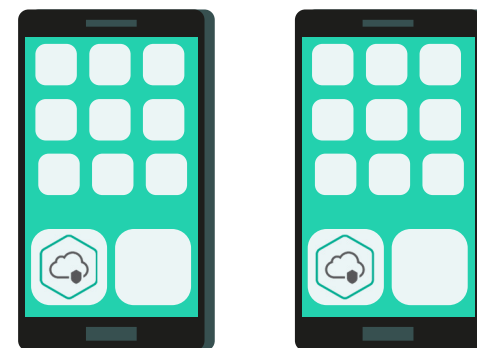
1 ユーザー

=



1 PC

+



2 モバイル端末
携帯・タブレット

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 $12 \div 2 = 6$ 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 $32 \div 2 = 16$ 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。

KES Cloudライセンス

Kaspersky Endpoint Security Cloud



Kaspersky Endpoint Security Cloud Plus、Pro



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 Endpoint Security Cloud Plus.




4 **20**

4 台のデスクトップ / ノート PC / ファイルサーバーお
よび 2 台のモバイルデバイスの使用

- 許可する 20 台のデスクトップ、ノート PC、および
ファイルサーバー
- 40 台の許可するモバイルデバイス

各ライセンスには、1 台のデスクトップ、ノート PC、
またはファイルサーバーと 2 台のモバイルデバイスが
含まれます。



Current license

License ID: [REDACTED]

Type: Commercial

Owner: [REDACTED]

Activation date: 16/12/2020 09:08:14 (UTC +09:00)

Expiration date: 18/12/2021 09:00:00 (UTC +09:00)

License limit: **30**

Licensed mailboxes: 3 out of 30

Licensed OneDrive users: 3 out of 30

[Replace](#)

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、各アプリケーションの資料もご参照ください。

脆弱性管理
エクスポイトブロック

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

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	○	○	○	—	—	—
ルートコース分析	—	○	○	—	—	—
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

ルートコース分析(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、ルートコース分析と同じ。

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

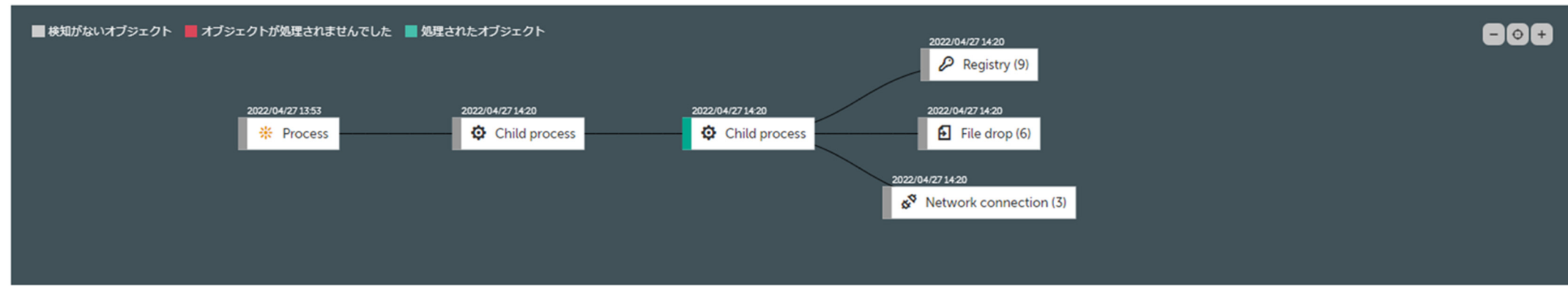
ルートコースズ分析(Root cause)

ルートコースズ分析の検知の詳細

[脅威の活動連鎖の図表を読み取る方法](#)

⊙ 処理済み: オブジェクトがブロックされました

検知日時: 2022/04/27 デバイスの所有者: _____ デバイス名: [KESC-PC03](#) セキュリティプロファイル: [Default](#)



作成日 パラメータ

2022/04/27 13:53	Process C:\Windows\explorer.exe		
2022/04/27 14:20	Child process C:\Users\admin\OneDrive - kas4test\デスクトップ\sw_test.exe		
	タイムスタンプ 2022/04/27 14:20	起動パラメータ "C:\Users\admin\OneDrive - kas4test\デスクトップ\sw_test.exe"	
	システム PID 8256	整合性レベル 高い整合性	
	ユーザーエイリアス KESC-PC03\admin	特権ユーザー はい	
2022/04/27 14:20	Child process C:\Users\admin\AppData\Local\Temp\sw_test.exe		
2022/04/27 14:20	Registry (9)		
2022/04/27 14:20	File drop (6)		
2022/04/27 14:20	Network connection (3)		

ルートコース分析(Root cause) 例2

2022/04/27 14:19	Child process C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
2022/04/27 14:19	Child process C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
2022/04/27 14:19	タイムスタンプ システム PID ユーザーエイリアス	2022/04/27 14:19 5328 KESC-PC03\admin	起動/パラメータ 整合性レベル 特権ユーザー
2022/04/27 14:19	Registry ¹³		
2022/04/27 14:19	File drop ¹⁰⁰⁰		
2022/04/27 14:19	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF18d7dd.TMP		
	名前 作成日	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF18d7dd.TMP 2022/04/27 14:19	信頼チェックの結果 変更日
			信頼しない 2022/04/27 14:19
2022/04/27 14:19	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\1f7db087-3918-4a15-846a-aa1a41a1931b.tmp		
	名前 作成日	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\1f7db087-3918-4a15-846a-aa1a41a1931b.tmp 2022/04/27 14:19	信頼チェックの結果 変更日
			信頼しない 2022/04/27 14:19
2022/04/27 14:19	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF18dcfd.TMP		
	名前 作成日	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF18dcfd.TMP 2022/04/27 14:19	信頼チェックの結果 変更日
			信頼しない 2022/04/27 14:19

File drop			
https://m	z/?te=he4tgm	ddf42tamzz	
処理	ブロック	日時	2022/04/27 14:20
脅威	not-a-virus:HEUR:AdWare.Script.Pusher.gen	オブジェクト名	https://m z/?te=he4tgm ddf42tamzz
スキャンモード	ダウンロード	オブジェクト種別	ファイル
MD5	c72d8aa94b07d25ebc47b01a51e16e8f	SHA256	89b360b8d22aec8de97ae498ff96fd019f66baa92f458979ddb312e1611f304a
ダウンロード URL	https://m z/?te=he4tgmrv 3ddf42tamzz	プログラム	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
ダウンローダー MD5	b3aa6a8bd3c89ca06706d81a0838776e	ダウンローダー SHA256	bfa534bc933726b6ce3b2cf7939587383e9acb535bd715de52b02f894134b4fc

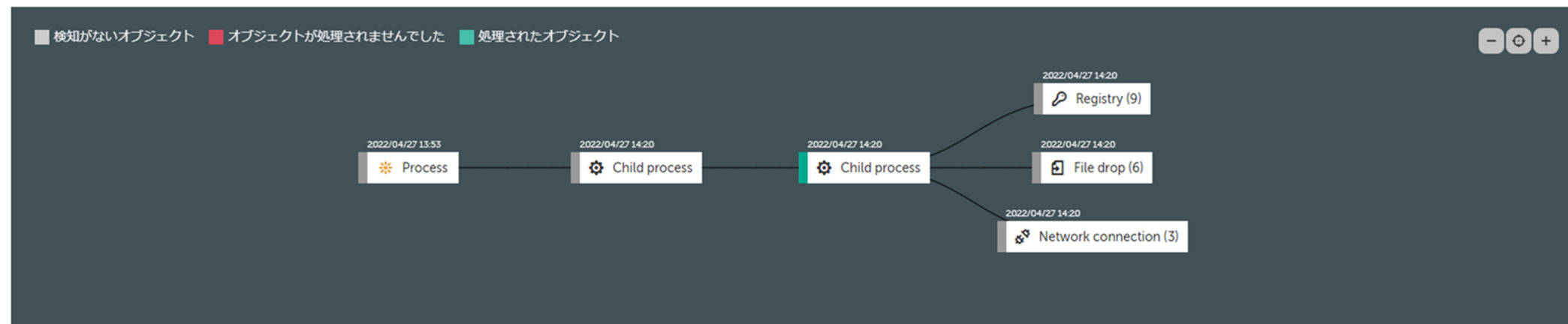
KES Cloud Pro Endpoint Detection and Response

脅威の活動連鎖の図表

[脅威の活動連鎖の図表を読み取る方法](#)

🟢 処理済み: オブジェクトがブロックされました

検知日時: 04/27/2022 デバイスの所有者: _____ デバイス名: [KESC-PC03](#) セキュリティプロファイル: [Default](#) ...



作成日

パラメータ

作成日	パラメータ	
2022/04/27 13:53	Process C:\Windows\explorer.exe	...
2022/04/27 14:20	Child process C:\Users\admin\OneDrive - kas4test\デスクトップ\sw_test.exe	...
2022/04/27 14:20	Child process C:\Users\admin\AppData\Local\Temp\sw_test.exe	loC スキャンに追加 実行を防止 隔離に移動
2022/04/27 14:20	Registry ⁽⁹⁾	...
2022/04/27 14:20	File drop ⁽⁶⁾	...

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

🟢 処理済み：オブジェクトがブロックされました
検知日時： 2022/04/27 デバイスの所有者： _____ **デバイス名： KESC-PC03** セキュリティプロファイル： Default ...

■ 検知がないオブジェクト ■ オブジェクトが処理されませんでした ■ 処理されたオブジェクト

2022/04/27 13:33 2022/04/27 14:20 2022/04/27 14:20

🌟 Process ⚙️ Child process ⚙️ Child process

デバイスを...

デバイスを分離 KESC-PC03

分離されたデバイスのロックを自動的に解除するまでの時間：

8 時間

! 分離するには注意してください。デバイスの所有者にこの処理を実行することを通知してください。

デバイスを分離 キャンセル

Kaspersky Endpoint Security Cloud 推し機能 その2 Cloud Discovery



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。

The screenshot displays the Kaspersky Endpoint Security Cloud management console. The left sidebar contains navigation options: 情報パネル, ユーザー, デバイス, セキュリティ管理, 隔離, 配布パッケージ, and 設定. The main content area is titled 'Cloud Discovery' and includes a donut chart showing 90 total services, with 49 blocked. A table lists the top 5 services: Google ドライブ (33), Box (9), and OneDrive (7). On the right, a detailed view of the 'SNS' category shows 14 services, with one blocked. A dropdown menu for 'Facebook' is open, showing options for '許可' (Allow), '許可' (Allow), and 'ブロック' (Block).

KES Cloud Plus, Proではブロックが可能

Cloud Discovery が有効です

Windows デバイスで使用されるクラウドサービスを監視し、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します。

暗号化された接続のスキャンを有効にすることを推奨します。これにより、クラウドサービスへのアクセス試行の検知、および不要と思われるクラウドサービスへのアクセスのブロックの効率が向上します。

会社で使用しているクラウドサービスが見つからない場合 [お知らせください](#)

カテゴリまたはサービスを探す

名前	操作
SNS	14 個中 1 個のサービスがブロック対象です カテゴリ全体をブロック
ASKfm	許可
Facebook	許可 ブロック
Foursquare	許可
Instagram	許可
LinkedIn	ブロック

ウィジェットからブロックを簡単に実行

使用の開始 **監視** レポート イベントログ ライセンス

ウィジェット

各ウィジェットには、すべての管理対象デバイスに関する情報が含まれています。特に指定がない限り、ウィジェットには過去 30 日間の情報が表示されます。

Cloud Discovery

Windows デバイスでよく使用されるクラウドサービスを監視し、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します。
会社で使用しているクラウドサービスが見つからない場合 [お知らせください](#)

Cloud Discovery 情報



4 ■ メッセンジャー
2 ■ ファイル共有

表示される数には、既にブロックされているサービスが含まれる場合があります。

上位 5 つのサービス

3	Microsoft Teams	許可
1	Skype	許可

上位 10 サービスのユーザー [レポートに移動](#)

強度	ユーザーエイリアス	デバイス名	サービス名	セキュリティプロファイル	アクセスのステータス
1	test	KESC-PC03	Skype	暗号テスト用	🟢 許可 ^

⊗ プロファイルでサービスをブロックする

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れます。

管理

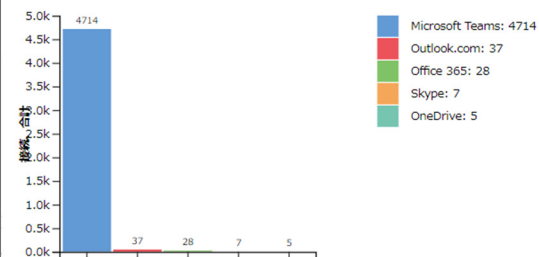
[デバイスコントロールによる検知](#) [PDF | CSV]
このレポートには、デバイスコントロールによって検知された接続デバイスが表示されます。

[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）へのアクセス試行が表示されます。

Cloud Discovery : クラウドサービスへのアクセスの成功

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	ブラウザからの接続	クライアントアプリケーションからの接続	
ki	iki	DESKTOP-EJICQDR	その他	Office 365	28	0
t	a	DESKTOP-94J4JBK	ファイル共有	OneDrive	0	1
k	jki	DESKTOP-EJICQDR	ファイル共有	OneDrive	0	2
si	i	DESKTOP-NRHMP3E	ファイル共有	OneDrive	0	2
ki	iki	DESKTOP-EJICQDR	メール	Outlook.com	36	1
k	uki	DESKTOP-EJICQDR	メッセージャー	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

The screenshot shows the '脆弱性診断とパッチ管理' (Vulnerability Assessment and Patch Management) section in the KES Cloud Plus/Pro interface. The left sidebar contains navigation options: 情報パネル, ユーザー, デバイス, セキュリティ管理 (selected), セキュリティプロファイル, 脆弱性診断とパッチ管理 (checked), Data Discovery, Endpoint Detection and Response, and 暗号化. The main content area has a title and a description: 'ユーザーの Windows デバイスで検知されたソフトウェアの脆弱性、およびデバイスにインストール済みのアプリケーションのアップデート。検知された脆弱性を修正するパッチも含まれます。' Below this are three cards: 1. '脆弱性' (Vulnerabilities) with detection frequency '毎日、17:20', 30 uncorrected items, and 1 corrected item. 2. 'パッチとアップデート' (Patches and Updates) with status 'インストールが計画されていません', 27 items not installed, and 0 items installed. 3. 'レポート' (Reports) with a description and a 'レポートに移動' button.

KES Cloudの場合

The screenshot shows the '脆弱性診断とパッチ管理' (Vulnerability Assessment and Patch Management) section in the KES Cloud interface. The left sidebar contains navigation options: 情報パネル, ユーザー, デバイス, セキュリティ管理 (selected), セキュリティプロファイル, 脆弱性診断とパッチ管理 (checked), and 設定. The main content area has a title and a description: 'ユーザーの Windows デバイスで検知されたソフトウェアの脆弱性、およびデバイスにインストール済みのアプリケーションのアップデート。検知された脆弱性を修正するパッチも含まれます。' Below this are three cards: 1. '脆弱性' (Vulnerabilities) with detection frequency '毎日、17:20', 30 uncorrected items, and 1 corrected item. 2. 'パッチとアップデート' (Patches and Updates) with status 'インストールが使用できません', a description about automatic installation settings, and a 'ファイルに関する情報を表示' button. 3. 'レポート' (Reports) with a description and a 'レポートに移動' button.

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。

- 情報パネル
- ユーザー
- デバイス
- セキュリティ管理
- セキュリティプロファイル
- 脆弱性診断とパッチ管理
- Data Discovery
- Endpoint Detection and Response
- 暗号化
- ヘルプ
- サポート
- フィードバックの送信
- 法律上の通知
- 契約書

脆弱性診断 (31) [戻る](#)

Windows を実行中の管理対象デバイスで検知されたソフトウェアの脆弱性。
レポートで見つけた脆弱性の全体的な情報。 [「脆弱性」レポートを表示する](#)

未修正 30 修正済み 1

深刻度 修正のステータス アプリケーション種別 検知のスケジュール
すべて すべて すべて 毎日、17:20 変更

検知の設定

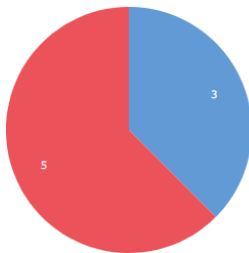
深刻度	修正のステータス	脆弱性	アプリケーション	デバイスで修正済み
緊急	計画していない	KLA12602	Windows 11	0/2
緊急	計画していない	KLA20117		0/1
緊急	計画していない	KLA12502		0/2
緊急	計画していない	KLA12470	Mozilla Firefox	0/1
緊急	計画していない	KLA10682	Adobe Reader X	0/1
緊急	計画していない	KLA10575	Adobe Reader X	0/1

レポートを管理者にメールで定期配信可能

脆弱性

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。 [CSVファイルを作成](#) [PDFファイルを作成](#)

緊急レベルの脆弱性があるデバイス： 5. 高レベルの脆弱性があるデバイス： 0. 中程度の脆弱性を持つデバイス： 0. 脆弱性が検知されていないデバイス： 3.



- 緊急レベルの脆弱性があるデバイス
- 高レベルの脆弱性があるデバイス
- 中程度の脆弱性を持つデバイス
- 脆弱性が検知されていないデバイス

詳細

レポート生成日時：2023/01/20 15:24

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

深刻度	製造元	アプリケーション	バージョン	デバイス	脆弱性名	オブジェクト	検知時間	パッチが適用可能です
Critical	Adobe Systems	Adobe Reader X	10.1.4	KESC-PC04	KLA10005	C:\Program Files (x86)\Adobe\Reader 10.0\Reader\	2021/05/31 13:19	Yes
Critical	Adobe Systems	Adobe Reader X	10.1.4	KESC-PC04	KLA10734	C:\Program Files (x86)\Adobe\Reader 10.0\Reader\	2021/05/31 13:19	Yes
Critical	Adobe Systems	Adobe Reader X	10.1.4	KESC-PC04	KLA10004	C:\Program Files (x86)\Adobe\Reader	2021/05/31 13:19	Yes

脆弱性診断 (31)
[< 戻る](#)

Windows を実行中の管理対象デバイスで検知されたソフトウェアの脆弱性。
 レポートで見つけた脆弱性の全体的な情報。 [「脆弱性」レポートを表示する](#)

未修正 30 修正済み 1

深刻度 [すべて](#) ↓ 修正のステータス [すべて](#) ↓ アプリケーション種別 [すべて](#) ↓ 検知のスケジュール
 毎日、17:20 [変更](#)

⚙️ 検知の設定 🔍 検索

深刻度	修正のステータス	脆弱性	アプリケーション	デバイスで修正済み
🚨 緊急	計画していない	KLA10628	Adobe Reader X	0/1
🚨 緊急	計画していない	KLA11273	Adobe Reader X	0/1
🚨 緊急	計画していない	KLA10457	Adobe Reader X	0/1
🚨 緊急	計画していない	KLA10004	Adobe Reader X	0/1
🚨 緊急	計画していない	KLA10734	Adobe Reader X	0/1

どの端末に脆弱性が残っているかを一覧表示。

脆弱性が検知されたデバイス (1) ✕

脆弱性: [KLA10004](#)
 アプリケーション: Adobe Reader X
 アプリケーションのバージョン: 10.1.4

デバイスを表示: [すべて 1](#) | [計画していない \(1\)](#) | [計画中 \(0\)](#) | [進行中 \(0\)](#) | [操作が必要です \(0\)](#) | [修正エラー \(0\)](#) | [修正済み \(0\)](#)

修正のステータス	デバイス名	デバイスの所有者	グループ	推奨事項
計画していない 自動修正は使用できません	KESC-PC04	[redacted]	-	修正する方法

脆弱性に対し、パッチ適用を実行。

パッチの管理 (77)
[< 戻る](#)

Windows を実行中のユーザーデバイスにインストールされたアプリケーションのアップデート (デバイスで検知されたソフトウェアの脆弱性を修正するパッチを含む)。

'インストールされていません' 77 インストール済み 0

インストールステータス	重要度	アプリケーション種別	インストールスケジュール
すべて ↓	すべて ↓	すべて ↓	無効 設定
<input checked="" type="radio"/> 承認	<input checked="" type="radio"/> 承認却下	<input checked="" type="radio"/> 設定	
<input type="checkbox"/> インストールステータス ▲	アップデート	重要度 ⓘ	デバイスにインストール済み
<input type="checkbox"/> 無効	7-Zip 21.07 セキュリティパッチ	🚨 緊急	0 / 2
<input type="checkbox"/> 無効	2022-04 x64 ベース システム用 Windows 10 Version 21H1 の累積更新プログラム (KB5012599) セキュリティパッチ	🚨 緊急	0 / 1
<input type="checkbox"/> 無効	Windows 10、バージョン 21H2 の機能更新プログラム セキュリティパッチ	🚨 緊急	0 / 1
<input type="checkbox"/> 無効	Feature update to Windows 10, version 21H2 セキュリティパッチ	🚨 緊急	0 / 1

インストールステータス	重要度	アプリケーション種別
すべて ↓	すべて ▲	すべて ↓
<input checked="" type="radio"/> 承認	<input checked="" type="radio"/> 承認却下	<input checked="" type="radio"/> 設定
<input type="checkbox"/> インストールステータス ▲	アップデート	重要度 ⓘ
<input type="checkbox"/> 無効	7-Zip 21.07 セキュリティパッチ	🚨 緊急
<input type="checkbox"/> 無効	2022-04 x64 ベース システム用 Windows 10 Version 21H1 の累積更新プログラム	🚨 緊急

すべて

緊急

高

中

低

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]@[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]@[redacted].com	—	アップデートのインストール設定へ移動

パッチの管理 (77)
Windows を実行中のユーザーデバイスにインストールされたアプリケーションを修正するパッチを含む。

インストールされていません 77 インストール済み 0

インストールステータス	重要度	アプリケーション種別
すべて ↓	すべて ↓	すべて ↓

承認 承認却下 設定

インストールステータス ▲ アップデート

<input type="checkbox"/> 無効	7-Zip 21.07 セキュリティパッチ
<input type="checkbox"/> 無効	2022-04 x64 ベース システム用 Windows 10 Version 21H1 の累積更新プログラム (KB5012599) セキュリティパッチ
<input type="checkbox"/> 無効	Windows 10、バージョン 21H2 の累積更新プログラム セキュリティパッチ
<input type="checkbox"/> 無効	Feature update to Windows 10, version 21H2 セキュリティパッチ
<input type="checkbox"/> 無効	2022-12 Cumulative Update for Windows 10, version 21H2 for x64-based Systems (KB5021234)

アップデートのプロパティ

全般的なプロパティ

アップデート
7-Zip 21.07
セキュリティパッチ

アプリケーション
7-Zip

重要度 ⓘ
緊急

インストールの詳細

インストールステータス
無効

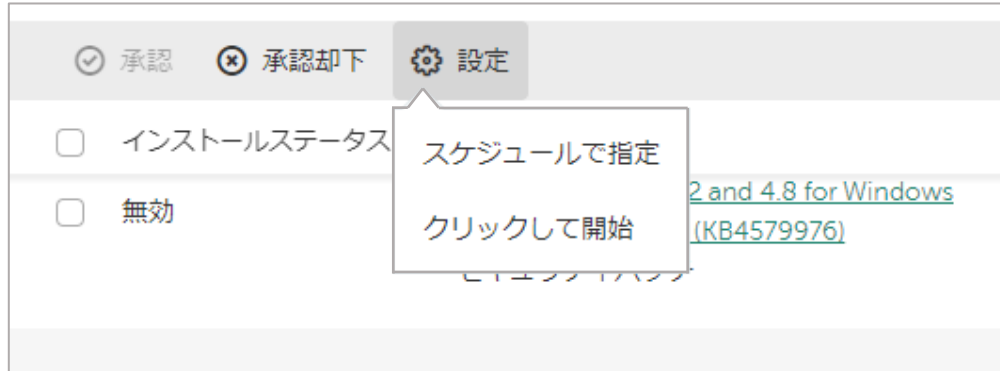
デバイスにインストール済み
0 / 2

自動的にインストール
アップデートは、Windows を実行しているすべての管理対象デバイスの全般的なインストール設定に従ってインストールされます。
[アップデートのインストール設定へ移動](#)

テストのために手動でインストール ▲
複数のデバイスでテストするために、手動でアップデートをインストールできます
[ダウンロード](#)

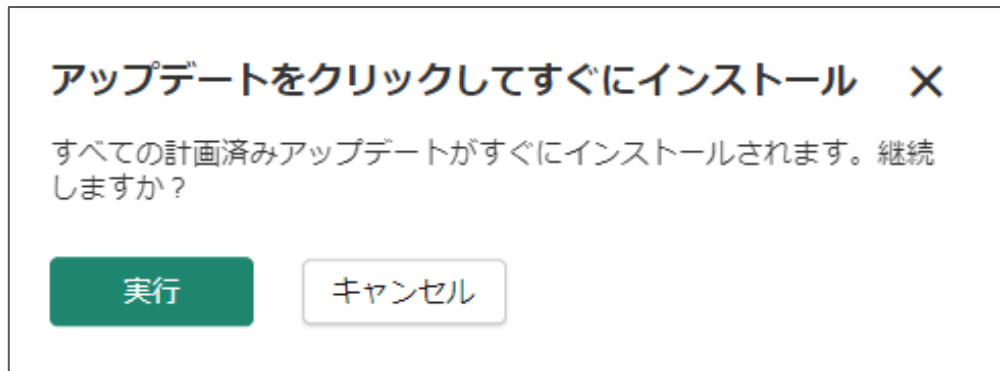
OK

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。



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。



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。

アップデートのインストール設定

インストール方法
承認されたアップデートのみをインストール

デバイス種別
すべてのデバイス

インストールスケジュール
保護されたデバイスがスケジュールされた時間にオフラインの場合、デバイスがオンラインになるとすぐにアップデートのインストールが実行されます。

毎週

曜日
月曜日

開始時刻
00:00:00

タイムゾーン
(UTC+09:00) Tokyo, Seoul

インストール設定
 デバイスの再起動時またはシャットダウン時にインストールを開始する

デバイス種別

すべてのデバイス

すべてのデバイス

ワークステーションのみ

サーバーのみ

再起動オプション

オペレーティングシステムの再起動オプション

デバイスを再起動しない

デバイスを再起動する

ユーザーによる操作を要求

次の時間の経過後にデバイスを再起動：
30 分

アップデートは正常にインストールされました。インストールを完全に完了するには再起動が必要です。

Kaspersky Endpoint Security Cloud その他の機能

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。

暗号化設定

- ハードウェア暗号化
暗号化を高速化し、コンピューターリソースの使用量を低減します。
- Trusted Platform Module (TPM) を使用した認証
Trusted Platform Module (TPM) は、セキュリティに関連する基本機能 (暗号化キーの保存など) を提供するために開発されたマイクロチップです。
TPM は通常、コンピューターのマザーボードにインストールされ、ハードウェアバスを介して他のすべてのシステムコンポーネントと対話します。

PIN の最小桁数 : 6
パスワードの最小文字数 : 8
[設定...](#)
- Windows タブレットで BitLocker 認証の使用を有効にする
この設定により、プリブート環境でのデータ入力が必要な認証の使用が有効になります。プリブート入力できないプラットフォームの場合も有効です (例 : タブレットのタッチスクリーンキーボード) 。

TPM 認証設定 :

PIN コードの使用を設定し、TPM に保管されている暗号化キーへのアクセスを取得する :

- 可能な場合は PIN を使用する

暗証番号の最小桁数 :

TPM を使用しないか、TPM が失敗した場合の認証

パスワードの使用を設定し、TPM が使用できない時の暗号化キーへのアクセスを取得する

- パスワードを使用した認証

パスワードの最小文字数 :

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

The screenshot shows a window titled "Kaspersky Endpoint Security" with the following text and fields:

BitLocker ドライブ暗号化技術でのドライブ暗号化用のパスワード

このコンピューター上のハードドライブが暗号化される前に、パスワードを入力する必要があります。

パスワードを入力してください :

パスワードの確認 :

OK

- 回復キーは KES Cloudに保存される。

The screenshot shows the management console for device "デバイス (18) / KESC-PC03". It includes a "戻る" button and a "デバイス名を変更" button. The following information is displayed:

- 定義データベースの最終アップデート日 : 2021/09/24 12:03
- サーバーへの最終接続 : 2021/09/24 12:35
- ネットワークに最後に表示された時間 : 2021/09/24 12:35
- 定義データベース : 定義データベースのアップデートは必要ありません
- オペレーティングシステム : Microsoft Windows 10
- Kaspersky Endpoint Security for Windows のバージョン : 11.6.0.394
- 暗号化回復キー :**
 - ▼ ローカルドライブ : C (起動ドライブ)
 - 回復キー ID : {1F8DF266-6C78-4377-9020-3260B1B415E9}
 - 回復キー : 589347-672870-575806-252626-044561-078463-348557-329483

コンテンツカテゴリブロック

「0002」セキュリティプロファイル設定

セキュリティプロファイルの監査

プロファイルによる保護の強度

Windows

セキュリティ設定

管理設定

Cloud Discovery

ホスト侵入防止

デバイスコントロール

ウェブコントロール

暗号化

詳細

Mac

セキュリティ設定

管理設定

セキュリティプロファイル / 0002 / 管理設定 / ウェブコントロール / Web サイトアクセスルール / 新記録

スキャン対象のカテゴリを選択し、これらのカテゴリでスキャンするデータ種別を指定します

指定した設定が同時に適用されます。

名前:

コンテンツカテゴリ

コンテンツカテゴリが定義されていません。すべての種別のコンテンツをスキャンします。

設定...

選択したカテゴリのコンテンツをフィルタリング

本製品はすべての種別のデータをスキャンします。

設定...

URL

選択したカテゴリ内でスキャンする URL を指定します

設定...

処理

許可

ブロック

警告する

「0002」セキュリティプロファイル設定

セキュリティプロファイルの監査

プロファイルによる保護の強度

Windows

セキュリティ設定

管理設定

Cloud Discovery

ホスト侵入防止

デバイスコントロール

ウェブコントロール

暗号化

詳細

セキュリティプロファイル / 0002 / 管理設定 / ウェブコントロール / Web サイトアクセスルール / 新記録 / カテゴリ

コンテンツカテゴリ

本製品がスキャンするコンテンツカテゴリ

アダルト

ソフトウェア、音楽、映像

Torrent

ファイル共有

音声と映像

アルコール、タバコ、ドラッグ

暴力

過激な表現、わいせつな表現

武器、爆発物、パイロテクニクス

ギャンブル、宝くじ、懸賞

インターネットコミュニケーション

Web メール

SNS

デバイス種別で許可・ブロックを設定。

「0002」セキュリティプロファイル設定

セキュリティプロファイルの監査

プロファイルによる保護の強度

Windows

- セキュリティ設定
- 管理設定
- Cloud Discovery
- ホスト侵入防止
- デバイスコントロール
- ウェブコントロール
- 暗号化
- 詳細

セキュリティプロファイル / 0002 / 管理設定 / デバイスコントロール / デバイスカテゴリをブロックするためのルール

ここでは、ユーザーのネットワークおよびストレージデバイスへのアクセスを制限できます。「デバイスコントロールからの除外」ページで、ブロックされたデバイスカテゴリから除外を追加できます。

デバイス	アクセス
ハードディスク	許可
リムーバブルドライブ	許可
プリンター	許可
フロッピーディスク	
CD/DVD ドライブ	
モデム	
テープデバイス	

モデルやシリアルNoでの除外設定可能

セキュリティプロファイル / 既定値 / 管理設定 / デバイスコントロール / デバイスコントロールからの除外 / 新記録

名前

リムーバブルドライブ

マスク

コメント

サイレントモードで、デバイスからデータをリモートで削除します。 [データ消去に関するオンラインヘルプを表示](#)

消去する方法

- 完全に削除
ファイルはランダムなデータで上書きされます。削除後のファイルデータの復旧がほぼ不可能になります。
- 単純な削除
オペレーティングシステムのリソースを使用してファイルが削除されます。ファイルはごみ箱に送られません。

消去する対象

- すべての標準フォルダー
[ドキュメント] フォルダー、クッキー、[デスクトップ] フォルダー、Internet Explorer の一時ファイル、一時ファイル、Outlook のファイル、ユーザープロファイル。
- カスタムフォルダー
削除する標準フォルダーを選択します。
 - ドキュメント
 - Cookie
 - デスクトップ
 - Internet Explorer の一時ファイル
 - 一時ファイル
 - Outlook ファイル
 - ユーザープロファイル

消去

キャンセル

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。

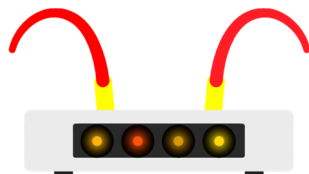
The screenshot shows the '設定 / イベント通知' (Settings / Event Notifications) page in the Kaspersky Endpoint Security Cloud interface. The left sidebar contains navigation options like '情報パネル', 'ユーザー', 'デバイス', 'セキュリティ管理', '隔離', '配布パッケージ', and '設定'. The main content area explains that this section is for configuring event messages and their distribution to company email addresses. It shows a list of recipients, including one with a Kaspersky.com address and another with a Gmail address. Below this, there are sections for 'イベントのリスト' (Event List) and '緊急イベント' (Critical Events), where various system events like automatic startup, activation errors, and malware detection can be configured for notification.

The screenshot shows an email client interface displaying a critical alert message. The message is from 'cloudnoreply' and is titled 'Critical: 悪意のあるオブジェクトが検知されました' (Critical: Malicious object detected). The body of the email contains detailed information about the detected threat, including the device name (DESKTOP-94J4JBK), the time of detection (January 26, 2021, 10:39:39 AM), the type of threat (Trojan-PSW.Win32.XShadow.b), the user (DESKTOP-94J4JBK\admin), and the file path (C:\Users\admin\OneDrive - k...t\Desktop\...h.exe). The reason for detection is listed as 'エキスパートによる分析' (Analysis by experts).

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



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

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。

オペレーティングシステム：

Microsoft Windows Server 2016

Kaspersky Endpoint Security for Windows のバージョン：

11.6.0.394

ネットワークエージェントのバージョン：

13.0.0.11247

デバイスの IP アドレス：

192.168.1.16

接続 IP アドレス：

デバイスがサーバーへの接続に使用するネットワークデバイス（例：ルーター）の IP アドレス。

1■■.58■■.1■■

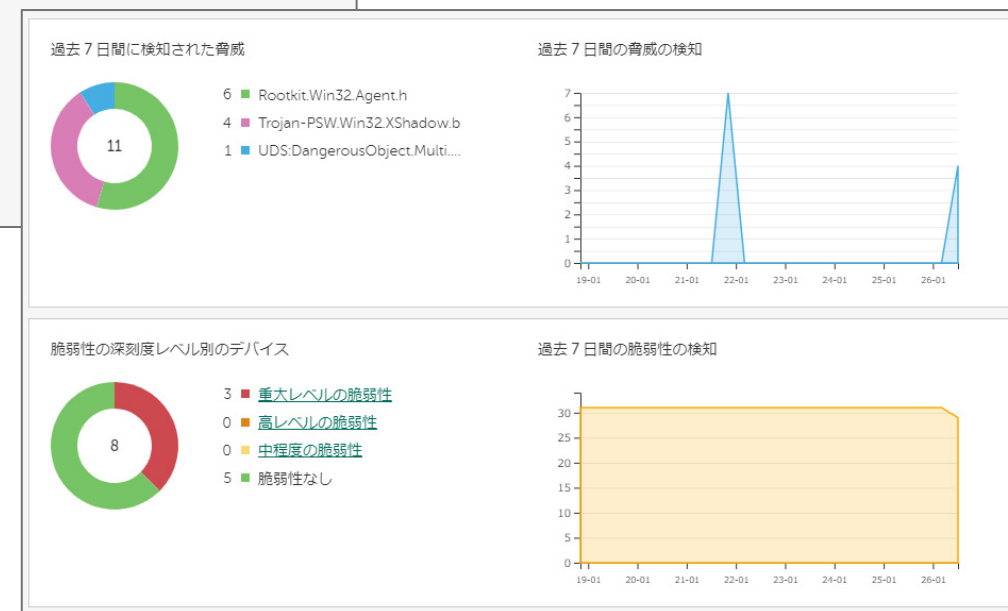
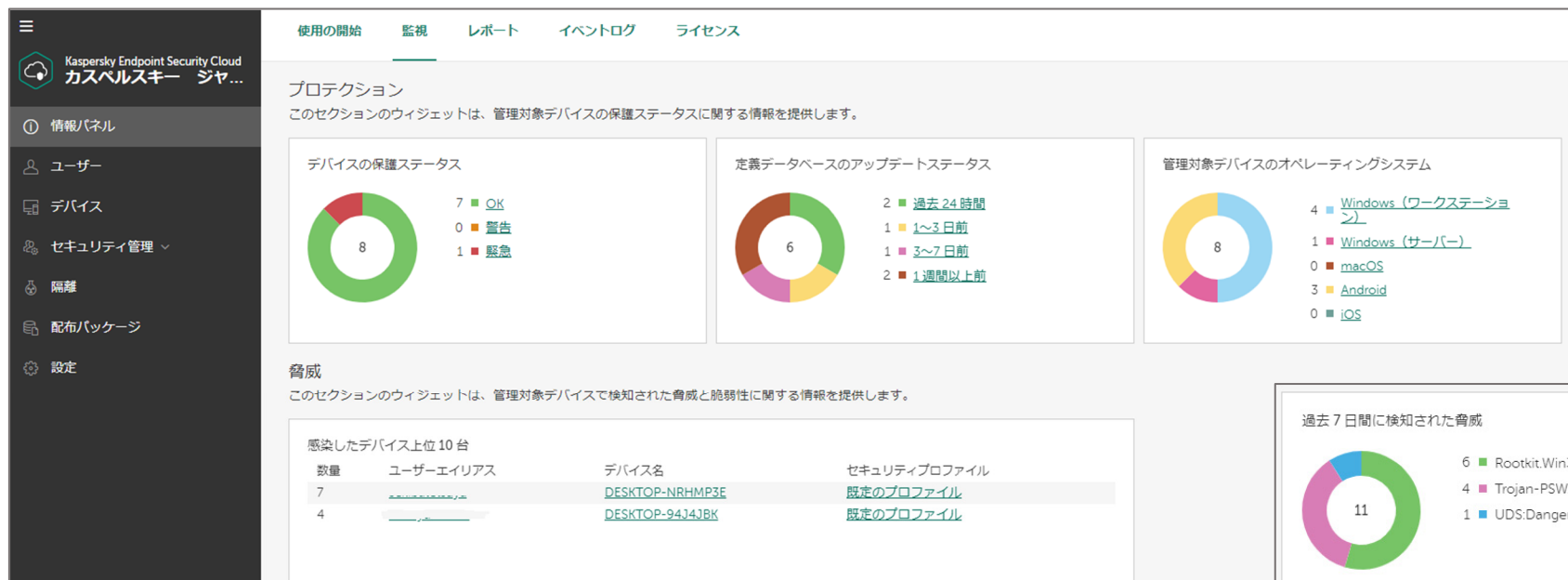
Kaspersky Endpoint Security Cloud 機能紹介

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。

名前	プロファイルによる保護の強度	割り当て先
<input type="checkbox"/> 既定値	高	6ユーザー
<input type="checkbox"/> サーバーグループ	高	1ユーザー

Windows、MAC、Android、iOS向け設定

総合力
高い強度 : 12 / 12

グローバルコンポーネント
次のコンポーネントは、すべてのセキュリティプロファイルで同時に有効になります。これらのコンポーネントを有効にして、プロファイル強度を高めてください。

KSN Kaspersky Security Network の使用 : 2 / 2
Kaspersky Endpoint Security for Android で Kaspersky Security Network を使用するには、ユーザーがデバイスで有効にする必要があります。
✓ Kaspersky Endpoint Security for Windows での Kaspersky Security Network の使用が有効です
✓ Kaspersky Endpoint Security for Mac での Kaspersky Security Network の使用が有効です

ローカルコンポーネント
次のコンポーネントは、各セキュリティプロファイルで個別に有効になります。これらのコンポーネントを有効にして、プロファイル強度を高めてください。

PC Windows デバイスの保護 : 6 / 6
✓ ファイル脅威対策
✓ メール脅威対策
✓ ウェブ脅威対策
✓ ネットワーク脅威対策
✓ ふるまい検知、脆弱性攻撃ブロック、修復エンジン
✓ セルフディフェンス

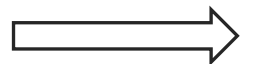
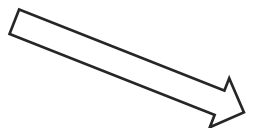
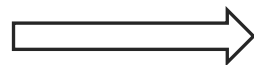
Mac macOS デバイスの保護 : 3 / 3
✓ ファイル脅威対策
✓ ウェブ脅威対策
✓ ネットワーク脅威対策

And Android デバイスの保護 : 1 / 1
Kaspersky Endpoint Security for Android で Kaspersky Security Network を使用するには、ユーザーがデバイスで有効にする必要があります。
✓ アンチウイルスによる保護

プロフィー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。

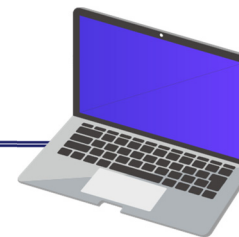
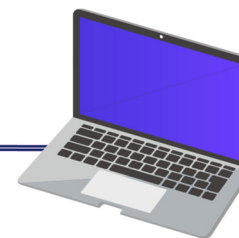
セキュリティプロファイル
(各種設定)



ユーザー



デバイス



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の監査

🔄 プロファイルによる保護の強度

Windows

🔒 セキュリティ設定

ファイル脅威対策

メール脅威対策

ウェブ脅威対策

ネットワーク脅威対策

ファイアウォール

🔧 管理設定

☰ 詳細

セキュリティプロファイル / 既定値 / [セキュリティ設定](#) / ウェブ脅威対策

ウェブ脅威対策が有効です
コンピューター上の受信トラフィックをスキャンします。

セキュリティレベル

高

中 (推奨)

低

セキュリティレベル設定：中
最適な保護。ほとんどのユーザーに推奨します。

脅威の検知時の処理

ダウンロードをブロック

ダウンロードを許可

ウェブ脅威対策の除外リスト
除外は未定義です。

[設定...](#)

セキュリティプロファイルの監査

🔄 プロファイルによる保護の強度

Windows

🔒 セキュリティ設定

🔧 管理設定

Cloud Discovery

ホスト侵入防止

デバイスコントロール

ウェブコントロール

暗号化

☰ 詳細

セキュリティプロファイル / 既定値 / 管理設定

Cloud Discovery が有効です
Windows デバイスで使用されるクラウドサービスを監視し、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します。
[設定...](#)

ホスト侵入防止が有効です
システム内のアプリケーション活動を追跡し、ステータスに応じてアプリケーション活動を規制します。
[設定...](#)

デバイスコントロールが無効です
外部デバイスとリムーバブルドライブの接続を制御します。
[設定...](#)

ウェブコントロールが有効です
コンテンツと場所に基づいて Web サイトへのアクセスを監視します。
[設定...](#)

暗号化の管理が無効です
Windows を実行している管理対象デバイスのディスク全体の暗号化を管理します。
[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。

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。

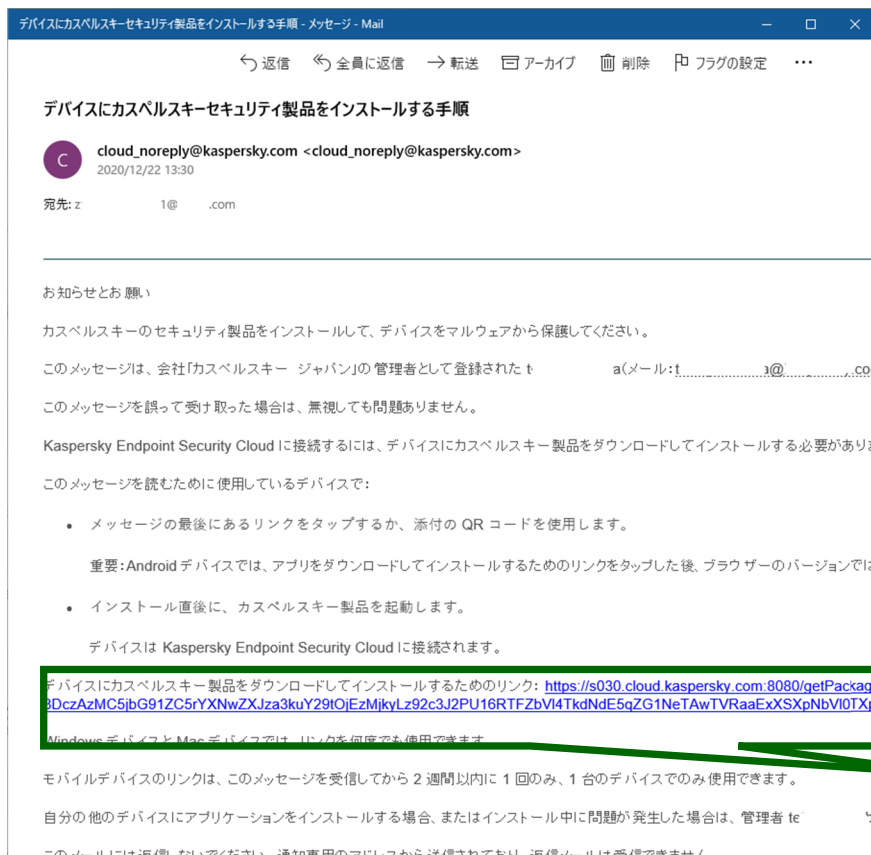
ユーザーエイリアス:
z 1

ユーザーのメールアドレス
z 1@com

セキュリティプロファイル:
[既定値](#)

コマンド:

受信したメールからリンクをクリック。
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。

The screenshot shows the Kaspersky Endpoint Security Cloud management console. The left sidebar contains navigation options: 情報パネル, ユーザー, デバイス, セキュリティ管理, 隔離, 配布パッケージ (highlighted), and 設定. Below these are links for プライバシーポリシー, 法律上の通知, ヘルプ, and サポート. The main content area is titled '配布パッケージ' and contains two entries:

- Win Kaspersky Endpoint Security for Windows (11.8.0)** (ビルド 11.8.0.384) with a 'ダウンロード' button. Description: Kaspersky Endpoint Security for Windows は、様々な種類の脅威、ネットワーク攻撃、詐欺からサーバーとワークステーションを包括的に保護します。保護コンポーネントは、セキュリティプロファイルで設定できます。プロキシサーバー経由でインターネットにアクセスするWindows デバイスにセキュリティ製品をインストールする場合は、必要なプロキシサーバー設定を指定できます。 [プロキシサーバー](#)
- Mac Kaspersky Endpoint Security for Mac (11.2)** (ビルド 11.2.0.185) with a 'ダウンロード' button. Description: Kaspersky Endpoint Security for Mac は、様々な種類の脅威、ネットワーク攻撃、および不正行為からコンピューターを包括的に保護します。保護コンポーネントは、セキュリティプロファイルで設定できます。プロキシサーバー経由でインターネットにアクセスする Mac デバイスにセキュリティ製品をインストールする場合は、プロキシサーバーの設定を指定します。 [プロキシサーバー](#)

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 のインストーラー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：

- 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。

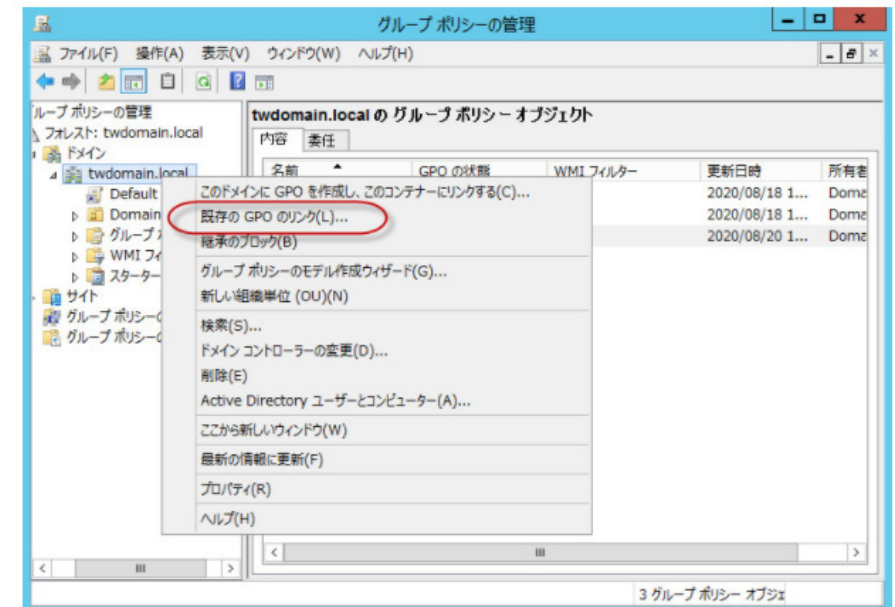
パッケージ名にスペースが含まれている場合は、それを削除するか、アンダースコア (_) に変更します。

- 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 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)



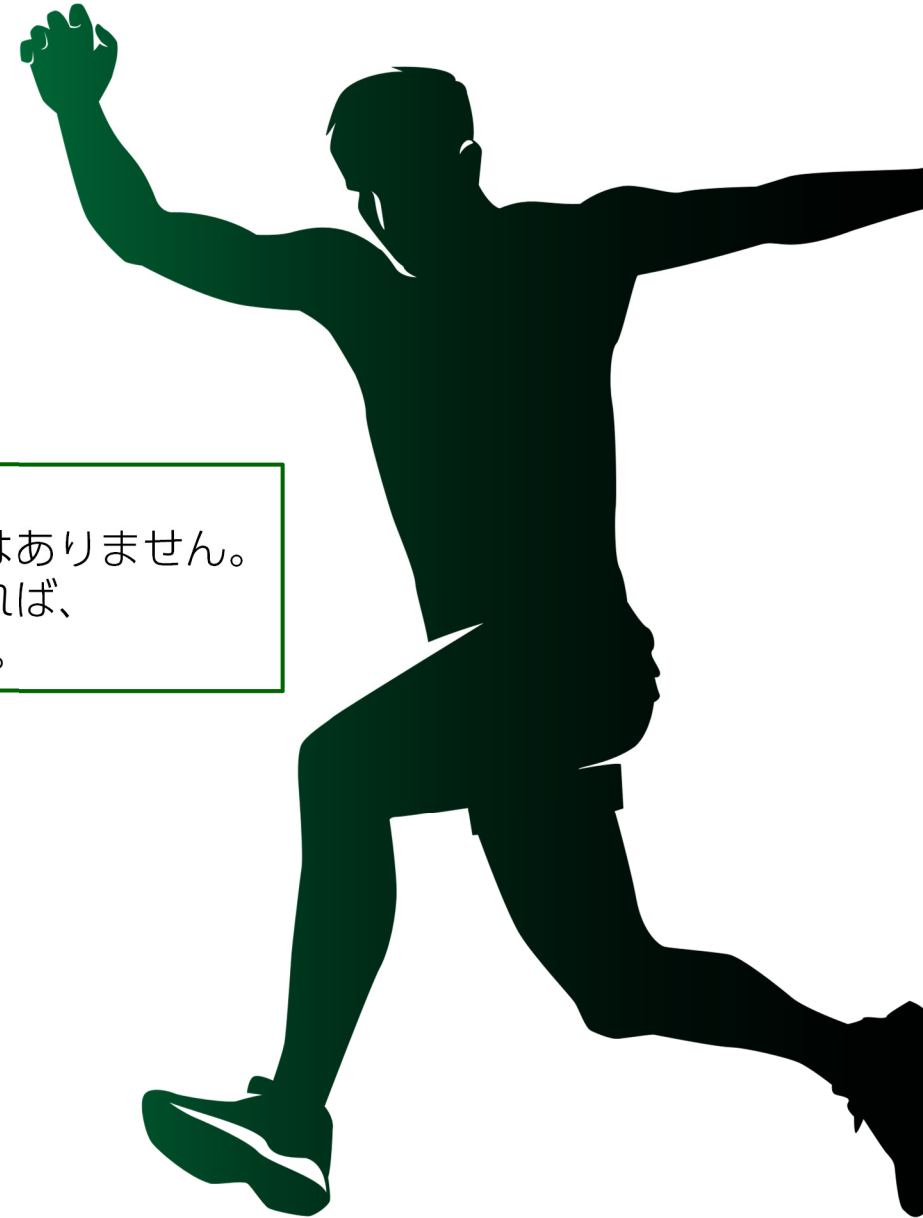
Kaspersky Endpoint Security Cloud Kaspersky Security for Microsoft Office 365

製品の評価・試用

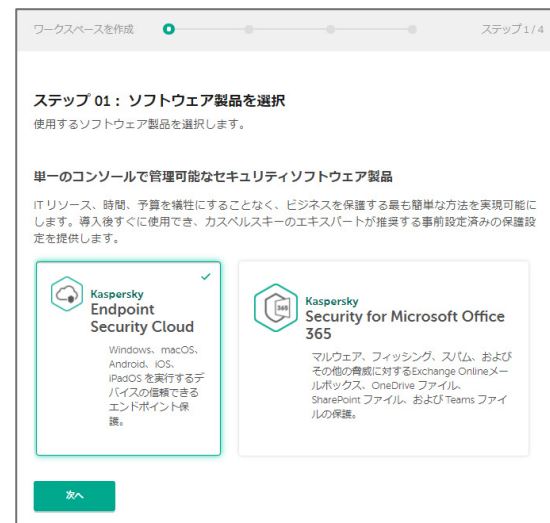


製品の評価・試用

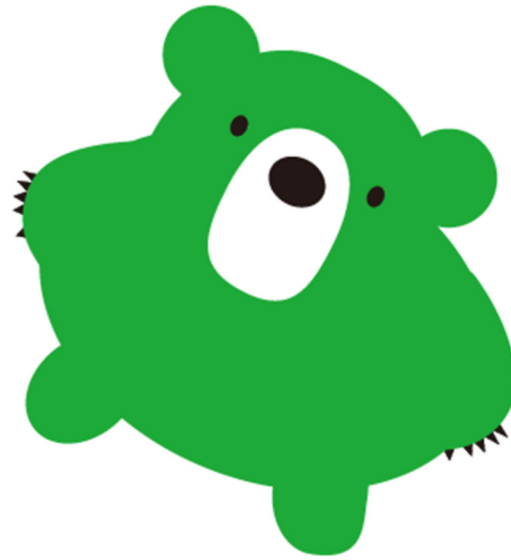
- ① <https://cloud.kaspersky.com/> にアクセス。
- ② アカウントを作成し、ログイン。
- ③ ワークスペースを作成し、準備完了。



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、引き続き使用することが出来ます。



Thank you



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