



Kaspersky® Endpoint Security for Business

Select

Kaspersky Endpoint Security for Business Select は、さまざまなプラットフォームのサーバーおよびエンドポイントに対して、次世代の HuMachine ベースの保護を提供します。疑わしいふるまいを検知してランサムウェアをはじめとした脅威をブロックする多層保護セキュリティを採用し、クラウドベースの管理により、攻撃を受ける可能性を低減します。またモバイルプラットフォームの保護に効果的なモバイル管理機能も搭載しています。

保護機能と管理機能

カスペルスキーでは、エンタープライズクラスのままさまざまな機能を構築し、複数のソリューションに組み込んでいます。これらのテクノロジーの利用には、複雑なプロセスは不要で、企業の規模に関わらずすべてのお客様が簡単にご利用いただけます。

Kaspersky Endpoint Security for Business の
ラインナップ

- Select
- Advanced

多層防御機能で以下のプラットフォームを保護

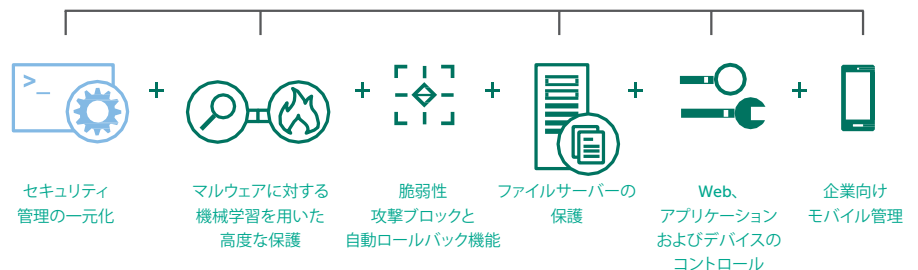
- Windows、Linux、Mac のワークステーション
- Windows、Linux サーバー
- Android
- リムーバブルストレージ

優れたセキュリティ機能で以下の脅威から保護

- ソフトウェアエクスプロイト
- ランサムウェア
- モバイルマルウェア
- 高度な脅威
- ファイルレス攻撃の脅威
- PowerShell およびスクリプトベースの攻撃
- Web の脅威

優れたセキュリティ・管理機能

- アンチマルウェア 機能強化
- 静的な機械学習
- 動的な機械学習 新機能
- プロセスアイソレーション
- ファイアウォール
- OS のファイアウォールの管理 新機能
- クラウド支援型の保護
- 統合された EDR エージェント 新機能
- アプリケーションコントロール 機能強化
- ダイナミックホワイトリスト
- Web コントロール
- デバイスコントロール 機能強化
- サーバー保護 機能強化
- ターミナルサーバー保護 機能強化
- 企業向けモバイル管理 機能強化
- モバイル向けエンドポイントセキュリティ 機能強化
- レポート機能 機能強化



すべてのエンドポイントに対応する次世代の保護と管理

一元化された管理コンソール

管理者は単一の管理コンソールからセキュリティの情報をすべて把握・管理でき、また選択したセキュリティポリシーを組織内のすべてのエンドポイントに適用できます。そのため、セキュリティ機能の導入においても、事前設定済みのさまざまなシナリオを活用し、業務の中断や組織内の混乱を招くことなく迅速に導入することができます。

拡張性のある高度なセキュリティ

本製品は、あらゆる IT 環境で機能するようにデザインされています。実績のある次世代テクノロジーを豊富に用いているほか、Endpoint Detection and Response (EDR) との統合および組み込みセンサーにより、大量のデータを取得・分析し、極めて認識の難しい高度なサイバー攻撃をも検知できるよう設計されています。

追加のコストのいらぬ単一の製品

さまざまなセキュリティテクノロジーを 1 つの製品に統合しているため、追加コストが発生することはありません。ライセンスも 1 つのため、面倒な複数のライセンス管理や適用も不要です。

主な機能

次世代技術を用いた脅威保護機能

脆弱性攻撃ブロック

未知のゼロデイ脅威に対抗できる新たな保護層を設けて、マルウェアの実行およびソフトウェアへの攻撃を回避します。

ふるまい検知と自動ロールバック

ランサムウェア、ファイルレス攻撃、管理者アカウントの乗っ取りなど、高度な攻撃を特定し、これらの攻撃から保護します。ふるまい検知は攻撃をブロックし、自動ロールバックは不審な変更が行われた場合でも、元の状態に戻すことができます。

共有フォルダーの暗号化保護

独自の暗号化防止メカニズムで、同じネットワーク内の別のマシンから実行される攻撃プロセスによって、共有フォルダ内のファイルを暗号化が行われた場合でも、その攻撃をブロックします。

ネットワーク上の脅威保護

バッファオーバーラン攻撃を使用するマルウェアは、すでにメモリにて実行されているプロセスを変更して、悪意のあるコードを実行します。ネットワーク上の脅威保護では、ネットワーク攻撃を特定し、その場で攻撃を阻止します。

アンチルートキットテクノロジー

攻撃者はルートキットおよびブートキットを使用して、自らの行動がセキュリティソリューションから検知されないようにします。アンチルートキットテクノロジーは、極めて巧妙に隠されている感染も検知し、それらを無効化します。

モバイルセキュリティ機能

革新的なアンチマルウェアテクノロジー

シグネチャベース、プロアクティブ、およびクラウド支援型の検知機能を組み合わせることで、リアルタイムの保護を提供します。Safe Browser、オンデマンドと定期的なスキャンで、セキュリティを高めます。

OTA (Over The Air) プロビジョニングによるデプロイ

SMS、メール、PC を使用して、アプリケーションの事前構成とデプロイを一元管理する機能を提供します。

リモート盗難対策ツール

SIM 監視、リモートロック、消去、検索はすべて、モバイルデバイスの紛失または盗難があった場合に、企業データへの不正アクセスを阻止します。

モバイル端末向けのアプリケーションコントロール

アプリケーションコントロールにより、インストール済みのソフトウェアのデータを取得でき、また管理者は特定のアプリケーションのインストールおよび使用を強制できます。

クラウドによるエンドポイントコントロール

アプリケーションコントロール

カスペルスキーから提供されるダイナミックホワイトリストにより、PC でのソフトウェアを実行可能にするかを総合的にコントロールできるため、攻撃を受ける可能性を低減することができます。このコントロールは、デフォルト許可およびデフォルト不許可のシナリオに対応しています。

ダイナミックホワイトリスト

アプリケーションコントロールでは、アプリケーションを適切に分類するため、カスペルスキーが開発した正規のソフトウェアに関するナレッジを体系化した [ダイナミックホワイトリストデータベース](#) を使用しています。

デバイスコントロール

デバイスコントロールでは、ユーザーはデータポリシーを作成してスケジューリング設定し、USB または他の種類のバスで接続されるリムーバブルストレージや他の周辺機器にそれらを適用することができます。

ホスト型侵入検知システム (HIPS)

ローカルおよび Kaspersky Security Network にあるレピュテーションデータベースを使用して、承認済みのアプリケーションのパフォーマンスに影響を及ぼすことなく、機密データや記録デバイスへのアクセスを管理します。

保守とサポート

当社のプロフェッショナルサービスチームは世界中に展開する 35 のオフィスから 200 か国以上をカバーし、クライアントの皆様がカスペルスキーのセキュリティサービスから最大限のメリットを得られるよう、サポート体制を整えています。

評価版のご利用

HuMachine インテリジェンスと優れたセキュリティ機能を組み合わせ、あらゆるタイプの脅威から組織を保護できるのはカスペルスキーの製品だけです。Kaspersky Endpoint Security for Business のフルバージョンは、[こちらのページ](#)から評価版を 30 日間お試しください。

株式会社カスペルスキー
パートナー一覧: www.kaspersky.co.jp/find-a-partner
Kaspersky for Business: www.kaspersky.co.jp/business-security
ご購入相談窓口: jp-sales@kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.co.jp

© 2018 Kaspersky Lab. All rights reserved.
Kaspersky およびカスペルスキーは Kaspersky Lab の登録です。
その他記載された製品名などは、各社の商標もしくは登録商標です。
なお、本文では、TM、®は記載していません。