



Kaspersky® Endpoint Security for Business

Advanced



Ready
for GDPR

Kaspersky Endpoint Security for Business Advanced は、多層防御と豊富な管理ツールを組み合わせ、新しい脅威にも迅速に対応できる優れたセキュリティソリューションを提供します。多層防御を用いることで、脆弱性を減らし、機密データを保護する上で効果的です。またすべての機能は、使いやすい一元集中型の管理コンソールから管理できます。

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
- Windows、Linuxサーバー
- Windowsサーバーコンテナ
- Androidおよびその他のモバイルデバイス
- リムーバブルストレージ

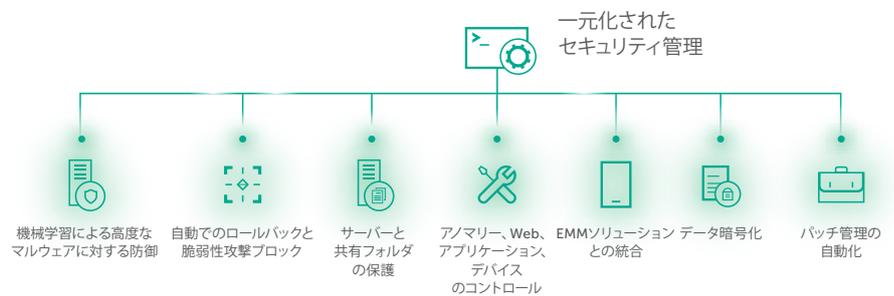
優れたセキュリティ機能で以下の脅威から保護

- 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**
- 脆弱性管理
- セキュリティポリシーアドバイザー
- AIベースの機械学習
- AMSIへの対応 **新機能**
- 暗号化通信のスキャン **新機能**
- プロセスアイソレーション
- 脆弱性攻撃対策とロールバック機能
- OSのファイアウォールの管理
- クラウドベースの保護
- 統合された EDR エージェント
- アダプティブアノマリーコントロール **新機能**
- アプリケーション、Web、デバイスのコントロール
- サーバーおよびコンテナの保護 **機能強化**
- ターミナルサーバーの保護
- Windows Linux subsystem対応 **新機能**
- モバイル脅威対策 **機能強化**
- OSによる暗号化の管理
- システム構成とデプロイメント
- パッチ管理 **機能強化**
- レポート機能

詳細は[こちらのWeb](#)をご覧ください。



管理機能とデータ保護機能でさらにセキュリティを強化

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状況のすべてを把握・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。

高い顧客満足度

お客様が必要とする高性能な製品を提供するために、当社はR&Dへの投資を重視しています。第三者機関による調査やレポートが示す通り、カスペルスキーの製品は高い評価と優れたテスト結果を得ています。

主な機能

クラウドによるエンドポイントコントロール

独自のアンマリーアプリケーションコントロール

アダプティブアンマリーコントロールは、組織内の各役割を把握し、最高のセキュリティレベルを自動的に設定します。さらに、エンタープライズクラスのアプリケーションコントロールと最新のホワイトリストデータベースによってより強固な保護を提供します。

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。

デバイスコントロール、Web コントロール、その他のさまざまな機能

暗号化とデータ保護

包括的な暗号化

FIPS 140-2 認定の暗号化をファイルやディスク、デバイスレベルで一元的に導入でき、Microsoft BitLocker や macOS FileVault といったネイティブ暗号化ツールの管理も可能になります。

独自の総合的ポリシー作成

暗号化とアプリケーションおよびデバイスコントロールを独自に統合することで、セキュリティをさらに高め、管理も簡単になります。

次世代技術を用いた脅威保護機能

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。

共有フォルダーへ悪意のある暗号化に対する保護

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、共有フォルダー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。

コンテナとターミナルサーバーの保護

Microsoft のターミナルサービスや Citrix の XenApp および Xen Desktop を含め、Windows サーバーコンテナおよび各種リモートアクセス環境を保護します。またトラフィックセキュリティコンポーネントにより、ターミナルサーバーのウェブおよびメールのトラフィックを保護します。

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

© 2019 Kaspersky Lab. All rights reserved.
Kaspersky およびカスペルスキーは Kaspersky Lab の登録商標です。
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。

脆弱性攻撃ブロック、アンチルートキットテクノロジー、その他さまざまな機能を実装

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

機械学習ベース、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、その他さまざまな機能を実装

システム、脆弱性、パッチ管理

パッチ管理

脆弱性を徹底的にスキャンする高度な機能を、パッチの自動配布機能と組み合わせました。

迅速な OS およびソフトウェアのデプロイ

管理コンソールからのシステムイメージの作成、保存、デプロイが可能。たとえば Microsoft Windows 10 への移行や Kaspersky SecurityNetwork にて特定されている 150 種にもおよび一般的に使われているアプリケーションのデプロイにも最適です。

ハードウェア、ソフトウェア、ライセンスの管理

ハードウェアとソフトウェアの棚卸資産レポートは、ソフトウェアライセンスに関する義務を管理するのに役立ちます。ソフトウェアの権利を一元的にプロビジョニングすることによって、コストを削減できます。

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 34 のオフィスから 200 以上国以上をカバーし、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

ぜひ真のサイバーセキュリティをお試ください。[こちらのページ](#)から、Kaspersky Endpoint Security for Business の評価版をお試しいただけます。

