KASPERSKY

Kaspersky Endpoint Security

真のサイバーセキュリティ技術を基盤とした、最先端の多層防御型エンドポイントプラットフォーム

世界に広まるサイバー脅威がさらに進化している中、ビジネスに重要な基幹業務、財務などの重要な情報が日々増大するゼロデイ攻撃の脅威にさらされています。過去 12 か月の間で、全企業の 38 % が何らかの形態のマルウェアによる影響を受けています。このリスクを軽減するためには、企業を狙うサイバー攻撃を仕掛ける高度な技術を持つ犯罪者より、多くの防御手段を備える必要があります。

企業を標的にしたほとんどのサイバー攻撃はエンドポイントを通して行われています。企業が所有しているITインフラストラクチャ（物理環境、仮想環境およびモバイルなどのすべてのエンドポイント）を効果的に保護できれば、企業レベルの強固なセキュリティ基盤を構築することができます。

Kaspersky Labは、標的型攻撃など巧妙化している最新の脅威や攻撃から企業を保護する高度な保護技術と脅威インテリジェンスのさらなる技術革新に努めています。

既知および未知の脅威に対し迅速に対処する保護機能は、強力なアクセスコントロール機能およびデータ保護機能（暗号化、パッチ適用の自動化、モバイル端末の保護など）によってさらに強化されます。これらの機能は、すべて Kaspersky Security Center で一元管理します。

脅威の回避

HuMachine インテリジェンスを利用した、Kaspersky Labの最先端の保護エンジンによって、ランサムウェア、エクスプロイト、および最先端のサイバー脅威からお客様のビジネスを保護します。

高度なエンドポイントコントロール

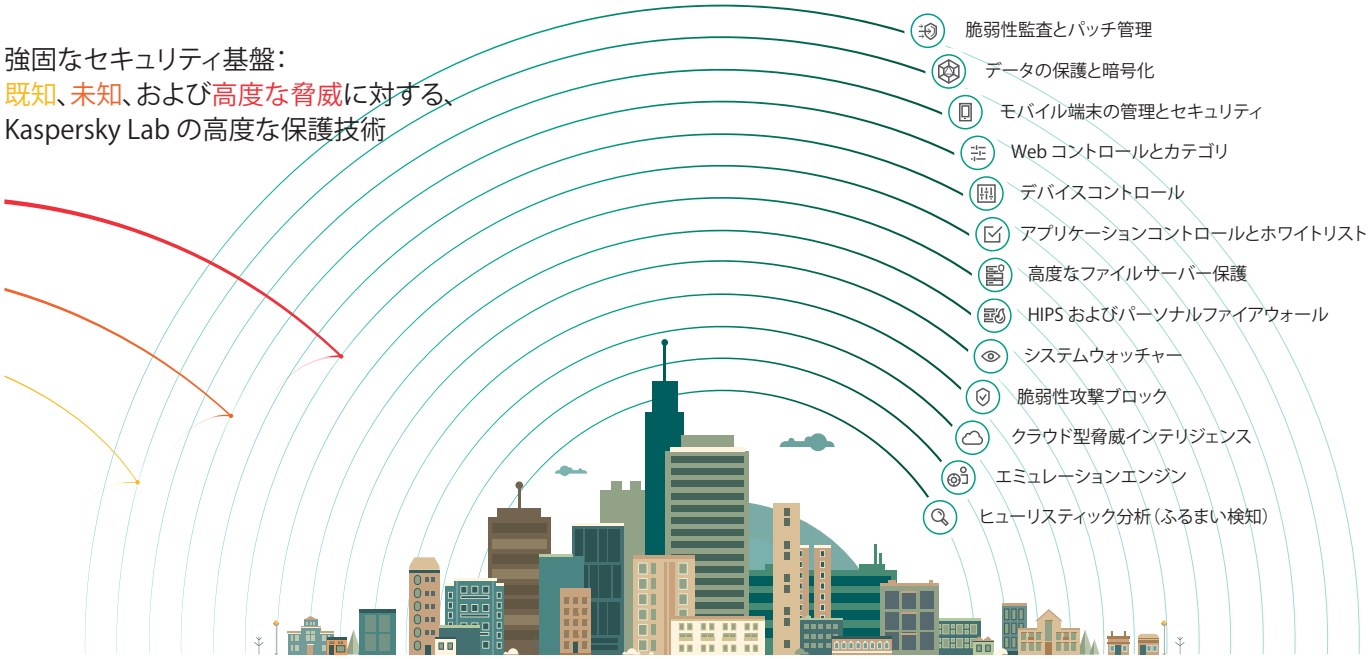
簡単で効率的、かつ一元的なWeb、デバイス、アプリケーションのコントロール機能でサイバー脅威に遭遇する機会を減らし、利用者が安全に業務を遂行できるようにします。

情報漏洩の防止

FIPS 140.2 認定を受けたディスク全体の暗号化機能によって、企業で使用しているデスクトップやモバイル端末に保存されている重要な情報を完全に保護します。

多層防御型の保護

強固なセキュリティ基盤：
既知、未知、および高度な脅威に対する、
Kaspersky Lab の高度な保護技術



あらゆる形態のサイバー脅威からビジネスを守る強力な多層型防御

機械学習に基づく高度なセキュリティ

あらゆる形態の既知および未知のサイバー脅威からビジネスを守るには、すべてのエンドポイントを完全に保護することが重要です。従来型のアンチマルウェア保護では、もはやこれらの脅威から企業を守ることはできません。多層型防御による最先端のセキュリティプラットフォームを導入しなければ、社内外のあらゆるエンドポイントを安全に保護することはできません。

高いパフォーマンス

Kaspersky Labの統合型セキュリティは常に IT インフラストラクチャの内部で機能します。単一のエンドポイントエージェントによって、コンピューターのパフォーマンスやシステムリソースへの影響を最小限に抑えた強固で堅牢な保護が可能です。このソリューションは拡張性の高い統合型プラットフォームとして社内に構築でき、すべてのエンドポイントを完全に保護し、かつシステムのパフォーマンスを最適化します。

強力な脅威インテリジェンス

リアルタイムで提供される高度な脅威インテリジェンスを活用して、Kaspersky Labのテクノロジーは、絶えず進化し続けるゼロディエクスプロイトを含む最新の脅威からも企業を保護します。高度な脅威を検知できる優れたセキュリティソリューションを企業のセキュリティ戦略に適用することによって、将来にわたってすべてのエンドポイントを最も安全に保護された状態に維持できます。

統合型の一元管理

複数のプラットフォームと端末を他のエンドポイントと同様に同じ管理コンソールで管理できます。管理に必要な作業や技術を新たに用意することなく、セキュリティシステムの可視化と管理の作業効率が向上します。

次世代の高度な脅威に対抗する優れた保護技術

高度な技術を搭載したエンドポイント保護エンジンは、第三者機関が実施する検証を受け[※1]、常に最高の賞を獲得しているセキュリティインテリジェンスと機械学習の技術によって開発されており、企業のセキュリティ戦略の中核となるものです。

感染を未然に防ぐインテリジェントな保護機能を多層構造で組み合わせることで、巧妙かつ高度な既知および未知のサイバー脅威に対し、より強力なセキュリティ防御システムが構築できます。

- マルチアルゴリズムを利用したヒューリスティックおよび脅威エミュレーション分析：
  従来のシグネチャーベースの技術を補完して、未知のマルウェアを検知します。
- クラウド型脅威インテリジェンス（Kaspersky Security Network）：
  リアルタイムの脅威情報を活用して新しいマルウェア脅威に対しても、迅速に検知してブロックします。
- 脆弱性攻撃ブロック：
  サイバー犯罪者が使用するエクスプロイトをブロックすることで、高度な攻撃を防止します。
- システムウォッチャー：
  疑わしいふるまいのパターンを検知することで未知の脅威をブロックし、 万一感染した場合は、感染する前の状態にファイルを復元し、ランサムウェアによる攻撃を防止します。
- ホスト型侵入防止システム(HIPS)：
  不正な振る舞いのパケットや通信を検知するとファイアウォール機能と連携して通信を遮断します。
- パーソナルファイアウォール：
  事前に設定したネットワークルールに従ってすべてのネットワークアクティビティをフィルタリングします。
- ネットワーク攻撃防御：
  ネットワークを使用するプログラムやサービスに対するポートスキャン、DOS攻撃、バッファオーバーランなどの不正な行為をブロックします。

ランサムウェアやエクスプロイトからの保護

システムウォッチャー（ふるまい検知）によってデータを保護し、サイバー犯罪者に身代金を払う状況に陥らないようにします。Kaspersky Security for Windows Server によって、進化した CryptoLocker から共有フォルダーに保存されているファイルを保護します。また脆弱性攻撃ブロック技術によって、最新のエクスプロイトからエンドポイントを保護します。

アプリケーションを利用した攻撃からの保護

ホワイトリストとアプリケーションコントロールによって実行できるアプリケーションを制御し、ブラックリストに登録されたアプリケーションの起動を禁止できるため、ゼロデイ攻撃にさらされる危険性を大幅に減らすことができます。疑わしい、または不適切なふるまいをするアプリケーションはシステムウォッチャーによって分析され、HIPS によってブロックまたは動作が制限されます。また、信頼されたアプリケーションは、問題なく安全に利用できます。

クラウド型ホワイトリストの利用

Kaspersky Labが提供するホワイトリストを利用して実行アプリケーションを制限できます。

Web アクセスによる危険性の回避

利用者が職場でアクセスする Web サイトを Web コントロール機能によってフィルタリング、アクセス可否が設定でき、脆弱性が Web サイトやソーシャルメディアを経由してシステムへの侵入、または潜入する危険性を低減させ、利用者が安全に業務を遂行できるようにします。

ポータブルデバイス使用の制御

デバイスコントロール機能によって、未承認または暗号化されていないポータブルデバイスに保存されている企業情報や顧客情報の漏洩や、デバイスから感染したデータが社内サーバーにアップロードされないように制御します。

サーバーに対する高度な保護の適用

サーバーで実行するアプリケーション起動コントロールでは、起動ルールが設定された実行ファイル、スクリプトおよび MSI パッケージの起動の許可と禁止、またはサーバーへの DLL モジュールのロードの許可と禁止ができるため、非常に高いセキュリティ機能でサーバーを保護します。

すべてのエンドポイントを完全に制御

アプリケーション、Web サイト、デバイスへのアクセスをコントロールする機能を利用して、許可されていない不正なアクセスを識別してブロックし、業務に必要のないアクセスを規制することができ、利用者の生産性を上げながら、脅威に遭遇する危険性を低減できます。

これらのコントロール機能は Active Directory と統合されているため、ポリシーを自動的に作成、またはセキュリティ要件に応じてカスタマイズが容易です。さらにポリシーを一括設定、または利用者の役割別に設定することもできます。

FIPS 140-2 認定の暗号化によるデータ保護

強力な暗号化機能で PC、モバイル端末およびポータブルデバイスに保存されている重要な情報が漏洩しないよう完全に保護します。暗号化技術との統合によって、グループ毎または個々のデバイスに設定されたセキュリティポリシーに沿って、ファイル、ディスクおよびデバイスを一元的に暗号化します。これらの機能をすべて ひとつの管理コンソールを利用して、Kaspersky Labが提供するすべてのエンドポイントセキュリティと Microsoft Windows で標準提供されている Microsoft BitLocker の暗号化機能も統合して管理できます。

自動化された脆弱性管理で最新の状態を維持

信頼されたアプリケーションで見つかった脆弱性を悪用し、エンドポイントから IT インフラストラクチャに侵入する方法が最も一般的です。発見された脆弱性に対し迅速かつ効率的にパッチ適用の作業工程を管理するには、エクスプロイトとそのふるまい、およびその攻撃対象を正確に把握する必要があります。Kaspersky Labの自動化された脆弱性監査およびパッチ管理システムは、リアルタイムでKaspersky Labのグローバルインテリジェンスから提供されるエクスプロイトに関する情報を活用して、稼働中のシステムや利用者の業務に与える影響を抑えながら脆弱性を検知してパッチを適用でき、システム環境を脆弱性のない最新の状態に維持します。

社外で利用するモバイル端末の保護

スマートフォンやタブレット端末は、場所や時間を選ばずにアクセスできるため、今日の業務遂行に必要不可欠なツールです。モバイルセキュリティは、モバイル端末のセキュリティ上の弱点を狙った攻撃によって、モバイル端末に保存されている重要なデータが盗まれたり、モバイル端末を経由して企業システムに侵入を試みる脅威からモバイル端末と企業システムを保護します。

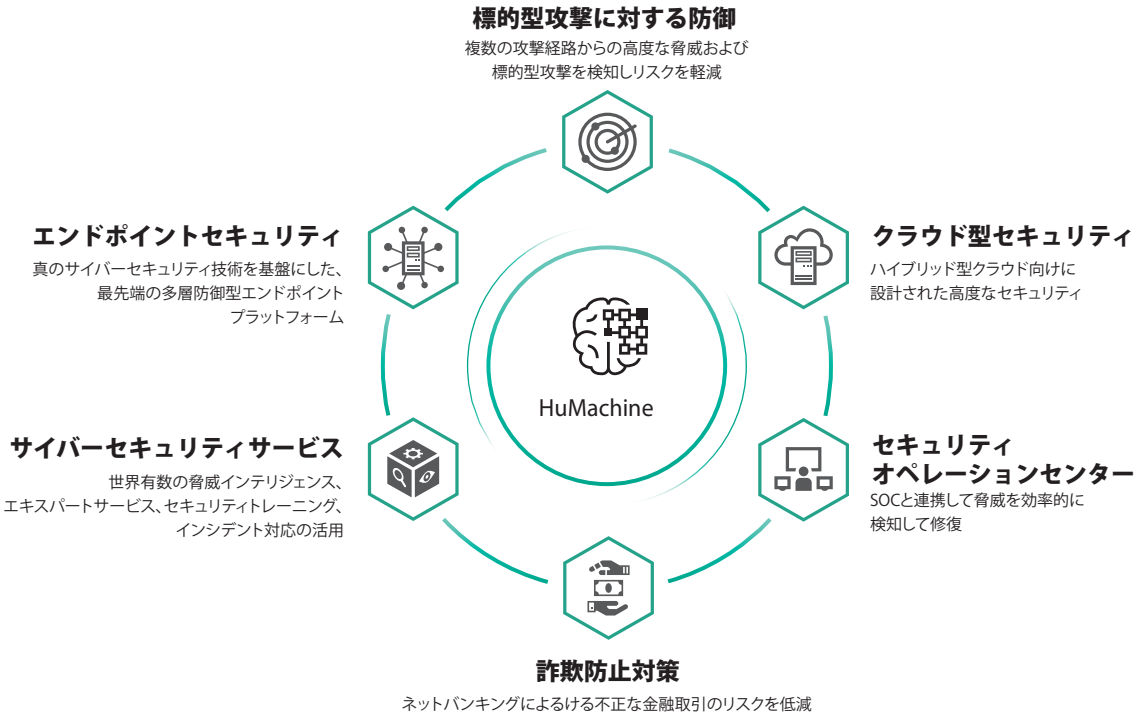
統合管理で作業効率の向上

Kaspersky Endpoint Security を利用して企業のセキュリティ担当部門がすべての PC、サーバーおよびモバイル端末を設置場所、利用場所および利用形態を問わず正確に保護状態を監視し、管理できます。この管理ソリューションは非常に拡張性が高く、IT資産、ライセンス管理およびリモートアクセスを利用した障害対応およびネットワークの制御をすべてひとつのコンソールで一元管理できます。

単一コンソールによる一元管理は役割別の管理機能によって、管理業務の一部を他の管理者に委譲することができます。

Kaspersky Enterprise Security ソリューションの全体像

Kaspersky Labでは、エンドポイントの保護だけでなく、企業のあらゆるレベルのセキュリティ戦略に対応した製品とサービスを組み合わせて利用できるエンタープライズソリューション、または個別要件に応じて選択可能な製品とサービスを提供しています。Kaspersky Labのソリューションは仮想化環境やクラウド型のシステム、および物理的なエンドポイント、サーバー、ITインフラストラクチャを脅威から保護します。また金融サービス、医療、行政機関など、特定の業種や業界向けサイバーセキュリティソリューションも提供しています。



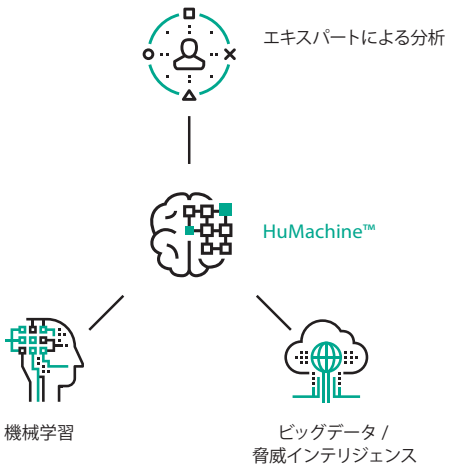
プレミアムサポートサービス

必要に応じて、セキュリティエキスパートの支援を得られます。世界中の 200 を超える国々の 34 のオフィスから、24 時間 365 日対応のサービスを提供しています。Kaspersky Labのセキュリティ製品を最大限に活用するため、Maintenance Service Agreement（MSA）を提供しています。

株式会社カスペルスキー

製品情報：www.kaspersky.co.jp/business-security/small-to-medium-business
セキュリティサービス：www.kaspersky.co.jp/enterprise-security/intelligence-services
プレミアムサポートサービス：www.kaspersky.co.jp/business-security/services
ご購入相談窓口：jp-sales@kaspersky.com

www.kaspersky.co.jp
#truecybersecurity



PMM-1016-201705