

▶ カスペルスキー 法人向け製品ポートフォリオ



サイバー攻撃よりネットワークを守る



企業は規模の大小にかかわらず、常にマルウェアの脅威にさらされています。カスペルスキーは、そうした脅威を発見し対処する力を備えた世界でも他に例のないセキュリティベンダーです。

標的型攻撃やAPT攻撃、未知の攻撃などを含むサイバー攻撃による脅威はますますエスカレートしています。個人や企業をターゲットとした新しいマルウェアの攻撃は1日あたり32万5,000件(ユニーク件数)を越えています。

カスペルスキーでは、マルウェアの脅威とそれがビジネスにもたらすリスクへの対応に取り組んでおりますが、お客様となる企業に対しても、自社のITセキュリティ戦略が以下の3つのセキュリティ要件を満たしているか確認することをお勧めしています。

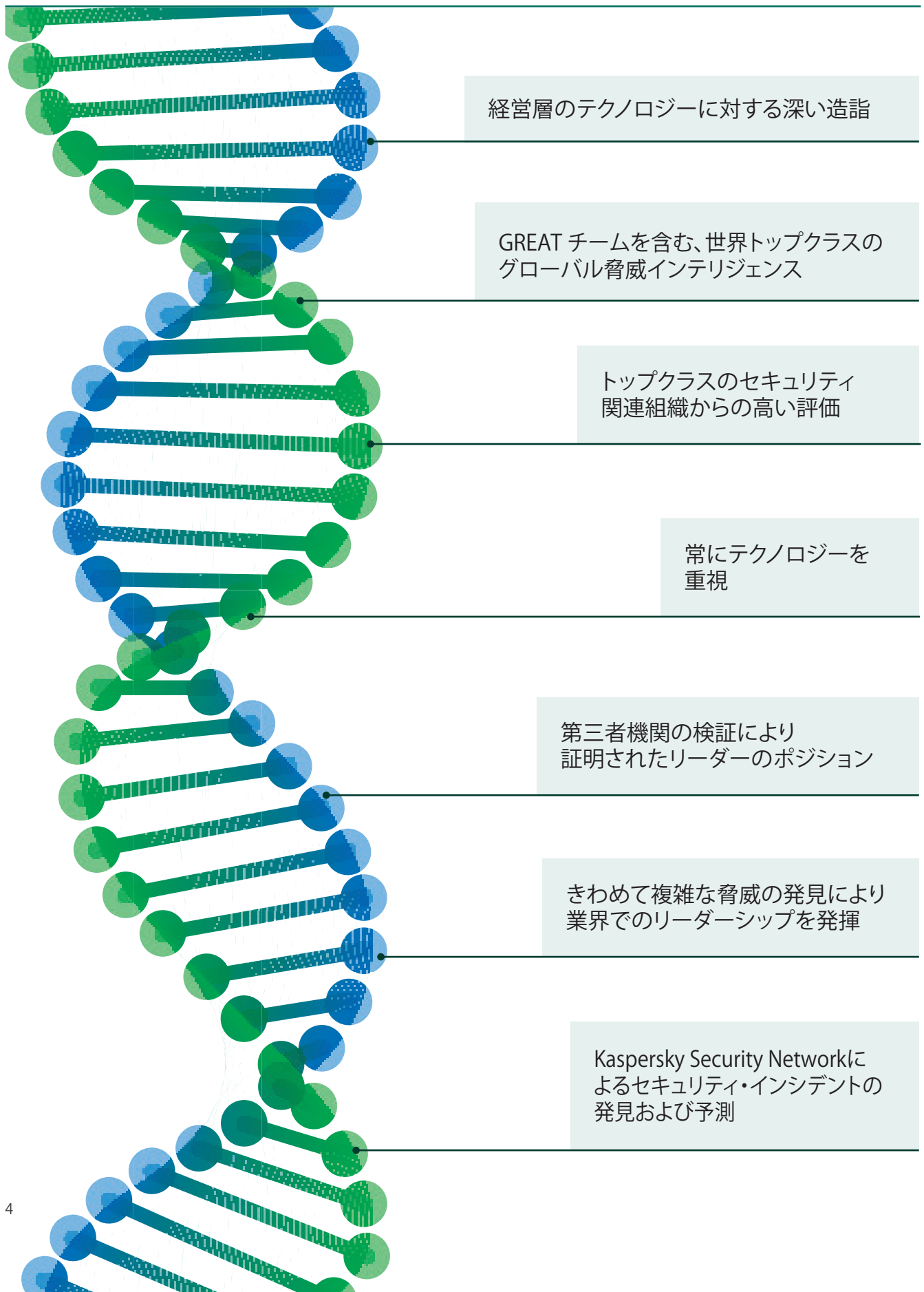
1. 真に優れた脅威インテリジェンス情報へアクセスする必要があります。このような情報を活用することで、マルウェアの実態やどのように書かれコンパイルされたかなどについて理解を深めることが可能になります。セキュリティシステムを正しく運用していくためには、常に最新のインテリジェンス情報を継続的に入手してゆくことが非常に重要であり、またベンダーは世界中のマルウェアホットゾーンを徹底的に調べ上げ、将来に備えることが求められます。
2. セキュリティ・システムは、既知や未知、または最新のマルウェアを検出し排除することが可能なツールや技術を導入することが不可欠です。また、セキュリティ・ソフトウェアはセキュリティシステムに負担をかけることなく、高速スキャンを実現することで業務の中断を回避できるものでなければなりません。
3. ビジネス IT 環境が複雑さを増す中で、物理的なエンドポイント・クライアントやモバイル端末、仮想上で動作するエンドポイントの増加などビジネスIT環境はますます複雑さを増しています。このような状況下でも、セキュリティ・ソフトウェアは、シームレスに効率よく、さらにソフトウェア間での競合を起こすことなく単一のセキュリティ・プラットフォームより管理を行えることが求められます。

企業が必要とする、世界トップレベルの脅威インテリジェンスとそれを活用するための、ユニークな包括的セキュリティ・プラットフォームに組み込まれたテクノロジーを提供できるのはカスペルスキーだけです。

カスペルスキー製品は、導入先のセキュリティ要件や、導入目的に応じて必要な機能を利用できる柔軟性を備えた製品設計となっています。言い換えれば、物理的エンドポイントや仮想エンドポイント、モバイルデバイス、メールシステム、サーバー、ゲートウェイなどに対する脅威から企業を守る万全の体制ができています。本書で取り上げている製品、ソリューション、およびサービスにつきましては、弊社または弊社製品取扱い代理店までお問い合わせください。

サイバー攻撃よりビジネスを守る、カスペルスキーのセキュリティ・ソリューションを、是非お試しください。

▶ セキュリティ・インテリジェンスこそが カスペルスキーの DNA



▶ カスペルスキーのセキュリティは 何が違うのか？

カスペルスキーは、弊社のあらゆる製品や活動に業界をリードするセキュリティ・インテリジェンス情報をDNAとして活用することで、市場で最も強力なアンチマルウェア・ソリューションを提供しています。

- Kaspersky は、CEO であるユージン・カスペルスキーを頂点とする、テクノロジーを主眼に置いたセキュリティ専門ベンダーです。
- 選り抜かれた IT セキュリティ専門家の集団である Global Research & Analysis Team (GReAT) は、世界で初めて地上最凶のマルウェア脅威や標的型攻撃を発見しました。
- Kaspersky Labは、世界で高く評価されているセキュリティ関連組織や、法執行機関等の組織に対しセキュリティ支援を提供しています。
- Kaspersky Lab では、コアテクノロジーをすべて自社内で開発し完成させており、その製品は高い安定性と効率性を備えています。
- Kaspersky Lab では毎年、他のどのベンダーよりも多くの第三者機関による検証に参加しており、また、他ベンダーと比べ非常に多くの第一位を獲得しています。
- Gartner, Inc や Forrester Research、International Data Corporation (IDC) などリサーチ会社により、多くの IT セキュリティカテゴリにおいて Kaspersky Lab をリーダーとして位置付けています。
- カスペルスキーのテクノロジーは、Microsoft®、Cisco® Meraki、Juniper Networks、Alcatel Lucent などを含む130社以上のベンダーの製品にOEMとして採用されています。

これらの理由がカスペルスキーの優位性です。

▶ カスペルスキーのアンチマルウェアテクノロジーについて

IT セキュリティ・ソフトウェアの能力はその中心となるセキュリティエンジンによって決まります。パッチ管理、MDM、暗号化、デバイスコントロール、アンチフィッシングなどを始めとする多くのテクノロジーにより、強力なセキュリティ・レイヤが構築されます。企業は、既知や未知、あるいは新しい脅威に対して屈することがあってはなりません。

カスペルスキーのセキュリティエンジンは、その卓越したダイナミックな脅威インテリジェンスによって常に強化され、改良が続けられています。脅威インテリジェンスとグローバルエクスペリエンスに基づいた、セキュリティへの特化がカスペルスキーの存在を際立たせているのです。

Kaspersky Endpoint Security for Business プラットフォームに組み込まれたアンチマルウェアエンジンが業界トップクラスの性能を有しているということは、最新の第三者機関による検証結果によっても実証されています。このカスペルスキーのプラットフォームを利用し、正しく運用することにより、より安全なセキュリティ環境を維持することが可能となります。

以下、カスペルスキーのアンチマルウェア保護がパワフルで、他社製品よりもはるかに効果的である理由についてご説明します。

主要製品機能	特長	機能
• 既知や未知、また最新の脅威の検知 • ふるまいおよびヒューリスティック分析 • クラウドベースのマルウェア検出 - Kaspersky Security Network (KSN) • アクティブ駆除 • 暗号化およびランサムウェア防御 • 脆弱性攻撃ブロック • HIPS およびパーソナルファイアウォール • ネットワーク攻撃防御 • シンプルで透過的な管理コンソール	多層防御のセキュリティ・アプローチ 今日、カスペルスキーが市場で最も効果的なセキュリティを提供できる理由の1つが多層型のアプローチです。カスペルスキーのテクノロジーは自社で開発しているため、複数のセキュリティ・レイヤによる、パフォーマンスへの影響を最小限に抑えつつシームレスに実現することができます。 各セキュリティ・レイヤはそれぞれが異なる面よりサイバー攻撃に対応するよう設計されており、IT 担当者は強固に結び付いた各種テクノロジーを利用し、より高度で、より広範なセキュリティを実現することができます。 世界をリードする脅威インテリジェンスと、常に保護されている安心感 カスペルスキーのグローバルな脅威インテリジェンス情報は世界的に知られており、またその専門的知識は、変化を続けるITネットワーク環境で常に進化するよう設計されたカスペルスキーのセキュリティ製品にダイレクトにフィードバックされています。	ヒューリスティックセキュリティ - システムの負荷を軽減 パターン・マッチング技術をベースにした他社製品と比べ、より高いマルウェア検知力によりセキュリティ強化を実現します。また、これまでに比べパターンファイル更新時のファイルサイズは小さくなりましたが、セキュリティは向上しました。 ふるまい分析 Kaspersky Lab のアンチマルウェアには、プログラム動作分析用のコンポーネントが2つ組み込まれています。 • エミュレーター - プログラムに想定されている動作を再現し、検証します。 • システムウォッチャー - 実行中のプログラムの動作を追跡し、マルウェアに特有の動作パターンを識別し分析します。

クラウドベースのマルウェア検出 - KASPERSKY SECURITY NETWORK (KSN)

新たなマルウェアや未知のマルウェアによる脅威へのリアルタイムな対応を可能にします。カスペルスキー製品を利用するユーザーのうち、ボランティアとしてご協力いただいている6000万人以上のユーザーより、ユーザー環境に対し実際に行われたサイバー攻撃やマルウェアに関する最新情報をご提供いただいた上で、インスタント・ファイル判断を作成します。これにより、すべてのお客様は非常に誤検知の少ないリアルタイム保護によるセキュリティ防御を利用し、特にゼロデイ攻撃による未知の攻撃によるリスクを最小限化することが可能となります。

脆弱性攻撃ブロック (AUTOMATIC EXPLOIT PREVENTION)

脆弱性攻撃ブロックは、マルウェアの典型的な行動パターンや疑わしい行動パターンを判別することにより、多くのユーザーにより利用されているアプリケーションの脆弱性を悪用するマルウェアを防御します。このテクノロジーはエクスプロイトコードの実行を食い止め、マルウェアによりダウンロードされた悪意のあるコードが実行されることを防ぎます。

ランサムウェアによる暗号化への対抗
重要ファイルにアクセスして処理を試みる疑わしい動きがあると、システムウォッチャーは重要ファイルのコピーをテンポラリストレージに保存します。ランサムウェアがオリジナルファイルを暗号化しようとしても、暗号化される前の状態に戻すことができます。

アクティブ駆除

感染が確認されると、オートスタート、マルウェアの破壊、および保存済みファイルのオリジナル状態への「ロールバック」などさまざまな技術を駆使して「治療」し、ファイルを保護します。

ホストベースの侵入防止システム (HIPS) およびパーソナルファイア ウォール

プログラムの動作の中には、悪意あるものとは断定できないものの、きわめてリスクが高く、制限する方が安全であると考えられるものがあります。Kaspersky Lab のホストベースの侵入防止システム (HIPS) は、ネットワーク動作を制限するアプリケーションレベルのパーソナルファイアウォールと連動して、アプリケーションの信頼レベルに基づきシステム内での動作を制限します。

ネットワーク攻撃防御

ネットワーク上での疑わしい動作を監視します。また、疑わしい行動が検出されたときに、システムにどのように対応させるかをあらかじめ設定しておくことができます。

頻繁なアップデート

新たに発見されたマルウェアに関する最新情報は、マルウェア攻撃を防ぐアップデートプログラムと共に、業界最速のサイクルで Kaspersky Security Network (KSN) クラウドからお客様のセキュリティデータベースへ提供されます。

業界トップクラスの 保護性能 - 第三者機関での検証

2014 年、カスペルスキー製品は、第三者機関での検証による評価およびレビューを 93 回受けました。

その結果、トップ 3 には 66 回選ばれ、トップ 3 スコアの 71% に当たるスコアを獲得し、さらに第 1 位には 51 回選ばれましたが、これは受けたテストの半分以上に相当します。

他社の製品またはソリューションでこれに近い成績を残したものはありません。

▶ 企業向けセキュリティ製品、ソリューションおよびサービス

Kaspersky Endpoint Security for Business (KESB)

世界有数の脅威インテリジェンス情報を共有するエコシステムによる専門知識を活用することで、Kaspersky Endpoint Security for Business は、堅牢なアプリケーション、デバイスコントロールツール、ウェブコントロールツール、データ暗号化、モバイルエンドポイントセキュリティ、MDM、システム管理およびパッチ管理などの機能を含む統合プラットフォームに基づいた、多層セキュリティアプローチを提供します。

すべての機能は、管理サーバーとして機能する、Kaspersky Security Center より集中管理を行えます。

Kaspersky Targeted Solutions

Kaspersky Lab によるセキュリティを IT システムの特定環境においてご利用いただくためのスタンドアロン製品です。

Kaspersky Vulnerability and Patch Management など一部の製品は、Kaspersky Endpoint Security for Business の一部として利用することが可能です。

Kaspersky Security for Virtualization などその他の製品については Targeted Solutions のみで提供されています。

すべてのカスペルスキー製品は、同一の最先端テクノロジーと脅威インテリジェンスに基づいて構築されており、物理エンドポイント、モバイルエンドポイントおよび仮想エンドポイントのセキュリティソリューションは Kaspersky Security Center により集中管理が可能です。

Kaspersky セキュリティインテリジェンスサービスおよびエンタープライズソリューション

カスペルスキーの脅威インテリジェンス、技術的専門知識、データ、教育スキルを活用して、お客様のブランド、会社および社員のセキュリティ・スキルを大幅に向上させます。

エンタープライズソリューションは、個別の業界およびインフラストラクチャに関するセキュリティ問題や、分散型サービス妨害攻撃 (DDoS) のような特定の形態の攻撃に対しては、エンタープライズ・ソリューションにより対応が可能です。

保守およびサービス契約

カスペルスキーのセキュリティ製品を対象とした幅広いサポートオプションです。

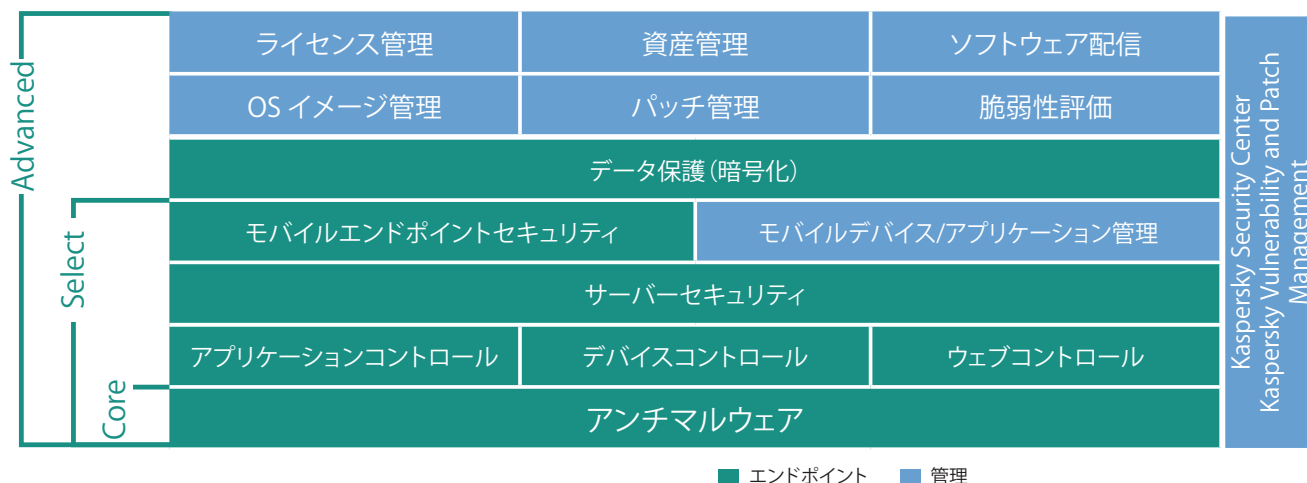
▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS について

(カスペルスキー エンドポイント セキュリティ フォー ビジネス)

Kaspersky Endpoint Security for Business (KESB) は世界トップクラスのセキュリティエキスパートが設計した、セキュリティ製品です。セキュリティ防御に必要な各セキュリティ・コンポーネント機能に基づき構成された非常に強固で、先進的な保護機能と効率のよいパフォーマンス、そしてシンプルな管理が企業のセキュリティを万全なものにします。

本製品で提供される各コンポーネントはすべてカスペルスキー自身が設計および開発しており、それらを組み合わせることでお客様のビジネスニーズに合った1つのセキュリティ・プラットフォームを構築することができます。その結果、各コンポーネント間でのギャップや互換性に関する問題や、規模やセキュリティ実施が増えるに従い激増する管理負荷も大きく抑えることを実現した、非常に安定した統合ソリューションが誕生しました。

管理者は、Kaspersky Endpoint Security for Business によって、ITネットワーク環境における保護の実施、管理の実行、状況の確認などを総合的に行うことが可能です。セキュリティと IT に対するニーズの進化に対応するために、日々進化が求められるIT環境や、新たなサイバー脅威へ確実に対応するために、カスペルスキーの製品では、各ソリューション群において提供されるツールやテクノロジーのバランスが常に最適になるように調整され、常に最適なセキュリティ対策を最も効果的な管理を両立し実現します。

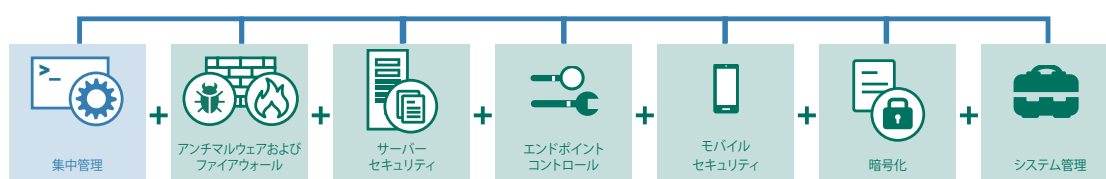


カスペルスキーではすべての製品が同じコードをベースに動作し、最新の脅威に対しては、クラウドベースの Kaspersky Security Network によるサポートを受け、お客様が必要とする世界トップクラスの保護を提供することができる、多彩なテクノロジーを用意しております。

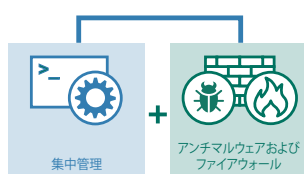
お客様は、このセキュリティ対策に特化したこの優れたセキュリティ・プラットフォームを利用しカスペルスキー製品を利用することで、セキュリティ実施、管理、モニタリングを容易に行うことができます。

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

業界トップのセキュリティ・エキスパートが設計し製品化した強力な多層セキュリティ防御を提供する Kaspersky Endpoint Security for Businessは、世界的に多くの実績のある脅威インテリジェンス情報を活用することにより、既知のリスクだけでなく、未知の攻撃やAPTなど最新のセキュリティ脅威への防御策と統合セキュリティ管理を提供します。



▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS - CORE



アンチマルウェアに特化した製品 - カスペルスキー・セキュリティ・プラットフォームのベース製品

カスペルスキーのセキュリティを熟知したセキュリティ・スペシャリストにより開発され、提供される多層防御テクノロジーは、多くの第三者機関による検証レポートにより公表されている通り、業界で最も強力な効果的なセキュリティ対策を実現します。

既知や未知の脅威、最新の脅威に対する保護 - 先進の独自技術により、未知や既知の攻撃を認識し、確実に防御します。

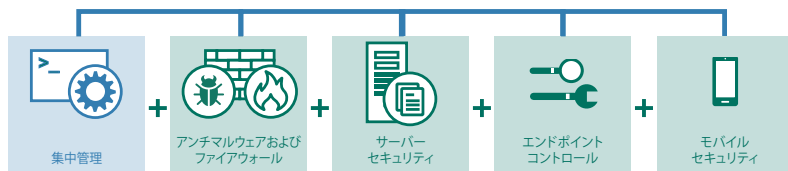
脆弱性攻撃ブロック - 未知および洗練された最新の脅威に対するプロアクティブな防御を提供します。

クラウドベースの保護 - 世界的なネットワークによる Kaspersky Security Network より提供されるリアルタイム情報を活用しています。

システムウォッチャー - 万が一システム自身が攻撃を受けた際に、高度なファイル修復機能を発揮します。

パーソナルファイアウォールによるホストベースの侵入防止システム (HIPS) - HIPSは、アプリケーションの信頼レベルと、ネットワーク上での動作を制限するアプリケーションレベルのパーソナル・ファイアウォールと連携し、動作の制限を実施します。

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT



モバイルデバイスおよびデータ用のプロアクティブセキュリティと管理を組み込んだ、パワフルで緻密なエンドポイントの管理

カスペルスキーのセキュリティラボが提供するダイナミックホワイトリストを含む、アプリケーションコントロール、ウェブコントロール、デバイスコントロールなどのさまざまな特徴的な機能は、新たな局面のエンドポイント・セキュリティをネットワークにもたらします。また、企業や社員がBYODとして利用するモバイル端末に対するセキュリティも同時に実現します。Kaspersky Security Centerの管理コンソールを利用すると、すべてのプラットフォーム及び保護対象となるエンドポイントは、集約的に管理を行えるようになります。さらに、強力なファイルサーバー保護テクノロジーにより、万が一のマルウェア感染の際も、感染がエンドポイントに拡散してしまうことを防御します。ファイルサーバー保護により、保存データを介してエンドポイントに感染が広がることはありません。

エンドポイントコントロール

ダイナミックホワイトリストによるアプリケーションコントロール - ネットワーク管理者は、Kaspersky Security Networkが提供するリアルタイム・ファイルレピュテーション情報により、ホワイトリストをベースにした「デフォルト拒否」ポリシーを用いたアプリケーションの許可、ブロック、制限等のコントロールを実際の環境や、検証環境において利用することが可能となります。アプリケーションの権限コントロールと脆弱性スキャンは、疑わしい動作を行うアプリケーションを監視します。

ウェブコントロール - プリセットとして事前設定されたポリシーか、環境に応じてカスタマイズを行った設定を基にWebブラウジングに関するポリシーの設定が可能で、包括的な監視や、効率的な管理を行えます。

デバイスコントロール - PCに接続されるリムーバブル・ディスクや、USBメモリ、その他接続機器類に対するデバイスコントロールは、利用権限や部門など利用環境での目的に応じて段階的な設定を行えます。スケジュールを設定したり、一括でのデバイス登録など、細かいコントロールにも対応します。

サーバーセキュリティ

Kaspersky Security Center を通じて、エンドポイントセキュリティと集約的な統合管理を行えます。

モバイルセキュリティ:

モバイルデバイス用の強力なセキュリティ - 洗練されたプロアクティブなクラウドベースのテクノロジーにより、モバイル・エンドポイントに対するリアルタイムな多層防御を実現します。

Webプロテクション、アンチスパム、アンチフィッシングのコンポーネントにより、高度なデバイスセキュリティを実現します。

リモート盗難対策 - ロック、消去、位置の特定、SIMの監視、アラーム、遠隔撮影、全体または一部データの消去などの機能により、モバイルデバイスを紛失したり、盗難に遭った際の企業データへの不正アクセスを防ぎます。管理者またはユーザーの利用開始時には、Google Cloud Management による機器のクイック認証を利用することにも対応しています。

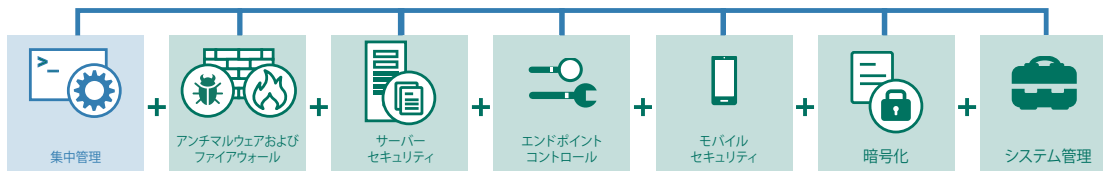
Mobile Application Management (MAM) - ユーザーがホワイトリストにあるアプリケーションを実行できないように制限し、不要または未知のソフトウェアを導入しないようにします。「アプリケーションラッピング」は、社員が所有するデバイス上に存在する企業データを隔離します。データの暗号化やデータの消去等のコントロールも必要に応じてリモートより実行が可能です。

Mobile Device Management (MDM) - Microsoft® Exchange ActiveSync およびOTA(Over The Air)のポリシーマネージメントによるiOS MDMデバイスに対する統合管理インターフェースを提供します。

セルフサービスポータル - ネットワーク利用者によるデバイス管理が可能なポータルで、アクセスに必要な証明書やキーの自動インストールや、機器が盗難された際の緊急アクティベーション等の対応等を含むさまざまな機能が提供され、特にIT管理者の管理負荷を大幅に低減します。

Kaspersky Endpoint Security for Business - SELECT は、CORE のすべての機能を含み提供いたします。

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED



システム管理ツールが IT の効率とセキュリティを最適化し、統合された暗号化テクノロジーが重要データを保護

自動パッチ管理、OS イメージ管理、リモートソフトウェア配信、SIEM との連携により管理業務の合理化を図ります。また、ハードウェアおよびソフトウェアのインベントリと、ライセンス管理によって、IT ネットワーク環境を可視化し、客観的な判断の基に管理を行えるよう改善します。

Advancedでは、暗号化機能が新たに追加され、データ保護による情報漏洩対策も行えます。統合された暗号化テクノロジーにより、データ保護がさらに厚みを増します。

システム管理

脆弱性およびパッチ管理 - OS とアプリケーションの脆弱性を自動で検知して優先順位を設定し、パッチとアップデートプログラムをいち早く自動配布します。

オペレーティングシステムの展開 - OS 「ゴールデン」イメージを一箇所から容易に作成、保存、展開します。UEFI もサポートします。

ソフトウェアの配信とトラブルシューティング - リモートでのソフトウェア展開や、アプリケーションと OS の更新は、オンデマンドでの実行も定期実行も可能で、Wake-on-LANにも対応します。時間節約に有効なリモート・トラブルシューティングと効率的ソフトウェア配信は、マルチキャスト技術によってサポートされています。

ハードウェアおよびソフトウェア・インベントリとライセンス管理 - ID、可視化機能、制御機能（ブロックなど）と、ライセンス使用状況の管理機能を組み合わせることで、IT 環境全体に展開されたすべてのソフトウェアとハードウェアの状態を（リムーバブルデバイスを含め）正確に把握することができます。さらに、ソフトウェアとハードウェアのライセンス管理、ゲストデバイス検出、権限コントロール、アクセス・プロビジョニングも備えます。

SIEM 統合 - IBM® QRadar および HP ArcSight SIEM システムをサポートします。

担当業務に応じたアクセス制御（RBAC） - 管理上の責任を複雑なネットワーク全体にわたって割り当てます。コンソールビューは、割り当てられたロールと権限に基づいてカスタマイズ可能です。

暗号化

強力なデータ保護 - ファイル/フォルダーレベル暗号化（FLE）とフルディスク（FDE）暗号化をエンドポイントに適用することができます。「ポータブルモード」のサポートによって、管理ドメインから離れるデバイスの暗号化も管理できます。

柔軟なユーザーログイン - セキュリティ強化のための起動前認証（PBA）には、「シングルサインオン」オプションがあり、ユーザーが意識せずに利用することができます。2 段階認証やトークンベースの認証も可能です。

統合されたポリシー作成 - 暗号化にアプリケーションとデバイスの制御を組み合わせるという独自のアプローチにより、セキュリティをいっそう強化するとともに、管理業務を簡素化します。

Kaspersky Endpoint Security for Business - ADVANCED は、SELECT および CORE のすべての機能を含み提供いたします。

▶ 製品機能

各製品で提供される機能

	Core	Select	Advanced	Security Center による管理	Targeted Solution として提供
アンチマルウェア	●	●	●	●	
ファイアウォール	●	●	●	●	
アプリケーションコントロール		●	●	●	
デバイスコントロール		●	●	●	
ウェブコントロール		●	●	●	
ファイルサーバーのセキュリティ		●	●	●	●
モバイルエンドポイントの保護		●	●	●	
モバイルデバイス/アプリケーションの管理		●	●	●	
暗号化			●	●	
脆弱性監査			●	●	●
パッチ管理			●	●	●
資産管理			●	●	●
ライセンス管理			●	●	●
ソフトウェア配信			●	●	●
オペレーティングシステムの展開			●	●	●
メールサーバーセキュリティ				▲	●
インターネットゲートウェイのセキュリティ					●
仮想環境のセキュリティ				●	●

● 対応

▲ 一部対応 - 詳細については製品ページを参照してください。

▶ KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server は、費用効果、信頼性、スケーラビリティにすぐれたセキュリティソリューションで、システムパフォーマンスに大きな影響を与えることなく、共有ファイルストレージを保護します。

特長

強力なアンチマルウェア保護

さまざまな賞の受賞歴があるカスペルスキーのアンチマルウェア・エンジンが、サーバーを強力に保護します。既知のマルウェアだけでなく、最新の未知の脅威であったとしても、悪意のあるプログラムや、疑わしいプログラムなどのネットワークへの侵入を確実に防御します。

高いパフォーマンスと信頼性

Kaspersky Security for File Server は、ネットワークが高負荷な状態にある場合でも、システムの動作速度が著しく低下することはなく、業務の妨げとなることもありません。

マルチプラットフォームのサポート

さまざまな異なるサーバーが混在する環境においても、単一のセキュリティ・ソリューションにより確実なセキュリティ効果を実施できます。ターミナル、クラスター、仮想サーバーといった最新のプラットフォームやサーバーをサポートし、互換性の問題は発生しません。

強力な管理機能とレポート機能

効果的で使いやすい管理ツール、サーバーの保護ステータスに関する情報、スキャン時間の柔軟な設定、包括的なレポートシステムによって、ファイルサーバーのセキュリティを効率的に管理することができ、TCO を低減します。

機能

- リアルタイムのアンチマルウェア保護 - 最新バージョンの Windows[®] (Windows Server[®] 2012/R2 を含む)、Linux[®]、FreeBSD (共に Samba を含む) が動作するファイルサーバーに対応します。

- Citrix および Microsoft[®] のターミナルサーバーの保護

- クラスターサーバーを全面的にサポート

- スケーラビリティ - さまざまな機種により構成される複雑なネットワーク環境においても、簡単に導入でき、確実な保護を実施可能です。

- 信頼性、安定性、高度な耐障害性

- 最適化されたインテリジェントなスキャン技術 - オンデマンドスキャンや、重要なシステム領域のスキャンにも対応します。

- 信頼リスト - セキュリティ・パフォーマンスを高める一方で、スキャンに必要なリソースレベルを低減します。

- データの隔離とバックアップ - 駆除や削除の前に実行します。

- 柔軟な構成オプションによる集中インストール、管理、アップデート

- 柔軟なインシデント対応シナリオ

- ネットワーク保護の状況に関する包括的なレポート

- アプリケーション・ステータス通知システム

- 階層型ストレージ管理 (HSM) システムのサポート

- 定評ある Hyper-V と Xen Desktop のサポート

- VMware Ready 認定

- ReFS のサポート

Kaspersky Security for File Server は、Kaspersky Endpoint Security for Business - SELECT および ADVANCED のすべての機能を含み提供いたします。また、Targeted Solution として別途購入することもできます。

[illegible]

▶ カスペルスキーのエンドポイント コントロール・テクノロジーについて

最新鋭のアンチマルウェアや、業界唯一のホワイトリスト専門ラボと緊密に統合された強力なエンドポイント・コントロール・ツールによって、常に変化するサイバー脅威より企業の IT 環境を確実に守ります。

保護、実施、制御

• 信頼するアプリケーションの脆弱性や Web 上のマルウェアの存在、周辺機器に対するコントロールの欠如などが、脅威を取り巻く状況をますます複雑なものとしています。カスペルスキーのアプリケーションコントロール、ウェブコントロール、デバイスコントロール・ツールは、生産性を損なうことなく、エンドポイント全体の管理を実現します。

アプリケーションコントロールとダイナミックホワイトリスト
エンドユーザーのふるまいにかかわらず、エンドポイントでの使用が認められたアプリケーションやプログラムに関する全面的な制御権限を管理者に与えることで、既知の脅威と未知の脅威からシステムを保護します。さらに、アプリケーションのふるまいを監視、評価し、エンドポイントやネットワークを危険に

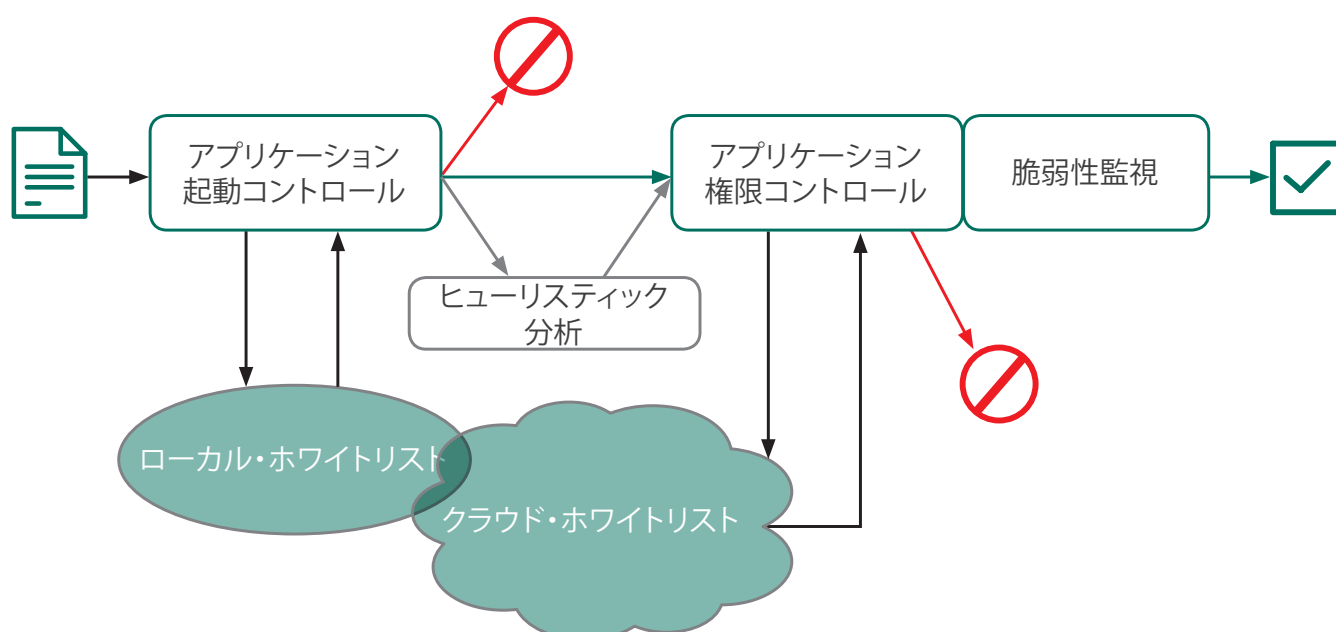
さらすおそれのある想定外の動作を未然に防ぎます。簡素化、カスタマイズ、自動化が可能なポリシーの作成と実施により、以下のことが実現します。

- アプリケーション起動コントロール：アプリケーション立ち上げの許可、ブロック、監査が可能です。業務に無関係なアプリケーションへのアクセスを制限することにより、生産性が向上します。
- アプリケーション権限コントロール：システムリソースやデータへのアプリケーションアクセスを規制し、管理します。アプリケーションを「信頼できる」「信頼できない」「禁止」に分類します。Web ブラウザーや Skype から投稿された情報など、エンドポイントにある暗号化データへのアプリケーションアクセスを管理します。

• アプリケーション脆弱性スキャン：信頼するアプリケーションの脆弱性を狙った攻撃をプロアクティブに防御します。

管理ソリューションの多くは、基本的なブロック機能やアクセス機能しか備えていません。カスペルスキーのコントロールツールは、クラウドベースのホワイトリスト・データベースを使用し、最新のアプリケーション情報にほぼリアルタイムでアクセスできる点において、他に例がないユニークなツールです。

カスペルスキーのアプリケーションコントロールツールは、クラウドベースのホワイトリスト・データベースを使用して、ダウンロード、インストール、実行といったあらゆる段階で、アプリケーションの分析と監視を行います。



ダイナミックホワイトリストは、全体的な「デフォルト拒否」によって有効化され、管理者が明確に許可した場合を除き、任意のワークステーション上でのアプリケーションの起動をすべてブロックします。

カスペルスキーは、ホワイトリスト専用ラボを保有する唯一のセキュリティ企業であり、5 億以上のプログラムが登録されたデータベースを常時監視し、アップデートを行っています。

カスペルスキーのデフォルト拒否はテスト環境で適用できるため、管理者はブロックを行う前にアプリケーションの動作を確認することができます。さらに、デジタル署名に基づいてアプリケーションのカテゴリを作成することができ、マルウェアによって改竄された正規ソフトウェアや、不審なソースからダウンロードされたソフトウェアの起動を防ぎます。

容易な管理

カスペルスキーのコントロールツールはすべて Active Directory と統合することが可能で、包括的なポリシーを短時間で容易に設定できます。エンドポイント・コントロールはすべて、同じコンソールから1つのインターフェイスで管理します。

ウェブコントロール

エンドユーザーが職場からアクセスする可能性のある Web サイトの監視、フィルタリング、制御が可能です。生産性を高めつつ、Web ベースのマルウェアと攻撃を防ぎます。

カスペルスキーの高度なウェブコントロール機能は、随時アップデートされる Web サイト・ディレクトリに組み込まれており、各サイトが複数のカテゴリに分類されています(アダルト、ゲーム、ソーシャルネットワーク、ギャンブルなど)。管理者は、エンドユーザーによる個々のサイトやサイトカテゴリの使用を禁止、制限、または監査するポリシーを簡単に作成できるほか、独自のリストを作成することも可能です。悪意のあるサイトは自動的にブロックされます。

カスペルスキーのウェブコントロールは、サイトの使用を制限することにより、ソーシャルネットワークやインスタントメッセージ・サービスからの情報漏洩を防ぎます。ポリシーを柔軟に設定でき、たとえば、業務時間中のある特定の時間にのみブラウジングを許可することも可能です。Active Directory と統合されているため、ポリシーを組織全体にわたって、短時間で容易に適用することができます。

セキュリティをいっそう強化するため、カスペルスキーのウェブコントロールはエンドポイントで直接有効化されます。そのため、ユーザーがネットワークにアクセスしていないときでもポリシーが適用されます。

デバイスコントロール

USB ポートを無効化しても、リムーバブルデバイスの問題を解決できるとは限りません。たとえば、USBポートを全てのデバイスに対し無効化してしまうと、トークンを利用したVPNアクセスができなくなるなど、他のセキュリティ対策に影響を与える可能性があります。

カスペルスキーのデバイスコントロールは、バス、タイプ、デバイスの各レベルにおいて、さらにきめ細かな設定と管理が可能であり、ユーザーの生産性の維持と、セキュリティの最適化を同時に実現することができます。デバイスコントロールは、デバイスに固有のシリアル番号に基づいて適用することができます。

- デバイスの接続、読み取り、書き込み権限のほか、利用可能時間を設定できます。
- マスクに基づいてデバイスコントロールのルールを作成でき、ホワイトリスト作成のためにデバイスを物理的に接続する必要がありません。複数のデバイスを同時にホワイトリスト登録できます。
- 社内外のリムーバブルデバイスによるデータ交換を管理します。データ消失や盗難のリスクを低減します。
- カスペルスキーの暗号化テクノロジーと統合することで、特定のデバイスタイプに暗号化ポリシーを適用することができます。

エンドポイント・コントロール・テクノロジーは、Kaspersky Endpoint Security for Business - SELECT および ADVANCED のすべての機能を含み提供いたします。

▶ KASPERSKY SECURITY FOR MOBILE

モバイルデバイスがサイバー攻撃の標的となることが増えています。その一方で、BYOD (Bring Your Own Device) によって社内で利用されるデバイスの種類が増大し、IT 管理者にとって管理が難しい複雑な環境が生まれつつあります。

Kaspersky Security for Mobile は、どんな場所で使用されるモバイルデバイスであっても、進化を続けるモバイルデバイスをターゲットとしたマルウェアより強力に保護します。自社環境内のスマートフォンやタブレットの追跡や管理も短時間で容易に実行でき、リスクの最小化と集中管理による管理効率の向上を実現します。

主要製品機能

- 強力なアンチマルウェア
- アンチフィッシングおよびアンチスパム
- 危険サイトブロック
- アプリケーションコントロール
- ルート化/脱獄 (Jailbreak) 検知
- コンテナ化
- 盗難対策
- モバイルデバイス管理
- セルフサービスポータル
- 集中管理
- Web コンソール
- サポート対象プラットフォーム
 - Android™
 - iOS

特長

モバイルデバイスとデータの保護に特化した高度なアンチマルウェア
カスペルスキーは 2014 年だけでも、約140万件 (重複は除く) ものモバイルマルウェア攻撃に対処しました。Kaspersky Security for Mobile はアンチマルウェア機能を基本に、複数の保護技術を組み合わせ、モバイルデバイス内のデータを狙う既知および未知の脅威に対抗するソリューションです。

モバイルデバイス管理 (MDM)
すべての主要モバイルデバイス管理プラットフォームとの統合により、リモート OTA (Over The Air) での導入と管理が可能になりました。Android、iOS デバイスのユーザービリティが向上し、管理が容易になります。

モバイルアプリケーション管理 (MAM)
コンテナ化と選択的消去機能によって、単一デバイス上での業務データと個人データを分離し、BYOD導入時の管理性を向上します。暗号化機能やアンチマルウェアと組み合わせることで、デバイスやデータを単に分離するだけでなく、プロアクティブな保護が可能なモバイルソリューションとなります。

集中管理

複数のプラットフォームやデバイスを他のエンドポイントと同じ管理コンソールから管理します。これにより、さらなる工程や管理技術を追加することなく可視性を高め、管理を強化することができます。

モバイル向けのセキュリティおよび管理機能

強力なアンチマルウェア
シグネチャを用いた検知と、クラウドを活用 (Kaspersky Security Network: KSN) したプロアクティブな保護機能で、既知および未知のモバイルマルウェア脅威をブロックします。オンデマンドスキャンと定期スキャンに、自動アップデートを組み合わせることで、保護能力がさらに高まります。

アンチフィッシングおよびアンチスパム
強力なアンチフィッシングおよびアンチスパムテクノロジーが、フィッシング攻撃からデバイスとデータを守り、迷惑電話やスパムメッセージを排除します。

ウェブコントロール/セーフブラウザ

これらのテクノロジーは、Kaspersky Security Network (KSN) との連携により、リアルタイムで機能し、悪意のある Web サイトや不正な Web サイトへのアクセスをブロックします。定期的にアップデートされるセーフブラウザのレピュテーション分析機能は、モバイルデバイスでの安全な Web 閲覧を可能にします。

アプリケーションコントロール

KSN と統合されたアプリケーションコントロールは、ユーザーによるアプリケーション利用を管理者が承認したアプリケーションに限定し、グレーゾーンのソフトウェアや未承認のソフトウェアの使用を禁止します。デバイス機能を、必須アプリケーションのインストールに応じて有効化または無効化します。管理者が設定した一定期間アプリケーションが操作されなかった場合、ユーザーに再ログインを求めよう設定することも可能です。そのため、デバイスの紛失や盗難の際にアプリケーションが起動していたとしても、データは確実に保護されます。

ルート化/脱獄 (JAILBREAK) 検知

ルート化や脱獄 (Jailbreak) を自動で検知してレポートします。さらにコンテンツへのアクセスの自動ブロック、選択的消去、デバイスデータ全体の消去といった操作を実行することができます。

盗難対策

デバイスの紛失や盗難の際は、ワイプ、デバイスロック、追跡、SIM 監視、「遠隔撮影」および「アラーム」デバイス検知などのリモート盗難対策機能が起動します。場合によっては、盗難対策コマンドは非常に柔軟な方法で起動させることが可能です。たとえば、Google Cloud Management (GCM) との統合により、コマンドをほぼリアルタイムで送信することで、セキュリティを向上させることができます。また、セルフサービスポータルからコマンドを送信する場合、管理者による対応が不要になります。

モバイルデバイス管理 (MDM)

Microsoft® Exchange ActiveSync、Apple MDM などをサポートします。プラットフォームとは無関係に、統一されたインターフェイスから幅広いポリシーの適用が可能です。たとえば、暗号化やパスワードの使用、カメラ利用の管理、個人ユーザーやグループへのポリシーの適用、APN/VPN 設定の管理等を行えます。

セルフサービスポータル

日常的なセキュリティ管理を社員自身に任せ、承認済みデバイスを各自が登録できます。新しいデバイスの有効化プロセスでは、必要な証明書はすべてこのセルフサービスポータルを通じて自動的に配布されるため、管理者が介入する必要はありません。デバイスを紛失した場合、社員は使用可能なすべての盗難対策措置をこのポータルより実行することができます。

集中管理

すべてのモバイルデバイスを 1 台のコンソールから集中的に管理します。これにより、他のすべてのエンドポイントの IT セキュリティも管理することができます。管理者は Web コンソールを使用して、任意のコンピューターからデバイスをリモートコントロールし、管理することができます。

Kaspersky Security for Mobile は、Kaspersky Endpoint Security for Business - SELECT および ADVANCED のすべての機能を含み提供いたします。

▶ カスペルスキーの暗号化テクノロジーについて

デバイスの紛失や盗難、データ窃盗を行うマルウェアに起因する不正アクセスからデータを保護します。

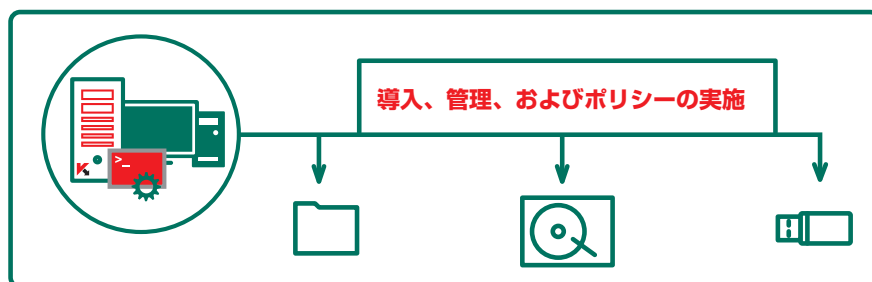
プロアクティブなデータ保護とコンプライアンス対応は、早急に対策を行うべき課題の一つです。カスペルスキーの暗号化テクノロジーは、デバイスの置き忘れや盗難、標的型マルウェア攻撃から重要なデータを守ります。カスペルスキーの強力な暗号化テクノロジーと業界トップクラスのエンドポイント保護テクノロジーが統合されたプラットフォームは、保存データおよび送信データを確実に保護します。

カスペルスキーの暗号化テクノロジーは、カスペルスキー製品の集中管理コンソールより1つのポリシーを使用して、短時間で簡単な導入と管理が可能です。

カスペルスキーが提供する以下の暗号化テクノロジーは、データの消失や情報への不正アクセスを防止：

- フルディスク暗号化 (FDE)
- ファイル/フォルダーレベル暗号化 (FLE)
- リムーバブルデバイスおよび内蔵デバイス

単一の管理コンソールによる集中管理



業界標準の安全な暗号化

カスペルスキーの暗号化は、鍵長 256 ビットの Advanced Encryption Standard (AES) で、鍵の管理やエスクローも容易です。Intel® AES-NI テクノロジー、UEFI、GPT プラットフォームをサポートしています。

高い柔軟性

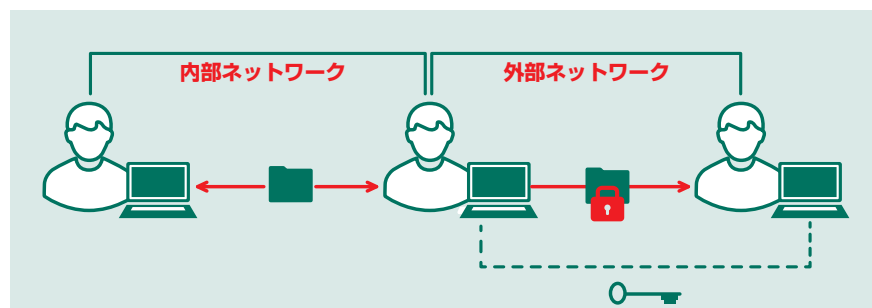
カスペルスキーは、ファイル/フォルダーレベル暗号化 (FLE) とフルディスク暗号化 (FDE) を提供し、さまざまな導入シナリオに対応しています。データは、ハードディスクとリムーバブルデバイスの両方で保護することが可能です。「ポータブルモード」では、暗号化されたリムーバブルメディアのみならず、暗号化ソフトウェアがインストールされていないコンピューターでもデータの使

用や転送が可能であるため、「境界を越えた」安全なデータ交換が実現します。

エンドユーザーが意識することなく利用できるシングル・サインオン機能
カスペルスキーの暗号化テクノロジーは、設定から日常の使用まで、エンドユーザーの生産性を常に損なうことなく、すべてのアプリケーションにわたっ

て透過的に機能します。シングル・サインオンにより、暗号化がシームレスに機能。エンドユーザーは暗号化が実行されていることに気付くことがありません。

カスペルスキーの暗号化テクノロジーは、ネットワーク内外のユーザー間で、シームレスで透過的なファイル転送を可能にします。



暗号化機能

カスペルスキーのセキュリティテクノロジーにシームレスに統合
カスペルスキーのアンチマルウェア、エンドポイントコントロール・管理テクノロジーとの包括的な統合により、共通のコードを利用し構築された真の多層セキュリティが実現します。たとえば 1 つのポリシーだけで、複数のリムーバブルデバイスで暗号化を実行することも可能です。アンチマルウェア、デバイスコントロール、その他のエンドポイントにおけるセキュリティ構成要件と同一のポリシーに基づいて、暗号化に関する設定を適用することが可能です。

暗号化を導入する場合でも、複数の異なるソリューションを導入し、異なる管理方法を導入する必要は一切ありません。暗号化を行うハードウェアの互換性については、暗号化を実行する前に自動的に確認されます。UEFI および GPT プラットフォームを標準でサポートします。

役割ベースのアクセスコントロール
大規模環境では、各管理者の業務内容に応じたアクセスコントロール機能による管理権限の設定を行えます。これにより、暗号化管理の複雑さを軽減することができます。

プリブート認証 (PBA)
オペレーティングシステムのブート前にユーザー認証情報を要求することで、より高いレベルのセキュリティを実現します (オプションのシングル・サインオンも利用可能)。カスペルスキーの暗号化テクノロジーである PBA は、QWERTY 配列以外のキーボードにも対応しています。

スマートカードおよびトークン認証
広く利用されているスマートカードやトークンによる二要素認証をサポートしています。ユーザー名やパスワードの追加設定が不要となり、ユーザーの操作性が向上します。

緊急復元

ハードウェアまたはソフトウェアで障害が発生した場合、管理者はデータの複合化を行えます。PBA や暗号化されたデータへアクセスするためのユーザー・パスワードの復元は、チャレンジ/レスポンス認証メカニズムを利用できます。

導入の最適化、カスタマイズ可能な設定

カスペルスキーの暗号化機能は、Kaspersky Endpoint Security for Business の「Advanced」で利用が可能で、簡単に導入いただけます。暗号化の設定は事前に定義されていますが、[マイ ドキュメント]、[デスクトップ]、[新しいフォルダー]などの一般的なフォルダー、ファイル拡張子、Microsoft® Office 文書、メッセージアーカイブなどのグループに関してはカスタマイズすることができます。

暗号化テクノロジーは、Kaspersky Endpoint Security for Business - ADVANCED でご提供いたします。

▶ KASPERSKY VULNERABILITY AND PATCH MANAGEMENT

集中型 IT 管理ツールによりセキュリティを強化し、複雑なIT環境の管理を容易にします。

一般的に多く使われているさまざまなアプリケーションに存在する脆弱性に対するパッチ適用の課題は、企業のITセキュリティ部門にとって、大きな課題の一つです。この脆弱性への対応に関するリスクは、IT 環境がより複雑化することで、さらに深刻なものとなっています。管理を行うITネットワーク環境内には何が存在し、どういう状況にあるのかを把握できなければ、適切な対応を行い、確実なセキュリティ対策を実施することはできません。

脆弱性評価、パッチ配信、アップデート配信、インベントリ管理、アプリケーションの導入やインストールなど、セキュリティ、設定、管理にかかわる重要タスクの集中処理と自動化によって、IT 管理者は時間を節約するだけでなく、セキュリティの最適化を図ることも可能になります。

Kaspersky Vulnerability and Patch Management は、IT セキュリティのリスクを最小限に抑え、IT の複雑さを解消します。IT マネージャーは、多数のデバイス、アプリケーション、ユーザーを単一の管理コンソールよりリアルタイムで管理し、環境全体を把握することができます。

主な製品機能

- 脆弱性監査とパッチ管理
- ハードウェアおよびソフトウェアのインベントリ
- リモートでのソフトウェアのインストールとトラブルシューティング (リモートオフィスにも対応)
- オペレーティングシステムの導入
- SIEM との統合
- ロールベースのアクセスコントロール
- 集中管理

セキュリティの強化

タイムリーな自動パッチ配信とアップデートにより、IT セキュリティを強化し、日常業務の負荷を軽減します。脆弱性の発見と優先順位設定が自動で行われるため、効率が高まり、管理リソースへの負荷が軽減されます。第三者機関による検証¹で、カスペルスキーは最も広範な自動パッチ配信およびアップデート配信を最も短時間で提供していることが証明されました。

管理対象の総合的な可視化

単一の管理コンソールによりネットワーク全体を見渡せることから、管理者は推測に頼る必要がなく、ネットワークにアクセスするアプリケーションやデバイス (ゲストデバイスを含む) をすべて把握することができます。これにより、企業データやアプリケーションにアクセスするユーザーとデバイスを、IT ポリシーに沿って漏れの無い集中管理を行うことが可能となります。

集中管理

カスペルスキーの Vulnerability and Patch Management は、Kaspersky Security Center と同時利用を行えるプログラムです。機能はすべて管理コンソールより、集約的なアクセスおよび管理を行い、一貫性のある直観的なコマンドとインターフェイスを使って日常的な IT タスクを自動化します。

機能

脆弱性監査とパッチ管理

自動ソフトウェアスキャンにより、脆弱性の検出、緊急度や優先度の設定、対応を迅速に実行することができます。Microsoft® 社製の OS やアプリケーションおよびそれ以外の各種アプリケーションに対するパッチおよびアップグレードの配信は、非常に短時間のうち²に自動的に実行されます。管理者はパッチのインストール状況に関する通知を受け取ることが可能です。

1, 2 カスペルスキーが委託し、AV-TEST GmBH が実施したパッチ管理ソリューションテスト (2013 年 7 月)

重要度の低い修正プログラムの適用は、夜間などに行うよう設定を行えます。その際シャットダウンしている PC は Wake-on-LAN 機能を利用し更新を行います。マルチキャスト・ブロードキャストによって、リモートオフィスへのパッチおよびアップデートのローカル配信が可能になり、ネットワーク帯域への影響を最小限に抑えます。

ハードウェアとソフトウェアのインベントリ

リムーバブルデバイスを含むハードウェアとソフトウェアの自動検出、インベントリ、通知、追跡機能により、管理者は自社のネットワークで使われているデバイスや IT 資産情報を詳細に得ることが可能です。ゲストデバイスを検出し、一時的なインターネットアクセスを許可することも可能です。アプリケーションなどのライセンス管理機能は、実際に利用しているノード数や有効期限の把握に役立ちます。

オペレーティングシステムとアプリケーションを柔軟にプロビジョニング最適に保護されたシステムイメージの作成、保存、クローン作成、導入が集中的かつ容易に行えます。インストール後編集機能による、Wake-on-LAN 機能を利用した、夜間などの自動インストールに対応しています。フレキシビリティ性が向上しました。UEFI をサポートしています。

ソフトウェアの導入支援

単一の管理コンソールより、リモートからのソフトウェアの導入やアップデートを行えます。Kaspersky Security Network を介して識別した 100 以上の一般的なアプリケーションを、必要に応じてスケジュール化し自動インストールすることができます。セッションログや、監査、ユーザー権限の適切な設定などセキュリティを配慮した上でのリモートからトラブルシューティングに対応しています。ソフトウェア配信に最適化されたマルチキャスト・テクノロジーにより、リモートオフィスへのトラフィックを軽減します。

SIEM 統合

IBM® QRadar や HP ArcSight などさまざまな SIEM 製品に直接イベント転送を実行します。ログやその他のセキュリティ関連データを収集し、管理者の負荷とツールの数を最小限に抑えつつ、エンタープライズ・レベルのレポートを簡単に行えます。

役割ベースのアクセスコントロール

複雑な更生のネットワーク環境において、管理者の役割に応じて管理権限を設定することが可能です。役割と管理権限に応じて管理コンソールの表示内容もカスタマイズすることも可能です。

集中管理

カスペルスキーのセキュリティ製品を管理するための統合管理ツールである、Kaspersky Security Center の管理コンソールより、ネットワーク全体におけるデスクトップ、モバイル、仮想エンドポイントのシステムセキュリティ管理をサポートします。

Kaspersky Vulnerability and Patch Management は、Kaspersky Endpoint Security for Business - ADVANCED に含まれます。または、Targetted Solution として単一製品にて購入いただけます。

▶ KASPERSKY SECURITY FOR LINUX MAIL SERVER

Kaspersky Security For Linux Mail Server は、複雑でさまざまな機種が混在するネットワーク環境において、スパムやフィッシングメール、高度なマルウェアなどのマルウェアよりメールサーバーを通過するトラフィックを守ります。

特長

マルウェア攻撃に対する保護
さまざまな賞の受賞歴のあるカスペルスキーのアンチマルウェア・エンジンは、プロアクティブなエクスプロイト保護や、疑わしい URL のフィルタリングなどの機能は、クラウドベースの Kaspersky Security Network(KSN) と共に強力なマルウェア防御機能を提供します。

アンチスパムによる保護
カスペルスキーのクラウドベースのアンチスパム・エンジンは Linux[®] ベースのメールサーバーに関して、誤検知を最小限に抑えた上で、時間やリソースを浪費するスパムを 99.96 % ブロックすることが証明されています。

シンプルで柔軟な管理
ユーザーフレンドリーな管理およびレポートツールと、フレキシブルなスキャン設定によって、メールやドキュメントのセキュリティを効果的に管理することが可能になり、総所有コストの低減を実現します。

機能

- クラウドベースの Kaspersky Security Network の情報を活用するアンチマルウェアによるリアルタイムの保護
- 未知のエクスプロイトやゼロデイ脆弱性に対する迅速な保護
- スパムに対抗する高度な保護 - カスペルスキーのアンチスパム・エンジンにより、迷惑メールトラフィックの 99 % 以上をブロック
- 認識された添付ファイルの形式、サイズ、名称によるメッセージのフィルタリング
- 簡単で便利なアンチマルウェアおよびアンチスパムデータベースのアップデートプロセス
- 駆除または削除の前にデータのバックアップ保存を実行
- スケーラビリティと耐障害性

- 簡単なインストールと柔軟な統合管理
- 強力な通知システム
- ネットワークの保護ステータスに関する包括的なレポート

▶ KASPERSKY ANTI-VIRUS FOR PROXY SERVER

Kaspersky Anti-Virus for Proxy Server は、内部ネットワーク環境へのマルウェアの侵入や攻撃を効果的に防御します。

特長

強力なセキュリティ保護により、ネットワークのダウンは最小限に悪意のあるプログラムにより未知および既知のマルウェアや潜在的なセキュリティ脅威がネットワーク内部へ侵入を試みた場合でも、数々の受賞歴のあるカスペルスキーのアンチマルウェア・エンジンが確実に防御し、内部ネットワーク環境を保護します。

最適化によるパフォーマンス効率
最適なインテリジェント・スキャンと負荷分散テクノロジーにより、リソースにかかる負荷を軽減し、セキュリティパフォーマンスを損なうことなく、ネットワーク帯域の浪費を防ぎます。

シンプルな管理とレポート機能
シンプルでユーザーフレンドリーな管理ツール、フレキシブルなスキャン設定、保護ステータス報告システム等の機能を提供します。

機能

- 新たな脅威と既知の脅威に対する常時稼働のプロアクティブ保護
- すぐれたマルウェア検知率と非常に少ない誤検知
- 最適化されたインテリジェント・スキャンテクノロジー
- 公開サーバーからのHTTP、HTTPS、FTP トラフィックのリアルタイムスキャン
- 広く普及している Linux プロキシサーバー Squidの保護
- インストール、管理、アップデート用の使いやすいツール
- フレキシブルなスキャンツールとインシデント対応シナリオ
- サーバープロセッサの負荷分散
- スケーラビリティと耐障害性
- ネットワークの保護ステータスに関する包括的なレポート

▶ KASPERSKY SECURITY FOR VIRTUALIZATION

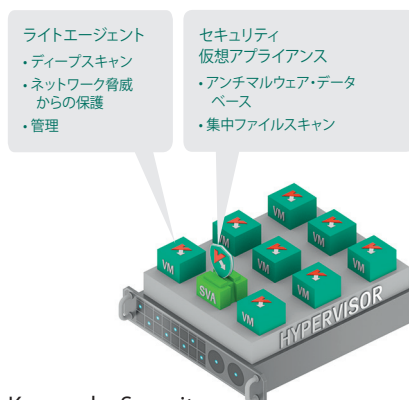
Kaspersky Security for Virtualization は、環境の保護とパフォーマンスを両立するフレキシブルなソリューションです。

高度な保護のための ライトエージェント

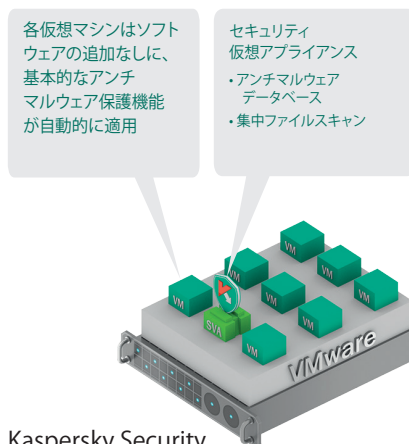
Kaspersky Security for Virtualization には、各仮想マシンに導入される軽量ながらも強力なエージェントが用意されています。このライトエージェントにより、高度なエンドポイントセキュリティ機能を起動することができます。これには、脆弱性の監視、アプリケーションコントロール、デバイスコントロール、ウェブコントロール、インスタントメッセージ/メール/Web 用アンチウイルス保護、高度なヒューリスティックが含まれます。その結果、効率的なパフォーマンスを備えた強力な多層セキュリティが実現します。

VMWARE 環境向けエージェントレス構成 (オプション)

VMware テクノロジーとの緊密な統合により、Kaspersky Security for Virtualization はエージェントレスセキュリティ構成のこのプラットフォーム上で非常に容易な導入と管理が可能です。すべてのセキュリティ活動が Security Virtual Appliance にまとめられており、迅速な自動仮想マシン保護のための vShield とのインターフェイスやネットワーク保護のための vCloud とのインターフェイスも備えています。



Kaspersky Security for Virtualization
ライトエージェント構成



Kaspersky Security for Virtualization
エージェントレス構成*

主要製品機能

- Kaspersky Security Center による集中管理
- SVA ベースの集中的な VM 保護
- 高度なアンチマルウェア
- ホストベースの侵入防止システム (HIPS) およびファイアウォール
- アプリケーション、Web アクセス、境界におけるエンドポイントコントロール
- Kaspersky Security Network によるクラウドベースのセキュリティ
- ネットワーク攻撃のブロック
- アンチフィッシング
- IM、メール、インターネットトラフィック用アンチウイルス
- 新たに VM を作成する際も追加インストールや再起動は不要**

マルチプラットフォーム：
シングルコスト

Kaspersky Security for Virtualization
のライセンスには、Citrix、Microsoft®、
VMware に基づいた仮想環境に対する
サポートが含まれています。

プラットフォーム・アーキテクチャと
の統合

Kaspersky Security for Virtualization
は、VMware、Microsoft® Hyper-V®、
Citrix Xen プラットフォームとそれぞ
れのコアテクノロジーをサポートして
います。

セキュリティ仮想アプライアンス
(SVA)

カスペルスキーはこの分野用に 2 つ
の重要な製品を提供しています。い
ずれもセキュリティ仮想アプライア
ンスを使用するソリューションです。

カスペルスキーの Security Virtual
Appliance (SVA) は、ホスト環境にある
すべての VM を集中的にスキャンしま
す。このアーキテクチャにより、エンド
ポイントリソースを犠牲にすることな
く効果的な VM 保護を行うことがで
き、アンチウイルス・スキャンやアッ
プデート「ストーム」、「インスタント ON」
ギャップを除外し、統合率を大幅に向
上することができます。

VMware	Microsoft Hyper-V	Citrix Xen
ハイアベイラビリティ	ダイナミックメモリ	ダイナミックメモリ管理
vCenter 統合	クラスター共有ボリューム	VM 保護および復元 (VMPR)
vMotion - ホスト DRS	ライブ・バックアップ	Xenmotion (ライブマイグレーション)
Horizon View (フルクローンおよびリンク済み クローン)	ライブ・マイグレーション	マルチストリーム ICA
		Citrix レシーバー
		パーソナル vdisk

* この構成では、ファイル隔離、HIPS、脆弱性スキャン、エンドポイントコントロールなどの高度なセキュリティ機能は使用できません。

** 非持続的 VM に関しては、ライトエージェントを VM のイメージに含めた後、インスタント保護が使用できるようになります。
持続的 VM に関しては、管理者はインストール中に、手動でライトエージェントを導入する必要があります。

注意：一部機能及び対応プラットフォームは、日本語版では今後対応となるものも含まれます。最新情報については、弊社までお問い合わせいただくか、
弊社Webサイトをご覧ください。

▶ KASPERSKY SECURITY INTELLIGENCE SERVICES

CISO/シニアレベルのセキュリティ担当者は、自社のネットワーク環境を常に最新の脅威より確実に保護し、将来予想される危険に備えておくことが求められます。そのため、一部の企業しか自社開発できない戦略的なセキュリティ・インテリジェンスが必要になります。

カスペルスキーは多様な経路を通じて入手した最新のインテリジェンス情報提供するビジネスパートナーで、お客様の SOC/IT セキュリティチームがオンライン脅威から自社を守るため万全の備えをできるようサポートいたします。

サイバーセキュリティ教育

カスペルスキーのサイバーセキュリティ教育プログラムは、自社のインフラストラクチャや知的財産をより確実に保護するためにサイバーセキュリティの役割を拡大することを考えている企業を念頭に開発されたものです。

カスペルスキーのサイバーセキュリティ教育プログラムは、お客様が次の 3 つの主要分野でサイバーセキュリティに関する知識を広げること支援するため、セキュリティの基礎から高度なデジタルフォレンジック、マルウェア分析まで、あらゆるテーマを取り上げています。

- サイバーセキュリティの基礎知識
- デジタルフォレンジックおよびインシデント・レスポンス
- マルウェア分析およびリバースエンジニアリング

THREAT DATA FEED

カスペルスキーの Threat Data Feed は、最新のセキュリティ・インテリジェンス情報と既存のセキュリティ情報/イベント管理 (SIEM) システムを統合して、新たな保護階層を構築するものです。

マルウェア分析、デジタルフォレンジック、インシデント対応

カスペルスキーの調査サービスは、詳細な脅威分析やセキュリティ・インシデントを解決するための適切な手段に関するアドバイスなどを通じて、企業による防御戦略の策定を支援します。

本サービスは、3 種類の調査レベルを用意しています。

- マルウェア分析 - 企業を狙う具体的なマルウェアファイルのふるまいや目的の解明を支援します。
- デジタルフォレンジック - インシデントの全体像を解明すると共に、企業がどのような影響を受けているかを明らかにします。
- インシデント・レスポンス - カスペルスキーの専門家たちの現場訪問を含む、フルサイクルのインシデント調査を行います。

ボットネット脅威の追跡

カスペルスキーのエキスパートソリューションがボットネットの動きを追跡し、個別のオンライン支払システムやバンキングシステムのユーザーに関係する脅威を迅速に (20 分以内に) 通知します。ユーザーはその情報を活用し、顧客やセキュリティサービスプロバイダー、地域の法執行機関に対して脅威を通知したり、勧告したりすることができます。

インテリジェンスレポート

カスペルスキーのインテリジェンスレポートによって、世界 200 か国で収集した 8,000 万件以上のユーザー統計に基づく最新の関連情報にアクセスすることができ、自社が直面している脅威に対する認識を高め、知識を深めることができます。

カスペルスキーの知識、経験、広範なインテリジェンスこそ、カスペルスキーが世界中の主要法執行機関および政府機関の信頼されるパートナーという地位を築き上げることができた原動力です。ぜひこのインテリジェンス情報をお役立てください。

▶ カスペルスキー エンタープライズソリューション

DDoS 保護 - トータルディフェンスと軽減

分散型サービス妨害 (DDoS) 攻撃からビジネスを守るために必要なあらゆる対策を実施

Kaspersky DDoS Protection は、あらゆるタイプの DDoS 攻撃から自社を守り、またその影響を軽減するために企業が必要とするすべてのものを提供します。これには、すべてのオンライントラフィックの継続分析、攻撃の可能性に関する警告、ユーザーがリダイレクトしたトラフィックの受信、トラフィックのクリーニング、「クリーン」なトラフィックの返信などがあります。

重要インフラストラクチャの保護

産業用制御システムおよびネットワークのセキュリティ

Kaspersky Endpoint Security for Business は効果的な「産業モード」保護を備えており、ICS/SCADA エンドポイントを脅威から守り、犯罪者が重要システムを選ぶ際の目安となるバックドアを形成する脆弱性を防ぎます。

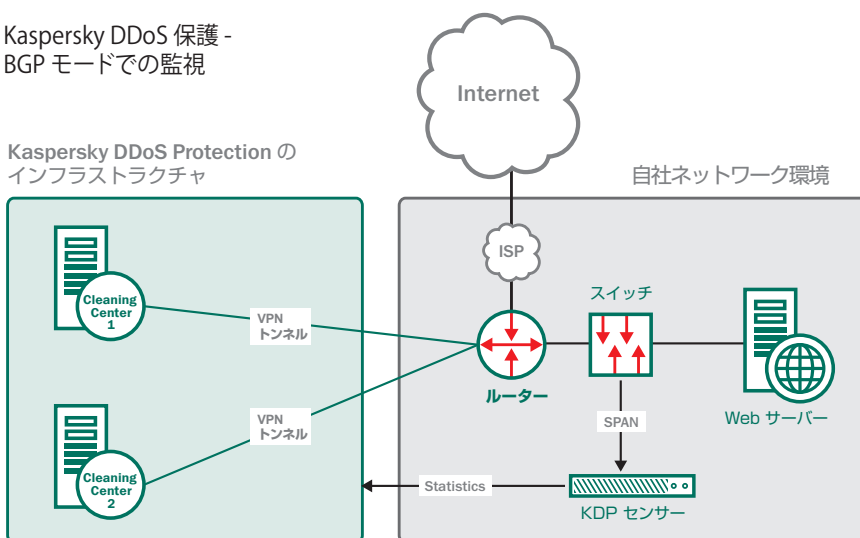
Emerson や Rockwell Automation、Siemens など業界を代表する自動化ベンダーとの協力により、カスペルスキーは、確実に承認を得るための数多くの特別な手順、および顧客の事業技術との互換性を確立してきました。その結果、事業の継続および一貫性に一切影響することなく、重要インフラストラクチャを効果的に守ることができるようになりました。

KASPERSKY LAB PROFESSIONAL SERVICES

複雑な IT 環境で運用されているお客様に関して、Kaspersky Professional Deployment、Upgrade、Training および Health Check の各サービスは、Kaspersky Security for Business の正しい構成、導入、管理を行い、最適なパフォーマンスを引き出すよう開発されたものです。

Kaspersky DDoS 保護 - BGP モードでの監視

Kaspersky DDoS Protection の
インフラストラクチャ



▶ カスペルスキーのメンテナンス およびサポート契約

インシデント、構成問題、非互換性、その他の IT セキュリティ問題に対する高品質なサポートは、安心と共に最適なアップタイムを求める企業にとってはきわめて重要なことです。

カスペルスキーのメンテナンスおよびサポート契約 (MSA) は、アップタイム保証のほか、企業の IT セキュリティネットワークに対する継続的なクオリティケアを提供します。MSA は、不適切な構成からマルウェアアウトブレイクまで、想定外のインシデントが発生した場合にすぐれたサポートを提供し、企業組織全体の安定と効率に寄与します。

カスペルスキーのメンテナンスおよびサポート契約は、以下の問題をカバーしています。

- ・ 想定外の世界規模のウイルスアウトブレイク
- ・ 複雑なインフラストラクチャに起因した深刻なダウンタイム
- ・ 導入の最適化およびカスタマイズされた修正プログラム
- ・ ネットワークにおける非互換性問題
- ・ カスペルスキー製品のアップグレードプロセス
- ・ マルウェアに関するインシデント調査
- ・ 製品のインストールと設定のサポート*
- ・ パッチおよびその他のアップデートの導入*

支援が必要なとき、カスペルスキーの専門技術者は専用の優先電話回線により、お客様の言語で、お客様の企業ニーズに合わせて設定した応答期間を通じていつでも対応いたします。下記の表は利用可能なサポートオプションをまとめたものです。

拡張サポート

	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
優先電話回線	対応	対応	対応	対応
テクニカルアカウントマネージャー	未対応	未対応	対応	専任対応
ローカル言語サポート	週 5 日間、1 日 8 時間	週 5 日間、1 日 8 時間	24 時間 365 日	24 時間 365 日
重大度 1 サポート	週 5 日間、1 日 8 時間	週 5 日間、1 日 8 時間	24 時間 365 日	24 時間 365 日
重大度 1 応答時間	8 営業時間以内	6 営業時間以内	4 時間以内	30 分以内
重大度 2 サポート	週 5 日間、1 日 8 時間	週 5 日間、1 日 8 時間	週 5 日間、1 日 8 時間	24 時間 365 日
プロフェッショナルサービス コンサルティング	未対応	未対応	費用別途	正常性チェックおよび カスタムレポート
インシデント制限数	6	12	36	無制限

* Enterpriseのみ。

This image shows a full page of a worksheet designed for handwriting practice. It features 20 evenly spaced, horizontal dashed lines across the entire width of the page. The background is plain white, providing a clear guide for letter height and placement. There are no margins, text, or other markings present.

30日間利用可能な無料試用版ダウンロード: <http://www.kaspersky.co.jp/trials#tab=tab-3>

最新情報はウェブサイトをご確認ください ▶ <http://www.kaspersky.co.jp/business-security>



株式会社カスペルスキー

カスペルスキー Web サイト
ご購入相談窓口

www.kaspersky.co.jp/
jp-sales@kaspersky.com

© 2017 Kaspersky Lab. All rights reserved. 本資料登録中に記載されている商標、サービスマーク、ブランド名、製品名、またはサービス名称は、それぞれ該当する所有者の商標またはサービスマークである可能性があります。
MacはApple Inc.の登録商標です。CiscoおよびiOSは、Cisco Systems, Inc.および/またはその関連会社の米国およびその他の国における商標または登録商標です。IBMおよびLotus Dominoは、世界各国で登録されたInternational Business Machines Corporationの登録商標です。Linuxは、米国およびその他の国におけるLinus Torvaldsの登録商標です。Microsoft、Windows、Windows Server、ForefrontおよびHyper-Vは、米国およびその他の国におけるMicrosoft Corporationの登録商標です。Android™は、Google, Inc.の登録商標です。

製品・サービスに関するお問い合わせは下記へ