Kaspersky Endpoint Security 10

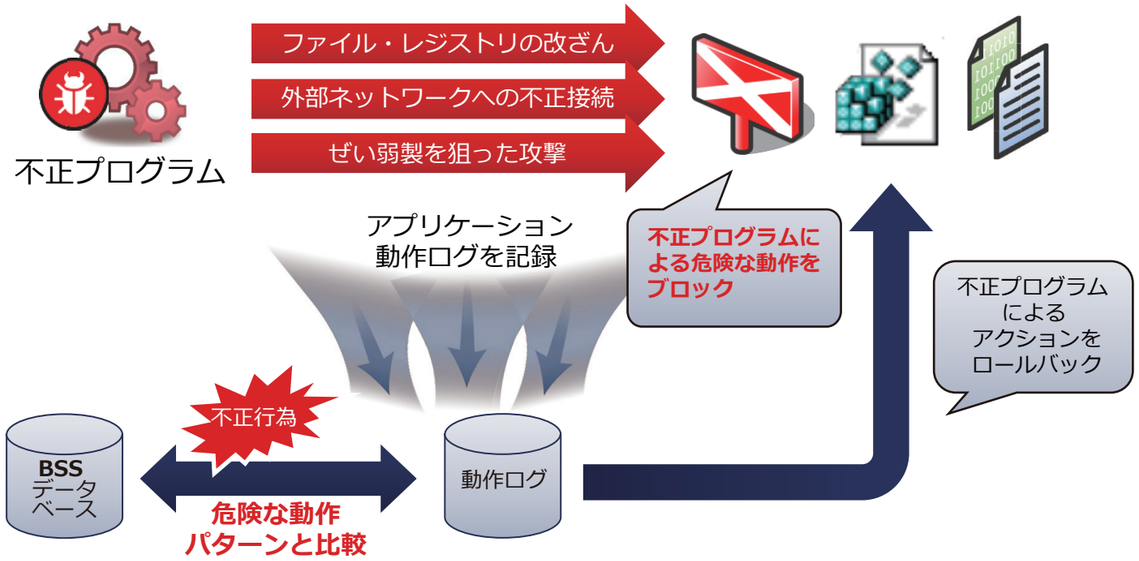
◆ Kaspersky Security Network (KSN)

クラウド上の実行形式ファイル、WEBサイトの評価情報を活用
不正プログラムの検知率向上および誤検知率低減を実現

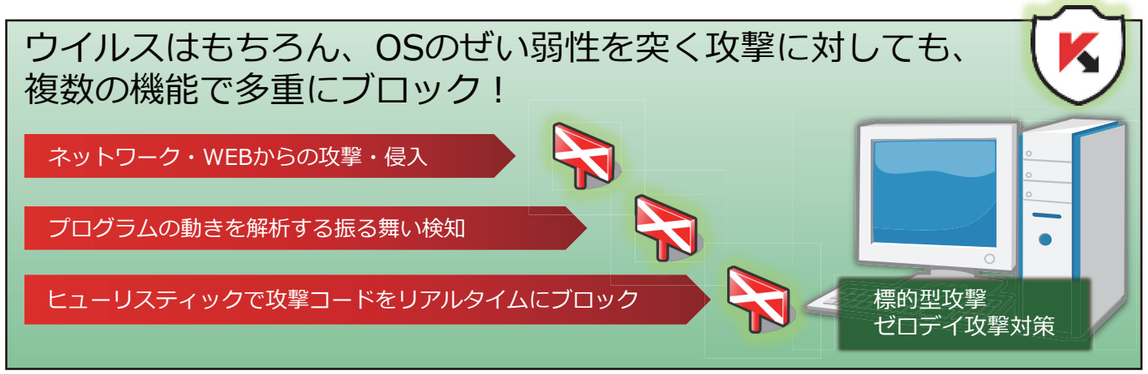
◆ システムウォッチャー　振る舞い検知機能

未知の脅威をブロックする４つの特徴

- プロアクティブディフェンス
- BSS-Behavior Stream Signatures
- 脆弱性攻撃ブロック
- ロールバック



ウイルスはもちろん、OSのぜい弱性を突く攻撃に対しても、
複数の機能で多重にブロック！



株式会社カスペルスキー KASPERSKY
カスペルスキーWebサイト　www.kaspersky.co.jp
ご購入相談窓口　jp-sales@kaspersky.com

KASPERSKY
月刊事業構想
PROJECT DESIGN
より抜粋

未知の脅威・脆弱性対策を実現

自治体に迫る
サイバー攻撃の脅威

姫路市　ソフト・ハードの両面でセキュリティ対策を強化

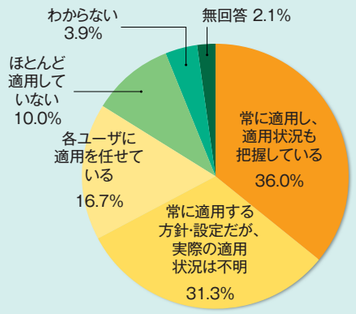
世界で認められた保護性能

セキュリティ対策の見直しと強化は、企業をはじめ地方公共団体にとっても必要不可欠の課題。姫路市では、セキュリティ対策の見直しの一環として、世界最高レベルの保護力に定評のある、セキュリティ・ソフトウェア「Kaspersky Endpoint Security for Business」を導入した。

世界最高レベルの保護力を実現し、サーバー・モバイルを含むすべてのエンドポイント（主にクライアントPCなど）を保護するカスペルスキーのセキュリティ・ソフトウェア「Kaspersky Endpoint Security for Business」を姫路市が導入したのは、2014年12月。ちょうど年明けにサーバーの更新時期を迎えるタイミングでもあったこの時期に、他のシステムと併せてセキュリティ・システムの改善・強化へと踏み切った。総務局総務部情報政策課・藪上憲二氏は、次のように語る。

藪上憲二
姫路市 総務局総務部情報政策課 情報化推進担当

クライアント（パソコン）へのセキュリティパッチ適用の有無



（N=1,881）

ほとんどの組織で、各社員・各職員が使用するPCのセキュリティ状況を把握できていないのが実態。また、「常に適用し、適用状況も把握している」（36.0%）と回答した組織でも、それが本当に実践されているかをチェックする仕組みを持たないと、漏れが発生してしまう。

出典：情報処理推進機構（IPA）
「2013年度 情報セキュリティ事象被害状況調査」

「情報通信技術（ICT）の急激な発展と普及に対応すべく、姫路市でも情報化計画を策定し、情報化施策の総合的な推進に伴い、セキュリティの確保についても万全の体制を整えています。昨今深刻な社会問題としても取り上げられている『標的型サイバー攻撃』にも備えながら、市民の皆さまに安心して暮らしに必要な情報やサービスをお届けできるよう、今回、サーバーのリース期間更新のタイミングに合わせてセキュリティ・システムの大幅な見直しを行いました」

カスペルスキーのセキュリティ・ソフトウェアに移行した理由として、藪上氏は「高い安全性」、「利便性」、「経済性」の3つを挙げる。

「世界でも認められた保護性能の高さは、何より大きな信頼であり、魅力だと感じました。やはり、セキュリティ・ソフト開発一本に特化して世界を相手にビジネスを展開し、その名を着実に広められているだけのことはありますね」

利便性・コスト性能も申し分なし

カスペルスキーのセキュリティは既知の脅威だけでなく、未知の脅威にも対応する優れた検知力を強みとしており、ウィルスへの感染防止対策として最新の脆弱性攻撃をもしっかりブロックする脆弱性攻撃ブロックや、未知の脅威に対する振る舞い検知機能など、さまざまな側面から大切な情報資産の保護が可能。

この多層防御性能に、姫路市の情報政策を進める藪上氏も大きな期待を寄せており、「サイバー攻撃からシステム環境や大切な情報を守るためには、正直、これをやっていれば100%大丈夫ということはありません。だからこそ、あらゆる脅威に備えるカスペルスキーのセキュリティ・ソフトのきめ細やかで高い保護機能性に信頼感を覚えました」。

他にも、国際的で専門的な知識を有するエキスパート集団がサポートに当たるという点や、移行がスムーズに進められるのはもちろんのこと、動きもこれまで以上に軽快になり通常業務にも何ら支障はなくストレスを感じることもないという利便性の高さ、コストパフォーマンス面に至るまで、総合評価は上々。また、シンプルな一元管理が可能となった点についても、藪上氏は高く評価している。

「セキュリティ・ソフトを『Kaspersky Endpoint Security for Business』へと移行して1ヵ月ほどですが、この高い保護性能を活用して、脆弱性のあるソフトの洗い出しや見直し、強化対策を積極的に行っていきたいと考えています」

情報セキュリティへの意識を強化

どんなに優秀なセキュリティ・ソフトも、結局は使いこなすのは“人”。姫路市ではその点にも配慮し、セキュリティ対策に関する職員の知識を深め、意識を高める工夫にも余念がない。藪上氏は、こうも語っている。

「情報セキュリティに関する最新の情報を常日頃からしっかりとキャッチし、専門的な知識を深め、サイバー攻撃から自分たちを取り巻くIT環境をしっかりと守り、被害を未然に防ぐ、あるいは最小限にとどめるのだという高い意識を持つことが必要です。そのために、各部門の情報セキュリティの責任者を対象に毎年研修を行い、Eラーニングを受講してもらったりといった取り組みも積極的に行っています」

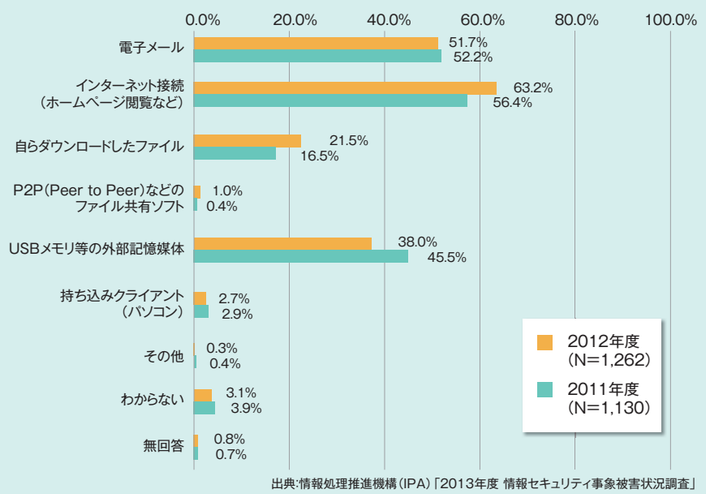
さらに、姫路市役所に隣接する「防災センター」は2007年に免震棟としての機能を備え建てられたビルでもあるが、この一画にも市の情報システムの一部を移行し共有化することで、震災発生時にも肝心の情報機能が完全に停滞してしまわないようなサポート体制も整えた。

「この防災センターは24時間有人の監視システムが敷かれていますので、あらゆる側面から大切な情報をしっかりと守り抜くことができます」

繰り返しになるが、情報セキュリティ対策に100%はない。だからこそ、ソフト面とハード面両方の環境面の充実を図ることはもちろん、それらを使いこなす人材の育成まで、多方面から柔軟で時代に即した対策をとることが必要ではないだろうか。 J

2007年に立てられた防災センター。姫路市では、免震機能を備えた防災センターに一部の情報システムを移行した

コンピュータウイルスの侵入経路



出典：情報処理推進機構（IPA）「2013年度 情報セキュリティ事象被害状況調査」

カスペルスキー　未知の脅威・脆弱性対策を実現

自治体に迫るサイバー攻撃の脅威

現在、企業・自治体の情報システムに対する攻撃の手口は、多様化・巧妙化しており、
既存のセキュリティ対策では防げない「未知の脅威」も増大している。
そうした中で、世界最高レベルのセキュリティを提供するのが、カスペルスキーだ。

サイバー攻撃といえば、以前は個人の愉快犯がウイルスを作成・拡散し感染させるといったケースも多く見られたが、現在は金銭になりうる情報の取得を狙ったプロフェッショナル集団の活動が目立っている。

特に自治体は、住民の個人情報など金銭価値の高いデータを所持しているため標的にされやすい。また公的機関ゆえに、インフラの停止やウェブサイトの改ざんによる示威行為など、社会的な混乱を誘発するテロ行為を仕掛けられる恐れもある。

既存システムでは防げない脅威

ロシアのセキュリティ企業・カスペルスキーは、法人向けのエンドポイント（主にクライアントPCなど）分野で、世界第3位のシェアを誇る世界大手だ。国際警察機関のインターポール（ICPO）ともサイバー犯罪対策で協力体制を築くなど、同社の技術力は世界的に評価されている。

カスペルスキーのエンジニアリング統括部統括部長・関場哲也氏は、現在の情報システムが直面している脅威について次のように語る。

「サイバー攻撃で一番狙われるのは、Adobe Acrobat ReaderやInternet Explorer 、Java、Flashなど、ほとんどのPCにインストールされていて、多くの人が日常的に使っているアプリケーション・技術です。 そうしたアプリケーション・技術が標的になり、脆弱性が数多く見つかるのが実状です。セキュリティを強化するために、脆弱性対策、未知の脅威対策が急務になっています」

以前ならば、ネット上に拡散している疑わしいプログラムを検体（解析対象）として採取し、個別に対策をとることは難しくなかった。しかし、未知の脅威が増大している中では、ウイルスの入手そのものが困難だ。

さらに近年は、ユーザーが閲覧しそうなサイトにあらかじめトラップを仕掛けるといった巧妙な手口も見られる。ソーシャルエンジニアリングも使われ、個々人が閲覧しそうなサイトを予測し誘導することが行われている。対象者の情報源としてSNSも利用されるため、業務外での行動も重要だ。

実際、自治体においても、担当者がイベント候補地を探す際に閲覧したサイトが改ざんされていたため、ウイルスの侵入を許したケースがあるという。

「すでに他社のセキュリティ対策ソフトを導入している自治体がほとんどですが、検知することなくウイルスの侵入を許してしまい、それをきっかけに当社製品へ乗り換えた事例もあります」

組織内の脆弱性を一覧表示

多くの組織では、一度ソフトを入れて安定稼働させた後は、リプレースせずにそのまま運用しがちだ。しかし表面的には問題がないように見えても、手口がどんどん巧妙になり多様化していく中では、敵の動向に気づかないまま脆弱性が放置されているケースが多々ある。

「ソフト更新のスパンを長くとっている組織は、特に注意が必要です」

アプリケーションの脆弱性は深刻な問題であり、それを把握できないセキュリティ対策ソフトでは意味がない。

「対策として、パソコンに入っているアプリの種類やバージョン、脆弱性の緊急レベルを絶えず把握しておくことが重要になります」

カスペルスキーの製品を例に挙げれば、『Kaspersky Endpoint Security for Business』などが、そうした機能を完備している。同製品は、脆弱性をリスト形式で表示するインターフェースを備え、組織内のどのパソコンにどのアプリケーションが入っているのかが一覧で把握できるため、情報システムの担当者は、各アプリケーションの稼働状況、対策の緊急レベルについて、一目でわかるようになる。

さらに、既知の脅威はもちろん、未知のものに対しても優れた検知力を発揮し、不審な実行ファイルの起動を感知した際には、追加のセキュリティ・チェックを実行してブロックを行う脆弱性攻撃ブロック機能を備えている。

Windowsとマッキントッシュが混在するようなマルチOSの環境であっても、一つのレポートに出力されるため管理しやすい。それは、管理者の運用負担の軽減にもつながる。また、導入済みのセキュリティ・システムからの移行のしやすさ、動作の快適性も特徴だ。実際、ここ数年、自治体において、カスペルスキー製品の導入は増え続けているという。

「人」の教育活動に力を注ぐ

関場氏は、「非上場会社であることも、当社の特徴の一つ」と語る。

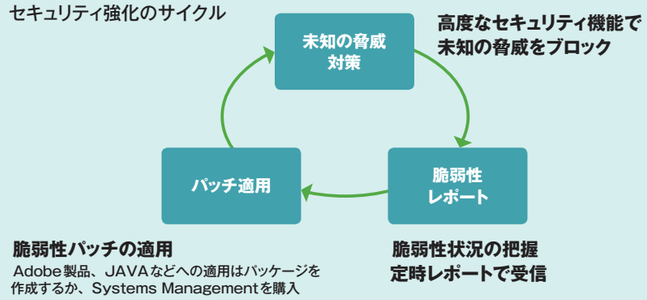
「株主からの圧力を受けることなく、安定して事業を展開することができます」

カスペルスキーでは、経営理念である「IT上の脅威から世界を守る“Save the World from it Threats.”」を基本方針に、啓発活動を通してユーザーのセキュリティ・リテラシー向上にも力を注ぐ。近年、子供のスマートフォン利用が問題となっているが、カスペルスキーは保護者向けにインターネットの安全利用に関するセミナーを支援するなど、CSR活動を展開している。

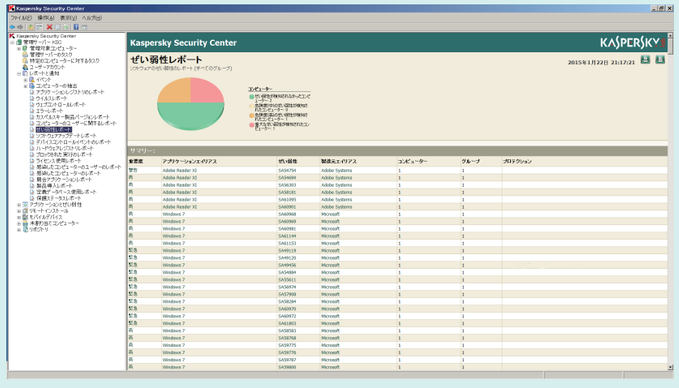
一家に1台パソコンがある時代から1人1台のスマートフォンを持つ時代へと変化している昨今。インターネットが身近な存在になるにつれ、サイバー犯罪もより複雑で巧妙なものへと進化している。自治体にとっても脆弱性の問題が深刻化する中で、それに立ち向かえる高度なセキュリティの導入が喫緊の課題となっているのだ。 J

子供のスマートフォン利用が問題となっていることに対応し、カスペルスキーは、保護者向けのインターネット安全利用啓発セミナーの開催を支援

「Kaspersky Endpoint Security」の強み



アプリケーションごとの対策の緊急性が一目でわかる「脆弱性レポート」



カスペルスキー製品の特徴の一つが「脆弱性レポート」。どのパソコンにどのアプリケーションが入っているのかを一覧のリスト形式で表示しており、それぞれのアプリケーションについて、対策の緊急性が一目でわかるようになっている。

お問い合わせ

KASPERSKY

株式会社カスペルスキー
〒101-0021
東京都千代田区外神田3-12-8
住友不動産秋葉原ビル7F
http://www.kaspersky.co.jp/
Mail : jp-sales@kaspersky.com

Kaspersky Systems Management

こんな課題を抱えていませんか？

KSMはシングルコンソール、シングルエージェントで、
Kaspersky Endpoint Securityと統合管理

① ぜい弱性を突いた攻撃が怖い

WebやE-Mailなどからやってくるぜい弱性を突いた不正攻撃の対策がしたい。
どのアプリケーションにぜい弱性があるのか分からない！？

② パッチ適用が出来ていない

緊急性が高いのは、どのパッチ？
パッチ適用がユーザー任せのため、適用されていないPCがあるかもしれない…
アプリケーションごとにパッチ適用方法が違うのが面倒だ。

ぜい弱性レポートおよびパッチ配信機能で解決

ぜい弱性の把握

Microsoft製品だけでなく、Adobe Acrobat、JAVAなどの
サードパーティ製アプリケーションのぜい弱性の有無を確認可能。
緊急性を表示するため、すぐに対処すべきパッチが判断出来ます。

パッチ配信

Microsoft製品だけでなく、サードパーティ製アプリのパッチ配信が可能。
ぜい弱性のリストから右クリックで簡単にパッチ配信タスクが作成可能。
面倒なパッケージ作成は不要。
ルールに基づいた自動配信もスケジュール可能。

③ ライセンス違反をしていないか心配

購入したライセンスを超えてインストールしてしまっていないか確認したい。
パッケージ版で購入しているので、バージョン毎に管理しなければならない。

ライセンス管理機能で解決

保有する製品を指定し、本数を入力するだけ。
保有を超えた使用を検知したらアラート発生。

④ セキュリティが弱いPCは接続をブロックしたい

アンチウイルス定義が古いPCはネットワークに接続させたくない。
マルウェアの疑いを検知したPCはネットワークに接続させたくない。
持ち込みPCを接続させたくない。

NAC機能で解決（ネットワークアクセスコントロール）

NACエージェントが不正な通信をブロック。
PCの状態で通信許可をコントロール。

OSイメージ配布

・SysPrep処理も、イメージ取得時に自動で設定。
・PXEを使用してWindowsPEをネットワークブートするので、配布が簡単。
・設定ファイルによるSysPrep設定も可能。

リモートコントロール

- コンソールからPCを右クリックして接続。
- PCで使用している同じセッションを共有。
- ヘルプデスク業務を効率的運用。
- 操作監査機能