



▶ 脆弱性レポートで“リスクを常時監視→即解決”！
社内の“セキュリティ意識”まで底上げ



赤城乳業株式会社

- 事業紹介
アイスクリーム等の企画開発、製造、販売、生産設備・装置の自社開発等、アイスクリームカンパニーとして常においしさと夢を提供しています。
- 主な商品
「ガリガリ君」、「ガリガリ君リッチ」、「ガツン、とみかん」、「ミルクレア」、「イペール」、「シャビィ」、「Q's」、「パフェデザート」、「赤城しぐれ」
- 本店所在地
埼玉県
- 利用環境
PC 350台
- 導入製品/サービス
Kaspersky Endpoint Security for Business Select
Kaspersky Systems Management



赤城乳業株式会社
財務本部
情報システム部 課長
高橋 一仁氏



赤城乳業株式会社
財務本部
情報システム部 係長
荒井 健司氏

「ガリガリ君」で有名な赤城乳業では、2014年から大規模なICT基盤の刷新に着手。その一環として、カスペルスキー製品を採用し、エンドポイントのセキュリティを飛躍的に強化させています。

商品開発に際して、常に「遊び心」を忘れない赤城株式会社では、看板商品である『ガリガリ君』に、毎年のように“意外”な新商品を加えてきました。2016年には、誰も想像していなかった“メロンパン味”を期間限定で発売するなど、同社のお客様を楽しませる姿勢にブレはありません。

こうした自由な発想を得るためには、日頃からの情報収集も重要です。特に、インターネットを通じて、主なターゲットとなる若者層の興味や反応が即座に見えるようになった今、社内PCを介したWebの閲覧などに過剰な制限をかけることは、同社としても「できない」と言います。

しかし一方で、サイバーセキュリティの重要性は刻々と高まっています。ユーザーにも管理者側にも過剰な負担をかけず、PCを末端とする情報系システムの安全を、より確実なものにする対策が求められていたのです。

マルウェア感染から、セキュリティ コンサルタントへの相談などを経て、情報システムを支えるセキュリティの抜本的な改革へ

そして2014年、同社のPCを守る“エンドポイントセキュリティ”を刷新させるきっかけが生じます。それが、「マルウェアへの感染発覚」でした。同社情報システム部 課長 高橋一仁氏は、次のように説明します。

「幸運にして、該当の社員が、『PCの具合が悪い』とすぐに相談に来たため、特段の被害は生じませんでした。後日、セキュリティコンサルタントなどに相談して感染源の解析を試みたのですが、完全に特定するには至りませんでした。社内にICTが導入されて以降、厳格とは言えない運用が続いてきた結果としてセキュリティパッチの不適用など、さまざまな脆弱性が存在していたために追跡しきれなかったのです」

もちろん、赤城乳業社内のPCすべてにアンチウイルスソフトが導入されていました。しかし、それだけでは悪質なWebサイトの場合、ユーザーがマルウェアを、それとは知らずにクリック（実行）してしまうと、感染を防ぐことはできません。

それ以上に問題であったことは、既存のアンチウイルスソフトの検知力を過信していたこと。そして、「セキュリティアップデートがきちんと適用されているか?」「危険なソフトがインストールされていないか?」など、社内PCのステータスを管理していなかったことにあります。

そこで、赤城乳業は上記の課題を改善すべく、セキュリティベンダー数社のソリューションを比較検討した結果、機能・信頼性・コストなど、すべての面で条件をクリアしたのが、法人向けセキュリティ統合プラットフォーム「Kaspersky Endpoint Security for Business」と、脆弱性管理製品「Kaspersky Systems Management」でした。

<http://www.akagi.com>



社内ネットワーク上にある全PCの状態を一元管理。簡易な操作で、効率よく脆弱性克服へ

赤城乳業がKaspersky Endpoint Security for Businessと共に導入したKaspersky Systems Managementは、企業のネットワーク上に接続しているWindows端末の脆弱性情報を収集し、パッチが必要な端末を特定し適用するといった「脆弱性管理」や、端末上にどのようなソフトウェアがインストールされているかといった「IT資産管理」など、さまざまな機能を有しています。

Kaspersky Endpoint Security for Businessに含まれているKaspersky Security Centerだけでも、カスペルスキー製品のセキュリティ設定やタスク、イベント状況などの一元管理は行えますが、「Kaspersky Systems Managementを導入して、本当に良かったです！」と、同情報システム部荒井健司氏は言います。

「実際に使い込んでみて『もう、この製品は手放せない!』と実感しました。正直、“初年度だけテスト的に運用してみようか”という程度の気持ちだったのですが、パッチの自動配信などは操作が簡単で利用頻度も高く、私たちの作業効率は大幅に向上しました」

高橋氏も、「不要なアプリケーションを、遠隔で削除できるのはありがたい」と続けます。

「ユーザー自身が気づかないうちに、何らかのアプリケーションが適用されてしまうことがあります。本人が自覚していないのですから、申告制で管理しても意味はありません。しかし、Kaspersky Systems Managementを活用すれば、誰のPCに、何が入っているか一覽で把握できる上に、そのアプリケーションに危険があるかどうか、判定されます。危険なものがあれば、削除するか、脆弱性のない最新バージョンにアップデートすればいい。私たち管理者は、画面の表示に沿って作業するだけですから、非常に簡単です」

検知力の高さと、効率的な脆弱性管理でセキュリティが飛躍的に向上し、ROIの初期目標を100%達成

Kaspersky Endpoint Security for Businessの検知能力は非常に高く、「従来使っていた製品では検知されなかったマルウェアまで検知してくれますし、即座に私たちに警告メールが届くので、迅速な対処できるようになりました」と荒井氏。「定義ファイルの更新も非常に早く、最新の脅威に対しても、安心感が持てるようになりました。しかも、PCに対する負荷も少なく、軽快に動作することも、評価しています。導入後の費用対効果は非常に高く、すでに初期投資費用分に相当する効果が得られています」

高橋氏も、カスペルスキー製品導入の成果を、次のように説明します。「まず、すべてのきっかけとなったマルウェア感染事故があのまま放置されて、被害が拡大した場合、少なく見積もっても私たち管理側の労力が、初期対応だけで4人日以上必要になり、その後の監視に10人日前後を要したでしょう。そうした中規模被害やさらにもっと大きな被害も発生し続けた可能性が高く、対処するための工数だけでも甚大なものになったと想定しています。カスペルスキー導入後は感染事故も無く、監視や管理も非常



USABILITY 管理画面から簡単に社内350台の脆弱性対策が可能

「Kaspersky Systems Managementのソフトウェアの脆弱性画面を確認して、PCの脆弱性管理を行っています。パッチが適用されていなければ、その場で適用し、不適切なアプリケーションがあれば、それもその場で対処します。しかも、どのアプリケーションが危険で、どれが安全か自動判別されて、色分けもされていますから、ひと目で何をどうすればいいか分かります。非常に便利です」(荒井氏)



SUPPORT 導入検討時から運用開始後まで常にサポートが充実

「当社では、取引先の選定に際しても、“人”を重視する風土がありまして、今回の導入においても、カスペルスキーの方々の対応の細やかさが判断材料の一つになっています。

導入後、電話サポートに何度も相談していますが、長い電話待ちの状態や、つながらないといったこともなく、こちらの質問にも、分かりやすく丁寧に答えてくれます。非常にありがたいですね」(荒井氏)



SCALABILITY スマートフォンなどすべてのエンドポイントのセキュリティ強化へ

「今後の展望として、スマートフォンなどのモバイル活用も検討しています。今はまだ、OSの選定など終わっていませんが、Kaspersky Endpoint Security for Businessではすでに、モバイル端末までカバーできる機能が揃っています。今後もモバイルの変化に合わせて機能強化を続けていただけるとありがたいです。また、今後のセキュリティ強化としてはまず、PCのHDD暗号化オプションを検討しています。会社全体のセキュリティ施策をきれいに整えるためにも、情報系端末はすべてカスペルスキーで統一したいと思っています」(高橋氏)



DETECT 高い検知力で、マルウェア などの被害を最小限に

「検討時から、カスペルスキーは『検知力が高い』と聞いていましたが、その言葉に嘘はありませんでした。従来使っていた製品では、まったく検知されなかったマルウェアも、しっかりと検知されています。むしろ、『検知力が高すぎて、ユーザーが不便を感じていないか?』とってしまうほどです」(高橋氏)



ROI 初期投資コストは、 すでに回収済み。 さらなる価値創出に期待

「投資対効果についてですが、今回のカスペルスキー製品導入時に試算した目標は、すでにクリアしています。年間約60人日もの管理コストを削減できた計算です。今後、活用を深めていくことで、投資対効果がさらにプラスされていくでしょう」(高橋氏)



KASPERSKY Lab

<問い合わせ先>
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>
jp-sales@kaspersky.com

© 2016 Kaspersky Lab. All rights reserved.
KasperskyおよびカスペルスキーはKaspersky Labの商標登録です。その他記載された会社名または製品名などは、各社の登録商標または商標です。
なお、本文中では、TM、®マークは明記していません。記載内容は2016年12月現在のものです。記載された内容は、改良の為に予告なく変更されることがあります。

に楽になり、大きな効果を実感しています。

さらに、業務文書の喪失や、機密文書の流出などの被害が出たら、どれだけの被害金額になるかわかりません。

しかし今は、かつてない検知力でPCの守りを高めると共に、全PCの脆弱性管理まで行えます。このリスク削減効果は明らかです。後は、今後の活用深化によって、投資費用を超える価値が得られると期待しています」

エンドポイントの状況を可視化することでIT管理者のみならず、ユーザーのセキュリティ意識が向上

加えて、荒井氏は「社内のセキュリティに対する意識が向上してきた」と話します。

「Kaspersky Systems Managementによって、社内PCすべてのセキュリティステータスが可視化されたことで、まず私たち管理側のセキュリティ意識に変化が現れました。脆弱性レポートのおかげで、今まで“見えなかったもの”が見えるようになり、その危険度や次に取るべきアクションまで明確に提示されたことが良かったのかもしれない。

また、カスペルスキー製品導入に伴い社内のセキュリティ設定を見直す際、ユーザー側へ継続して案内や説明を実施したことにより、以前よりセキュリティに関心を示してくれるようになってきたと感じます。

この変化は、非常に大きな効果であったと思います。セキュリティの徹底には、人の教育は欠かせないですからね」

「Kaspersky Systems Managementの脆弱性レポートのおかげで、社内のPCがどうなっているか、ひと目で分かるようになり、アプリケーションなどの危険度も、カスペルスキーのガイドラインに沿って自動判別されます。しかも、次に取るべきアクションも合わせて提示されますので、私たちIT管理者も、業務の中でごく自然に、さまざまな学びと気付きを得ることができます。さらに、危険が検知されるWebサイトを閲覧できないよう、自動制限をかけたことなどで、ユーザーのセキュリティに対する意識も高まりました」

赤城乳業株式会社

財務本部

情報システム部 課長

高橋 一仁 氏

「マルウェアの検知力は、期待通りに優れていますし、Kaspersky Systems Managementのおかげで、管理業務の効率が大幅に向上しました。もう、このシステムなしで作業することは考えられないですね。何か分からないことがあっても、電話サポートが丁寧に対応してくれます。いつ電話してもつながらないことがないのも、ありがたいですね」

赤城乳業株式会社

財務本部

情報システム部 係長

荒井 健司 氏