HP Sure Click Enterprise 導入事例

巧妙化する脅威からシステムを守る HP Sure Click Enterprise

上越地域消防局

HP WOLF SECURITY

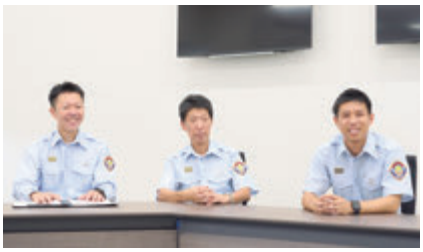
目的
- 最新のランサムウェアに対応するあらたなセキュリティシステムの導入

アプローチ
- HP SCEの導入によるセキュリティ強化

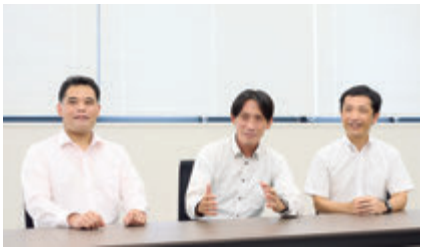
システムの効果
- ユーザビリティを損なわず添付ファイルが扱える
- 既存システムへの影響が最小限
- エンドポイント強化の実現

ビジネスへの効果
- PCを使った業務の生産性の維持・向上
- 別途EDRの導入なしでも同様の機能を提供
- 不安の少ないセキュリティ運用の実現

新庁舎外観



左から、上越地域消防局 指令統制課施設管理係主任 山下 陽介氏、総務課長 猪俣 浩之氏 指令統制課施設管理係主任 永井 隆博氏



左から、株式会社ハイパー セキュリティア推進部 部長 渡邊 裕介氏、販売推進統括部 セキュリティア推進部 第一課 課長 渡会 弘樹氏、株式会社 横瀬オーディオ 営業本部 部長 南波 健治氏

近年の脅威が巧妙さを増し、常に進化しているのはみなさんご存じの通りだ。企業はもちろん、自治体や行政機関にとってもその脅威は変わらず、セキュリティリスクの最重点課題として取り組んでいく必要がある。2020 年に組織変更および拠点の移転を行った上越地域消防局においても同じ課題を抱えていたが、HP Sure Click Enterprise を導入することで解決を図ったという。どのような取り組みだったのか話を伺ってきたので紹介しよう。

市民の安心・安全を守る拠点のセキュリティ

上越地域消防局は、新潟県上越市および妙高市を管轄する。2020年には、さらなる消防力や災害対応力の向上を目指し、新たな防災拠点である新庁舎を建設して市民の生命や財産を守っている。

そんな上越地域消防局では、IT運用に関してある課題が浮上していたのだという。「Emotetをはじめとするランサムウェアが流行する中、これまで以上のセキュリティが必要になると考えました。従来のセキュリティをかいくぐってくる脅威に対して、適切な対応ができるソリューションの検討が急務だと思い行動を開始しました」と語るのは同局の永井氏。

上越地域消防局が課題解決に向けて動き始めたのが、2021年秋。当初から最新の脅威に対応するにはエンドポイント強化がカギになることを想定し、自治体などが実践している分離型ソリューションによる対策を検討していたのだという。「とはいえ、新潟県が運用している自治体クラウドの利用はできませんでした。そこで独自にソリューションの選定と調達を行わなければならず、最適解を見つけるために様々なSIerに話を伺い、調査を進めていきました」と同局の山下氏は語る。

悪意を仮想空間に封じ込める

「分離型ソリューションの構築には大幅なシステム変更やオペレーションの教育などが必要になりますが、『HP Sure Click Enterprise（以降、HP SCE）』ならクライアントPC内の仮想空間内で脅威を排除できるため、システム全体への影響がほとんどないという点が良いと感じました」と同局の永井氏は語る。

「お話を伺い、まさに求めていたソリューションだと感じました。ユーザーの利便性はそのまま、万が一脅威が入り込んでもファイルを閉じれば無かったことにできる。生産性はそのままに、エンドポイント強化が達成できる点を高く評価しました」と同局 山下氏は語る。

ランサムウェアをはじめとしたマルウェアは、従来型のシグネチャー型ウイルス対策ソフトをあざむいてクライアントPCへ侵入しようとする。巧妙に仕組まれた手口でメール添付ファイルやWebサイトからのファイルダウンロードへと誘導し、ファイルが実行された瞬間に小さなプログラムを侵入させるという手口だ。これを防ぐにはファイルが正しいものかを判断する必要があるが、一般的なセキュリティソリューションでは小さな悪意を検知することが難しいのだ。

HP SCEはエンドポイントとなるクライアントPC内の仮想空間でそれらのファイルをオープンさせる。これにより、ユーザーは中身を安全に閲覧することができ、目的と違うファイルであればすぐさまそれを閉じることで、仮想空間ごと悪意を封じ込めることが可能だ。上越地域消防局が達成したいエンドポイント強化を実現できるベストソリューションといえる。

こうした機能について納得した上越地域消防局は、課題を解決するセキュリティソリューションとしてHP SCEを選択。厳正な入札の結果、地域事業者の株式会社 横瀬オーディオが受注することになり、導入計画を立案。まずは小規模なPoC（Proof of Concept：概念実証）を実施することとなった。

Emotetの脅威を体験

PoCの段階から導入支援としてSIerの株式会社ハイパーも参加。本格導入へ向けテストを進めていった。「全体的に順調でしたが、何もなかったわけではありません。特に威力調査の段階でEmotetを検出したときには緊張しました」と語るハイパー 渡会氏。しかし、想定の範囲内であったこともあり、HP SECがすぐに検知・隔離をし、その信頼性を証明することにもなったのだという。

「本当に身近に悪意が潜んでいることを実感し

HP SCEの導入を振り返るプロジェクト主要メンバーと上越地域消防局メンバー

ました。普段は開かないようなファイルでしたが、どのような状況から攻撃されるのかを目の当たりにしたので十分な対策が必要なことが理解できましたね。同時にHP SCEがこうしたマルウェアの蔓延防止に最適であることも分かったのは大きな収穫でした」と同局の山下氏は当時を振り返る。

そのほか、細かな調整は必要であったものの、横瀬オーディオとハイパーの連携による対応ですべての問題を解決。2022年7月には本格導入が開始され、9月にはサービスインする運びとなった。

安全安心なセキュリティ運用を達成

「HP SCEの導入により、課題となっていたエンドポイント強化とマルウェア対策が実現できたと思います。特にユーザーに負担をかけず、従来のオペレーションをほとんど変えないで、高いセキュリティ対策ができたことは本当にうれしく思います」と語る同局の永井氏。

「管理者目線でみても、HP SCEによるセキュリティ面での組織全体の一元管理やEDR機能などにより、管理がとても便利になりました。ランサムウェアは手口を次々と変えてきますから、傾向の分析などが迅速に行えるのは強い武器になります」と同局で情報セキュリティ全体を管理している猪俣氏は導入を振り返る。

HP SCEにより、エンドポイント強化を達成した上越地域消防局。「当初の目的であったランサムウェア、特にEmotetへの対策ができたことは本当に良かったと感じています。HP SCEが米国国防総省にも採用されていることを伺っていましたが、私たちの組織でもガバメントレベルのセキュリティを実装することができたことをうれしく思います。これから本格運用がはじまりますが、それでも侵入を試みようとする脅威はあるはずです。横瀬オーディオさん、ハイパーさんにもこれまで通りのサポートをお願いしつつ、私たちも気を引き締めてセキュリティ運用をしていきたいと考えています」と最後に永井氏は語ってくれた。HPはこれからも地域の安心安全のために日夜活動を続ける上越地域消防局をサポートしていく。

※野外撮影参加者 左から3人目 上越地域消防局 指令統制課 施設管理係長 佐藤 隆介氏、左から4人目 指令統制課 副課長 三浦 功氏

記事を共有する

© Copyright 2022 HP Development Company, L.P.
記載されている情報は取材時におけるものであり、閲覧される時点で変更されている可能性があります。予めご了承下さい。
本書に含まれる技術情報は、予告なく変更されることがあります。
記載されている会社名および商品名は、各社の商標または登録商標です。
記事事項は 2022 年 8 月現在のものです。