voices

CrowdStrike 導入事例

サッポロホールディングス株式会社

サッポログループが6,000台強のエンドポイントに選んだ次世代アンチウイルスは CrowdStrike Falcon Prevent

Emotetへの連続感染で 既存ウイルス対策からの脱却を決断

サッポログループは1876年、北海道・札幌の地で「開拓使麦酒醸造所」として創業した。以来、140年以上にわたって、酒類事業はもとより、食品飲料、不動産と、消費者生活のさまざまな場面で潤いと豊かさを提供してきた。現在、グローバル展開も果敢に進めており、すでにビールは約45か国、飲料は約60か国で展開している。イノベーションと品質の追求による新たな価値の創造で、同グループは世界中の人々のより豊かな生活の実現に貢献している。

2019年の年末、グループ内事業会社のPC環境でEmotetへの感染が確認された。それも、時間を置かずに2回起こった。幸い、実害はなかったのだが、担当として現状のまま放置するのはリスクが高いことを認識した。サッポロホールディングス株式会社 IT統括部 イノベーションエキスパート 布施川 貴久氏は、次のように振り返る。

「このインシデントで、パターンマッチング方式の既存アンチウイルスソフトではもう防御しきれないことを実感しました。また従来の体制では、何か怪しいインシデントが報告されると、IT統括部が従業員から話を聞き、原因究明と対策に当たっていました。毎月数件程度は発生するため、そのたび我々も従業員も業務の手を止めなければなりませんでした」

さらに「従来のアンチウイルスソフトは社内サーバが必要でした。日常の運用管理やバージョンアップ対応に、IT統括部内で少なからぬ工数やコストがかかっていました」と後ろに隠れていた課題もあったという。

こうした背景から、従来から製品切り替えに向け少しずつ調査を進めていた。それがEmotet感染で一気に気運が高まり、2020年初頭から本格的に動き始めた。

市場の評価が高く、運用負荷の低い CrowdStrike Falcon Preventを選択

サッポログループには、同グループ全体のITセキュリティ運用をサポートするパートナー企業が存在する。アンチウイルスソフト切り替え後は、このパートナー企業が日常の運用管理も担うことになる。パートナー企業とともに評価、検討を進めた結果、選ばれたのが次世代アンチウイルス CrowdStrike Falcon Preventだった。

導入の決め手を布施川氏は次のように語る。

「クラウドストライクのことはガートナーのイベントで知りました。運用パートナー企業でも製品導入から日常の運用管理まで実績があり自信があると回答が返ってきたのがこの製品でした。調査会社の評価や価格競争力が高かったこと、管理サーバ不要ですべてをクラウドで提供することも安心材料でしたね」

一方、サッポロホールディングス株式会社 IT統括部 高度情報推進グループ グループリーダー 伊藤 淳氏は、次のように語る。

「CrowdStrike Falconは機械学習でふるまい検知を行う次世代アンチウイルスを始め、多彩な機能を有している製品です。それが1つのエージェントをインストールすることで実現可能でありながら、段階的に導入できる点がいいと思いました。まずは次世代アンチウイルスとして使い始めて、時が来たらEDR機能を追加する。そういう展開ができるのは他の製品にはない利点でした。

また、PCでの動きが重いとクレームの対象になるのがアンチウイルスソフトの常ですが、この製品はPCへの負担が軽くエンドユーザーに存在を意識させないことも選択を後押ししました」

ただ、課題を抱えているとはいえ、なじんでいた製品を切り替えることに、現場が不安を抱いた

SAPPORO

業種
食料品

所在地
東京都渋谷区恵比寿4-20-1

サッポロホールディングス株式会社

酒類事業はもとより、食品・飲料、外食、不動産と、消費者の生活の様々な場面に関わってきたサッポロホールディングス株式会社。喜びや感動を届ける新しいシーンを提供し続け、消費者と積み重ねてきた対話をもとにイノベーションや品質の向上を追求してきた。同グループでは、これらを大事な「ブランド」資産だと位置づけ、「個性かがやくブランドカンパニー」をめざして、常に変化に対応しつつ、挑戦を続けている。

URL：https://www.sapporoholdings.jp/

導入製品

- CrowdStrike Falcon Prevent™ 次世代アンチウイルス

導入時期：2020年9月

ことも事実だった。「本当にPCへの負担は軽いのか？」「ふるまい検知という技術は信じられるのか？」といった声に対しては、クラウドストライク側も定量的資料や第三者評価資料を積極的に提出、エンドユーザーの納得を得ることに注力した。

2カ月足らずでグループ6,000台強に展開
エンドポイント保護はCrowdStrike Falcon一本に

そこからの展開は速かった。セキュリティ投資の重要性を認識する経営トップからは迅速に導入承認が下り、IT統括部のインフラチームで先行導入を開始。まずは検知したマルウェアを表示する検知モードから使い出した。またこの段階で誤検知、過検知のチューニングを行ったが、想定したほどではなかった。次はIT統括部全体へ広げていった。そうして、国内の事業会社や一部海外法人のエンドポイント、サーバ環境まで、対象6,000台強に対して2カ月足らずで一気に導入が敢行された。

既存アンチウイルスソフトは、CrowdStrike Falconの性能やグループ全体のセキュリティ体制全体の防御力を鑑みて、2020年年末に訪れた契約期間終了とともにアンインストールされた。その後、CrowdStrike Falcon Preventは、マルウェアの検知から隔離までを単体で担うブロックモードで運用されている。

導入後、インシデント発生に関する日常運用の流れは次のようになっている。一次対応の窓口を務めるのはパートナー企業だ。IT統括部でも状況は把握しつつも、監視により怪しい動きを検知したり、エンドユーザーから問い合わせが寄せられた場合、パートナー企業側で詳細分析を行い、その内容をもとに従業員に対してIT統括部から対応を指示する。また、パートナー企業は、セキュリティ体制全体の稼働状況とともにCrowdStrike Falconの運用状況を定期的にIT統括部に報告する。

検知はあっても感染事例なしに防御力向上を実感
IT統括部の業務生産性も向上

CrowdStrikeの次世代アンチウイルス導入から約1年が経過した現在、その効果を伊藤氏は次のように語る。

「まずいえることは、導入以降に検知はあっても、その後の感染、不正通信発生の事例は起きていないということで、防御力は向上したと思います。また、以前はセキュリティ専門家とはいえないわれわれが一次対応に当たっていましたが、オペレーションで判断できるログが提供されるので、運用パートナー企業で判断することができています。CrowdStrike Falconの管理画面は視認性が高くてわかりやすく、パートナー企業も日常の運用管理が行いやすいとの報告を受けています」

実際、布施川氏は一次対応のために業務の手を止めるケースがなくなった。IT統括部の生産性向上にも寄与しているのだ。また、生産性向上という観点では、既存アンチウイルスソフトでは我慢せざるを得なかったPCのフルスキャンがなくなり、エンドユーザーがアンチウイルスソフトの存在を意識することなく、業務に集中できるようになっているという。

そして、アンチウイルスソフトの管理のためのサーバ運用管理やバージョンアップからの解放だ。CrowdStrike Falconはサーバがクラウドに移るというしくみでもなく、全く管理サーバが存在しない。すべてクラウドプラットフォームとエンドポイント側の1つのエージェントで完結するため管理対象が減少した。主たる目的ではなかったが、いざ実施してみると業務負荷軽減効果は小さくなかった。

サッポログループにおいても、コロナ禍を機に全社でテレワークシフトが進んだ。部門によっては出社率が2割を切るところもあるという。このように、オフィスの外で仕事をするのが当たり前になると、従業員が業務を行うエンドポイントをより手厚く守ることが重要になってくる。伊藤氏は語る。

「もう境界防御という水際対策だけでは十分でなく、侵入されることを前提として対策を講じるのが重要であると理解しています。だからこそ先を見据えてCrowdStrike Falconを導入しました。テレワークシフトが急速に進んでも、慌てることはありませんでした」

時代に合わなくなったウイルス対策からの脱却をめざしたサッポログループが、選びとったのはCrowdStrike Falconだった。それは、クラウドならではの仕組みで多彩なセキュリティ機能を段階を踏みながら導入が可能な、将来を見据えた選択だった。

サッポロホールディングス株式会社
IT統括部 高度情報推進グループ
グループリーダー
伊藤 淳 氏

サッポロホールディングス株式会社
IT統括部
イノベーションエキスパート
布施川 貴久 氏

POINT

- 従来型から新しい方式への社内懸念を払拭した第三者評価、市場での優位性
- エージェント1つで多彩な機能を段階的に導入可能
- エンドユーザーに存在を意識させないPC上での軽快な動作
- 導入以降、感染、不正通信事例はなく、グループ全体の防御力が向上

CROWDSTRIKE

we stop breaches

クラウドストライク 株式会社
お問い合わせ: **crowdstrike.jp/request-information/**