HP Wolf Pro Security Service導入事例

迫りくる最新の脅威を防御する仕組みを HP Wolf Pro Security Serviceで構築

株式会社 IT コミュニケーションズ

HP WOLF SECURITY

目的（導入までの課題）
- 新世代の脅威に対抗可能なセキュリティシステムの構築
- 管理・運用負荷低減

アプローチ
- 次世代アンチウイルスと隔離実行による多段防御の実現
- マネージドサービスによる運用負荷低減

システムの効果
- NW負荷低減
- オンプレ管理サーバ不要

ビジネスへの効果
- 事業継続性の担保
- 顧客情報の保護

標的型攻撃が遠い国の話ではなく、現実に身近に起こりえる状況になっている現在、あらゆる企業にとって対策が急がれている。一方でそうと知りつつも実際にどのように対処すればよいか悩む時間が長くなってしまっているケースも多い。株式会社 IT コミュニケーションズはそんな中、新たな一歩を踏み出すことを決断。HP Wolf Pro Security Service および HP Proactive Insight によって、標的型攻撃に強い最新のセキュリティシステムを構築したという。同社に直接話を伺ってきたので紹介しよう。

IT Communications

株式会社 IT コミュニケーションズ
プロフェッショナルサービス部
テクニカルチーム
シニアテクニカルディレクター
五十嵐敏郎氏

クライアントサービス部
プロデュースチーム
シニアディレクター
村山 実氏

身近に起こりえる標的型攻撃への備え

株式会社 IT コミュニケーションズ（以下 “ITC”）は、総合広告代理店としてこれまで数多くの企業活動を支えてきた企業だ。SEM をはじめとしたインターネット広告やソリューション業務、Web サイトの構築・分析、システム設計・開発・運用、各種プロモーションなど、豊富なノウハウで幅広いサービスが提供できる強みを持っている。

同社は業種的にもクライアント企業の機密情報や個人情報を扱うことが多いため、セキュリティは積極的に強化してきた背景がある。「ですが、昨今の標的型攻撃は日々進化しており、従来のウイルス対策だけでは不十分だと認識していました」と語るのは、同社のシステム管理を担当するシニアテクニカルディレクターの五十嵐氏。しかし、多くの企業がそうであるように、ITC でも最新の脅威への対策が必要なことが分かりつつも、これまでなかなか検討をするタイミングがなかったのだという。

「そんな中、2021 年 2 月に社員から怪しいメールを受信したという報告がありました。調査の結果、最近猛威を振るっている Emotet による標的型攻撃だと判明しました。対象にされた社員のセキュリティリテラシーが高かったことと、早期発見ができたことで事なきを得ましたが、次世代の脅威が現実のものとなっていることがよくわかる事件でした」と振り返る五十嵐氏。同社では、もしも Emotet などが含まれるメールを社員が開いてしまったら、自社で運用しているセキュリティで果たして防げていたのかという疑問が持ち上がり、これを契機に本格的にセキュリティ対策の見直しに踏み切ることになったのだという。

セキュリティと管理性を共に向上させる

ITC が当時導入していたセキュリティシステムのうち、標的型攻撃の最前線となるエンドポイントでの対策はシグネチャ型のアンチウイルスソフトウェアに依存していた。この仕組みの場合、パターンファイルは日々更新されるが未知の脅威には一瞬無防備になる可能性が残る。また、このソフトウェアはクライアントサーバによって管理されるため、オンプレミスのサーバが必須であり、アップデートや最新パッチの適用の度に作業が発生し、管理負荷が大きかった。「最新パッチを適用するだけの作業時にもネットワーク負荷が増加し、社内のアクセス環境に大きな影響が出ていました」と五十嵐氏。

また、コロナ禍を受けて社員の 9 割がテレワーク中という時期だったため、社外で活動する社員のセキュリティ対策を整えることも急務となっていた。「社外から各社員のパソコンを管理するには、社内ネットワークに接続するか、VPN 接続をしないとならないため、コロナ禍によるテレワーク増加へどのように対応するかも議論されました」と振り返る五十嵐氏。現状の課題解決を含め、新たなセキュリティシステム選定は進んでいった。

「実はこの当時からセキュリティ管理に『HP Proactive Insight』を活用していました。HP には標的型攻撃に対して強さを持つ『HP Wolf Pro Security Service』があります。この両者はとても相性が良いので、最終選考の製品として残りました」と五十嵐氏は語る。

HP Wolf Pro Security Service は、ゼロデイ攻撃への防御も可能な AI 活用型の次世代アンチウイルス「HP Sure Sense Pro」と、標的型攻撃がよく使うマルウエアをマイクロ仮想マシン内に隔離し、保護された状態での監視が可能な「HP Suer Click Pro」からなる統合ソリューションだ。管理サーバは不要で、クライアントにはエージェントをインストールして利用する仕組みになる。

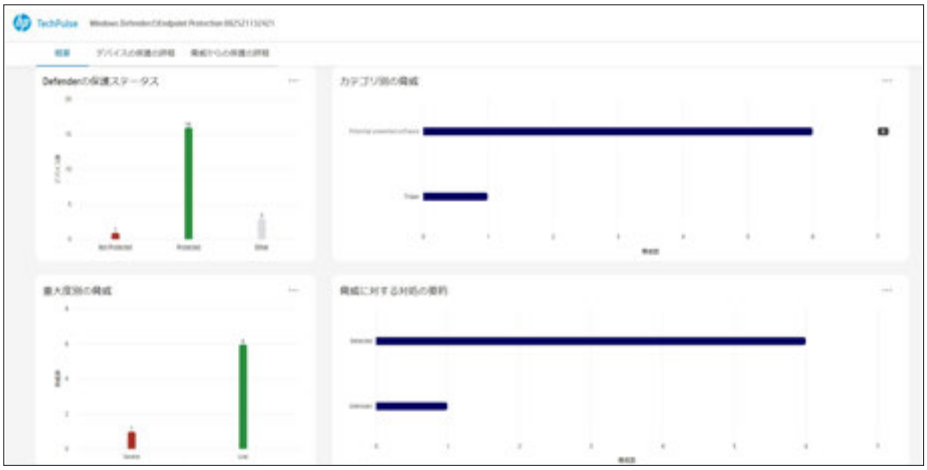
さらに HP Proactive Insight と組み合わせることで、社内の基幹システムにアクセスすることなく、デバイスの状態からセキュリティのモニタリングまでをひとつの画面で確認できるメ

リットもある。「管理機能についても、Windows Update の適用状況など、セキュリティ上の重要な情報も監視できるので、未適用の早期発見が可能です。悪意が介入しやすいタイミングを減らすことが可能になるため、的確なセキュリティ運用にも役立ってくれます」と五十嵐氏はいう。

ITC ではこれらのメリットを考慮し、導入するサービスを HP Wolf Pro Security Service に決定。HP へ正式に依頼することになった。

システム刷新で最大限の効果を獲得

既存のセキュリティシステムと相性が良いといっても、メインのセキュリティソフトを変更するという大掛かりなシステム更新となるため、一斉導入ではなく段階的に不具合を確認しながらの PoC を経て導入を目指すことになった。



Windows Defender の保護状況確認画面（画像はサンプル）

様々なセキュリティ情報が確認できる管理画面（画像はサンプル）

「2021 年 7 月から PoC を開始しました。最初は情報システム部内で試し、次に部門単位、最終的に全社導入を目指すというスケジュールです。結果からいうと、一連の PoC で大きな不具合はなく、とてもスムーズに導入できました」と振り返る五十嵐氏。7 月の PoC 開始から、約 1 カ月を経て適用範囲を拡大していったが、特に大きな不具合はなかったので、同月の最終週には本番運用が開始された。

「以前のセキュリティソフトはバックグラウンドで動いているとパソコンの動作が一時的に遅くなったり、朝の忙しい時間帯に社内のネットワークが重くなることもありましたが、今ではそれも感じません」と、PoC に参加した同社で Web ディレクション業務を行うプロデュースチーム マネージャーの村山氏は語る。「私からみても各社員がセキュリティソフトの動きを感じずに、作業に集中できていることが分かりました。セキュリティシステムは基本的にバックグラウンドで表に出ないように動いて欲しいので、実運用的に見ても HP Wolf Pro Security Service は理想的なソリューションだと感じています」と五十嵐氏は言葉を続ける。

また、HP Proactive Insight による管理性の向上はテレワーク時に大きな意味を持つと五十嵐氏はいう。「現在もほとんどの社員が在宅ワークをしています。そういう状況ですから、システム移行に関してもなかなか全社員の意見を吸い上げるのが難しいと思っていました。しかし、HP Proactive Insight のキャンペーン機能を使うことで、ユーザーアンケートが簡単に行えますから、様々なテーマで意見を聞くことができます」と五十嵐氏。「アンケートは OS のシステムトレイからポップアップに回答するだけなのでとても答えやすいです。負担の少ない UI なので、意見を伝えやすいのがうれしいです」と村山氏もシステム導入のメリットを語る。ITC ではこれらの機能を使って、ユーザーアンケートの結果をフィードバックすることで、社内のユーザーエクスペリエンス向上に寄与させる考えだ。

HP Wolf Pro Security Service および HP Proactive Insight による新たなセキュリティシステムの本格運用を開始した ITC。「これで最新の脅威にも十分対抗できるシステムが構築されたと感じています。テレワークの採用はコロナ禍が収束した後も継続していくでしょうから、ニューノーマル時代においても管理性が向上する今回のシステムには今後も期待したいと考えています」と五十嵐氏は最後に語ってくれた。セキュリティを高めつつ、システム負荷を大きく減らし、なおかつ管理性も向上させることに成功した IT コミュニケーションズ。今後も同社の活躍を支えるべく、HP はサポートを続けていく。