日本郵政株式会社

セキュリティ強化の「インターネット分離・無害化」ソリューションをわずか半年でグループ全社に一括導入

導入サービス：インターネット分離・無害化ソリューション（Menlo Security）

日本郵政株式会社
システム部門 執行役
正村 勉氏
「ネットワークのプロであるNTTコミュニケーションズであれば、我々が理解していないことも分かっているという信頼感がありました」

日本郵政株式会社
グループIT統括部 情報セキュリティ室
吉田 琢朗氏
「導入後の最初の1カ月間は特別対応として、ヘルプデスクやFAQを用意。NTTコミュニケーションズのスタッフも常駐し、迅速な対応が可能な体制を整えることができました」

企業情報

社名　日本郵政株式会社
事業概要　日本郵政グループは、日本郵便株式会社、株式会社ゆうちょ銀行、そして株式会社かんぽ生命保険から構成されている。「そばにいるから、できることがある。」をスローガンに、全国約24,000の郵便局ネットワークを通じて幅広いサービスや商品を提供。日本郵政株式会社は、その日本郵政グループの経営戦略策定を事業としている。
URL　https://www.japanpost.jp/

課題
- 情報セキュリティガバナンスにもとづいたインターネット分離の実現
- Webサイト経由でのサイバー攻撃に対するセキュリティ対策

対策
- インターネット分離・無害化ソリューションとしてMenlo Securityを導入
- 半年間のプロジェクトでグループ全社への一括導入を実現

効果
- 利用者の利便性向上とセキュリティ対策強化を両立して実現
- 経営層が求めるセキュリティガバナンス強化の基盤として機能

課題

Webサイト経由でマルウェアを感染させるサイバー攻撃への対策強化が急務に

日本全国に展開する郵便局ネットワークを通じ、郵便・貯金・保険の3事業を中心としたさまざまな商品とサービスを提供する日本郵政グループ。「そばにいるから、できることがある。」をスローガンに、「トータル生活サポート企業グループ」として多くの人たちの暮らしを支えている。

同グループの従業員数は、数十万人規模であり、そこで使われているクライアントPCは膨大な数になる。日本郵政グループで、従業員が利用するクライアントPCの企画・管理を担っているのは、持株会社である日本郵政のグループIT統括部。同グループの情報セキュリティを統括する執行役の正村勉氏は、「当グループはセキュリティ対策を重要な経営課題としてとらえ、サイバーセキュリティ経営宣言にもとづき、さまざまな対策を実施しています。添付ファイルなどからマルウェアに感染するメール攻撃、USBメモリーなど外部デバイスから感染する外部媒体攻撃、Webサイトへのアクセスで感染する水飲み場型攻撃とに分類して対策を進めてきました。おかげでメールと外部媒体の攻撃への対策はかなり進んだ一方、水飲み場攻撃はコンテンツフィルタとブラックリストによるアクセス禁止が主な対策手段であったため、Webサイト経由でのサイバー攻撃に対しては、さらなるセキュリティ対策を講じる必要性を認識していました」と話す。

昨今のサイバー攻撃では、マルウェアを感染させるための手法としてドライブバイダウンロード攻撃が広く使われている。これはWebサイトを閲覧するだけで、ユーザーの知らない間に何らかのソフトウェアが勝手にインストールされてしまう攻撃手法である。日本郵政

グループでは業務においてさまざまなWebサイトを閲覧するため、こうした攻撃への対策強化が課題であった。そんな折に総務省からインターネット分離に関するガイドラインが公表された。このガイドラインを参考に、同グループではインターネット分離を具体的に検討することになった。

対策

NTT Comをパートナーにインターネット分離・無害化ソリューション「Menlo Security」を半年間で導入

インターネット分離は、ネットワークやクライアントPCの物理的な分離のほか、仮想デスクトップ(VDI)や仮想Webブラウザーを利用する方法などがあるが、日本郵政グループが選んだのは「Menlo Security」を利用したWeb分離である。これはWebサイトにアクセスする際、クラウド上でサーバーから送られてきたコンテンツを処理し、クライアントであるWebブラウザーには画面上に表示する内容だけを送信するという無害化処理を実現するソリューションである。

正村氏は、ソリューション選定の経緯を振り返る。「当グループでは膨大な数のクライアントPCを利用していることから、全端末にツールをインストールする必要があるソリューションはコストと稼働の観点で候補から除外しました。またVDIは瞬間的な最大アクセスが予測しづらいという理由から除外することとしました。最終的にツールをインストールする必要がなく、なおかつ必要なリソースはスケールアウトで確保できることが決め手となりました」

グループIT統括部 情報セキュリティ室の吉田琢朗氏は操作性に変更がなく、利用に際しての制限がないこともMenlo Securityを選定した大きな理由と語る。「クライアントPCの操作性や利便性は多くの従業員の業務に関係することですので、導入に際しての影響が最小限ですむことも評価しました」(吉田氏)

導入パートナーとして、日本郵政グループが選んだのはNTTコミュニケーションズ株式会社(以下、NTT Com)である。正村氏は「インターネット上で提供されるSaaS型サービスであるため、NTT Comのネットワークとサービスの設計・コンサルティング力を評価しました。また導入後も運用において継続的なチューニングが必要になります。そのためNTT ComのMenlo Securityに関するコンサルティング力や運用体制も重視しました」と述べる。

導入プロジェクトは2018年7月からスタートした。最初に決定したのは、業務で利用する信頼できるWebサイトとそれ以外のWebサイトで、トラフィックを分離するという方針だ。その上で、前者のWebサイトについては従来どおりのアクセス、後者についてはMenlo Security経由でアクセスする構成とした。

方針と構成を決めた上で、各社、各部署で業務に必要なWebサイトの照会、調査、登録作業を半年間かけて行った。その後、切り替えを実施、2019年2月より正式にサービスの利用を開始する。最初の1カ月間は特別対応として、ヘルプデスクやFAQを用意。NTT Comのスタッフも常駐し、迅速な対応が可能な体制を整えた。「導入においてはネットワーク設計が大きく関係しますが、NTT Comは期待通りの設計・コンサルティング力を発揮して、プロジェクトを実行してくれました。プロジェクトの間、米国のMenlo Security本社ともコミュニケーションをとってくれたことも、半年間でのスピーディな導入実現につながりました」(正村氏)

効果

利便性向上とセキュリティ対策強化を両立して実現し、ガバナンス強化に向けた基盤として機能

Menlo Securityの導入効果だが、Webサイトにおけるマルウェア感染を確実に排除できるようになり、利用者の利便性が向上した。従来は危険性のあるWebサイトへのアクセスは禁止していたが、導入によって無害化処理が行われ、安全にアクセスできるためだ。「Menlo Security特有のメリットを強く感じています。利便性とセキュリティを同時に向上できる。利用者の理解を得ながらセキュリティ対策を推進する立場にある者として評価しています」(吉田氏)

加えて信頼できるWebサイトへのアクセスには広帯域のネットワークを使う構成にしたことも効果があったという。正村氏は「従来は業務外のサイトなどへのアクセスの影響により、業務利用クラウドサービスのレスポンスが遅くなるといった事象がありましたが、解消することができました」とその効果を語る。

また、Webアクセスの可視化と一元把握が実現できたことで、経営層が求めるセキュリティガバナンス強化の基盤として機能していることも大きな成果だという。「たとえば『ポータルサイトのヘッドラインにアクセスが集中したことがネットワーク遅延の原因である』などと、各社のCIO、CISOへの迅速な報告が可能になりました」(正村氏)

最後に正村氏は今後の計画をこう語る。「ブラウザー以外の外部への通信はマルウェアによるものと判断し、許可していない相手先への通信はすべて遮断する運用を今年度中にスタートさせる予定です。これによってマルウェア感染による外部への情報漏えいリスクはゼロになるので、インシデントの監視や報告を受けるために24時間誰かが稼働する必要がなくなる見込みです。セキュリティ運用におけるリソースシフト、働き方改革につながると期待しています。今後の運用においてもNTT Comのコンサルティング力とサポートに期待しています」

お問い合わせ
NTTコミュニケーションズ株式会社
サイト www.ntt.com/business/case-studies

2019.10