MENLO SECURITY

日本郵政株式会社

国内最大規模の企業グループにおいて
インターネット分離を実現
既存端末に影響を与えることなく
セキュリティと利便性が向上

JP HOLDINGS 日本郵政

Case Study

User Profile

日本郵政株式会社
所在地：　東京都千代田区大手町 2-3-1
導入時期：　2019 年 2 月
URL:　https://www.japanpost.jp/

日本郵便・ゆうちょ銀行・かんぽ生命保険からなる日本郵政グループの持株会社。グループ中期経営計画「JP ビジョン 2025」の実現に向けて「進化するぬくもり。」というグループ共通のキャッチコピーを掲げ、お客さまと地域を支える「共創プラットフォーム」となるべく、さまざまな企業や地域コミュニティとの連携や価値創造を推進。

執行役 グループCISO
正村勉氏

グループ IT 統括部
情報セキュリティ室
吉田琢朗氏

Overview

日本年金機構の事件を契機にインターネット分離の仕組みを検討

日本郵政公社を前身とし、日本郵便・ゆうちょ銀行・かんぽ生命保険からなる日本郵政グループの持株会社である日本郵政。2021 年に郵政事業創業 150 周年を迎えた同社は、グループ中期経営計画「JP ビジョン 2025」の実現に向けて「進化するぬくもり。」というグループ共通のキャッチコピーを掲げ、お客さまと地域を支える「共創プラットフォーム」となるべく日々挑戦を続けている。

同グループは従業員、総資産ともに国内企業の中でも最大規模を誇るが、そのセキュリティ対策については入口／出口／内部対策を 3 点セットとして継続的に取り組みを強化してきた。この点について同グループの情報セキュリティを統括する 執行役 グループ CISO の正村勉氏は「入口については、添付ファイルを開くなどの行為で感染するメール攻撃、USB メモリなど外部から持ち込まれたデバイスを使用することで感染する外部媒体攻撃、特定の Web サイトにアクセスすること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。このうち、メールと外部媒体の攻撃には対策がかなり進みましたが、水飲み場攻撃については対策が遅れがちで、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手段となっていました」と説明する。

そうした中、2015 年に日本年金機構をターゲットとした大規模なサイバー攻撃が発生。これを受けて、総務省は、業務端末の「インターネット分離のガイドライン」を発表し、その実施を強く推奨するようになった。

「日本郵政という冠をもつ企業の義務として、情報漏えいは絶対に許されません。郵便局に置いてある端末は、業務だけでなくインターネットやメールにも使われますので、こうした状況を考えると、インターネット分離もしくは同様の仕組みが必要だと考え、検討を始めることにしました」（正村氏）

導入の POINT

- 別の端末やツールが不要、かつ既存の端末へ影響を与えることなく導入可能
- ユーザのトラフィックがバーストした際もクラウド上でオートスケール
- セキュリティの向上と使い勝手の向上を同時に両立

端末を用意する、
ツールをインストールするなどの手間が不要
既存の端末にも影響なし

日本郵政では、2016 年から具体的なソリューションについて検討をスタート。端末をインターネット用と業務用に物理的に分ける方法、VDI（仮想デスクトップ）でアプリケーションを端末とは別の場所で稼働させる方法、セキュアブラウザを端末に実装し、実行環境を分離したり、画面を転送したりする方法などをピックアップした。

まず、物理的分離では端末の数が倍になるため、コストがかかることに加え、置くスペースを確保するのが困難という問題があった。また、端末にツールをインストールする方法では、全国にある膨大な数の端末に対して導入作業を行うことになり、やはり多くのコストと手間がかかる。VDI でも、瞬間的な最大アクセスがどれほどになるか読めないため、余裕をもってシステムを構築する必要があり、ここでもコストがネックになった。

一方、こうした問題とは無縁だったのが、Menlo Security 社の SaaS 型アイソレーション（分離）ソリューションであった。Menlo Security は、すべてのWebコンテンツをクラウド上で実行し、表示結果だけをエンドポイントに転送する。そのため、別の端末を用意したり、ツールをインストールしたりする必要がない。また、管理者側で一括してコントロールでき、瞬間的にアクセスがバーストした場合にもクラウド上でオートスケールされるので問題ない。グループ IT 統括部　情報セキュリティ室の吉田琢朗氏は「このほか当社が要件の中でこだわったのが、ユーザがとまどうことがないよう、既存の端末に影響を及ぼさないという点です。具体的には、操作性に変更がなく、利用に際しての制限がないことを求めたのですが、これを実現できたのは Menlo Security だけでした」とその特長を高く評価する。

セキュリティと使い勝手の向上が両立

2017 年末、入札が行われ Menlo Security の採用が決定。導入ベンダーにはNTT コミュニケーションズ（以下、NTT Com）が選ばれた。日本郵政グループの従業員数は、数十万人であり、そこで使われているクライアントPC も膨大な数になり国内最大規模の導入実績を誇る。

「導入にあたって、まずWeb サイトへのアクセスの方針を決めました。業務で使用するサイトは信頼できるサイトとしてホワイトリストに認定し、これまで通り使えるようにする一方、それ以外のサイトをMenlo Security によって分離することにしました」（吉田氏）

運用の切り替えに向けた作業は、2018 年7 月にスタート。業務で使用するサイトの情報を各社、各部署から収集しホワイトリストに登録する作業に半年を費やした。その後、Menlo Security への切り替えを実施し、2019 年2 月より正式にサービスの利用を開始した。なお、当初の一カ月間は特別対応として、ヘルプデスクやFAQ を用意するとともに、NTT Com のスタッフが常駐し、迅速な対応が可能な体制を整えた。

「米国の Menlo Security 本社ともしっかりコミュニケーションをとってくれたことで、スムーズに導入が進みました。これほど大規模な環境の切り替えとなると、通常であれば年単位の作業になるのですが、もともと NTT Com が当社のネットワークと深く関わっていたこともあり、その経験を活かすことで、今回のスピーディな導入につながりました」（正村氏）

導入の効果だが、なんといっても 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ったのが大きいという。

「一般に、セキュリティと利便性は相反する関係にありますが、Menlo Security の導入によって、従来であればセキュリティ上の懸念から閲覧を禁じていたようなサイトでも安全に閲覧できるようになるなど、セキュリティの向上と使い勝手の向上を同時に両立させることができました。これは他の製品にはない大きなメリットです」（吉田氏）

さらには、ユーザのサイトの閲覧状況を見える化したことで、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ワーク遅延の原因である」などと、各社の CIO、CISO にも報告できるようになった。

許可していない相手先への通信はすべて遮断 24 時間常時監視が不要に

今回の導入により、ホワイトリスト以外のサイトへのアップロードが制御されるとともに、許可したアップロードについてもログが残り、後からしっかり確認できるようにもなった。これがユーザへの抑止効果として機能しているという。

「これをさらに一歩進め、ブラウザ以外の外部への通信はマルウェアによるものと判断。許可していない相手先への通信はすべて遮断するという運用を計画しており、今年度中にスタートさせる予定です。これにより、個々の通信を24 時間常時監視する必要がなくなり、インシデントの報告を受けるために誰かが居残る必要もなくなります。結果として、働き方改革にも貢献するものと期待しています」（正村氏）

「Menlo Security は優れた製品ですので、ぜひほかの日本企業にも利用の輪が広がっていけばと思います。そのためにも、私たちが運用で蓄積した知見やノウハウをサービスへとフィードバックしていただき、Menlo Security をより良いものにしていてもらいたいと考えています」（正村氏）

Menlo Security について

Menlo Security は、Web、ドキュメント、メールからマルウェアの脅威を排除することによって、組織をサイバー攻撃から保護します。Menlo Security は、グローバル2000 に名を連ねる何百社もの企業と主要な政府機関におけるセキュアクラウドトランスフォーメーションの達成を支援してきました。Menlo Security のCloud Security Platform は、拡張性に優れており、あらゆる規模の企業に包括的な保護を実現します。エンドポイントソフトウェアは不要で、エンドユーザーの操作性にも影響しません。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com