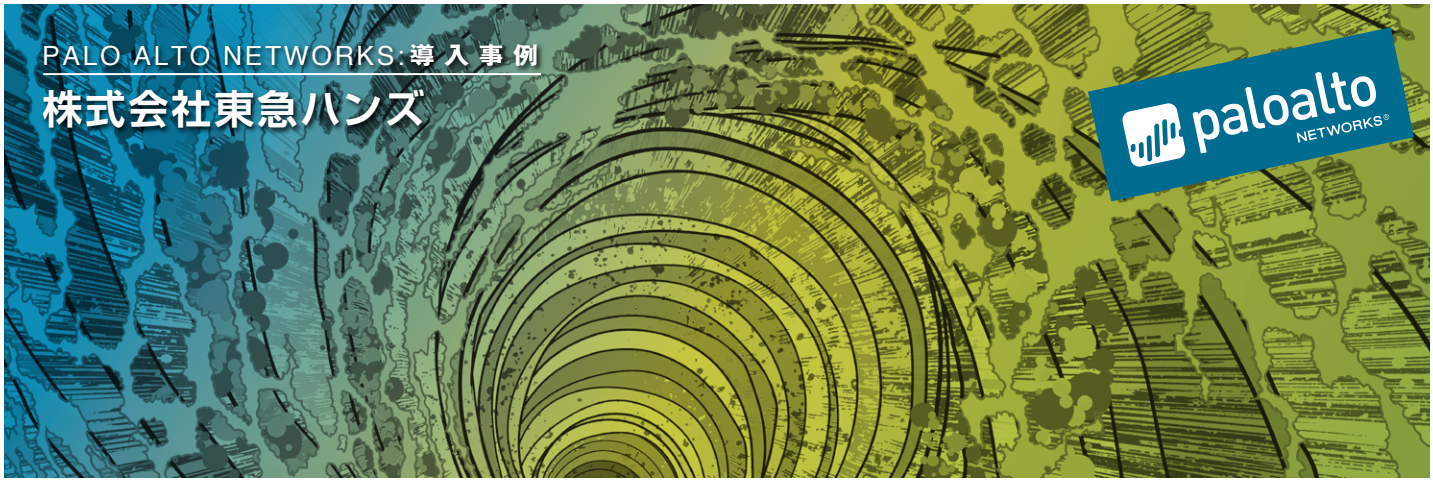


AWSによる“100%クラウド”の一環としてVM-Seriesを導入 出口対策に有効なセキュリティ ソリューションとして活用

株式会社東急ハンズ
執行役員 オムニチャネル推進部長
ハンズラボ株式会社
代表取締役社長
長谷川 秀樹 氏

株式会社東急ハンズ
オムニチャネル推進部
企画推進グループ グループリーダー
田木 清太 氏

株式会社東急ハンズ
オムニチャネル推進部
企画推進グループ
浅井 宏美 氏

株式会社東急ハンズ

東京都新宿区新宿6-27-30
新宿イーストサイドスクエア
https://www.tokyu-hands.co.jp/

分　野

小売業

導入背景

- セキュリティ強化の一環として標的型サイバー攻撃の出口対策を実施
- 社内ネットワークのインターネットゲートウェイをAWS上に設置
- アプリケーションの可視化・制御を行うソリューションの導入を検討

ソリューション

- AWS上で稼働するパロアルトネットワークスの仮想化次世代ファイアウォール「VM-Series」を導入
- ネットワークとセキュリティの状況を可視化する統合管理製品「Panorama」を導入

出口対策に有効な仮想化次世代ファイアウォールを導入

東急ハンズは2017年10月、内部ネットワークとインターネットのゲートウェイに設置するセキュリティ対策機能として、パロアルトネットワークスの仮想化次世代ファイアウォール「VM-Series」を導入、運用を開始した。アマゾン ウェブ サービス(AWS)による“100%クラウド”を推進する同社では、セキュリティ強化の一環として標的型サイバー攻撃の出口対策に有効なアプリケーションの可視化・制御を行うソリューションの導入を検討。日本のAWSユーザーが集まる「JAWS-UG(AWS Users Group-Japan)」での評価も参考にしながら機能・性能を比較した結果、VM-Seriesを選定したという。

セキュリティ強化策として出口対策に着手

東急ハンズは、1976年に創業した住まいと生活関連の商品・素材を扱う総合専門小売業。都市部を中心に国内外50店舗を展開し、日本の小売業界では屈指のブランド力を誇っている。「ここは、ヒント・マーケット。」をブランドステートメントとし、店舗を顧客にとっての“きっかけ売り場”“発想の一歩目”と位置づけ、ものづくりのヒントとなる商品・素材を品揃えしているという。2018年3月には東急ハンズ新宿店に6つのショップインショップを開設し、それぞれのジャンルに精通したスタッフが“店主”として就任。店主が各ジャンルの知識を駆使して売り場をプロデュースする「Hi! Tenshu」プロジェクトを始動させるなど、ユニークな取り組みも行っている。

そんな東急ハンズでは、社内システムについてもユニークな施策を進めてきた。同社は2012年に社内システム全体を“100%クラウド”化すると決断し、段階的にAWSへの移行を開始。現在までに基幹系のマーチャンダイジング システム、POSシステム、ECサイトなどの業務システムを中心にクラウド化を完了させている。

そうした中、2017年度に重点的に実施したのが、セキュリティ強化の取り組みだった。

「当社ではセキュリティ強化を目指し、2017年度にWebアプリケーションの脆弱性を悪用した攻撃からWebサーバーを保護する『WAF(Web Application Firewall)』、エンドポイントでの不正な挙動を迅速に検知・対処する『EDR(Endpoint Detection and Response)』といったソリューションを順次導入してきました。その一環として導

入を検討したのが、標的型サイバー攻撃の出口対策に有効なアプリケーションの可視化・制御を行うソリューションです」（東急ハンズ 執行役員 オムニチャネル推進部長 長谷川 秀樹氏）

専門家の評価が高い VM-Seriesを採用

東急ハンズでは、本社および各店舗で合計約1,700台のクライアントPC、約3,000台のモバイル端末（Apple iPhone）が稼働している。クライアントPCやモバイル端末は、売上・在庫の確認や予約注文、本社・店舗間の連絡などさまざまな用途に利用している。また、店舗では顧客からインターネットで見たという問い合わせも多く、その場で確認するためにもインターネットへのアクセスは不可欠だという。

そこで同社のネットワークは、AWSの専用線接続サービス「Direct Connect」を経由してAWSのゲートウェイからインターネットに接続する仕組みにしている。そのため、出口対策に有効なソリューションを選定するにあたって、「AWS上で稼働すること」が第一の要件だった。

「AWS上で稼働する複数の仮想セキュリティアプライアンス製品を候補に挙げ、当社にとって最適な製品を選定することにしました。ただし、比較表を作成して機能やコストの比較は行わず、日本のAWSユーザーが集まる『JAWS-UG（AWS Users Group-Japan）』での評価を重視することにしました。クラウド上のソリューションは日々機能強化が図られるので、ある時点の断面的な機能比較を行っても意味がありません。AWS上のセキュリティ対策にはベストプラクティスもないため、製品に利害関係のない専門家が高く評価するソリューションが適していると考えたからです。2016年から少しずつ情報収集を始め、2017年1月には第三者の評価・意見を参考にしながらパロアルトネットワークスの仮想化次世代ファイアウォール『VM-Series』を採用することに決めました」（長谷川氏）

ネットワークの可視化により QoSを実施

2017年1月にVM-Seriesの採用を決めた東急ハンズでは、すぐさまAWS上にVM-Seriesを導入する作業に着手した。AWS上へのインストール自体は容易に実施できたものの、VM-Seriesにネットワークを通す作業には時間を要したという。

「実は、VM-Seriesを導入するのと同時期にネットワークの変更作業も行っていました。当社のネットワークは、拠点からAWSへ直接接続しているものと、拠点からデータセンターを経由してAWSへ接続しているものが混在しており、それらの設定作業に想定していた以上の手間がかかりました。これはVM-Seriesが原因ではなく、AWSに難しさがあったという認識です。そもそもAWSをインターネットゲートウェイとして利用する企業は非常に少ないため、ノウハウもナレッジもほとんど存在しません。エンジニアも経験がなかったので、試行錯誤を繰り返しながら導入しました」（長谷川氏）

VM-Seriesの導入を担当したオムニチャネル推進部 企画推進グループ グループリーダーの田木 清太氏は、次のように振り返る。

「VM-Seriesの稼働を開始したのは、2017年7月のことです。最初に本社のネットワーク、続いて各拠点のネットワークを順番に通していきました。この間、一時的にルーターのトラフィックが逼迫したためVM-Seriesを見たところ、Google Driveへのアクセスが非常に多いことが分かりました。ちょうど同時期にファイルサーバーをGoogle Driveへ移行する作業を並行して行っていたことが原因でした。ネットワークを可視化して原因が究明できたため、業務の優先度を考えながらQoS（Quality of Service）を実施することができました。これもVM-Seriesを導入した効果の一つだと考えています」（田木氏）

社内感染を未然に防止するという効果を得る

東急ハンズが導入したVM-Seriesは、パロアルトネットワークスのクラウド脅威解析サービス「WildFire」サブスクリプションなども含むフルオプション構成となっている。VM-Seriesのセキュリティ対策状況やネットワーク パフォーマンスは、次世代ファイアウォールの統合管理製品「Panorama」を通じて可視化されている。ちなみに同社はセキュリティ監視を外部のマネージドサービスにアウトソーシングしており、VM-Seriesの監視も同サービスを通じて24時間365日体制で実施しているという。

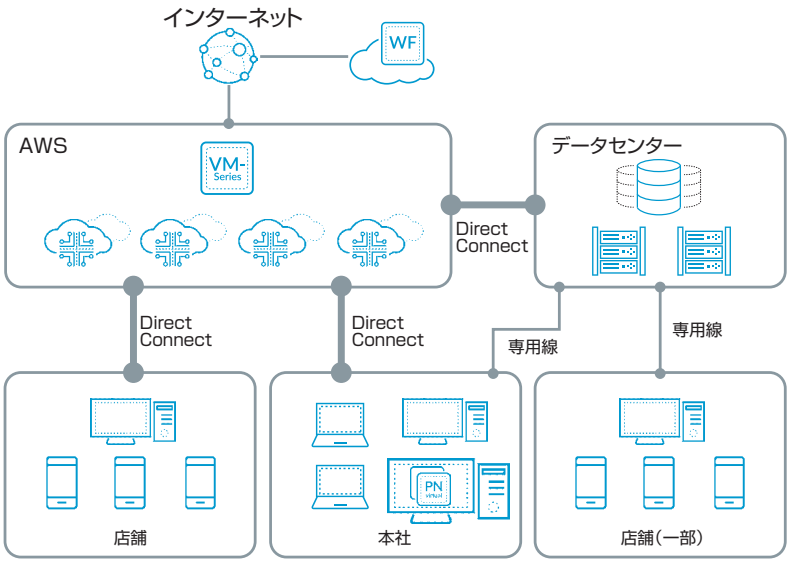
オムニチャネル推進部 企画推進グループ 浅井 宏美氏によると、VM-Seriesの導入効果はすぐに表れたという。

「VM-Seriesを導入してすぐに、ネットワーク内部のホストから不審なサイトへの通信を検知するというインシデントが2件発生しました。いずれもVM-Seriesがマルウェアを検知できたため、通信を遮断することで社内感染を未然に防止することができました」（浅井氏）

VM-Seriesを導入して約1年が経過したが、東急ハンズでは今後もVM-Seriesによる出口対策の効果を期待する。

「当社にとってネットワークやセキュリティの監視は本業ではありません。当社が直接手を動かさなくても、外部に委託したマネージドサービスとVM-Seriesがネットワークを守ってくれるものと期待しています」（長谷川氏）

株式会社東急ハンズのネットワーク構成概要図



〒102-0094
千代田区紀尾井町4番3号
泉館紀尾井町3F

電話番号: 03-3511-4050

www.paloaltonetworks.jp