導入事例

これまで可視化できなかった Web 経由の脅威を確実に検知して遮断
京王グループ約 6,000 台の PC を保護する BloxOne Threat Defense

企業プロフィール

京王電鉄株式会社
所在地 東京都多摩市関戸一丁目 9 番地 1
設立 1948 年 6 月 1 日
代表　代表取締役社長　紅村康
URL https://www.keio.co.jp/

導入前の課題

- Web 閲覧経由での不正アクセスやマルウェア感染への対処が急務
- セキュリティシステムの導入・運用保守にまつわる負荷の抑制

ソリューションの利点

- DNS ベースのセキュリティ対策により、Web 経由での脅威を検知、遮断
- クラウドベースのソリューションによる容易な導入と柔軟な展開

導入後の効果

- これまでは検知が困難だった脅威を確実に可視化し遮断
- グループ会社を含め、約 6,000 台の PC を脅威から保護

京王電鉄株式会社
所在地：東京都多摩市関戸一丁目 9 番地 1
設　立：1948 年 6 月 1 日
代　表：代表取締役社長　紅村康
URL：https://www.keio.co.jp/

日本の大手私鉄の 1 社である京王電鉄株式会社では、社会的に重要インフラを担う企業として、グループ会社を含めた IT 基盤におけるセキュリティ強化を継続的に推進しています。そうした同社において課題として浮上していたのが、近年、急速に拡大しつつある Web サイトを介したマルウェア感染と不正アクセスへの対処でした。この課題を解決するために同社が採用したのが、Infoblox の DNS セキュリティソリューション「BloxOne Threat Defense」でした。

重要インフラ事業者として継続的なセキュリティ強化を推進

日本の大手私鉄企業であり、57 社から構成される京王グループの中核企業を担う京王電鉄。近年ではシステム展開の迅速化やコスト削減、外部環境の変化への柔軟な対応等を目的にクラウドシフトを推進するとともに、AI や IoT を活用したデジタル化にも積極的に取り組んでいます。そうした“攻めの IT”の展開に注力する一方、“守りの IT” としてのセキュリティ強化にも継続して努めてきました。京王電鉄 経営統括本部 IT 管理部 グループ IT 担当 課長の田村浩子氏は、「特に近年では、東京オリンピック／パラリンピック大会の開催に向け、交通機関等の重要インフラ事業者は政府からもセキュリティの強化が求められており、そうした要請に応える形で様々な取り組みを進めてきました」と語ります。

事実、2015 年 6 月に「京王 SIRT」を立ち上げ、京王グループを横断的にカバーするセキュリティ対策の実施に踏み出したのをはじめ、メールセキュリティソリューションの強化により、メールを介したマルウェア感染を削減するなど、様々な施策を講じるとともに効果を上げてきました。

「しかし、数年前から不正な通信を検知、分析していく中で、検索エンジンの検索結果の上位にマルウェア等を含む悪質なサイトを表示させ、詐欺サイトに転送したりマルウェアに感染させたりする『SEO ポイズニング』と呼ばれる脅威に遭遇するケースが頻出し始めていました」と、経営統括本部 IT 管理部 グループ IT 担当の佐藤賢一氏は説明します。

「さらに、前述した SEO ポイズニングの原因について調査を行いました。Web サイトを構成するものとしては、大きく 2 つに分かれます。OS などのプラットフォーム部分と Web アプリケーションです。セキュリティベンダー発行の調査資料に Web アプリケーションについては、88.2%脆弱性があるという記載がありました。そもそも、現状の Web サイト側に安全性の問題があることが分りました。攻撃者により脆弱性のある Web サイトは改ざんされ SEO ポイズニングの原因の一つに結びつくと考えました。実際、URL フィルタ等のソリューションも導入していましたが、それだけでは対処が難しい攻撃が増加しており、より多層的な防御が可能な仕組みの構築が求められていたのです」（佐藤氏）

京王電鉄株式会社
経営統括本部
IT 管理部グループ
IT 担当

課長 田村浩子氏

京王電鉄株式会社
経営統括本部
IT 管理部グループ
IT 担当

佐藤賢一氏

Web を介した脅威を遮断するため DNS ファイアウォールに着目

そうした課題を解決するものとして、同社が着目したのが、「DNS ファイアウォール」でした。「DNS のログ監視が効果的であるとの情報を得て、さらに調査を進めていく中で、DNS ファイアウォールの存在を知りました。DNS ベースでトラフィックを制御し、不正なドメインに対する DNS 通信を遮断する DNS ファイアウォールであれば、これまで対処が難しかった Web 閲覧を介したマルウェア感染による情報漏えいを、事前に阻止できるようになると考えたのです。JPCERT の資料が特にヒントになりました。例えば、デリバリの攻撃段階でブロックできなかった場合、後日 Infoblox 側の脅威情報等が更新され、新たな不正通信を検知できれば、エクスプロイト、C&C、目的の実行において再度 DNS のチェックができ、（JPCERT 資料参照）デリバリの攻撃段階ですり抜けた不正通信がブロックできる確率が上がると考えました」と佐藤氏は語ります。

京王電鉄は「誤検知が少なく導入が容易で、かつ十分な検証（PoC）の期間を提供してくれること」（佐藤氏）の 3 点を要件に複数の DNS ファイアウォール製品の比較検討を実施。最終的に選択されたのが、Infoblox の DNS セキュリティソリューション「BloxOne Threat Defense」です。BloxOne Threat Defense は、アナリティクスや機械学習を用いることで DNS ベースの攻撃による情報漏えいをはじめ、ドメイン名生成アルゴリズム（DGA）や DNS Messenger、fast-flux 攻撃といった最新の脅威も検知、遮断するものです。さらに DDI（DNS ／ DHCP ／ IP アドレス管理）、脅威情報、コンテキスト情報の連携により、高い検知精度を実現。これらの機能の優位性により、脅威への迅速な対処を可能としています。

京王電鉄は BloxOne Threat Defense の実力を確認するため、2018 年 10 ～ 11 月、翌 2019 年 3 ～ 4 月の 2 度に亘って検証を実施。「結果、これまで気づかなかった、遮断すべき URL への通信が 50 件ほど検知されるなど、その効果を十分に確認することができ、『これを導入しない理由はない』と判断しました」と佐藤氏は振り返ります。田村氏も「クラウドサービスとしても提供されているため、京王グループ企業の各社への展開が容易であることをはじめ、新機能の追加にも柔軟に対応可能であること、オンプレミスの製品のようにハードウェアの保守運用にかかるコストや負荷も抑制できる点も評価ポイントでした」と強調します。

これまで検知できなかった脅威を可視化した BloxOne Threat Defense

2019 年 6 月、京王電鉄は BloxOne Threat Defense の導入を正式に決定。京王グループ各社との調整および導入作業を経て、9 月からの本番運用を開始しました。現在では、グループ会社を含む約 6,000 台のクライアント PC が、BloxOne Threat Defense によって保護されています。BloxOne Threat Defense は、期待した通りの効果を京王電鉄にもたらしているようだ。佐藤氏は、「例えば、昨年末より猛威を振るっていた『Emotet』のダウンロードサイトに端末が通信しているのを検知、遮断しています。また、懸案事項であった SEO ポイズニングも減少しています」と話します。

攻撃段階および攻撃内容とログの関係

攻撃段階		ログで検知可能な攻撃内容	ログ取得対象機器
1	偵察	-	-
2	武器化	-	-
3	デリバリ	攻撃者によるマルウエア添付メールの送信	メールサーバ
		攻撃者によるマルウエア設置サイトへの誘導メールの送信と誘導	メールサーバ Web プロキシサーバ **DNS サーバ**
4	エクスプロイト	コールバック（Web プロキシサーバを介さない外部への通信）	Firewall **DNS サーバ**
		コールバック（HTTP, HTTPS 等のプロトコルによる外部への通信）	Web プロキシサーバ **DNS サーバ**
5	インストール	-	-
		-	-
6	C&C	コールバック（Web プロキシサーバを介さない外部への通信）	Firewall **DNS サーバ**
		コールバック（HTTP, HTTPS 等のプロトコルによる外部への通信）	Web プロキシサーバ **DNS サーバ**
		感染活動（脆弱な PC や内部サーバの探索など）	Firewall
		ファイルサーバなどへのアクセスや権限の奪取	AD ログ Firewall
7	目的の実行	コールバック（Web プロキシサーバを介さない外部への通信）	Firewall **DNS サーバ**
		コールバック（HTTP, HTTPS 等のプロトコルによる外部への通信）	Web プロキシサーバ **DNS サーバ**
		機密情報持ち出し (メールサーバ経由)	メールサーバ **DNS サーバ**

引用元 : JPCERT コーディネーションセンター「ログを活用した高度サイバー攻撃の早期発見と分析」
https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf

田村氏も「これまで気付けていなかった脅威を検知、遮断できるようになったことが大きいと考えています。また、以前であれば脅威の発生時に検知できず、また、時間が経ってから発覚した場合、原因となった端末の特定等が困難だったのですが、BloxOne Threat Defense のログを分析することで調査、確認が可能になりました」と語ります。

「特に運用面では BloxOne Threat Defense のレポート機能が有効であるほか、検知、遮断したマルウェアに関連する情報のリンクを一覧表示する『Dossier』機能により、都度、情報が掲載された Web サイトを検索してアクセスしなくても済むようになり、とても重宝しています」（佐藤氏）

京王電鉄は Infoblox のサポートについても評価しています。「同社のスタッフは、こちらからの新機能の要望にも親身に耳を傾け、対応してくれるよう動いてくれています。他のソリューションとの組み合わせに対する問い合わせにも、踏み込んだところまで話を聞いてくれるなど、とても助かっています」（田村氏）

BloxOne Threat Defense の導入により、重要インフラ企業としてのセキュリティをさらに強化した京王電鉄。最後に田村氏は、今後のセキュリティ強化に向けた展望と Infoblox への要望について、「現在の課題は、疑わしい通信を行う PC の迅速な特定です。今後、働き方改革の一環として、テレワーク等、社外での PC 活用増も予想されています。そうした中で、ファイアウォールや他のセキュリティツールとの自動的な連携により、疑わしい端末の特定から、通信の遮断による二次感染の防止までを自動で行ってくれるなど、私たちの運用負荷をさらに削減してくれるような機能強化や提案を期待しています」と締め括っています。

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37 VORT外苑前Ⅰ 3階
Tel：03-5772-7211
Email：info@infoblox.com
https://www.infoblox.co.jp