セキュリティ対策を統合しつつ、仮想ファイアウォール機能を活用してグループ各社のニーズに柔軟に対応

重要インフラ事業者としてセキュリティレベルの底上げを進める京王グループ

鉄道事業を中心に、運輸、流通、不動産など幅広い事業をグループ全体で手がける京王グループは、人々の生活を支える重要インフラ事業者としてセキュリティ対策の強化に努めてきた。そして東京オリンピック・パラリンピックを前に、グループ全体のセキュリティレベルの底上げを図る手段として、セキュリティ対策を統合しつつ強化し、多様な業種のグループ各社のニーズに応じてセキュリティポリシーを柔軟に構成できるFortiGateをインターネット基盤に採用した。

京王電鉄株式会社

東京都多摩市関戸一丁目9番地1
設　　立 1948年6月1日
資 本 金 590億23百万円
従業員数 2,547人

株式会社 京王ITソリューションズ

東京都調布市小島町1丁目32番地2
設　　立 2001年4月2日
資 本 金 65百万円
株　　主 京王電鉄株式会社100%
従業員数 60人

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
田中 淳一郎氏

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

株式会社
京王ITソリューションズ
IT企画開発部
スペシャリスト
向井 和弘氏

導入・構築のポイント

(1) 次世代ファイアウォールとプロキシサーバのセキュリティ機能を統合しつつ、SSLインスペクションをはじめセキュリティを強化

(2) 仮想ファイアウォール機能により、多様な業種にまたがる30社をこえるグループ会社ごとのニーズに応じて柔軟なセキュリティポリシーの構成を実現

(3) グループ各社のセキュリティの運用監視も提供してグループの統制を強化

東京オリンピック競技会場が沿線、重要インフラ事業者として対策を推進

近年、電力や水道、ガスといった重要インフラに関する分野では特にサイバーセキュリティの強化が求められている。日々、通勤・通学や日常の足となる鉄道も例外ではない。

京王電鉄を中心に運輸、流通、不動産といった多様な事業を展開している京王グループの場合は、さらに真剣に取り組まなければならない事情があった。京王線の沿線には、味の素スタジアムをはじめとする東京オリンピック・パラリンピックの会場が設けられる。大会を支えるインフラがサイバー攻撃によって妨げられることのないよう、「情報セキュリティ分科会」を設け、セキュリティ対策に力を入れてきた。

「沿線に競技会場が設けられることもあり、2015年、情報セキュリティ分科会の中にCSIRTの役割を担う『京王SIRT』を設置しました」（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 田中 淳一郎氏）。

それでなくてもこの十数年、企業を狙うサイバー攻撃は高度化し、その量も急増している。そこで京王ITソリューションズの力も借りながらグループ全体のセキュリティレベルの底上げに努めてきた。

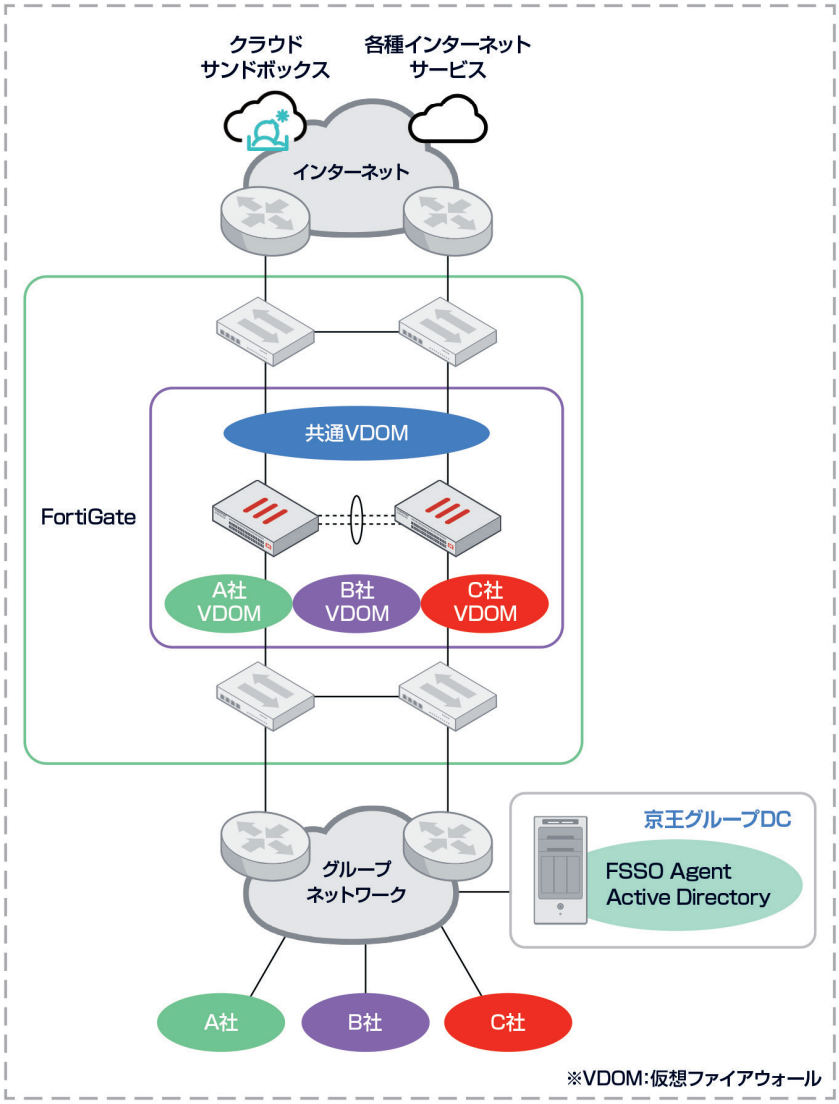
セキュリティ対策を統合しつつ、仮想ファイアウォール機能でグループ各社のニーズに柔軟に対応

この中で京王電鉄が力を入れてきたのが、脅威の「見える化」だ。「セキュリティ、特に外部からの攻撃は見えづらい部分があります」（田中氏）。そこで専門事業者のSOCサービスを活用し、インターネットとの境界を守る次世代ファイアウォールやプロキシサーバのログに加え、エンドポイントセキュリティ製品のログも収集して統合的に監視し、深刻な問題があれば通知してもらう運用を回してきた。

ただ、やはりアラートの中には「空振り」、いわゆる過検知も含まれる。アラートを受け取って社内やグループ各社に通知し、詳細を確認してもらう手間もさることながら、過検知が繰り返されることで「またアラートだけれど、今回も大したことはないでしょう」と受け止められかねない懸念があった。また、セキュリティ製品の設定を変更するにも手間と時間がかかることがストレスとなっていたという。

そこで2019年、京王グループのインターネット基盤の更改を機に、セキュリティ製品も検討し直すことにした。そこで採用したのがフォーティネットの次世代ファイアウォール「FortiGate」だった。

これまで別々の製品で実現していた次世代ファイアウォールと、認証やWebフィルタリングを行うプロキシサーバのセキュリティ機能を引き継ぎつつ統合し、さらにこれまで以上のセキュリティ対策の強化を実現することが第一の条件だった。Webサイトの HTTPS化が進む中、SSL通信の中身をひもといて検査できるSSLインスペクション機能の有無もポイントだったという。



そして、京王グループ各社に安全なインターネットへの接続をサービスとして提供する立場から必須の要件だったのが、仮想ファイアウォール（VDOM）機能だった。

「グループ全体で守るべきベースラインはありますが、業種が多様なため、一律に同じ設定を適用するわけにはいきません。同じWebサイトでも、ある会社ではブロックしたいけれど、別の会社ではブロックしてはまずい、ということがあります。そうしたとき、仮想ファイアウォールのセキュリティポリシーをグループ会社ごとに個別に構成することで柔軟に運用できるところが選定の鍵となりました。そして、求める要件を一番満たしたのがFortiGateでした」（京王ITソリューションズ IT企画開発部 スペシャリスト 向井 和弘氏）

関連して、管理コンソールを提供するのはもちろん、権限に応じて操作範囲を制限できる管理機能も運用面でのポイントとなった。グループ会社への一部機能の権限移譲もしてい

るという。
また、昨今のオンプレミスからクラウドへの過渡期にある中、新型コロナウイルスの影響もあってテレワークが可能な体制を整え、クラウドサービスの活用にも積極的な京王グループとしても、これまでの境界型防御からゼロトラストセキュリティを中心としたクラウドベースの対策を視野に入れている。そこで、次世代ファイアウォールからゼロトラストセキュリティやSASEに向けた拡張性を備えていることも選定材料のひとつとなった。

セキュリティの運用監視でグループの統制を強化

京王電鉄では2021年1月末からFortiGateを活用した新たなインターネット基盤の環境へ切り替え、本体のほか、グループ会社のほぼ全て、具体的には三十数社に対し「インターネットコネクションサービス」という名称で、FortiGateによるセキュリティ機能やSOCの運用監視も含めた形でインターネットへの接続を提供している。それ以前は、個別にインターネット接続を用意していた会社もあったが、集約できるところは集約してグループ共通の基盤として提供する形だ。
「集約せずに各社バラバラに基盤を整備していくと、各社それぞれに導入・運用のコストがかかってしまいます。ですから、集約して効率を上げるのは不可欠ですが、同時に各社単位で柔軟性を持たせたいと考えていました。仮想ファイアウォールによって個別にセキュリティポリシーをチューニングできる点は、まさにそこにぴったりはまりました」（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）
またグループ各社にとって、専門知識の求められるセキュリティ監視とインシデント対応は荷の重い作業となっていた。そこでFortiGateによる保護とともにセキュリティの運用監視も担うことにした。この体制により、万一インシデントが起きた場合にはSOC経由でアラートが上がり、グループ会社に対し「そちらのこのIPアドレスを利用している端末が、どうも疑わしい動きをしていますよ」と通知し、主体的にアクションを起こせるようになり、グループの統制の強化にもつながっている。
端末に導入したエンドポイントセキュリティ製品のログとの統合分析も行い、こつこつと多層防御を積み重ね、検知能力を高めてきた京王グループでは、「脅威の侵入から、検知、対応までの時間が非常に短くなりました。大事に至る前に被害を食い止められると自負しています」（田中氏）
もちろんこれはFortiGateだけでなく、京王SIRTをはじめとする体制、運用面の整備もあってはじめて実現されていることだ。ただ「FortiGateの導入によってセキュリティレベルの底上げに一定の成果が得られました。我々の守備範囲が広がり、グループ会社側から見ても安全を確保できたと思っていただけているのではないでしょうか。重要インフラ事業者として、何か起こったとしてもお客様に迷惑をかけたり、評価が下がる前に対応できる体制を整え、オリンピック前に目的を達成できたと思っています」と田中氏は述べた。
FortiGateでは以前より細かくトラフィックを検査できるようになったこともあり、以前の次世代ファイアウォール製品に比べ、切り替え直後はアラート数が増えたという。その内容を精査し、チューニング作業を進めている段階だ。「フォーティネット社にも相談しながら使いこなしていきたいと思います」（田村氏）

OTシステムのセキュリティ対策も視野に、引き続きレベルアップを

クラウドサービスの活用をはじめ、デジタル化にも取り組んでいる京王グループだが、その中で、使い勝手の良さとセキュリティのバランスをどう取っていくかは常に課題だという。
「電鉄本体に限らず、グループ各社のユーザー側は、使い勝手のよい、生産性の高いITサービスを利用したいと考えています。それ自体はよいことですが、無秩序に使われてしまうとリスクを招く恐れがあります。統制は効かせていきますが、上から強制的に押しつけるのではなく、『安全安心で、使いやすいものはこれです』というお墨付きを与えたサービスを定義し、使ってもらうようにしていきたいと考えています」（田中氏）。FortiGateが搭載するアプリケーション制御機能なども活用し、うまくコントロールを利かせていきたいとした。
さらに、ITシステムだけでなく、鉄道事業部門のOTシステムのセキュリティ対策も重要な課題だ。「OTのIT化が進んでいる中、どのようにセキュリティを担保するかも大きな課題です。レガシーなOSが使われていたり、ネットワークにつながっていなかったりして、IT向けの対策をそのまま適用するのが難しい部分も

あります。対策は打っていますが、それが適切かどうかをあらためて検証し、OTの安全を担保する方法を模索していきたいと思います」（田中氏）

これからも情報セキュリティ分科会や京王SIRTを軸に、京王電鉄本体のみならず京王グループ全体での情報共有・連携を図りながら、セキュリティ対策を推進していく。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ