ケーススタディ

「重要インフラ企業」としての責任 JR九州が目指すセキュリティリスクの可視化と是正サイクル

九州旅客鉄道株式会社

業種
旅客鉄道事業

従業員数（2024年3月末現在）
JR九州7,567人
グループ14,677人

本社所在地
福岡市博多区

導入ソリューション
Tanium Core, Asset, Comply, Deploy, Discover, Enforce, Patch, Performance, Provision

Taniumの導入効果

- グループ全体のIT資産の一元管理を実現
- すべてのエンドポイントの状態把握と是正サイクルの構築
- ダッシュボードを使った正確で円滑なコミュニケーション

九州地方を中心に鉄道事業を展開する九州旅客鉄道株式会社（以下、JR九州）は、新幹線や在来線の運営に加え、不動産、ホテル、外食、観光事業といった多角経営を推進。Taniumを活用して全グループのエンドポイントのリスクを可視化し、グループ全体でセキュリティ基盤の構築に取り組んでいる。

DXを支えるデジタル人材の育成とIT基盤の整備

「パンデミックを経て、人流だけに頼る経営の危うさを痛感しました。グループ全体として、鉄道以外の事業の多角化をより進めています」と語るのは執行役員　デジタル変革推進部長　長﨑　剛氏だ。同社のDX戦略の方針は「お客様体験価値の向上」、「オペレーション・メンテナンス改革」、「働き方改革・生産性向上」の3つがある。これを支えるためにデジタル人材の育成とIT基盤の整備に取り組んできた。ローコード開発といったデジタル技術の活用で生産性を上げた社員を認定する「デジタルヒーロー認定制度」は、同社が事業会社でありながらデジタル活用を主体的に推進していることを示している。

九州旅客鉄道株式会社
執行役員 デジタル変革推進部長
長﨑 剛氏

セキュリティ被害を自分ごととして意識できた

一方で多角化にともなってIT資産は断片化し、状況把握の精度に課題を抱えていた。JR九州は2016年の株式上場を機にグループ全体でセキュリティ基盤を整えている。このタイミングでは「セキュリティに関する意識や対策を一段上げることができた」と、デジタル変革推進部 副課長 三嶋 利治氏は振り返る。ところがセキュリティの脅威は手法の高度化を続け、ついに同社でもホームページへの不正アクセスというインシデントが発生する。これを受けて同社はさらなるセキュリティ対策を続け、公開サーバーへの着手に始まり、CSIRTの立ち上げとさらなるセキュリティ対策を続けた。変化し続ける攻撃手法はその後、ランサムウェアとして世の中を席巻することになる。「過去の経験から、ランサムウェアの被害を自分ごととしてしっかり捉えることができ、いよいよエンドポイント管理ソリューションとしてTanium

> サイバーハイジーンの考え方は非常に重要。セキュリティに関するコミュニケーションの解像度が上がった。今後構築する情報システムのセキュリティレベルもより上がると思います

九州旅客鉄道株式会社
執行役員 デジタル変革推進部長
長﨑 剛氏

九州旅客鉄道株式会社
デジタル変革推進部 副課長
三嶋 利治氏

JR九州システムソリューションズ株式会社
基盤本部第2部 部長
末永 剛氏

の導入を検討しました」と三嶋氏は背景を説明する。同グループは多くのIT資産をエンドポイントとして一元的に可視化・診断し、対策へ進めるための礎づくりを開始した。

「JR九州は国から『重要インフラ』と指定されている以上、義務がある」と長崎氏が語るように、同グループ全体で10名以上がセキュリティに関わっている。体制を増強するだけでなく、より守りを固めるためにTaniumの導入が決断された。

導入時に再認識した、可視化と是正措置サイクルの重要性

今回JR九州が取り組んだセキュリティ対策には2つの大きな柱がある。一つ目はIT資産を特定・可視化し、サーバーOSや各種ソフトウェアの脆弱性を是正する「サイバーハイジーン」の考え方だ。ここを担うのがTaniumである。二つ目の考え方は、サイバー攻撃に対して予防だけでなく、攻撃を検知し、対応・復旧までおこなうことで、攻撃を受けてもビジネスを止めない「サイバーレジリエンス」。この実現には、EDR（Endpoint Detection and Response）ソリューションを適用した。

「従来はIT資産の管理台帳の正しさを証明できない問題がありました」とJR九州グループの情報システムの運営を担うJR九州システムソリューションズ株式会社　基盤本部第２部　部長　末永　剛氏は振り返る。最新の状況は担当者に聞くしかなく、確認はグループの各システム担当者、その先のベンダーまで行き、返ってきた回答を信じるしかない状況だった。その管理台数は実に1万台。これをTaniumによって機械的かつ網羅的に管理することで大幅な効率化と情報精度の向上を実現した。「ベンダー選定時に重要視したものは全数把握の手法でした。Taniumであれば、いわゆる台帳になかったものまで見つけ出すことができます。単なるIT資産管理ツールではないと理解しています」と末永氏は選定の決め手を説明した。「Taniumであれば、可視化と是正措置のサイクルができます。このことの重要性については導入していく中であらためて理解しました。Taniumのダッシュボードでは全体像を把握できます」と同氏は続ける。

可視化されたファクトで生まれた説得力 対策におけるコミュニケーションの解像度が上がった

「想定はしていたものの、可視化された脆弱性情報の多さには驚きました」末永氏は導入後の印象を振り返る。対応の方針はTaniumの導入から運用までをサポートする、エンタープライズサービス（ESO）のチームとともに、優先度付けの運用ルールを設計し、是正措置に取り組んでいった。「運用設計の6か月間が大事でした。現在は担当者が迷うことはありません」と、末永氏はサポート体制を評価する。「Taniumでは複数人が同じダッシュボードを見て会話できます。かつてはレポートの準備をしていたことを考えると大きく変わりました。可視化されたファクトがあることで説得力が増し、関連部門への対応依頼もしやすくなりました」（末永氏）。

セキュリティへの対策に終わりはない。「全数把握→状態把握による可視化はできた。可視化→是正のサイクルをより効率的に回す仕組み・体制を作っていきます」と三嶋氏。「サイバーハイジーンの考え方は非常に重要。セキュリティに関するコミュニケーションの解像度が上がった。今後構築する情報システムのセキュリティレベルもより上がると思います」と長崎氏は締めくくった。

※所属・役職等はインタビュー当時の情報です。

お問い合わせ
TANIUM
タニウム合同会社
〒100-0004　東京都千代田区大手町２丁目６－４ 常盤橋タワー25階
https://www.tanium.jp
jpmarketing@tanium.com