JR東日本におけるサイバーセキュリティ強化の歩み

東日本旅客鉄道副社長・イノベーション戦略本部長
池田裕彦（いけだ　ひろひこ）

鉄道事業は、人々の移動を支える基幹的な社会インフラとして、社会・経済活動の基盤を成している。JR東日本は、日本最大規模の鉄道事業者として、安全の確保を経営の最優先事項に位置付け、日々の安定輸送を通じてお客さまに安心を提供する責務を担っている。

近年、サイバー攻撃は高度化・巧妙化の一途をたどっており、当社においてひとたび重大なインシデントが発生すれば、安全・安定輸送に影響を及ぼし、社会的混乱を招きかねない。こうした環境下において、鉄道事業を支える情報システムの安全性確保は、現場レベルの課題にとどまらず、経営そのものの持続性を左右する重要テーマである。

当社が過去のインシデントから得た教訓をどのように制度・体制へ反映してきたのか、その基本的な考え方と取り組みの概要を紹介したい。

JR東日本のインシデント事例

当社のサイバーセキュリティ対策において大きな転機となったのが、2009年に発生した「JR東日本ホームページ改ざん事案」である。本事案では、保守作業に使用していた端末が外部から攻撃を受け、認証情報が窃取（せっしゅ）された結果、公式ホームページが改ざんされた。

この事象は、保守端末管理を含む日常業務の運用の適否が、企業全体のセキュリティリスクにつながり得ることを示すと同時に、企業の信頼性に重大な影響を及ぼすことを改めて認識させることとなった。

当社はこれを契機に、組織的・体系的なセキュリティルールの整備と体制構築を本格化させた。端末管理ルールの厳格化や社員へのセキュリティ教育の強化など、多層的な対策を講じ、現在のセキュリティ体制の基盤を築いてきた。

その後も脅威は継続するとともにその環境は変化し、2017年のランサムウエア感染、2023年、2024年のウェブサービスへの攻撃など、攻撃手法は多様化している。当社は、こうした変化を前提として、継続的な対策強化を経営課題として位置付けている。

JR東日本グループのセキュリティ体制

JR東日本グループは多数の事業会社で構成され、システム面でも相互に密接につながっている。この利便性の裏側で、1社の脆弱性がグループ全体に波及するサプライチェーンリスクが顕在化している。

この課題に対応するため、当社は「JR東日本エンドポイントセキュリティサービス（JRE-ESS）」という統一的なセキュリティサービスを構築した。JRE-ESSは、各種セキュリティ対策とインシデント管理を一体化し、グループ全体の端末を統一基準で保護する仕組みである（図表）。各社が個別最適で対策を講じるのではなく、共通基盤のもとで運用することで、グループ全体のセキュリティ水準の底上げと均質化を図っている。

あわせて、24時間365日体制でグループ全体を監視するセキュリティオペレーションセンター（SOC）を構築した。外部の専門企業と社内専門人材が連携する「ハイブリッドSOC」として運営し、異常の早期検知と迅速な対応を可能としている。

さらなるセキュリティ強化へのアプローチ

当社は、セキュリティレベルの向上と、現場における開発・運用負荷の軽減を両立させることを重視している。近年の他社事例では、ルールや技術的対策は整備されていたものの、その実施状況が十分に確認されておらず、結果として情報漏えいに至ったケースが見受けられる。

ルールの遵守を現場の努力に委ねるだけでは限界があり、見落としや内部不正のリスクも否定できない。こうした問題意識から、当社は「対策の実施状況を自動的に把握・検証する」セキュリティ基盤の整備を進めている。

本基盤では、システムやネットワーク機器の状態を常時把握し、セキュリティルールへの適合状況を自動的に監視する。また、脆弱性の検知から是正完了までを一元管理し、リスクに応じた優先順位付けを自動化することで、対応の迅速化と精度向上を図っている。これにより運用負荷とコストを抑制し、限られた人的リソースをより付加価値の高い業務へ振り向けることが可能となる。

制御系システムへの取り組み

鉄道事業において、とりわけ重要なのが列車運行を担う制御系システムのセキュリティである。制御系システムは、安全性と安定稼働が最優先される領域であり、一般的な情報系システムとは異なる配慮が求められる。

当社では、列車運行管理システムや電力制御システム等を対象に、制御系システムに特化したセキュリティルールを策定している。国のガイドラインを踏まえつつ、現場の運用実態を十分に考慮した実効性の高い内容とした。また、定期的に外部専門家による評価を実施し、客観的な視点から対策の妥当性を検証している。

技術面では、通常と異なる通信を検知する仕組みや、外部からのデータ通信を物理的に遮断する装置を導入している。加えて、人材育成にも注力し、情報処理推進機構（IPA）の人材育成プログラム等を活用しながら、システムと鉄道現場双方を熟知した「制御系セキュリティ人材」を計画的に育成している。

社会全体のレジリエンス向上に向けて当社の取り組みに共通する考え方は、「グループ全体を可能な限り統一された仕組みで守る」ことである。多数の関連会社を抱える企業グループにおいては、最も弱い部分が攻撃の起点となる。統一基準の策定と一元的な管理体制は、グループ経営の観点からも不可欠である。

また近年、官民連携によるサイバーセキュリティ対策の重要性が一層高まっている。当社は、経済安全保障や能動的サイバー防御に関する法令に基づき、重要システムに関する情報を政府と共有している。社会インフラを担う企業には、こうした枠組みに積極的に参画し、社会全体のレジリエンス向上に貢献する役割が求められている。

サイバーセキュリティは、もはや一企業で完結する課題ではない。産業界、そして国家レベルでの連携協調を通じて、持続可能な社会基盤を支えていくことが重要である。

図表　JRE-ESSとハイブリッドSOC