第96回運輸政策セミナー 交通サイバーセキュリティXIII
～鉄道分野におけるサイバー攻撃対策と事業継続の取り組み～

主催：一般財団法人運輸総合研究所
後援：一般社団法人交通ISAC

1．開会挨拶

宿利　正史
運輸総合研究所 会長

2．講演①

サイバーセキュリティに関する政府・国土交通省の取り組み

長井　総和
国土交通省 大臣官房政策立案総括審議官

3．講演②

JR東日本グループにおけるセキュリティ戦略と新たな取り組み

関口　義弘
株式会社JR東日本情報システム
ICT基盤本部セキュリティ対策室 次長

4．講演③

安定輸送を脅かす最新のサイバー脅威と事業継続のための要諦

名和　利男
サイバーセキュリティアドバイザー

4．パネルディスカッション

モデレーター

後藤　厚宏
情報セキュリティ大学院大学
教授

長井　総和
国土交通省
大臣官房政策立案総括審議官

関口　義弘
株式会社JR東日本情報システム
ICT基盤本部セキュリティ対策室 次長

名和　利男
サイバーセキュリティ
アドバイザー

5．閉会挨拶

大髙　豪太
運輸総合研究所 主席研究員 事務局長

開催趣旨

冒頭、宿利会長は開会挨拶において、「当研究所では、2020年の東京オリンピック・パラリンピックの際に主要な交通機関で問題が生じないようにという問題意識のもと、2015年度から5年間にわたり交通サイバーセキュリティに関する研究調査を行ってきました。その後も高度化するサイバー攻撃に関する最新情報や知見をアップデートするために、2020年からは交通サイバーセキュリティセミナーを毎年開催しています。本日のセミナーは2015年度から数えて通算13回目のセミナーとなります。

近年、国内で発生した事案では、被害を受けた会社に留まらず、サプライチェーン全体に影響が及んでいます。鉄道、海運、航空、港湾、空港、物流などのいわゆる基幹インフラが攻撃を受けた場合は、直ちに国民生活や経済活動に大きな影響が及ぶことから、これらの分野の対策を講じることは事業者の責務であると同時に社会全体も乗り越えなければならない課題です。

これまでのセミナーでは大手の製造業の情報セキュリティ責任者などにご登壇いただきましたが、参加者の皆様から、運輸交通分野に焦点を当ててほしいという強い要請がありましたので、鉄道分野におけるサイバー攻撃対策と事業継続の取り組みをテーマとして、本日のセミナーを開催します。」と述べました。

セミナーの概要

■講演①

サイバーセキュリティに関する政府・国土交通省の取り組み

長井 総和　国土交通省 大臣官房政策立案総括審議官

サイバーセキュリティ分野では、政府が近年取り組みを一段と強化しており、この１年だけでも多くの動きが見られた。

サイバーセキュリティに関係する主な法律には、１）サイバーセキュリティ対策の基本的な事項を定めたサイバーセキュリティ基本法、２）能動的サイバー防御措置を定めたサイバー対処能力強化法、３）重要設備の導入などに際してその事前審査を定めた経済安全保障推進法がある。このうち、2025年５月に成立したサイバー対処能力強化法には３つのポイントがある。１つ目は「官民連携の強化」で、官民の情報共有と連携強化により、迅速かつ効果的な対策を講じること。２つ目は「通信情報の利用」で、攻撃サーバー等の検知のために通信情報を国と共有し分析を進めること。３つ目は、この分析結果を踏まえ、警察等が攻撃サーバー等に対して「アクセス・無害化措置」を講じることである。

一方、政府においては、今後５年程度を想定した新たなサイバーセキュリティ戦略の策定を進めており、2025年内の閣議決定を目指している*注。この新戦略は、近年の国際情勢の変化を背景としたサイバー脅威の増大を踏まえた「深刻化する脅威に対する防御・抑止」、社会全体のデジタル化の進展によるサイバー脅威の増大を踏まえた「社会全体のセキュリティ及びレジリエンスの向上」、AIや量子技術といった技術革新を踏まえた「サイバーセキュリティの人材・技術のエコシステム形成」という３つの柱で構成されている。また、この戦略の特徴として、官民連携において国がサイバー防御と抑止の要となること、さらに中小企業やベンダーを含むサプライチェーン全体の対策強化に言及していることなどが挙げられる。政府は事業者向けに行動計画とガイドラインを示しているところであるが、取り組みの底上げを図るため、重要インフラ事業者が取り組むべき事項について統一基準を示すことも検討している。さらに、実践に近い形での訓練・演習も行っており、2025年11月には内閣官房主催で全分野を対象とした統一訓練が実施され、12月には内閣官房と東京都の共催で首都圏における大規模インフラ障害をテーマとした机上訓練が行われる。

こうした政府全体の動きと並行して、国土交通省でもさまざまな取り組みを進めている。主な取り組みは以下のとおりである。

１）行動計画に基づく分野別の安全ガイドラインに加え、重要インフラ以外の事業者や中小事業者向けの情報セキュリティ対策のチェックリストを公表している。

２）サイバーセキュリティ対策を事業法体系に明確に位置付けるため、省令改正の作業を進めている。鉄道分野では安全管理規程にサイバーセキュリティの確保を盛り込むべく、鉄道局を中心に具体的な検討が進められている。

３）事業者支援として、ASM（アタックサーフェスマネジメント）を導入している。これはインターネットからアクセス可能なIT資産を外部から調査し、攻撃リスクを評価する取り組みである。

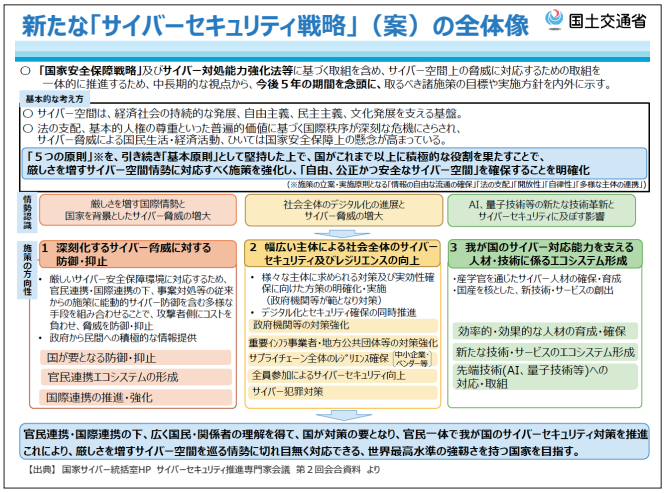
４）2025年度からSNSのモニタリングを開始している。SNS上の書き込み情報を収集し、サイバー攻撃の予兆と見られる情報があれば注意喚起を行うもので、今後さらに充実させたいと考えている。

５）事案が発生した際、サイバーセキュリティの知見を有する職員を派遣する制度も2025年度から開始した。第三者の立場から助言等を行い、セカンドオピニオンとしての役割も果たせると考えている。

６）情報共有が重要となることから交通ISACとの連携も引き続き強化していきたい。事業者ネットワーク拡大、人材育成等で協力していきたいと考えている。

７）インフラサービスの安定な提供がサイバー攻撃等によって妨げられることのないよう経済安全保障推進法に基づく事前審査も継続して実施している。

交通サービスは、国民生活や経済活動に不可欠なものとなっていることから、国土交通省としては、政府の一員として関係省庁と緊密に連携しつつ、事業者と着実にコミュニケーションを重ねながら、サイバーセキュリティ対策の強化を引き続き進めていきたい。



長井総括審議官の講演資料

■講演②

JR東日本グループにおけるセキュリティ戦略と新たな取り組み

関口 義弘　株式会社JR東日本情報システム セキュリティ対策室次長

JR東日本グループのサイバーセキュリティ対策について、これまでの概要と変遷、現在取り組んでいる施策をご紹介する。

2009年に発生したJR東日本のホームページ改ざん事案により、グループ全体のサイバーセキュリティ対策を見直すこととなった。セキュリティ対策を見直すにあたり、まず全てのグループ会社を訪問し、各社のシステムとセキュリティ対策の実態を確認した。その上で、技術的な支援やセキュリティ教育、サイバーインシデントへの対策の強化を行ってきた。近年では安全なクラウドサービスを選ぶための与信調査や、グループ会社に対する内部統制の高度化に取り組んでいる。

JR東日本グループのセキュリティ政策を、対象（OA環境、業務サーバー）と手法（技術的対策、組織的対策）の２つの軸で整理して、６つの取り組みをプロットした。それぞれの取り組みについ

＊注　2025年12月23日閣議決定

て、第１象限から第４象限まで、順番に説明する。

1）イントラ環境の技術的な対策

グループ会社に対し、JR東日本エンドポイントセキュリティサービス（JRE-ESS）を展開している。グループ会社の全約7万3,000台のOA端末のログを24時間365日体制で監視している。こうした対策の結果、2024年度のウイルス感染はゼロ件であった。2025年度内に海外のグループ会社への対策を完了させる予定である。

2）ハイブリッド型のSOC(Security Operation Center)

JR東日本グループでは外部SOCと内部SOCの両輪によるハイブリッド型のSOCでセキュリティ監視を行っている。外部SOCでは、セキュリティ専門のベンダーによるマネージドセキュリティサービスを活用し、攻撃者の痕跡や不審なIPアドレス・ドメインへのアクセスの有無を監視・分析している。内部SOCでは、JRE-ESSのログを用いて、インシデント発生時の被害範囲の調査や内部不正などの対応を行っている。このように、外部の専門的な知見と社内技術者を組み合わせた監視体制を構築している。

3）次世代のセキュリティ基盤

従来のオンプレミス（自社運用）型システムをパブリッククラウドへ本格的に移行することを見据え、クラウド特有のリスクに対応するために、次世代セキュリティ基盤の構築を進めている。また、マルチクラウドへの対応にあたり、設計・構築・試験といった全てのフェーズをカバーできるセキュリティ基盤を整えることで、グループ全体のガバナンスの向上を図っていく。次世代のセキュリティ基盤の構築にあたっては、ルールどおりに運用されているかを自動的に監査し、逸脱がある場合には是正を促す機能を備えることを目指していきたい。

4）制御系のセキュリティ対策

列車の運行管理や電力の制御はOT（Operational Technology）で運用している。これらのシステムは、国土交通省の安全ガイドラインに基づいて構築しており、外部の専門家によるアセスメントを毎年実施している。

5）セキュリティ教育・訓練

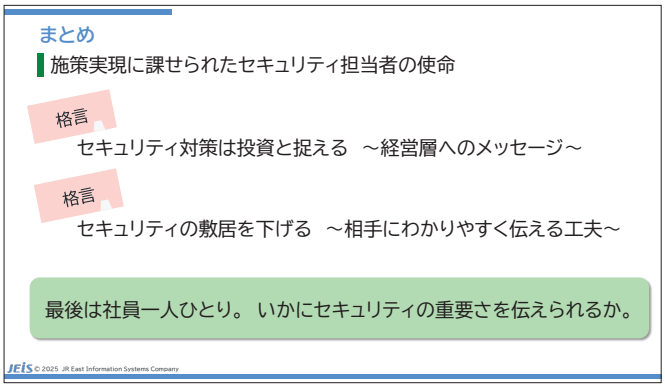
JR東日本では危機管理部門や広報部門などを含めたCSIRT（Computer Security Incident Response Team）訓練を毎年実施している。グループ会社に対しても各社の業務実態に合わせてカスタマイズしたシナリオをベースに、CSIRT訓練を毎年実施している。

6）情報セキュリティ10か条

全社員が遵守すべきセキュリティルールを10か条にまとめ、アニメーションや動画を織り交ぜたルールブックを作成している。グループが一体となってこの10か条を遵守することで多くの事案を防ぐことができるので、その重要性は非常に高い。

その他、直近ではグループ会社に対する注意喚起を行い、サイバー攻撃による事業停止や情報漏えいは経営責任であることを明確にし、グループ会社の社長が一堂に会する社長会で注意喚起を行っている。

最後に、「セキュリティ対策は投資である」という経営層へのメッセージについて触れたい。セキュリティ対策が直接的に収益に結びつくケースは稀であるが、経営層がセキュリティ対策へ積極的に投資する姿勢を示すことは、現場のシステム担当者にとって大きな後押しとなる。また、システム分野は専門用語や仕組みが分かりにくいため、経営層に理解をしてもらうには工夫が求められる。分かりやすい説明を心がけ、「セキュリティの敷居を下げる」ことが重要となる。社員一人ひとりがセキュリティの最後の砦となるため、サイバーセキュリティの重要性について、今後もしっかり伝えていきたい。



関口次長の講演資料

■講演③

安定輸送を脅かす最新のサイバー脅威と事業継続のための要諦

名和 利男　サイバーセキュリティアドバイザー

サイバー攻撃が安定輸送に影響を及ぼすことが広く認識されている一方で、その仕組みや対処は現場の経験と知識に依存する傾向が強くなっており、講じた対策が成功しない例も少なくない。

攻撃グループは鉄道事業者そのものではなく、その先にあるクリティカルな対象に危害を及ぼす目的で、鉄道事業者のサービス停止を手段として利用する。安定輸送を揺るがした事案としては、デンマーク国鉄（DSB）の事例がある。これは保守会社がランサム攻撃を受けたことにより、デンマーク全土で列車の運行が停止した。委託先やサプライヤーへの攻撃が、サプライチェーンを通じて国全体の輸送に波及することを示す事例である。

攻撃者の思考は、費用対効果の最大化となっており、企業の経営者の意思決定に近い。少ないコストで、いかに大きな影響を与えられるかを常に計算している。攻撃者が重視することは、輸送停止の損失とニュース性、復旧に要する時間と代替輸送手段の有無、セキュリティの脆弱性（レガシーシステムでの運用、多重委託、権限管理の不備）となっている。最近はセキュリティ対策が脆弱な委託先を踏み台にして、大企業へ侵入するケースが多くなっている。また、事案発生後の情報開示が「ランサムウェアによる攻撃を受けた」という最低限の内容にとどまるケースが多く、攻撃を受けるまでの経路が共有されづらいことも課題となっている。特に諸外国では株価への影響を避けるために必要最小限の情報しか公表しない企業も多く、その結果として、サイバー攻撃に関する有益な教訓が十分共有されず、横展開されにくい状況になっている。

鉄道事業者への攻撃パターンは、主として①運行・業務ITを停止させる攻撃、②制御を行うOTシステムに侵入する攻撃、③サプライチェーン／ベンダーを経由する攻撃、④データ侵害による信頼失墜型攻撃の４つのパターンがある。特に④は、攻撃を仕掛けた側ではなく、被害を受けた交通事業者が責め立てられることになる。海外でもこうした事案が時々発生しており、日本でも起こり得るリスクである。攻撃者の狙いは、国際情勢の変化に応じて常に変化するため、その動向を継続的に注視することが重要である。こうした脅威の多様化と攻撃手法の変化を踏まえると、サイバー攻撃によるリスクを具体的に把握すること（どのシステムが停止すると、輸送にどの程度影響が生じるのか等）が不可欠であり、その上で運行に携わる経営層、運行・現場、IT/OT/CSIRTのそれぞれが議論できるよう、ある程度の粗さで構わないので可視化することが重要となる。

サイバー事案は技術部門だけでは完結しないため、経営層、運行・現場、IT/OT/CSIRT、それぞれの視点で、役割を認識することが必要となる。経営層、運行・現場、IT/OT/CSIRTの各部門の、初動24時間の各フェーズでの役割分担を示すRACIマトリクス（Responsible／Accountable／Consulted／Informed）を示した。例えば、「異常検知・一時解析」フェーズでは、CSIRTは実務上の責任“R”と最終決定責任者“A”の役割を担い、経営層は情報を受ける“I”の立場としてプロセスとフローを確認する。この役割分担が最も迅速で、当局への説明にも十分に対応できる。

こうした手順で机上演習を行うと、うまく進まない箇所が、しばしば攻撃の入口や復旧に最も時間を要する部分であることが明らかになる。このように難解なテクニカルイシューをわかりやすいプロセスへ落とし込むことで、「何をすべきか」、「何に投資すべきか」が具体的かつ明確になる。机上演習で得られた気づきはBCP（事業継続計画）に必ず反映し、課題を明文化したうえ、誰が、いつまでに、何を行うのかを決めなければ、単なる年１回のイベントに終わってしまう。

経営・ガバナンスの最初の一歩は、経営層が「サイバー攻撃は安全な輸送を揺るがす問題である」ことを全社、特に他の役員、外部執行役員、パートナーへ明確に伝えることである。これによりミドルマネジメント層がこれに準じた行動を取りやすくなる。また、「現場・技術・サプライチェーンのアクション」として、インシデント初動カードを作成し、簡潔なチェックリストとして共有していただきたい。このカードを紙で印刷しておけば、ファイル共有システムがランサム攻撃を受けて、メールが使用できない状況でも参照することが可能である。できれば役員や職員の引き出しの一番上にラミネート加工したものを置いておくと、緊急時に役立つ。

【表】初動24時間の RACI マトリクス

フェーズ / 行為	経営層	運行・現場部門	IT/OT部門	CSIRT・SOC
異常検知・一次解析	I (報告を受ける)	I	C (技術支援)	R/A
運行・安全への影響評価	C	R/A	C	C
初報(暫定評価)の経営層への共有	I	C	C	R
システム停止/減便/運休の意思決定	A	C	C	I
外部機関(国交省・警察 等)への連絡方針	A	C	C	C
技術的封じ込め・原因究明	I	I	C	R/A
再開条件の整理と合意	A	R/C	C	C

R：実務上の実行責任（Responsible）
A：最終決定責任（Accountable）
C：助言・協議（Consulted）
I：情報提供（Informed）

TLP:CLEAR

名和アドバイザーの講演資料

■パネルディスカッション

◇総括

後藤 厚宏　情報セキュリティ大学院大学 教授

政府の新しいサイバーセキュリティ戦略は、現在仕上げの段階にある。実行に移して成果を上げることは重要だが、取り組むべき事項が増えることで現場に過度な負担を与えないよう、優先順位の高い施策に絞り込むことが求められるのではないか。また、次のロードマップを策定し、それを柔軟に見直していく姿勢も重要である。新しいサイバーセキュリティ戦略では、全員参加によるサイバーセキュリティ向上が重要な方向性の一つとして掲げられており、海外を含むJR東日本グループ全体でのセキュリティ向上に関する取り組みに大きな期待を持っている。

ITはOTの効率性向上に寄与する一方、攻撃者の入口にもなり得る。社会全体がデジタルでつながる時代において、何をどう守るかを考えることが大きな課題となる。さらに、最悪のケースを想定することの重要性、その一方でその想定がいかに難しいかという点が心に残った。経営層の方々には、自社にとって、「最悪のケースとは何か」を改めて考えていただきたい。

◇テーマ1　OTとITの融合、利用者サービス高度化とセキュリティの両立

（後藤教授）OTとITが融合する中で、サービスの高度化・効率化とセキュリティの確保を両立できるのだろうか。

（長井審議官）サイバー基本法では、デジタル社会の推進とセキュリティ確保は表裏一体のものとして位置づけられている。これらを切り離して考えることは、結果として攻撃者を利するのではないか。OTがインターネットから切り離されてるから問題ないという従来の発想は通用しない。OTを更新する際、あらかじめセキュリティの概念を組み込むことが不可欠である。

（関口次長）外部からOT側には入り込めないようにするデータダイオードを用いることで、OTの安全性を高めている。そもそもOTとITはシステム更新のサイクルが大きく異なるため、簡単に融合させることは難しい。このため、セキュリティ人材を含む双方の専門家の人材交流を通じて、知識レベルの向上や対策の高度化を図っていくことが重要となる。

（名和アドバイザー）OTとITが融合するとIT側からOT領域への侵入可能性が高まり、結果として脅威も増大する。攻撃に変化に応じて防御方法を動的に調整するアダプティブディフェンスの訓練を実施すれば、サービスの高度化・効率化とセキュリティの確保の両立が可能であることは、さまざまな研究論文に示されている。

◇テーマ2　人材不足と外注依存のリスクと対策

（後藤教授）高齢化が進む中で、セキュリティに関わる人材の育成と確保について、経営層や人材育成を担う人事部がその重要性を十分に理解してもらえるかという課題がある。また、社内の人材だけでなく外注先の管理についても重要となる。

（長井審議官）巧妙化するサイバー攻撃に対応できる人材の確保と育成が急務である。事業者や各部署においてDX化が進められているので、それに合わせたサイバーセキュリティ教育が必要となる。外部と協力する場合は専門家へ丸投げするのではなく、双方で必要な対策や役割分担を明確にすることが重要となる。

（後藤教授）NISC（内閣サイバーセキュリティセンター、現・国家サイバー統括室（NCO））では、事業者にはセキュリティの専門家と円滑なコミュニケーションが取れる知識やスキルを持つ人材が必要であるという議論があった。幹部の人にセキュリティの重要性を理解してもらうためには、どのような方法があるか。

（関口次長）経営層が急にセキュリティの専門家になることは難しい。セキュリティ担当者は上層部にわかりやすく伝えることが重要となる。経営会議において、月に１回10分程度時間をつくり、経営層に向けて最新動向やリスクのアップデートを行うことも有効な手段の一つとなる。

（名和アドバイザー）人材不足を解消するためには、業務効率化に加え、インシデント対応の自動化支援ツール、AIの活用など、人が介在しない仕組みの導入が不可欠となる。経営層への説明の際、経営層が慣れている数字を使う方法がある。インシデント対応の分野で使われるTime to D（Detect、検知までの時間）、Time to C（Conclude、封じ込めまでの時間）、Time to R（Recover、復旧までの時間）である。これらの時間を継続的に計測・比較することで、投資によって時間が短縮したのか、投資を怠ったことで長くなったか可視化される。アクシデント発生時に、「事業がどれだけ止まるか」経営層の言葉で考えてもらう契機となる。これに関連する論文もあるので確認していただきたい。

（後藤教授）自動化を担当できる人材にはどのようなスキルが求められるのか。

（名和アドバイザー）国家警察、軍、コーストガード等の出身者は素晴らしい訓練を受けている。彼らは軍歴12、13年程度で民間へ出て即戦力になっている。専門的な訓練を長期間受けた実績のある方をアドバイザー等で採用できると良いのではないか。

（関口次長）そのような人材へのアプローチ方法は難しいが、セキュリティや重要インフラ、国家を守るような気概を持った学生や若手社員も増えている。加えて経験も必要となるので人材育成も重要である。

◇テーマ3　レジリエンスの確保

（後藤教授）サイバーセキュリティの環境は変化していくので、復旧だけではなくその先を見越して対応できることが理想形である。その観点で求められるレジリエンスの確保にどう取り組めばよいか。

（長井審議官）セキュリティ対策とレジリエンスは表裏一体だと思う。基本的な対策、ネットワーク環境の把握など、日頃の積み重ねが結果としてレジリエンスの確保にも繋がるのではないか。

（関口次長）複雑化したルールは順守だけでなく、その運用が適切になされているかの評価も難しくなる。パブリッククラウドの活用を視野に入れつつ、セキュリティを担保した基盤の上にアプリケーションを展開できれば、サプライチェーン全体で一定の程度のセキュリティが確保できるのではないか。交通ISACや金融ISACに加盟することで、鉄道分野以外の事例やアドバイスをもらえる点が大きい。

（名和アドバイザー）「防災から減災へ」という考え方である。物理空間ではすでに取り組みが進んでおり、同様の発想をサイバー空間にも適用できる。また、一人ひとりが自律的な判断と行動を取ることが不可欠となることから、平時から権限と役割を与えて準備しておく必要がある。さらに、コミュニティや絆である。過去の教訓を忘れずに共有し続けることが重要となる。

◇質疑応答

（質問者）経済安全保障推進法でのアクセス資格について、どの範囲の人材を教育の対象にするのか。企業はクリーンルームの設置等にどの程度負担を求められるのか。

（長井審議官）必要なクリアランス等を取得した人材が、必要な情報を扱うことになっている。経済安全保障推進法の見直しが進められていることからその中で議論がされていくと考えている。

（質問者）地震や停電に対するBCPと、サイバー攻撃に対するBCPに違いがあるのか。

（関口次長）BCPの基本的な考え方は共通している。ただし、サイバー攻撃への対応については、データを安全に復旧する方法や安全なバックアップが重要となる。

本開催概要は主催者の責任でまとめています。

会場の様子

当日の講演資料等は運輸総合研究所のWEBページでご覧いただけます。
https://www.jttri.or.jp/events/2025/semi251210.html