第１回　鉄道事業者の重要システムにおける情報セキュリティ対策等検討委員会

議事概要

日　時：令和７年７月 23 日（水）15:00 ～ 17:00
場　所：中央合同庁舎第３号館 ６階 鉄道局大会議室、Teams によるオンライン会議

１．開会

２．挨拶
五十嵐鉄道局長より挨拶。

３．議事
議事（１）本検討委員会の運営について
資料１「鉄道事業者の情報セキュリティ対策等検討委員会　設置要領」に基づき、事務局より説明。
委員の互選により、古関委員を座長として選出。

議事（２）鉄道分野における情報セキュリティ対策
資料２「鉄道事業者の情報セキュリティ対策」に基づき、事務局より説明。

【主な質疑・議論】
- この会議の具体的なアウトプットとしては、事業者への実効的な支援に関する情報提供も含めた全般を見つつ、特に法的な規制が必要な輸送安全に関わる安全管理規程について、より詳しい内容を定めたい。
- サプライチェーンのサイバー攻撃リスクについて広く考えていただきたい。ハードウェアだけでなく、今やソフトウェアのサプライチェーンの課題が大きくなっている。鉄道事業の停止が産業全体のサプライチェーン寸断という大きな被害に繋がるリスクがある。
- サイバー攻撃を受けるものとして覚悟した上で、どう復旧するか、いかに復旧を早めるかという観点が必要である。サイバー攻撃からの復旧には、時には対象システムを構築し直すくらいの覚悟が必要とも言われており、鉄道インフラのビジネス・レジリエンスのために、既に取り組んでいる自然災害対策とは異なる観点の対策があるべきである。
- 重要インフラの相互依存関係を分析し、それに沿った対処策、復旧の迅速化、被害拡大の防止を検討する取組が必要である。これは、社会全体のレジリエンスに繋がるものであり、他の重要インフラや政府・自治体と連携し、全体最適となる策を検討いただけるとよい。
- 言うまでもないが、トップマネジメントは重要。
- 安全管理規程については、ぜひ自然災害と同じレベルでサイバー攻撃事案を扱っていただきたい。加えて、重要インフラは相互連鎖して停止するため、復旧の観点では、他の重要インフラとの相互協力を促進する観点からも検討いただきたい。対象システムについては、自動運転に係るシステムについても検討をお願いしたい。また、鉄道サービス単独ではなく、社会全体の復旧を早めるための施策について、事前の準備や、他の重要インフラや自治体との調整という観点でのガイドライン等をぜひ考えていただきたい。
- 先般発生した他分野の事案は、システムによる効率化が進んだ時点で発生した。機械本体も労働者も無事なまま、IT の停止によりオペレーションが不可となった。バックアップがあり早期に復旧できたが、数か月規模の影響が起きてもおかしくない事案であった。
- こうした先行事例を踏まえれば、鉄道に関しては、IT 導入・自動化の拡大に伴い、どのような影

響が起こるのか把握し対処する必要性がある。安全運行を妨げるまではいかなくとも、安定運行を妨げる問題が長期にわたり発生する可能性もある。また、IT 停止という点では、ともするとサイバー攻撃の影響は過小評価されている。数日で解消するようなシステム障害とは異なり、サイバー攻撃では数か月にわたり止まる想定が必要だろう。

- また、IT 導入・自動化の拡大による影響度を最新の情報で考慮する必要がある。今や閉域網のままではいられない状況にあるが、要員に知見があるか。インターネットの世界とのギャップが非常に大きくなっている中、この難しさや厳しさを理解し、対応しなければならない。
- 経営層におかれては、サイバー攻撃のリスクが高まっているので、危機管理の対象として、自然災害やその他の災害と同列のことが起こりうるものとして、向き合っていただきたい。
- サプライチェーン攻撃が爆発的に増加している中、国内輸送網へのランサムウェア事例が発生しているものの、報道されていないものもあり、情報が共有されないことが課題である。これを解決するため、能動的サイバー防御に関する強制的なインシデント報告に大いに期待している。先月から特定の国や地域において、鉄道を含む OT 領域への攻撃が急激に増えており、サイバー対処能力強化法やセキュリティクリアランス制度を受けた必要な事項について検討する必要がある。日本より先に制度等を提起、実装した国は、民間企業に対して検知・通報・防御アクションを秒単位で求めており、中央に情報を集めるという強いモチベーションと強制力が働いている。このような制度が日本でも来年 11 月下旬までに施行となるため、官民で対応を進めている。
- サプライチェーン攻撃は激増しており、将来的な破壊攻撃を埋め込むこともある。某国で、通信会社以外に給電システムや給水システムに入っていたことが後でわかった。コスト面を理由としてセキュリティ対策が実施されていなかったと想定される。
- 金融分野においては、近年オペレーショナル・レジリエンスの考え方が一気に入ってきている。これは、大規模システム障害やサイバー攻撃被害といった深刻な事態が発生しても、組織が提供する重要なサービスを継続して、顧客・市場への影響を最小限に抑えるための能力である。日本においては、何をすべきかが判断者の状況次第とされていることが多いため、トップの意思決定を早く行うことが求められている。
- 対象システムについて、輸送安全への影響が大きい分野を追加することは自然ではないか。リスク分析で重要になるのは、機能として失ってはならない必須サービスを決めることであり、基本的にはセーフティ、すなわち安全性に関するものが含まれると理解している。OT セキュリティの脅威に関する環境変化を考えると、こうしたものを含めることが妥当であろう。それ以外について一律というのは非常に難しく、将来的には、現在は先進的とされている分野のもの等、各社でリスク分析の際に考慮するシステムが出てくると考えており、中長期的には対象も変わりうると認識している。
- 安全ガイドラインの改訂を考えると、対象によっては現行の基準とのギャップが少し増えるのではないか。安全基準等対策指針や他分野との整合を考えながら更新するのは難しいだろうが、鉄道分野の国際標準との紐付けや参照をお願いしたい。
- 教育を担当する方への支援も必要になると感じる。事業者の負担感等も確認いただき、必要であれば何か支援策をご検討いただきたい。
- 国際標準では「許容できないリスクがない」ということが安全とされているので、単に事故が起きないというだけではなく、安定した鉄道サービスが供給されることも含めた上で考えなければならない。鉄道側の不調によって都市機能として行政やビジネスもストップすることも避けなければならないリスクと考えれば、サービス安定も念頭に置いた対策が必要である。輸送安全に直結するシステムのみならず、サービス安定に大きな影響を与える旅客管理や情報連携のためのシステムも、混乱を起こそうとするアクター側から見ればターゲットになる。事業者側のモチベーションを考えると、輸送安全とサービス安定の両方をスコープに入れるべきではないか。
- 企業側はともするとサイバーセキュリティを誰かが守ってくれるものと捉えかねないので、自らが能動的な対応、行動を取ることを求められるということを入れていただきたい。

- 国交省に期待することとして、事業者間の連携、官民連携がある。サイバー攻撃に対しては、一事業者あるいは場合によっては一業界では対応しきれない。ぜひ事業者間における情報共有の仕組みをより早く作っていただくとともに、国交省としても他モードも含めて共有するようにするべきである。また、国交省を含めた官側からの情報共有にも期待したい。今回のサイバー対処能力強化法でも、様々なインシデント報告が義務的に国になされるので、いかに事業者側に提供するか、国家サイバー統括室と連携の上考えていただきたい。
- 金融庁は、金融機関に対するサイバーセキュリティのガイドラインにおいて、リスクマネジメントは経営者の判断、責任であるということを明確に示し、対応を求めている。一方、鉄道事業者では、鉄道の安全運行については経営者層も相当の専門知識を持っていると思うが、サイバーセキュリティについてはそうとは限らないと想像する。専門知識を高めていただくことも必要であるが、専門知識を有する専門家とのコミュニケーションや、サイバーセキュリティに関する外部委託者との連携という観点も、ぜひ運輸安全マネジメント評価の中に入れていただきたい。その意味でも、経営者に対しては、専門性を持った担当幹部とは切り分けて、知識を問うのではなくリーダーシップや情報発信といったスキルを確認するものとしていただきたい。
- 最近の技術として、携帯電話のための一般公衆無線を運行管理等に使う研究がなされている。これにより、脆弱性が増す可能性があ。その技術を、本会議で将来課題としてスコープに入れるのか、現在の課題に集中するのか考えなければならない。
- サイバー攻撃ではなくても、旅客に対する案内において、嘘の情報を持ち込まれたり、危険を誘導するようなフェイク情報を流されることは致命的であり、人命に関わったり、さらに社会の混乱を招く可能性もある。旅客に対してどういう情報を与えるかも重要ではないか。
- 鉄道システムは安全確保を第一に考えて作られてきた歴史がある。鉄道のサイバーセキュリティ規格も、安全確保と安定したサービス継続が非常に重要という認識の下で整備が進められている。安全確保に関しては、既に基本となる考え方や技術があり、規格等も整備されているので、ゼロから議論する必要はないと考える。それらを参照しつつ、いかに安全を堅持しながら安定してサービスを提供するかという観点で議論いただくとよいのではないか。
- 鉄道サービスを維持するために、いかに人材を確保し育てていくかも大きな課題。できるだけ設備を減らして人手のかからない軽いシステムにしていく流れにある方向にある中でサイバーセキュリティを確保していくための制度はどうあるべきか、検討いただけるとありがたい。
- 公衆通信回線の活用については、今後さらに拡大することが見込まれるため、使った場合のセキュリティも含めて考える方がよい。汎用品や汎用ソフトウェアを組み込むことも広がっているので、サプライチェーンの問題もある中、汎用品の活用という観点でも取り組んだ方がよいのではないか。

４．閉会