第２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：2025 年 10 月 20 日（月）10:30 ～ 12:30
場　所：Teams によるオンライン会議
議　事：
１．開会

２．議事
議事（１）鉄道分野における情報セキュリティ対策
資料１「鉄道事業者の情報セキュリティ対策」に基づき、事務局より説明が行われた。

【主な議論】
- ヒアリング結果に関する対応の考え方についてはいずれも非常に重要なものと考える。情報共有の場もそうであるし、社内体制についてもトップダウンの仕組みを作ることが重要である。
- 人材の採用・育成は重要であるが、人材採用は全ての業界において苦戦している。鉄道の皆様には社内人材の育成に力を入れていただきたい。国土交通省として、社員教育の支援は非常に重要であると考える。経営層の教育、管理職の教育については、IT に関する専門家を供給するのではなく、鉄道の専門家の方にプラスでサイバーセキュリティを理解いただく取組が必要である。また、全社員に向けての啓蒙活動もしっかりと取り組んでいただきたい。
- 重要インフラ間の相互依存性について、広い意味で物流・人流という観点では、鉄道の他、陸運・海運・空運がある。日本全体の物流・人流を支えることが必要であり、重要インフラが共通で依存している電力や通信との関係を見極めていただきたい。
- サービス安定の観点から監査対象とはしないが重要であるというサービスに対してガイドラインを通じて啓蒙していくことは重要である。
- 安全管理規程について、役員の責務として明記されていることが重要である。組織作り、組織全体の文化の考え方、文化を作る点でも重要である。サイバーセキュリティ責任者の責務も重要であり、今回、安全管理規程に関する改訂に関しては、期待できる内容であるという認識である。
- 今後チェックリストを作るという点に関しても、経営層の観点からのレジリエンス、つまり現場社員だけではなく、組織全体から見たチェックリストを目指しているように見受けられる。この点を高く評価したい。このチェックリストが形骸化しないような工夫についても、今後一緒に議論できるとよい。
- 縮退運転はレジリエンスの観点からも非常に大事なキーワードだと考える。本当にサイバー攻撃が深いところまで入ってしまうと、現システムは全て捨てて、新たにハードウェア、ソフトウェアを再構築せざるを得ないこともあり得る。その際に、どのような手順で可能なのか、開発担当の事業者とはどのような連携が可能なのか、経営者は見直すべきであろう。
- 強調したい点はサービス安定である。サービス安定については、IT の利活用、DX が拡大している状況を認識すべきである。事業者によって状況は異なるが、大手の事業者を中心に利活用は相当に進んでいる。特に人口密集地においては相当の混乱が起きることを認識すべきである。OT 領域はこれまでしっかり対策がなされていると思うが、IT 領域においては昨今ゼロデイ攻撃が増加している。メーカーが認識していない脆弱性を、攻撃者が先に見つけ出して悪用することも想定すべきである。最近は、国家を背景とする攻撃者だけではなく、ランサムウェアの攻撃グループもゼロデイ攻撃を行なっている。鉄道事業者が想定するのは当然、国家を背景とする攻撃者ではあるが、ランサムウェア攻撃による影響も相当甚大なものがある。ゼロデイ攻撃が一般化している

状況を踏まえると、防御だけではなく検知・対処が重要となってくるであろう。

- 重要なシステムが他の IT システムと同じネットワークに存在する場合、重要なシステム単独だけを見ていてはいけない。ネットワーク全体が攻撃で影響を受ける場合があるため、ネットワーク全体を見てリスク評価やセキュリティ対策を検討していく必要がある。重要システムが攻撃を受けていなくとも、ネットワークが稼働しないと重要システムも機能しない。重要システムは、十分な対策を行っているから大丈夫ということではなく、ネットワークを含めリスク評価やセキュリティ対策を進めていく必要があることを事業者の方は意識する必要がある。
- サイバー攻撃で破壊されないバックアップ方式とすることは言うまでもないが、バックアップから復旧ができるような手順の整備、テストの実施、それから、ネットワーク全体が影響を受けた際、必要な部分だけ復旧させるような回復プランの整備等が必要である。それを考える人材も非常に重要である。ベンダ任せではなく、人材を集めることが必要である。
- サイバー攻撃においては、2021 年 10 月に医療機関において大きな影響があった件があり、この際も医師は無事で医療業務は可能であるが、電子カルテへの影響により通常の医療業務が継続できなくなった。その翌年の 2022 年の 2 月、製造業の事案があり、工場は稼働しているものの受発注システムに影響があったため通常の生産ができなくなった。その後、2023 年 1 月の港湾での事案があり、幸いにも 3 日で復旧したが、港の施設や機器は無事であるがシステムが影響を受けたことで業務が停止した。もう数年前からこの種の事案が発生しているが、最近も類似の事案が起きており、この点についてどうすれば理解が進むのかは悩ましい点である。事案が全く起きないということは難しいが、ここまで被害が大きくなることに対して、どういう情報発信の取組をすれば事業者に届くのか等、深刻さがなかなか届かない前提の下、努力していかなければならない。
- チェックリストは様々なインフラ分野で使われているが、形骸化しているところもいくつか見受けられる。社外との関係については、チェックリストは何のためにあるのかの一文がないと、発注者としては終わってしまう、あるいは逆に下請法にも引っかかるような過度な要求をしがちになってしまう懸念がある。チェックリストは単なる道具であり、契約条項に書き込む必要があるのではないか。また、規程を定めた後の運用としては、実際の記録で確かめること、普段から確認し続けることの三段構えが必要である。これは、グローバルでよく見られるチェックリストの使い方であるが、日本では部分的な点のみ注目されている印象がある。人命を預かるような鉄道分野においては、書類としてのチェックだけではなく、運用としてのチェックリストを作り、委託事業者と密な対話をしていくことが重要である。これは、経済産業省が作成したサプライチェーン全体における運用指針にも明確に記載しているので遵守することを推奨したい。
- チェックリストのサプライチェーンの委託先管理であるが、2 つの重要な指標がある。1 つ目は委託先から提供されるソフトウェアの一覧と、それがサイバー攻撃の発生時どのように影響を与えるかを記述し、発注者と委託先で合意形成し基準として持つことが重要である。2 つ目は、遠隔作業のルールを厳格にする点である。緊急時やリソースの関係で遠隔作業のルールを逸脱することがある。これをギャップと言うが、このギャップが月単位でどれだけ発生したのか、何パーセントか等を指標で測る。これを週次、月次で経営陣が見る。これがチェックリストの使い方として記録で確認するというものである。
- ここ数年の状況を見ると、一番の目的は運行を止めないことで、どのようなシステムが止まると運行を止めてしまうのか把握すべきである。OT だけではなく IT も影響がある。お客様が直接関わるサービスは様々なシステムと IT 連携されており、時刻補正も重要になっている。新しい DX が進展している部分も重要性が増している。安全管理規程には配慮した形で読み解けるようにした方がよい。
- 規程について、読めば運用を再現できるよう、言葉を選ぶことがよい。「必要」という言葉が頻繁に出てくるが、事業者の立場で読むと、何をもって必要というのが国土交通省や他のガイドラインを見ても書かれていない。事案が発生するとよく責任問題となる。
- 現場の方々がどこに困っているか聴取することで、運用と乖離している点を見出し、「必要」とい

う言葉を少し具体化する方針を持っていただくことが重要である。

- 重要なのはログ、証跡である。フォレンジックを行うと、規定がないから残していないということが結構ある。社内で予算を調達する担当や上層部の意思決定において、本当にログが必要なのかの規定がないので、必要という基準を自ら作って自ら判断し行っていくことになりかねず、望ましくない方向に向かう懸念もある。そのため、ログの必要性を訴えることがよいのではないか。
- 鉄道の安全文化の中にサイバーセキュリティを浸透させていくには時間がかかるかもしれない。サイバーセキュリティ担当者は、鉄道部門ではないことが多いと考えられる。情報連携はできているようで杞憂かもしれないが、実際に制度を進めようとすると、別の部門と連動することが容易ではないことも想定されるので、それを念頭に仕組みを考える必要がある。
- 事業の実施管理の方法にリスク分析を行うという記載がある。このリスク分析は事業者ごとに行えることが本質的だが、実効性のあるものにするには、鉄道部門のシステム担当者においてもシステムライフサイクルの各フェーズでサイバーセキュリティを意識していただく必要がある。本日の資料にも情報共有をこれから行っていくという記載があり期待しているが、先行する事業者のベストプラクティス、例えばシステム発注の際に委託先に対して仕様書のセキュリティ要件の記載や、インシデントレスポンスのルールや訓練等が共有できるとよい。事業者間で情報共有の場に作って説明することは大変であるため、このようなきっかけが重要と考える。そして、各事業者においてもジョブローテーションがあると思うが、長期的には組織的に複数の方が適切なリスク分析ができるよう、制度の運用において支援できるとよい。
- チェックリストについては、何をやるべきか明確にすると事業者の方々の不安が払拭できるのではないか。形骸化しないようにするには難しいが、チェックリストの解釈に関する意見交換等、情報共有のきっかけも必要であろう。
- 適切な情報共有の範囲を検討する必要はある。現行で情報共有されているケースもあるようだが、鉄道分野の文化として根付かせていくために、情報共有のリスクも踏まえ、管理面も含めて進めていかなければならない。情報がないことで、何をやるのかわからず時間やお金を浪費してしまうことは懸念される。それを払拭できるものがあれば、情報共有に限ることではないが、思い悩む事業者ができるだけ少なくなるような仕掛けが必要と考える。
- 情報共有については、鉄道分野だけではなく、各事業分野でいかに進めていくかが、サイバーインテリジェンス、サイバーセキュリティの関係で課題になっている。鉄道事業者内でやるべきもの、他の交通事業者の方々とやるべきこと、重要インフラとしてNCOでやるべきこと等、多層的な情報共有が必要と考える。それぞれのコミュニティで意味のある情報共有をするには、情報がその外部に漏れるリスクをなくしていく努力も非常に重要である。例えば、各参加企業と秘密保持契約を行った上で、それぞれの情報についてどのような取り扱いをするのかやTLPを定めるなどして情報共有を行うことが必要で、場合によっては、どこからの情報かは伝えず匿名化をして情報共有を行うことも一つの手段である。
- サイバー攻撃については、セキュリティソリューションを使っての検知や阻止も可能と考えられがちであるが、現実には正規のアクセスを装った侵入や、新たな脆弱性に対するゼロデイ攻撃等があり、多くのシステムは検知する閾値を変えて対応することが難しい。実際の業務はシステムではなく人が行うものであり、具体的なレベルの情報共有が非常に重要である。そして、それがいかに難しいか、現実と基準とのギャップを考慮することが必要である。
- 他の事業者との連携がデジタル化・DX化している中、安全に関わるシステムの範囲が拡大している。ひとつ例を挙げれば、ランサムウェア、不正クレジットカード情報の利用などについては、多くの犯罪者、攻撃アクターが狙っているポイントは既にわかっている。DDoS攻撃により、航空事業者において大規模な混乱を生じた事実もある。製造業においても、製造は可能であっても受発注システムが狙われると生産を止めざるを得ない現実がある。ガイドラインにおいても、より広いシステムへの対策を啓蒙していくことも意味があると考える。
- 安全管理規程において、明確に経営層を取り上げていただいた意味は大きい。経営層の責任を最

も明確に記載しているのは金融分野だと思うが、そこに倣ってということではないものの、このような記載は鉄道の安全を優先する立場からすると当然であり、非常によいと考える。また、経営者に対する教育は、技術者に対する教育とは異なるため、経営層に責務として書く以上、教育機会を設ける努力も国土交通省に期待したい。

- 例えば、金融情報システムセンター（FISC）が、金融機関の経営陣に向けた研修会を実施している。研修会における指示事項は4項目あり、1点目はサイバーセキュリティ対策の必要性に対する理解を持つこと、2 点目は自社及び国内外の情勢を把握すること、3 点目はサイバーセキュリティに係る資源配分及び体制構築に関して経営判断及び実行支援を明確にすること、4 点目はサイバーセキュリティに係る政策遂行についてリーダーシップを発揮し情報発信を行うこと、とされている。
- サイバーセキュリティについては、どこまで予算をかけるかについて外部が判断することは難しく、どこまでやれば百点というものはないため、各々のシステムや事業者の経営規模等に応じて考える必要がある。そのような中で、経営者は何を判断しなければならないのかを明確に出すべきと考える。
- チェックリストは対策する人のヒントとして与えられるが、攻撃者にもヒントになる面もある。
- 経営者の方から見ると、サイバーセキュリティのためのソフトウェア導入や多重化、あるいは特別な教育プログラムを設けることは、売上増に結び付かない追加コストと見える点も懸念する。現在、サイバー攻撃の被害が社会で報道される中で意識は高まっていると考えられるが、必要な投資であるという点をどのように理解いただくかは課題である。
- 事務局の資料は、運行の安全に支障するリスクとサービス継続不可のリスクとを混同しているのではないか。情報の不一致で列車が停止するリスクを例示しているが、従来のフェールセーフの考え方からすると、ある意味正常な動作なのではないか。 もちろん、衝突や脱線があれば長期間列車が停止し、サービスの継続が止まることになるが、そもそも衝突や脱線はあってはならないことである。その意味で、情報の意図的な書き換えや嘘の情報により、従来のフェールセーフの考え方が崩れ衝突や脱線が起きることは、列車停止とは全く違うレベルで重要性の高いリスクだと考える。このリスク等の考え方が規程にどう反映するかわからないが、人命を預かる鉄道事業という視点では、人命や人の怪我につながることとそうでないものは、リスクの中で明確に分けて書くべきではないかと考える。また、サイバー攻撃の脅威という点では、フェールセーフに組まれてきた従来の論理を崩してしまうものは、特に注意して扱うべきではないかと考える。
- サービス継続の観点では、フェールセーフな仕組みが壊れない限り、鉄道事業者は縮小・縮退運転や、最後にマニュアルや手旗信号で動かすモードもある。そのような記述を入れられるとよいのではないか。
- リスクに関しては、安全に関わるものと、運行サービスの継続性に関わるものが混在しているように感じた。安全は鉄道の根幹であるため、サービス継続という観点も重要だが、安全が疎かになることはあってはならず、そのための明確な分離は必要と考える。
- モデルやチェックリストについては、鉄道事業者として実行可能な内容となるよう慎重に考える必要があると考える。運行サービスの継続性が担保できるモードや仕組みを踏まえた上で、新しいICTを使った際に追加で考えるべき点を議論できるとよいのではないか。

議事（2）その他

オブザーバーである警察庁より鉄道事業者に向けた要望に関して説明が行われた。

3．閉会

以上