第３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 12 月 18 日（木）15:00 ～ 16:36
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】
- 鉄道事業者の安全管理規程について、スコープを輸送の安全に限定することをより明確化し、いわゆるサービス安定に関するシステムを安全管理規程の対象外とするという整理については理解した。一方で、この整理は、サービス安定を重要インフラサービスや重要システムの対象から除外するという意味ではないと理解している。
- 今回、鉄道事業においては、安全管理規程と安全ガイドラインとで、それぞれの守備範囲が異なる形になる。この点について、関係者が十分に理解した上で、取組を進めていくことが重要と考える。
- チェックリストについて、全体として IT 寄りの一般的な内容となっている印象を受ける。制御系システムや鉄道事業特有の運用環境を踏まえ、当該分野の専門家や事業者の意見を取り入れながら、実効性の高いチェックリストへとブラッシュアップする必要があるのではないか。
- サイバーセキュリティに閉じずに、輸送の安全という観点で安全マネジメントに位置付けた点を強く支持する。
- チェックリストに関して、輸送の安全とサービス継続を分けることを強く推奨する。どちらも重要だが、混在させると優先順位が崩れ、現場の意思決定が遅れることがある。また、安全とサービス継続の相反する部分を現場に任せるチェックリストや相当する規定については厳しいと感じる。提案としては、安全に直結する機能を先に特定し、その機能が満たすべき性質を定義することが一般解ではないか。
- 対象システムに関しては、資料に記載のある範囲で妥当と考える。ただし、インシデント対応では、システム単体ではなく依存関係がボトルネックになることがある。範囲を無限に広げる必要はないが、安全に直結する機能を支える依存関係を確認することで、一つの枠として説明可能なものが作れると考える。
- クローズであるから大丈夫という誤解の排除をぜひ訴えていただきたい。
- 帳票が増えると現場が疲弊するため、評価運用を紙の監査に戻さないこと。チェックリストや評価項目の形骸化を防ぐため、①ログと証跡の目的を事前に合意すること、②復旧における手順とテストまでを評価に入れること、③ガバナンス、役員の責務を明確にすること、の３点が重要と考える。
- チェックリストは、安全機能の性質から逆算して項目化することを強く推奨する。変化の多いサイバー脅威や技術に対応可能となり、有用なチェックリストになると考える。
- 輸送の安全の位置付けの整理について、時間をかけて理解を促すことが必要であろう。
- 対象システムについては、輸送の安全に直接的に影響するシステムを特定するという点で、今回の主旨に合致すると考える。実際の運用においては、リスク分析の際に漏れがないよう意識する

とよい。事業者によってシステム範囲に幅があるので、実態に即して運用するとよい。

- サイバーセキュリティ評価について、記録の残し方、報告のあり方は今後の議論と考える。各事業者が公表する安全報告書に関しても、事業者が取扱いに迷うことがないよう指針があるとよい。
- チェックリストの指針を国土交通省から示されたことがメッセージとして重要である。チェックリストについては、ある対策ができなくても、他の対策によりカバーされる場合は、その旨を記録する等の形で運用されることが望ましい。事業者にとってリスク分析の助けやセキュリティ対策の改善の指標として、チェックリストを活用することを期待する。
- ログの取り扱いについても、何のログをどれぐらい取得するのかわからない。システムごとに事業者の想定するサイバーセキュリティリスクがあり、その上で現実的な実施事項を定めていく形にならざるを得ないのではないか。
- 「10. 国際規格」に関して、項目があることに賛同する。具体的にどう活用するかは今後の議論であろう。
- チェックリストについては、監査目的ではないと考えると、判断は各事業者で行うことになろう。ただし、レベル感を情報交換することで、運用において妥当な水準を揃えていくことも必要である。
- チェックリストの形骸化を防ぐための方法として、既に現場で使用されているもののうち、可能なものを収集・分析すれば対応可否は明確になる。一般的にアセスメントというかもしれないが、各々の用語、言い回し、文化、見えない前提等を可能な限り反映できるとよい。また、年１回でよいので、現場に負担をかけず変更管理を行う仕組み設計ができるとよい。
- チェックリストの形骸化を防ぐため、単に「対策の有無」を問う形式から、「バックアップから何時間で復旧可能か」といった、安全機能が満たすべき「性質」や「実効性」を問う表現への見直しを検討いただきたい。
- 輸送の安全と対象システムについて、鉄道事業法第１８条の２「輸送の安全」は、狭義の安全であることが確認できた。現在の国民が鉄道事業者に求める安全の中には当然、輸送事業の根幹である安定したサービスの提供も含まれるため、広義の安全と狭義の安全のギャップをどう埋めるべきかを考える必要がある。昨今、基幹インフラ事業者に対し、サービスに直結する部分に攻撃が向けられている事例もあり、対策をするべきではないか。また、攻撃を受けたシステムとは異なるシステムにも影響を及ぼすことから、対象システムを絞り込むことに対して危機感を持つ。引き続き議論の必要性があることを鉄道事業者及び国土交通省の皆様に認識いただきたい。
- 安全管理規程の中に、役員の責務としてサイバーセキュリティ対策が記載された点については非常に素晴らしい取組と評価する。リソース不足や社内他部門との利益相反等から、システム部門だけで対策を高め自己評価を行うことは難しいのが実情である。そのため、このサイバーセキュリティ評価がシステム部門にのみ行われるだけでは十分ではない。経営者が経営判断としてどう支えるかが問われている。
- 「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」に、鉄道の特性を捉えた記述がもう少しあってもいいのではないかと感じる。特に安定供給に関する部分は実はあまり記載がない。事業の社会的使命に合った形で、内容についてふさわしいものにしていく努力をぜひ行っていただきたい。
- 地域社会において鉄道事業は極めて重要な役割を担っており、今後さらに多様なサービスが追加されることが想定される。そのため、社会情勢や技術変化に合わせ、このチェックリストやガイドラインについて、不断の見直しを行っていただきたい。
- 輸送安全に特化した安全管理規程への懸念はもっともと考えるが、現在の議論では安全管理規程の改定が本検討委員会の成果として求められているため、安全管理規程の範囲を広げず、あえて絞り込む形としている。決してサービスに関するセキュリティを軽視している訳ではなく、その点については別の議論があり得ると理解している。
- 現在、国際規格 IEC 63452 において、輸送安全と鉄道サービスを分ける方針が明確に示されてい

る。この規格が国内基準に反映されることが想定され不整合が出ないよう、議論を進めた結果、この形に落ち着いた。

- 妨害を与えるという意味では、電磁波による攻撃もサイバー攻撃と同様であると認識しており、電磁波攻撃への対策の考え方はサイバーセキュリティ対策としても有効だろう。ただし、ネットワークで多くの設備と接続されることから、対策すべき箇所についてはシステムごとに新たに検討する必要がある。
- 安全管理規程における対象システムに対する運用の考え方について、他の委員の意見に賛同する。システムの構成法や利用環境、使われ方などによって想定すべきリスクが異なるので、各事業者が個々のシステムごとにリスク分析を行い、必要な対策を見極めることが重要と考える。チェックリストについても事業者の意見を取り入れながらブラッシュアップしていくことが重要である。
- 今回の対象システムの考え方については賛同する。ただし、提示された対象システムの示す範囲は、今後も変化するものと考える。また、対象システムと対象外としている周辺システムの境界線は必ずしも明確ではない。したがって、サイバーセキュリティリスクの今後の変化に伴い、どこまでを見なければならないのか、常に再チェックする姿勢が重要となる。
- 今回の対象システムと対象外システムの区分は、現時点のものと理解した方がよい。制度開始時点に事業者の急激な負担増は避けるべきであり、選定対象を絞ることは重要である。ただし、今後、経験や実績を積みながら将来的に対象を拡大する取り組みも必要となる。また、国土交通省も、対象システムを積極的に見直し、増やしていくというメッセージを打ち出す方が望ましい。
- 昨今のセキュリティ事故の原因となる問題として、ID マネジメントが十分にできていない点が挙げられる。情報システム担当者だけでなく、人事部門との連携が必要という点を明確なメッセージとして示せるとよい。
- チェックリスト自体が形骸化しないよう、運用状況や現場での課題・効果をモニタリングし、チェックリストの改善につなげる仕組みを、国土交通省として当初から準備できることが望ましい。
- サイバーセキュリティ関連の情勢が変化している。去年までの十年間の変化が今年一年で同じだけ変化した印象を持つ。政府のような大きな組織が作る規程類は頻度よく変えられない特性がある。一度作って終わりでは必ず形骸化する。制度として更新サイクルを是非とも残していただきたい。対象範囲、評価観点、インシデント事例、委託先、遠隔保守の実態変化等、見直しを回す枠組みを作っていただけると、後の方々の安全を守ることになると考える。
- 今後、鉄道事業者において、チェックリストの解釈に過度の負担が生じない形で制度が浸透することを願う。事業者ごとに解釈のぶれが出ないよう継続的に情報交換や議論の機会等を設けていただきたい。国際標準もうまく活用できるところを使っていけるとよい。本質的には、事業者の方々がリスク分析を適切にできることが重要であるため、IPA の教育プログラムや鉄道総研のセミナー等を活用いただくことも重要と考える。
- サイバーセキュリティで重要となる官民学の連携について。現在のサイバー攻撃、サイバー犯罪という情勢の中では、一事業者で対抗するのは極めて難しい。同じ課題を抱える民・民の連携機会、情報交換の機会を事業者の方々に作っていただきたい。また、国土交通省をはじめ各団体の方々には、民・民だけではなく官や学術の方々が情報共有あるいは対抗策について検討できるような共助の場を提供いただく、あるいは構築する努力をいただきたい。
- サイバーセキュリティについて年々関心が高まっていることを感じる。この危機感の共有をチャンスと捉え、業界全体のサイバーセキュリティ確保につなげていただきたい。その意味で、共助の観点で、交通 ISAC のような動きも含め、横連携をしながら情報交換等を行っていただき、業界全体として、鉄道の安全確保、それに関わるサイバーセキュリティ確保を進めていただくことを期待している。
- 先生方からは、継続的な検討の必要性と、不足点についてのご指摘をいただいた。しかし、継続的な見直しはごく自然に行われていくであろう。鉄道工学は事故にも学び、サイバーセキュリテ

ィがキーワードとしてアクションに明確に入ってきた。鉄道技術者の皆様は、各々の努力の中で改善するマインドを持っておられるので、サイバーセキュリティの先生方もそこは信頼いただき、温かく見守っていただきたい。

- 鉄道関係者に閉じず、他業種との情報交換を積極的にすべしとのご指導も、非常に重要なご示唆である。鉄道事業者の技術者の方々には、念頭に置いていただきたい。
- 本検討委員会では、鉄道事業者の方から直接意見を伺う場はなかったと思うが、それを具体的に日々の業務に落とし込んでいく中での共通認識、ルールや共通の考え方を育てていくのは、今後様々なところで行われ、インプリメンテーション（実装）の議論がなされることが期待される。
- 委員会としては本日で終わりであるが、皆で検討するスタートを切る日でもある。今後、関係の皆様が、さらに努力を続けてくださることを祈っている。

３．閉会

以上