鉄道事業者の情報セキュリティ対策

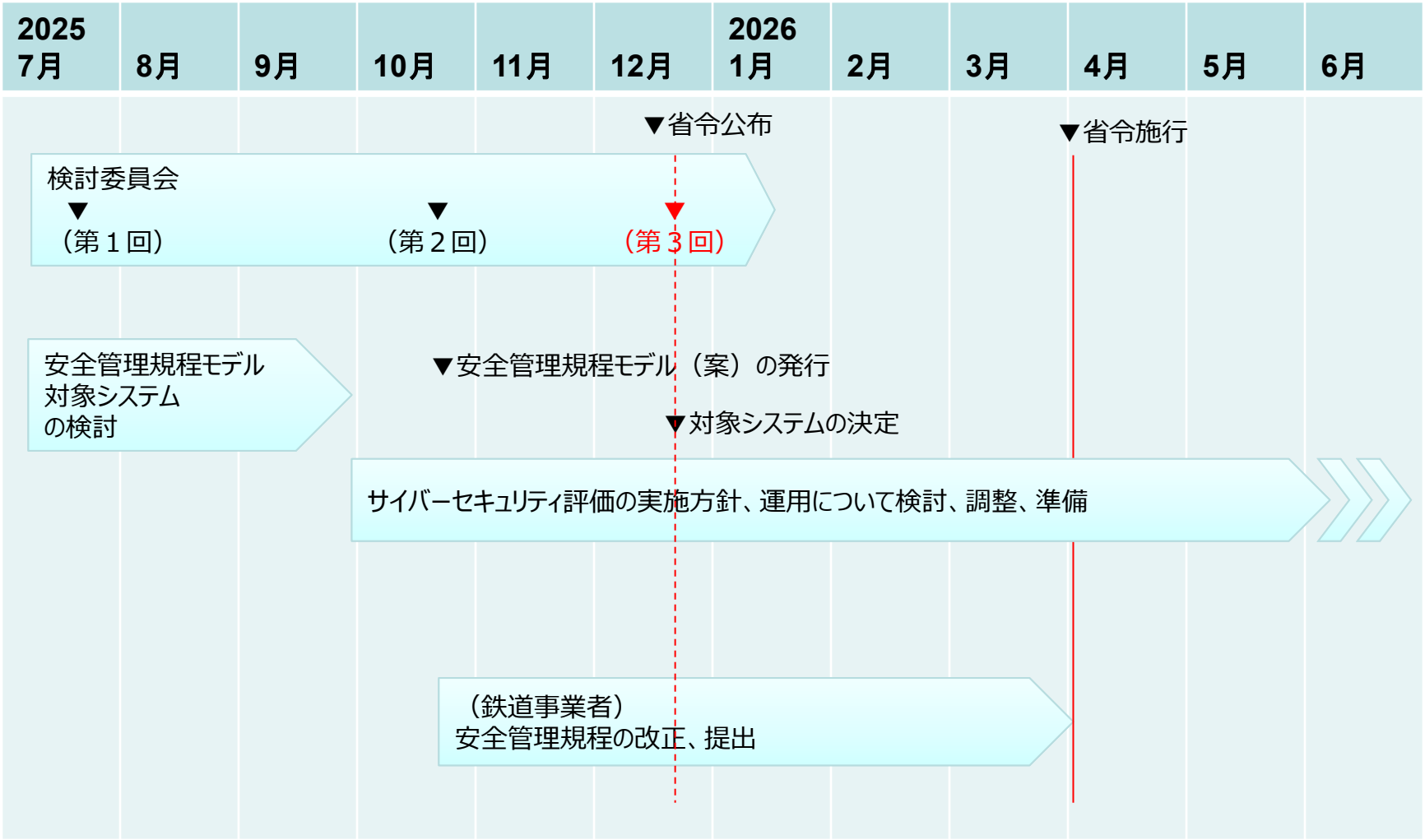
国土交通省 鉄道局
総務課危機管理室

令和7年12月

検討会スケジュール

国土交通省

来年4月1日の省令施行に向けて、調整を進めている。



第2回での主要な質疑や議論

国土交通省

【組織体制と人材育成】

- 安全管理規程において、**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、**セキュリティ文化を作る**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る。
- 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。
- 人材の採用・育成は重要であり、鉄道事業者において社内人材の育成に力を入れていただきたい。**経営層・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。**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。

【リスク評価とレジリエンス】

- ネットワーク全体が攻撃を受けて稼働しなくなれば、システムも機能しないこととなる。**システム単独ではなくネットワークも含めた広域での評価・対策の総合的検証**が必要となる。
- **サイバー攻撃で破壊されないバックアップ体制を確保する**ことの必要性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やテストの実施、また、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**等も重要である。
- ログ・証跡の保全は重要であるが、規定がないから残していないというような場面も見たため、社内での**予算確保や意思決定に当たり、「なぜログが必要か」のあらかじめの合意形成**が必要である。

【安全とサービス継続の考え方】

- リスクの捉え方において、輸送の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も感じられる。輸送の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。
- **従来のフェールセーフの前提がサイバー攻撃によって崩され**衝突や脱線が起きることは、列車を停止させられるようなものとは全く違うレベルで**重要性の高いリスク**だと考える。
- 安全管理規程モデルやチェックリストは、**鉄道事業者として実行可能な内容となるように考える必要**がある。

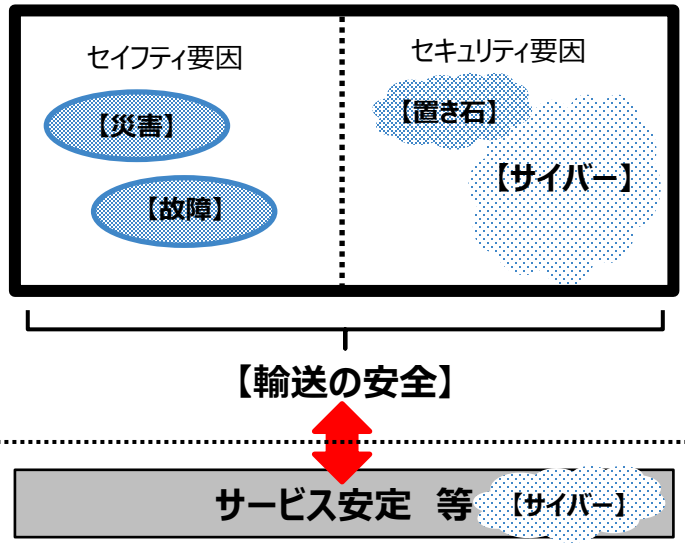
「輸送の安全」考え方の要点

国土交通省

- セキュリティとセイフティの概念は、ともに「安全」に包含される。「輸送の安全」も、セキュリティ要因とセイフティ要因の両者に起因するものを含む概念である。
- フェイルセーフが効かないリスクが顕在化する中、サイバーセキュリティについて、要因に重点を置いた対処が必要となる。
- セキュリティ分野とセイフティ分野のいずれの要因であっても、結果としての「輸送の安全」が、人身を中心とする最優先のリスクへの対処を指すものであることに変更はない。特定の要因に着目して対処を重点化するものである。

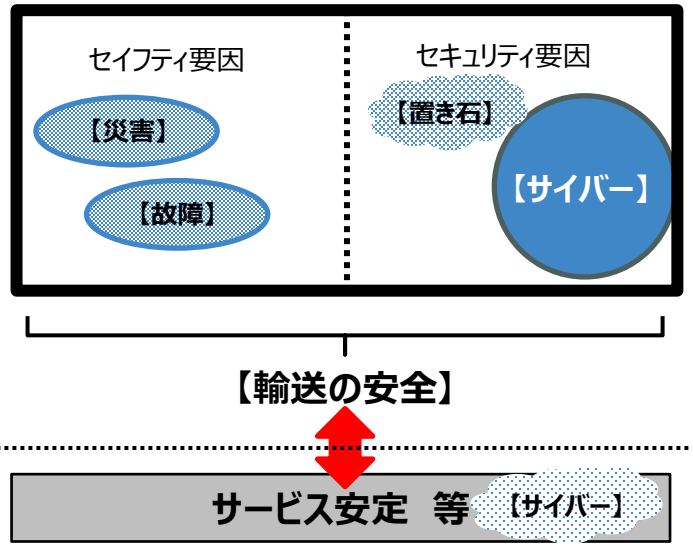
輸送の安全への位置づけのイメージ

〈従前〉これまでの実務上、災害等のセイフティ要因を主眼に置きつつ、必ずしも、個別の要因に特化した対処までは求めてこなかった。



元来包含されていたサイバーを
個別に対処すべき要因として重点化

〈今回〉サイバー攻撃により、フェイルセーフが破られる・迂回されるリスクが顕在化している。
そのような中で、着実に「輸送の安全」を確保するためにも、サイバー要因については特化した対処が必要となる。



「輸送の安全」が指す結果に影響を与えるものではなく、対処すべき要因のうち、「輸送の安全」の確保に必要となるサイバーセキュリティを重点化するものである。

ご議論いただきたい事項：対象システムについて

国土交通省

（非公表：情報公開法第5条第4号該当）

（参考）制御システムに対するサイバー攻撃事例

国土交通省

事案：マルウェアStuxnet感染による制御不能（イラン核燃料施設）

感染経路

1．内部犯行者を通じて持ち込まれた
2．制御システムのベンダーやエンジニアリングを担う請負業者が感染し、同事業者のエンジニアが知らずに感染したUSBを持ち込んだ

特　徴

1．遠心分離機を制御するPLC（プログラマブルロジックコントローラ）の設定ロジックが改ざんされ、モーターの速度を制御できる装置まで入り込まれた
2．制御ロジックを改ざんして制御システムの監視画面をダミー表示にすり替えたり警報アラームを密かに停止したりする、といったような特徴的な機能を保有していた
3．制御システムのインターネット接続の有無については不明である

問題点

1．制御システムの操作や改ざんが可能な状態であった
2．エアギャップ環境やクローズド環境においても発生しうる事案である

- クローズド環境や独立しているシステムであるからサイバーセキュリティの対象外であるという考えはできない
- マルウェアは常に進化しており、フェールセーフを脅かす機能を保有したマルウェアの出現もあり得る
- 操作者に対する表示をすり替えることで、操作を誤らせて不安全事象を生じさせる手口もあり得る
- 操作体系を自動から手動にフォールバックさせることで、操作者によるミスを誘発されるおそれもある

（参考、前回再掲）安全管理規程の記載について

国土交通省

安全管理規程にサイバーセキュリティ対策を記載する。詳細は別紙参照。

安全管理規程の章立て	サイバーセキュリティ対応の追記案（黒字は現行の項目）
第一編　総則 第一章　目的等 第二章　輸送の安全を確保するのための基本的な方針等	－
第三章　輸送の安全を確保するための事業の実施、管理の体制及び方法 第一節　輸送の安全の確保に関する組織体制	役員の責務として「サイバーセキュリティの対策」を記載する （以降の「事故・災害等」にサイバーセキュリティ侵害も含まれる） 「サイバーセキュリティ責任者」を組織体制、体制図に追加する
第二節　安全統括管理者等の責務	－
第三節　輸送の安全の確保に関する事業の実施及び管理の方法	－
第二編　輸送の安全を確保するための事業の実施及び管理の方法 第一章　運転の管理 第二章　鉄道施設の管理 第三章　車両の管理	－
第三編　サイバーセキュリティを確保するための事業の実施及び管理の方法 第一章　サイバーセキュリティ責任者の責務 第二章　事業の実施及び管理の方法	サイバーセキュリティ責任者の責務 サイバーセキュリティ侵害の防止対策の検討 サイバーセキュリティ侵害の報告及び対応 業務の確認（及び外部能力の活用） 安全管理体制の維持のための教育訓練 規程等の整備 規程、帳票類等の備え付け及び記録の管理等

サイバーセキュリティ評価について

国土交通省

安全管理規程

対象：経営層

運輸安全マネジメント評価

事業者の経営トップ等経営部門に対するインタビュー等を通じた、自主的な安全管理体制の構築に対する支援制度

【主な特徴】

○事業者の自主的な安全管理体制の構築のため評価・助言
○経営トップの主体的関与の下での自律的な安全管理体制の構築・改善（スパイラルアップ）を期待
○自律的な取組が継続的に効果を上げているかどうかを評価
○中長期的に効果が発現

対象：現場

基準策定・保安監査

事業者の現場における業務実施状況のチェックを通じた事後監督制度

【主な特徴】

○安全に関する法令等基準を策定
○事業者の基準への遵守状況等を確認し、改善命令
○現場における施設や取組内容等の基準等への適合を意図
○改善命令等による改善
○短期的に効果が発現

サイバーセキュリティ

（註）「サイバーセキュリティ評価」＝これまで「監査」と称していたものを改称

対象：システム部門

サイバーセキュリティ評価（新設）

事業者の対象システム部門等に対するインタビュー等を通じた、輸送の安全の確保に係るサイバーセキュリティ対策に向けた体制の構築に対する支援制度

【主な特徴】

○輸送の安全確保に係るサイバーセキュリティ対策に向けた体制の構築のため評価・助言
○サイバーセキュリティ責任者の全社を横串刺した関与の下での自律的な安全管理体制の構築・改善（スパイラルアップ）を期待
○自律的な取組が継続的に効果を上げているかどうかを評価
○中長期的に効果が発現

チェックリスト（仮称）についての考え方

国土交通省

1.既存のガイドラインの役割

- 現行の「**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**」は、「重要インフラのサイバーセキュリティに係る行動計画」及びそれに基づく「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」を踏まえたもの
- 個々の重要インフラ事業者等が自主的に取組、対策の実施や検証に当たっての目標を定めることを目的として、「**推奨基準**」を例示した「**ガイドライン**」としての位置づけ

2.チェックリスト（仮称）の概要

- 検討委員会での議論を踏まえ、鉄道事業者において実施が求められるセキュリティ対策について、「**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**」に記載の事項の一部及びその他鉄道事業者に求められる事項を「**チェックリスト（仮称）**」としてまとめる。
- 今後のサイバーセキュリティ評価において、本チェックリスト（仮称）の事項に沿って対策状況を確認するため、鉄道事業者におかれては内容を参考にされたい。
- 鉄道事業者においては、各社の多角的な経営及び自治体等の事情に基づき策定した方針・ポリシーに沿って自主的に点検していると思料するため、点検方法は事業者判断とする。

【内容（案）】
（１）方針・ルール（２）体制（３）経営層（４）レジリエンス（５）インシデントレスポンス
（６）社内教育・訓練、人材育成、コンプライアンス（７）サプライチェーン（８）統制（９）脅威情報
（10）国際規格（11）ID・パスワード・アカウント（12）全般的な対策　等

ご議論いただきたい事項：チェックリスト（案）について

国土交通省

項目	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　該当箇所
1．方針・ルール	
□ 情報セキュリティポリシー、対応方針及びルールの策定	3.1.1
□ 情報セキュリティポリシー等の従業員への周知	3.1.1
□ 情報セキュリティポリシー等の定期的な確認及び見直し	3.1.2
2．体制	
□ サイバーセキュリティ責任者の指定等、平時の体制、責任及び役割の明確化	3.4.1
□ サイバーセキュリティ侵害発生時の連絡体制の整備	4.7.2
□ サイバーセキュリティ侵害発生時の対応体制、責任及び役割の明確化	3.4.1
□ サイバーセキュリティに関する体制等の定期的な確認及び見直し	3.4.2
3．経営層	
□ サイバーセキュリティ侵害発生時、維持・継続が必要となる機能及び機器等の範囲や水準、それに必要な経営資源等の把握	4.2.1
4．レジリエンス	
□ サイバーセキュリティ侵害を想定した事業継続計画(BCP対策)の策定及び運用	4.9.2
□ システム復旧に必要なシステムソフトウェアやデータのバックアップ及びバックアップの隔離	5.1.3.3
5．インシデントレスポンス	
□ サイバーセキュリティ侵害の検知から復旧までの各過程や経営層へのエスカレーションにおいて行われた対応について、その正誤や要した時間に目標を設定するなどしたセキュリティ対策の評価の実施	5.1.4

ご議論いただきたい事項：チェックリスト（案）について

国土交通省

項目	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　該当箇所
6．教育、訓練	
□　従業員等に対するサイバーセキュリティ教育の実施	4.6
□　サイバーセキュリティ侵害への対応訓練の実施	4.10
□　サイバーセキュリティ人材の育成に向けたキャリアパスや外部人材の活用、外部研修への参加	4.6
7．サプライチェーン	
□　業務委託先や供給者等との契約書へのサプライチェーンリスクに関する事項の明記	4.4
□　業務委託先や供給者等のサイバーセキュリティ管理・対策状況の把握	5.6.1
□　事業継続計画等にサプライチェーンリスクを考慮した対策の策定	4.5.1
8．統制	
□　輸送の安全確保の観点からシステムの特性を踏まえたリスクアセスメントの実施	4.1.3
□　クローズド環境であることを考慮したリスク特定、分析及び対策	4.2.2
9．脅威情報	
□　国内外の脅威情報や事例の情報収集体制の構築	3.8.2
10．国際規格	
□　サイバーセキュリティ対策や機器等の調達において、セキュリティにかかる国際規格等の活用	別紙2 2.3.4
11．ID・パスワード・アカウント	
□　ID・パスワード・アカウントの適正な設置及び管理	5.4.3
12．全般的な対策	
□　重要な場所(サーバルーム)への入退室管理	5.3.1
□　各システムにおけるログの取得・管理	5.1.3.4
□　外部記録媒体の使用ルール設定や制限	5.1.1