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
概要版

国土交通省鉄道局

令和8年4月

改定履歴

国土交通省

改定日	版	改定概要
2026年4月22日	第6版	政府統一基準群、関連する最新の基準、ガイドライン等を踏まえた改定
2024年4月18日	第5版	「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（令和5年7月4日サイバーセキュリティ戦略本部決定）、関連する最新の基準、ガイドライン等を踏まえた改定
2019年3月29日	第4版	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）を踏まえた改定（ガイドラインの名称変更を含む）
2016年4月1日	第3版	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）を踏まえた改定
2012年10月29日	第2版	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針、関連する最新の基準を踏まえた改定
2006年9月29日	初版	初版策定

「情報セキュリティ確保に係る安全ガイドライン」改定の概要

国土交通省

改定のポイント

IoT機器のセキュリティ制度に合わせた修正

○別紙２．システムの取得・開発・保守に係るセキュリティ管理策

セキュリティ要件適合評価及びラベリング制度（JC-STAR）は、2024年8月に経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的としたもの。

重要インフラサービスの提供に必要なシステム、装置としてIoT機器等を調達する場合は、本制度を選定基準に含めるなど、必要なセキュリティ機能が適切に実装されていることを要求することを追記している。

その他

○用語及び参照文書等の細かな修正

組織名の変更、用語解説、参照文書の更新など細かな点の修正

改正安全ガイドラインの目次構成

国土交通省

✓ NCOが定める「安全基準等策定指針」の改定に則り、安全ガイドラインの構成を以下のとおりとしている。

はじめに
1．「安全ガイドライン」策定の背景

2．鉄道分野における
「安全ガイドラインの概要」

3．組織統治におけるサイバーセキュリティ

3.1 組織方針
- 3.1.1 組織方針とサイバーセキュリティ
- 3.1.2 サイバーセキュリティ方針

3.2 組織内外のコミュニケーション

3.3 経営リスクとしてのサイバーセキュリティ

3.4 責任及び権限の割当て
- 3.4.1 サイバーセキュリティ責任者の任命
- 3.4.2 責任者・組織などの役割
- 3.4.3 役割の分離

3.5 資源の確保

3.6 監査・モニタリング

3.7 情報開示

3.8 継続的改善
- 3.8.1 サイバーセキュリティ確保の取組の見直し
- 3.8.2 ITに係る環境変化に伴う脅威のための対策

4．リスクマネジメントの活用と危機管理

4.1 組織状況の理解
- 4.1.1 内部状況・外部状況の理解
- 4.1.2 関係主体からの要求事項の理解
- 4.1.3 重要インフラサービス継続に係る特性の理解
- 4.1.4 現在プロファイルの特定

4.2 リスクアセスメント
- 4.2.1 リスクアセスメントの実施
- 4.2.2 制御システムのリスクアセスメント
- 4.2.3 目標とする将来像の設定

4.3 サイバーセキュリティリスク対応
- 4.3.1 リスク対応の決定
- 4.3.2 個別方針の策定
- 4.3.3 リスク対応計画の策定

4.4 サプライチェーン・リスクマネジメント

4.5 事業継続計画等
- 4.5.1 事業継続計画等の作成
- 4.5.2 重要インフラサービス障害の対応
- 4.5.3 重要インフラサービス障害に対する防護・回復

4.6 人材育成・意識啓発

4.7 CSIRT等の整備
- 4.7.1 CSIRT等の整備、関連部門との役割分担等の合意
- 4.7.2 重要インフラサービス障害発生時の体制の整備

4.8 平時の運用
- 4.8.1 セキュリティ対策の導入、運用プロセスの確立・実行
- 4.8.2 情報共有

4.9 危機管理
- 4.9.1 サイバー攻撃の予兆
- 4.9.2 コンティンジェンシープラン及びBCPの実行
- 4.9.3 本社等重要拠点の機能の確保
- 4.9.4 セキュリティ対策状況の対外説明

4.10 演習・訓練

4.11 モニタリング及びレビュー
- 4.11.1 モニタリング実施計画の策定と実施
- 4.11.2 監査計画の策定と実施
- 4.11.3 セキュリティ対策の自己点検

5．対策項目

5.1 組織的対策
- 5.1.1 資産の管理
- 5.1.2 供給者管理
- 5.1.3 運用の管理
- 5.1.4 インシデント管理

5.2 人的対策
- 3.1.1 組織方針とサイバーセキュリティ
- 3.1.2 サイバーセキュリティ方針

5.3 物理的対策
- 5.3.1 セキュリティ確保が求められる領域
- 5.3.2 災害による障害の発生しにくい設備の設置及び管理
- 5.3.3 装置の管理

5.4 技術的対策
- 5.4.1 不正アクセス等の脅威への対策
- 5.4.2 情報システム等のアクセス制御
- 5.4.3 暗号を活用した情報管理
- 5.4.4 通信のセキュリティ
- 5.4.5 負荷分散・冗長化
- 5.4.6 多層防御

5.5 クラウドサービス

5.6 委託先管理
- 5.6.1 業務委託 （共通事項）
- 5.6.2 情報システムに関する業務委託
- 5.6.3 委託先に係る人的安全管理措置

6．参考文献
7．専門用語集

別紙１．情報の取扱い・個人情報保護

別紙２．システムの取得・開発・保守に
係るセキュリティ管理策

はじめに

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある。

国土交通省では、所管する**６分野（航空、空港、鉄道、水道、物流、港湾）**における各事業分野、及び関連事業者のセキュリティ管理策の現状に配慮しながら、各事業分野におけるセキュリティ管理策の向上に資する望ましいセキュリティ管理策の水準をまとめ、**サイバーセキュリティ確保に係る安全ガイドラインを策定**しており、各分野の安全ガイドラインの初版策定以降、**指針の改正や世の中の情勢を踏まえ、適宜本ガイドラインを改定する**こととしている。

「安全ガイドライン」の目的と形態

目的

重要インフラ事業者等は、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場であり、**任務保証の考え方**を踏まえ、以下に例示する必要な対策に取り組むことが重要である。

- ❒ サイバーセキュリティに係るリスクへの備えを経営戦略として位置づけ
- ❒ リスクマネジメントにおいてサイバーセキュリティも取り扱う
- ❒ サイバーセキュリティリスクへの必要な備えの実践
- ❒ 有事の際の適切な対処の実現　など

<任務保証の考え方>
「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」
重要インフラのサイバーセキュリティに係る行動計画より抜粋

形態

国家サイバー統括室（NCO）の策定する「安全基準等策定指針」においては、重要インフラ事業者等が参考とする文書類を「安全基準等」と呼び、次の①～④に分類している。

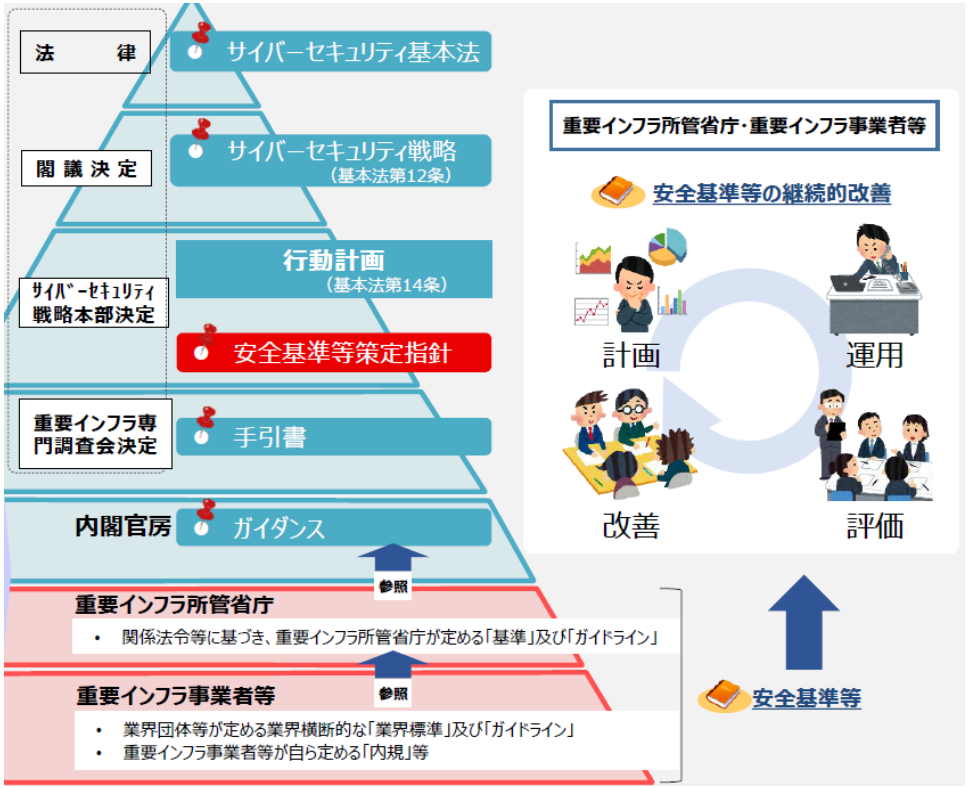
① 関係法令に基づき国が定める「強制基準」
② 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
③ 関係法令や国民からの期待に応えるべく、業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④ 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

本ガイドラインは②に対応し、国が定める「ガイドライン」として**推奨事項を列挙**しているものである。

1.「安全ガイドライン」の位置づけ

国土交通省

- ✓ 鉄道事業者は、内閣官房が定める重要インフラ事業者等として、「任務保証の考え方」を踏まえ、鉄道事業における重要インフラサービスの継続性を維持するため、サイバーセキュリティ確保に取り組むことが重要である。
- ✓ 本ガイドラインは、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策定されている。



※重要インフラのサイバーセキュリティに係る行動計画の概要より抜粋
https://www.cyber.go.jp/pdf/policy/infra/cip_policy_abst_2024.pdf

鉄道分野の重要インフラサービス例

2. 鉄道分野におけるサイバーセキュリティの現状

国土交通省

- ✓ 鉄道分野における国民生活や社会経済活動に影響を及ぼし、事業継続の取組対象となるような重要システムは、**「列車運行管理システム」「電力管理システム」「座席予約システム」**である。
- ✓ これらに対するサイバー攻撃の事例は、現状国内では多く見られない。しかし、海外では鉄道ネットワークに侵入され、鉄道輸送サービスが停止させられる事例が近年でも発生している。

鉄道分野においては以下の取組等により、ネットワーク化がより進んでいる。

- **保安設備のＤＸ化に伴う各種センサーの増加**
- **安全意識の高まりによる防犯カメラの普及**

保安設備へのサイバー攻撃は**鉄道人身事故を含む重大な被害をもたらすおそれ**がある。また、防犯カメラやその他情報の完全性・可用性が損なわれることが、鉄道事故に直結することはまれと考えられるが、**物理的な攻撃と組み合わせたテロ・犯罪の一環として行われる可能性**もあり、この点もサイバーセキュリティに関する新たなリスクとして注視しておく必要がある。

鉄道における、近年のサイバー攻撃国外事例

時期	被害状況
2022年11月　デンマーク	サイバー攻撃を受けシステムのシャットダウンを実施。4時間ほどの運行停止
2021年12月　カナダ	脆弱性への攻撃でWebサイト不通 Webサービスが24時間停止
2021年　9月　イラン	鉄道ネットワークに侵入 切符販売、ウェブサイト、貨物サービス等が中段し、列車の遅延・運休が発生し、駅内で大規模な混乱となった
2017年10月　スウェーデン	通信サービスプロバイダがDDoS攻撃に見舞われ、列車管理システムが停止

3. 組織統治におけるサイバーセキュリティ

国土交通省

ガイドラインの記載内容

【組織方針とサイバーセキュリティ】

✓ サイバー空間からの脅威が事業継続を脅かす状況にある現代においては、**サイバーリスクを許容水準まで低減**することは、鉄道事業者が果たすべき**社会的責任**であり、その実践は**経営層の責務**である。

【経営リスクとしてのサイバーセキュリティリスクの管理】

✓ 組織統治（ガバナンス）の一環として取り組んでいるリスクマネジメントサイクルにおいて、これまで一般に対象としてきた**自然災害、感染症、為替変動などのリスクに加え、サイバーセキュリティも取り扱う**。

組織方針とサイバーセキュリティ

事業者へ求めること

経営層は、組織方針（経営方針・リスクマネジメント方針等）にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れ、あわせて維持するサービス範囲・水準を示すことが望ましい。

組織方針に組み入れる事項の例

- 「日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施」
- 「サイバー攻撃の結果、生産活動やサービス提供に影響が生じるリスクを考慮し、サイバーセキュリティ推進体制を構築」

経営方針等への記載例

- 「経営方針等にサイバーセキュリティ確保に関する事項として「日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施」等を記載し、そのKPI（重要業績評価指標）として「システム障害によるサービス停止からサービス復旧までの時間○○時間以内」等を記載する。」

取締役会等においてサイバーセキュリティリスクも取扱い、適切にリスク管理をすることとし経営方針等に明記する

経営リスクとしてのサイバーセキュリティリスクの管理

事業者へ求めること

組織内におけるその他の経営リスク管理体制と整合をとり、サイバーセキュリティに関する責任及び権限（次スライド参照）を明確にした上で、リスク管理体制を構築する。

サイバーセキュリティリスク管理の例

- CISO*等が、組織内に設置された経営リスクに関する委員会に参加する。
- 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築・運用されているかを監査する。
- 内部統制の観点から、サイバーセキュリティ対策の有効性や信頼性確保等の目的達成を保証するための役割を体制内で明確化する。

*最高情報セキュリティ責任者（Chief Information Security Officer）リスク管理の一つとして、セキュリティ対策を推進する最終決定権をもつ責任者。役員クラスが相当

サイバーセキュリティリスクも経営リスクの一つであるという考え方

3. 組織統治におけるサイバーセキュリティ

国土交通省

ガイドラインの記載内容

【責任及び権限の割当て】

✓ サイバーセキュリティの確保を実践するためには、組織内の関係者が、職務に応じて与えられる権限と責務を理解し、全うすることが重要である。そのため、**権限と責務を明確**にし、**必要となる体制を確立**することが望ましい。

【情報開示】

✓ ステークホルダーの信頼・安心感の醸成のため、組織の情報開示の体制において、**サイバーセキュリティに関する取組も可能の範囲で開示する**ことが望ましい。

責任及び権限の割当て

事業者へ求めること

サイバーセキュリティリスクの管理について、担当する部署及び従業員を決定するとともに、役割及び権限を割り当てる。

設置する組織の例

- ❒ 情報セキュリティ委員会
  （セキュリティに関する自組織の関連事項を整理し、役員へ定期的に報告する会議体）
- ❒ CSIRT：Computer Security Incident Response Team
  （セキュリティインシデントが発生した際に対応するチーム。システム復旧だけでなく、社内調整、広報業務、組織外との情報共有などが主な役割となる）

割り当てる役割の例

- ❒ サイバーセキュリティに関する最高責任者（CISO等）
  CISOの任命にあたっては経営層の責任において実施する
- ❒ 脅威情報等の収集*及び関係主体との情報共有担当
- ❒ 事業継続計画の実行担当

*脆弱性情報やサイバー攻撃集団の活動認知

情報開示

事業者へ求めること

経営層には、平時におけるサイバーセキュリティ確保の取組に対する姿勢や、インシデント発生時の対応に関する情報の開示に取り組むことが望まれる。
ただし、開示する情報に際しては、機密情報推測のリスクなどを踏まえ、経営判断に委ねるべきであることに留意する。

開示することが望ましいサイバーセキュリティに関する情報

- ❒ 組織方針・サイバーセキュリティ方針
- ❒ インシデントの発生状況及び対応状況
- ❒ **維持するサービス範囲・水準（前スライド参照）**
- ❒ **リスク管理体制**
- ❒ **セキュリティ対策に必要な資源の確保（予算・人材等）**

4. リスクマネジメントの活用と危機管理

国土交通省

ガイドラインの記載内容

【組織状況及び特性の理解】

✓ 組織状況の理解はリスクマネジメントの中で非常に重要である。**鉄道サービスの特性を理解**するとともに、以下に例示するサイバーセキュリティ対処態勢の実態把握を行うのが望ましい。

- **自組織が果たすべき役割・機能**と、それを踏まえて**維持・継続することが必要なサービス**
- 最低限提供する**サービスの範囲・水準**
- サービス提供を維持するために**必要な業務や経営資源**

組織状況の理解

事業者へ求めること

以下に例示する内部・外部の状況及び特性を理解する。

内部状況の例

- ❒ 重要サービスを支える資源（設備、人材、予算）
- ❒ 従業員のセキュリティリテラシー（標的型メールへの対処等）
- ❒ 重要システムの環境（設置場所、ネットワーク的なつながり）

外部状況の例

- ❒ 自組織の関係主体（サプライチェーン、ステークホルダー）
- ❒ 自組織の関連法令の改正状況（事業法、個人情報保護法）
- ❒ 他組織におけるサイバーセキュリティインシデントの発生状況

特性の例（鉄道分野）

内部・外部の状況を踏まえ、重要インフラサービス継続に係る特性を理解する。

（例）

- ❒ 旅客輸送サービス等の停止が社会に与える影響
- ❒ 旅客輸送サービス等の障害時における復旧までの許容可能な時間
- ❒ 他の事業者との依存関係

（資金決済サービスが停止すると、発券・入出場手続きに影響がある。
電力供給が停止すると、駅構内の空調に影響がある等）

サイバーセキュリティ対処態勢の実態把握

事業者へ求めること

自組織のサイバーセキュリティ対処態勢を把握する（現状把握）。
現時点でのサイバーセキュリティに関する成熟度をはかる。

サイバーセキュリティ対処態勢の例

- ❒ サイバーセキュリティに関する役割・責任（前スライド参照）が明確であるか
- ❒ 情報共有体制が整備され、定期的に見直されているか
- ❒ 重要サービスを支える資産の脆弱性を把握しているか
- ❒ サイバー攻撃を検知できる体制にあるか
- ❒ 従業員に対するセキュリティトレーニングの実施状況
- ❒ サイバーインシデント発生時に、意思決定に必要な情報を把握できるか
- ❒ インシデントへの対応計画と復旧計画が策定されているか

成熟度をはかる上で、以下の文書等が参考となる。

- ✓ 米国 NIST サイバーセキュリティフレームワーク
- ✓ 英国 サイバーアセスメントフレームワーク
- ✓ サイバーセキュリティ能力成熟度モデル
- ✓ CIS Controls

4. リスクマネジメントの活用と危機管理

国土交通省

ガイドラインの記載内容

【リスクアセスメントの実施】

✓ 組織の状況と資産を踏まえ、**任務保証の考え方に基づくリスクアセスメント**を実施する。

✓ 制御システムを使用している場合には、**制御システムに対してもリスクアセスメント**を実施する。

【目標とする将来像の設定】

✓ リスクアセスメント結果や、組織の状況、ステークホルダーからの要求事項等を踏まえ、**サイバーセキュリティに関する自組織のあるべき姿**として、目標とする将来像を決定する。

リスクアセスメントの実施

事業者へ求めること

組織状況や特性（前スライド参照）を踏まえ、重要インフラサービスの提供に影響を与えるセキュリティリスクを適切に管理すべく、リスクアセスメントを実施する。
個々のサイバーセキュリティリスクに対し、「サービス・業務への影響度」や「事象の発生頻度」等を踏まえて、「低減」、「回避」、「移転」、「保有」の対応を選択する。

リスクアセスメントを踏まえた対応の選択

- 低減：リスクの発生確率を下げる対策
  （重要な情報へのアクセス制御、多要素認証）
- 回避：リスクの発生可能性を除去する対策
  （情報漏洩回避策として、個人所有端末へのデータ保存禁止）
- 移転：リスクを他者に移す対策
  （クラウドサービスの利用、サイバー保険への加入）
- 保有：リスクを把握しながら具体的な対策を取らない

制御システムについて

重要インフラサービスの提供に制御システムが使用されている場合には、制御システムについてもリスクアセスメントを実施する。
（例）
一般的に、制御システムは可用性（安全、安定稼働）が最優先される。
パッチ適用やバージョンアップ、暗号化などのリスク低減策の実施が、制御システムの安定稼働に影響を与えると判断できる場合には、ログや通信の監視等の代替策の実施によりリスク低減を図る。

目標とする将来像の決定

事業者へ求めること

左記リスクアセスメントの結果等を踏まえ、サイバーセキュリティ確保のための目標とする将来像を決定する。
現状把握（前スライド参照）と同様に、サイバーセキュリティに関する成熟度を参考とし、自組織が目指すべきサイバーセキュリティ対処態勢を定める。

目標とする将来像の例

- 重大なインシデント発生時に、○○時間以内に経営層までエスカレーションされること
- 資産管理を行い、脆弱性を把握し、適切な脆弱性管理を行うこと
- セキュリティ委員会を常設、定期開催することとし、必ずCISOが参加すること

◆目標とする将来像の考え方における留意点

成熟度をはかる上での参考文書（前スライド）では、様々なセキュリティ管理策が示されているが、幅広く対応することを目的とするのではなく、組織の特性を踏まえて必要な対応を選択することが重要である。

（例）

✓ 従業員が多く、異動等による入れ替わりも多いため、アカウント管理、アクセス制御の定期的な見直しや人的対策を重視する。

✓ 一部の重要サービスについては、運用をグループ組織に委託しているため、脆弱性管理は行わないこととするが、情報共有窓口を明確にして、有事の際の迅速なエスカレーションを重視する。

4. リスクマネジメントの活用と危機管理

国土交通省

ガイドラインの記載内容

【サイバーセキュリティリスク対応】

- ✓ 自組織にとって必要なセキュリティ管理策を実践するためには、組織の状況・特性に鑑み、また日々の**セキュリティ運用状況**に応じて適切に**リスクアセスメント**を行う必要がある。
- ✓ **システム運用中**においても、新たな脅威の発生等の環境変化に応じて、適宜リスクアセスメントを実施し、**リスクの特定・分析・評価**を行うことが望まれる。

サイバーセキュリティリスク対応

事業者へ求めること

前スライドの、目標とする将来像と現状の実態とのギャップを埋めるためのセキュリティ管理策を検討し、優先順位付けを行う

個別方針の策定

- ❒ 実施すべきセキュリティ管理策について、遵守すべき行為や判断等の基準を個別方針（アクセス制御方針、情報分類方針等）としてとりまとめ、関係者へ伝達する。

リスク対応計画の策定

- ❒ とりまとめた個別方針に基づき、サイバーセキュリティの達成目標を定めて、ロードマップ及び詳細化したリスク対応計画を作成し、サイバーセキュリティに係る取組を進める。

リスク対応計画に記載することが望ましい項目
- ✓ 実施事項
- ✓ 必要な資源（予算、人員）
- ✓ 責任者（策定した方針の実行責任者）
- ✓ 達成期限
- ✓ 結果の評価方法

現状のサイバーセキュリティ対処態勢の実態の例

- ❒ 情報システム部の課長がセキュリティ対策に関する責任者を兼任している。
- ❒ 従業員が業務上便利だからとクラウドサービスを自由に利用している。
- ❒ 標的型メール訓練を行ったときに、ダミーのメールを開いてしまった従業員の割合が20%。報告率が40%である。
- ❒ 前の部署で使用していた業務フォルダに、今でもアクセスすることがある。

目標とする将来像

現状に対して、目標とする将来像の設定の例

- ❒ 執行役員として専任でCISOを任命し、定期的な経営会議においてサイバーセキュリティを付議する。
- ❒ 情報資産を棚卸し、定期的に見直し、シャドーIT*を防止する。
- ❒ 標的型メール訓練を行ったときの、ダミーメール開封率5%、報告率100%を目標とする。
- ❒ 人事異動や退職時に、不要なアクセス権を適切に削除するよう、アカウント管理、アクセス制御ポリシーの運用体制を整備する。

*企業・組織側が把握せずに従業員または部門が業務に利用しているデバイスやクラウドサービスなどの情報技術

4. リスクマネジメントの活用と危機管理

国土交通省

ガイドラインの記載内容

【サプライチェーンリスクマネジメント】

✓ 直接の供給者を対象に、**事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化**する。

【情報共有】

✓ **サイバー攻撃被害とその被害に関連する情報**、その他の重要インフラ事業者等に影響を及ぼすおそれのある**システム不具合に関する情報等**を**関係主体と共有すること**が望ましい。

サプライチェーンリスクマネジメント

事業者へ求めること

法務部等と連携し、条項を検討の上、供給者との契約に含めることが望ましい。

サプライヤーへの要求事項、仕様書の記載例

❒ 委託先のサプライチェーン・リスクに係る管理体制が適切であることを確認するために必要な情報を、委託先に提示させる。

（仕様書の記載例）

受注者は、資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提示すること。

❒ サプライチェーン・リスクに係るセキュリティインシデントを認知した場合に、委託先の作業プロセス又は成果物を立入検査等で確認する。

（仕様書の記載例）

再委託を行う場合は、再委託先において意図せざる変更が加えられないための管理体制について発注者の確認（立入調査）を随時受け入れること。

代表的なサプライチェーンに係る脅威への対策も検討する。

（例）

- 委託先の管理不良による機密情報の意図しない公開
  （対策例：機密情報への厳格なアクセス制御の徹底）
- 成熟度の高くないグループ組織や取引先を経由したサイバー攻撃
  （対策例：なりすましを防ぐための多要素認証の仕組みの導入）

情報共有

事業者へ求めること

情報共有の取組については、重要インフラのサイバーセキュリティに係る行動計画に従い、「行動計画に基づく手引書」を参照し実施すること（次スライド参照）。

国土交通省への情報連絡を要するケース

❒ 法令等で国土交通省への報告が義務付けられている場合
❒ 国民生活や重要インフラサービスに深刻な影響があると判断され、重要インフラ事業者等が情報共有を行うことが適切と判断した場合
❒ 上記に該当するかどうか不明な場合については、国土交通省に相談することが望ましい。

情報共有活動

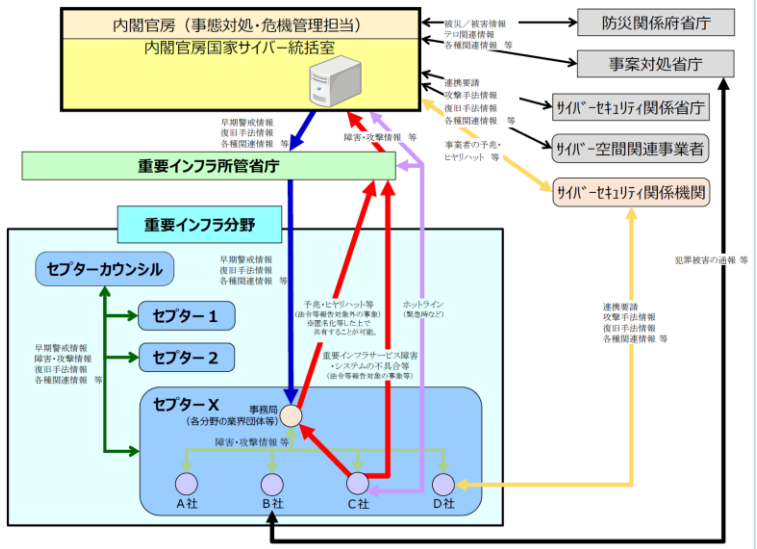
❒ 交通ISAC等の分野専門性の高い情報共有活動に参加し、情報収集することが望ましい。
❒ NCO「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有手引書」及び「サイバー被害に係る情報の共有・公表ガイダンス」を踏まえ、組織内外と情報共有を実施する（次スライド参照）。

4. リスクマネジメントの活用と危機管理

国土交通省

「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有手引書より抜粋

別紙４－２　情報共有体制(大規模重要インフラサービス障害対応時)

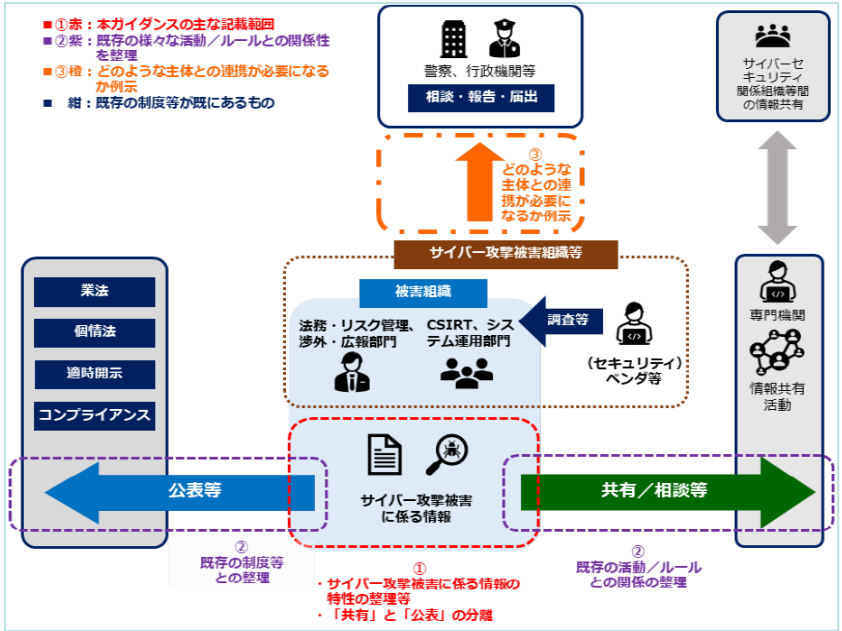


別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における[注]各関係主体の役割
○ 内閣官房（事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、国家サイバー統括室と相互に情報の共有を行う。	通常時の役割に加え、国家サイバー統括室と一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、国家サイバー統括室と相互に情報の共有を行う。
○ 内閣官房（国家サイバー統括室）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報を国家サイバー統括室及び必要に応じ該当するセプターに連絡する。国家サイバー統括室から受領したシステムの不具合等に関する情報を該当するセプターに提供する。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。
○ セプターカウンシル	セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。 主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。
○ セプター事務局	重要インフラ所管省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。
○ 重要インフラ事業者等	システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、「別添：情報連絡・情報提供について」に基づき重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。

注　災害やテロ等に起因する大規模重要インフラサービス障害が発生した場合、当該緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）に基づき、関係府省庁間で情報を集約及び共有する。

サイバー攻撃被害に係る情報の共有・公表ガイダンスより抜粋



情報共有と被害公表における情報の種類のチェックリスト（簡易版）

	情報共有	被害公表
タイミング	可能な限り早期のタイミング	ケースバイケース ※二次被害発生のおそれなど注意喚起を目的とする速報が必要な場合はただちに公表
被害内容・対応情報 ・被害組織名 ・被害業種／規模 ・被害内容 ・対応のタイムライン	―	○
中間の情報 ・攻撃のタイムライン ・攻撃対象システムについて ・脆弱性悪用の情報等	△ ※共有に必要なものは専門機関への相談等を踏まえて共有することが望ましい	○
攻撃技術情報 ・マルウェア ・不正通信先 ・その他攻撃手法に関する情報	○	△

○：主な内容となる情報　　△：内容／状況による　　―：基本的に対象外

4. リスクマネジメントの活用と危機管理

国土交通省

ガイドラインの記載内容

【人材育成・意識啓発】

✓ **「サイバーセキュリティは全員参加（Cybersecurity for All）」**との考え方のもと、全ての従業員がサイバーセキュリティの内規等への理解を深め、また、部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、**人材育成・意識啓発**を行う。

【CSIRT等の整備】

✓ サイバーセキュリティに関するインシデント対応のため、**CSIRT（又は同等機能を持つ組織）を重要インフラ事業者等内に整備し、役割分担、対応手順等について関連部門と合意しておく**ことが望まれる。

人材育成・意識啓発

事業者へ求めること

以下に例示する事項を実施することが望ましい。

人材育成において実施することが望ましい具体例

- ❒ 組織の全ての従業員を対象としたトレーニングを年1回以上実施する。フィッシング、ビジネスメール詐欺、パスワードセキュリティなど基本的な概念を網羅し、組織内での文化醸成に努める。
- ❒ セキュリティ対策が不十分であった場合の影響例を示すなど、セキュリティ対策の重要性について啓発を行う。
- ❒ セキュリティ対策業務に従事する人材に対する「情報処理安全確保支援士」等の資格取得の推進
- ❒ 制御システムに関するセキュリティ人材に対する、ICSCoE*による中核人材育成プログラムの活用の検討

*ICSCoE：IPA産業サイバーセキュリティセンター

CSIRT等の整備

事業者へ求めること

最高情報セキュリティ責任者は、セキュリティインシデントに備えた体制の整備を行うこと。

具体例

- ❒ CSIRT等は、役割分担や対応手順を関連部門と合意する。
- ❒ セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと。
- ❒ セキュリティインシデントが発生した際、直ちに報告が行われる体制を整備すること。
- ❒ 制御システムを保有する場合には、制御システム関連部門とも連携できる体制を整備することが望ましい

5. 対策項目（組織的対策）

国土交通省

ガイドラインの記載内容

【マルウェアからの保護】

✓ **マルウェアに感染した情報システム**は、他への再感染を引き起こす可能性のほか、サービス不能攻撃等の踏み台として利用される危険性など、**他者に対するセキュリティ脅威の原因となりうる**ため、**マルウェア対策を実施することが重要**である。

【バックアップ】

✓ 緊急事態が発生した際には、**必要なデータの欠落や不整合による障害**が発生するおそれがある。これらを防ぐための**詳細な復帰計画をあらかじめ策定**しておくことが重要である。

マルウェアからの保護

事業者へ求めること

システム管理者は、マルウェア感染の回避を目的とし、以下の留意事項を含む日常的実施事項を定めることが望まれる。

マルウェア対策における具体例

- ❒ マルウェアに関する情報の収集に努める。特段の対処が必要な場合には、対処の実施に関する指示を行うこと。
- ❒ 速やかなパッチ適用による脆弱性対策を講じること。
- ❒ サーバ装置、端末及び想定されるマルウェアの感染経路に対するマルウェア対策ソフトウェア等の導入
- ❒ マクロ等の埋め込みコードの実行を既定で無効とする。業務においてコードを実行する必要がある場合、許可されたユーザが特定の状況で実行できることを承認する仕組みを構築すること。
- ❒ ネットワークセグメントの分割、IPS/プロキシサーバ、EDR*等を導入すること。
- ❒ ベンダーなどとの関係者との協力関係の構築
- ❒ 攻撃が発覚した際には所管省庁や警察へ連絡し、逐次時系列で状況を保存できる体制構築

*Endpoint Detection and Response
PCやサーバといったエンドポイント（端末）におけるインシデント発生後の対応を、明確化・迅速化する機能を持つセキュリティ製品

バックアップ

事業者へ求めること

必要な情報のバックアップを取得し、バックアップ元と先が同時に被災しないように保存する。

バックアップにおいて考慮することが望まれる具体例

- ❒ バックアップ稼働・切り替え計画、復帰計画の策定
- ❒ バックアップを保存する媒体の種類
- ❒ バックアップの頻度、世代管理の方法
- ❒ 使用するバックアップツール
- ❒ **定期的なバックアップリカバリー検査の実施**
- ❒ 運用に必要なシステムについて、**年1回以上の定期的なバックアップを実施**する。

5. 対策項目（人的／物理的対策）

国土交通省

ガイドラインの記載内容

【リモートアクセス管理】

✓ 「リモート環境の不正利用」「接続されたサーバ、端末、通信回線装置等への不正アクセス」「リモート環境で取り扱う情報のセキュリティ低下」といったリスクを踏まえ、**リモートアクセス環境導入に関する対策基準**を定める

【セキュリティ確保が求められる領域】

✓ 重要情報システムがある領域を保護するため、**セキュリティ境界を定めた物理的保護対策**が求められる。

リモートアクセス環境（人的対策）

事業者へ求めること

システム管理者は、リモートアクセス環境をテレワークに適用する場合には、以降の事項を含む対策を講ずることが望ましい。

具体例

❒ リモートアクセス元で利用する無線LANルータ等の機器について、ファームウェアを最新版にするよう周知する。

❒ 無線LANルータ等の機器を利用する場合は、適切なセキュリティ方式（WPA2、WPA3等）や第三者に推測されにくいパスワードを利用するよう周知する。

❒ 以下に例示するトピックについて方針を定め、従業員が遠隔作業している場合のセキュリティ対策を実施すること。

- リモートアクセスの申請手続の整備
- 通信内容の暗号化
- 主体認証ログの取得及び管理
- リモートワイプ*の仕組みの導入

*パソコンやモバイル機器等の端末の、紛失や盗難の際に、遠隔操作で端末内のデータを全て消去すること

セキュリティ確保が求められる領域（物理的対策）

事業者へ求めること

セキュリティの保たれた領域（要管理対策区域）に、以下に例示する対策を講ずることが望ましい。

職員の入退室管理

❒ 要管理対策区域への全ての者の入退出を記録・管理し、立入りは業務上必要な者に限定すること。
（例：入室／退室共にIDカード等による認証を行い、時刻を記録する）

❒ 立入りに際しては、本人認証や責任者による事前承認などの管理を実施すること。
（例：生体認証等の信頼度の高い本人確認を行う）

❒ 立入りを許可された者については随時見直し、入室が不要となった者については、速やかに登録許可を解除すること。
（例：異動、退職により入室が不要となった者の登録削除）

訪問者及び受渡業者の管理

❒ 許可されていない者の入室手続きを定めること。
（例：従業員が必ず帯同すること）

❒ 情報システムに関連する機器の要管理対策区域への持込み及び要管理対策区域からの持出には、システム管理者の承認を求めること。

❒ 情報システムに関連する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行うこと。

5. 対策項目（技術的対策）

国土交通省

ガイドラインの記載内容

【情報システム等のアクセス制御】

✓ 認証を許可された者が情報システムを利用できる仕組みに加え、**どの情報にアクセスすることが可能なのかを情報ごとにアクセス制御**することも重要である。認証機能が実装されていない制御システム等においては、専用端末を設けるなど、利用場所の限定、利用者管理等の代替措置を取る。

【多層防御】

✓ 従来型の境界防御のみでは、侵入検知が困難であるため、複数の対策を組み合わせる**「多層防御」**の考え方のもと、セキュリティ対策を検討することが重要である。

情報システム等のアクセス制御

事業者へ求めること

各重要システムについて、アクセス制御を行う必要性の有無を検討し、アクセス制御を行う機能を設けることが重要である。

具体例

- ❒ 同一主体による複数アクセスの制限
- ❒ IP アドレスによる端末の制限
- ❒ ネットワークセグメントの分割によるアクセス制御
- ❒ 公開サーバなど、インターネット上の資産では、悪用可能なサービス（RDP、SSH、SMB* 等）を使用しない。また、インターネットに接続された情報資産では、不要なアプリケーションやネットワークプロトコルを全て無効化する。
- ❒ 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する。

* RDP（Remote Desktop Protocol）
→ コンピュータをリモートで使用するための技術
SSH（Secure Shell）
→ コンピュータやネットワーク装置をリモートで使用するための技術
SMB（Server Massage Block）
→ 主にWindowsの環境で、ネットワークを介してファイル共有を行う技術

多層防御

事業者へ求めること

重要業務を行う端末、ネットワーク、システム又はサービスには、多層防御を導入することが望ましい。

入口対策

- ❒ 不要なサービスについて機能を削除又は停止する。
- ❒ 不審なプログラムが実行されないよう設定する。
- ❒ パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

内部対策

- ❒ 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。
- ❒ 不要な管理者権限アカウントを削除する。
- ❒ 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。
- ❒ EDR等によるソフトウェアの挙動監視により未知のマルウェア等を検知する。

5. 対策項目（その他）

国土交通省

ガイドラインの記載内容

【クラウドサービス】

✓ インターネットを介したサービス（クラウドサービス等）を活用する際には、**国内外の法令や評価制度等の存在について留意**し、データの適切な保護を始めとした望ましい**データ管理**を行うこと。

【委託先管理】

✓ サイバー空間からの脅威（リスク）は、自組織のみでリスク対応をしていても、外部委託先等を経由して間接的に顕在化するおそれがあることから、**外部委託先に係る管理、責任分界点の明確化など、重要インフラサービス障害発生時の対処態勢等を整備する。**

クラウドサービス

事業者へ求めること

利用者が制御できない環境や領域が存在するクラウドサービスでは、クラウド事業者の作業によってインシデントが発生する場合がある。クラウド事業者が開示する情報の把握や変更管理などを適切に行うことが望ましい。

クラウドサービスを利用する際の考慮事項 例

- ❒ 脆弱性対策の実施内容を確認できる
- ❒ 情報の暗号化が確認できる（保存データ及び通信回線の暗号化）
- ❒ 情報の確実な削除・廃棄が確認できる

インシデント発生時

クラウドサービス利用において、インシデント発生時に、関連するステークホルダーとの連携が行える体制を整備することが望ましい。

- ❒ （サイバー攻撃を検知した場合）
- ❒ 影響範囲に応じてシステムの停止も検討する
- ❒ 顧客、構築ベンダー、クラウド事業者の窓口への情報共有
- ❒ 監督官庁への報告*
  （脆弱性や設定不備の場合）
- ❒ クラウド事業者の最新のサポート（サービス）情報の確認する
- ❒ ゼロデイ攻撃のリスクがある新たな脆弱性の場合には、緩和策や回避策を確認し、組織内での対応を検討できる体制

委託先管理

事業者へ求めること

委託先の選定の際や、委託先への要求事項を整備する際、以下を参考とすること。

業務委託（共通事項）

- ❒ セキュリティインシデント発生時の対処方法や体制報告
- ❒ 業務委託終了時の対策（情報が返却、破棄又は抹消されたことの確認等）
- ❒ 監査の受け入れやサービス品質の保証
- ❒ セキュリティ脅威に対処するための継続的なリスク評価

情報システムに関する業務委託

- ❒ 委託先に提供する情報を必要最低限とし、情報の格付けに従って、適切なセキュリティ管理策を講ずること。
- ❒ 委託先によって情報システムに意図しない変更が加えられないための対策
- ❒ 情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策

用語集

国土交通省

用語	定義
重要インフラ事業者等	サイバーセキュリティ基本法第12条第2項第3号に規定する重要社会基盤事業者等であり、具体的には、重要インフラ事業者及びその組織する団体並びに地方公共団体から構成される。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じることをいう。
重要インフラ利用者	重要インフラ事業者等が提供する重要インフラのサービスを利用する者をいう。
取扱者	重要インフラ事業者等が保有する重要インフラに関する情報システム及び情報資産を取り扱う重要インフラ事業関係者（情報資産や情報システムを直接扱う者を監督する立場にある者（経営層や幹部など）、委託先の関係者などを含む）をいう。
情報システム	ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいう。サーバ装置、端末、通信回線装置、複合機、IoT機器を含む特定用途機器（フィールド機器や監視・制御システム等の制御システム等で使われるものを含む。）、ソフトウェアが含まれる。
制御システム	鉄道インフラの重要システムである列車運行管理システム等において、信号や踏切を制御するための機械や設備があり、それを制御する端末及び、列車運行管理システム等とネットワークで接続されている機械や設備、その構成要素を指す。
情報資産	以下の2つの情報をいう。 ・ 取扱者が業務上使用することを目的 として重要インフラ事業者等が調達し、又は開発した情報システム若しくは 外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。） ・ 重要インフラ事業者等が調達し、又は開発した情報システムの設計又は運用管理に関する情報
任務保証	重要インフラ事業者等や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方をいう。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。広義では海外拠点やグループ会社、関連団体も含められる。 これらに加えてさらに、ITにおけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略称(CEPTOAR)。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
IT-BCP等	重要インフラサービスの提供に必要な情報システムに関する事業継続計画（関連マニュアル類を含む。）その他の事業継続計画。
コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。

鉄道分野特性から求められる取組の例（1/2）

国土交通省

《鉄道制御に係る制御システムについて》
列車運行管理システム・電力管理システムは原則、**クローズドな環境で構築**されている。

《マルウェア対策等》
鉄道重要システムでは**OSのバージョンアップを前提とせずに構築されているものがある**ため、脆弱性への対応を行うためのバージョンアップやパッチ適用の実施にあたっては、**事前の検証を含めた計画**をたてる必要がある。
また、マルウェア対策ソフトウェア等においても、**誤検知・誤動作**等を起こし、**安全安心輸送に支障をきたす可能性**がある。脆弱性対応やマルウェア対策を実施する際は慎重に検討する必要がある。

列車運行管理システム

電力管理システム

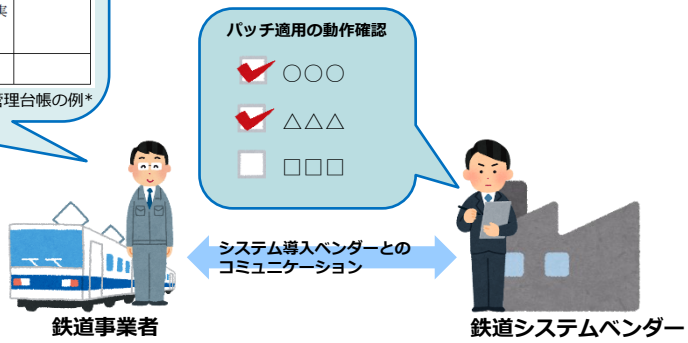
マルウェア対策ソフトの導入やパッチの適用を実施せず、運用による対処を行うという判断が必要な場合がある。

公表される脆弱性情報などについて、システムに対する深刻度パッチ適用の可否・適用時期・適用状況等を整理し、脆弱性管理を実施するのが望ましい。パッチ適用の判断にあたっては、システム導入ベンダーと協議し、事前に検証を行うといった方法が考えられる。

#	関連資産	脆弱性(CVE IDなど)	深刻度(CVSSなど)	パッチ適用可否	パッチ適用時期	パッチ適用状況
1	XXX	CVE XX	大	可	即時	済
2	XXX	CVE YY	小	可	保守に合わせて実施	未適用
3		…				

脆弱性管理台帳の例*

・システムに関する脆弱性を管理
パッチ適用の状況や、
パッチの適用を見送る判断をした際のリスクへの対応方針を定め、運用する



* IPA:スマート工場化でのシステムセキュリティ対策事例調査報告書より抜粋

鉄道分野特性から求められる取組の例（2/2）

《重要システムとのネットワーク境界について》
鉄道インフラの重要システムである列車運行管理システムは、**外部と通信をしないクローズドな環境で運用されることが一般的**である。利用者向けアプリへのリアルタイム情報通知（列車走行位置、遅延、種別等）といった**顧客サービスの品質向上や、オフィスエリアからの稼働状況のモニタリング等**の理由により、列車運行管理システムの一部を外部ネットワークと接続する必要がある場合には、**外部から重要システム側のネットワークへの侵入を防ぐための措置**を講じる。

**重要システムネットワークの情報を活用する必要がある場合には、
片方向通信制御等を活用し、列車運行管理システムが稼働するネットワークに対して、
一切送信ができない環境を構築することが望ましい**

列車運行管理システム等
の重要システム群

情報集約
サーバ

**片方向通信
制御装置**

通信可能

通信不可

●顧客サービス例
アプリへのリアルタイム情報通知
（遅延・列車位置等）

●システムの稼働状況の
モニタリング

重要システムネットワーク

サービス提供／
オフィスネットワーク