港湾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 港湾局
海岸・防災課　危機管理室
令和７年３月

目　次

安全ガイドラインについて

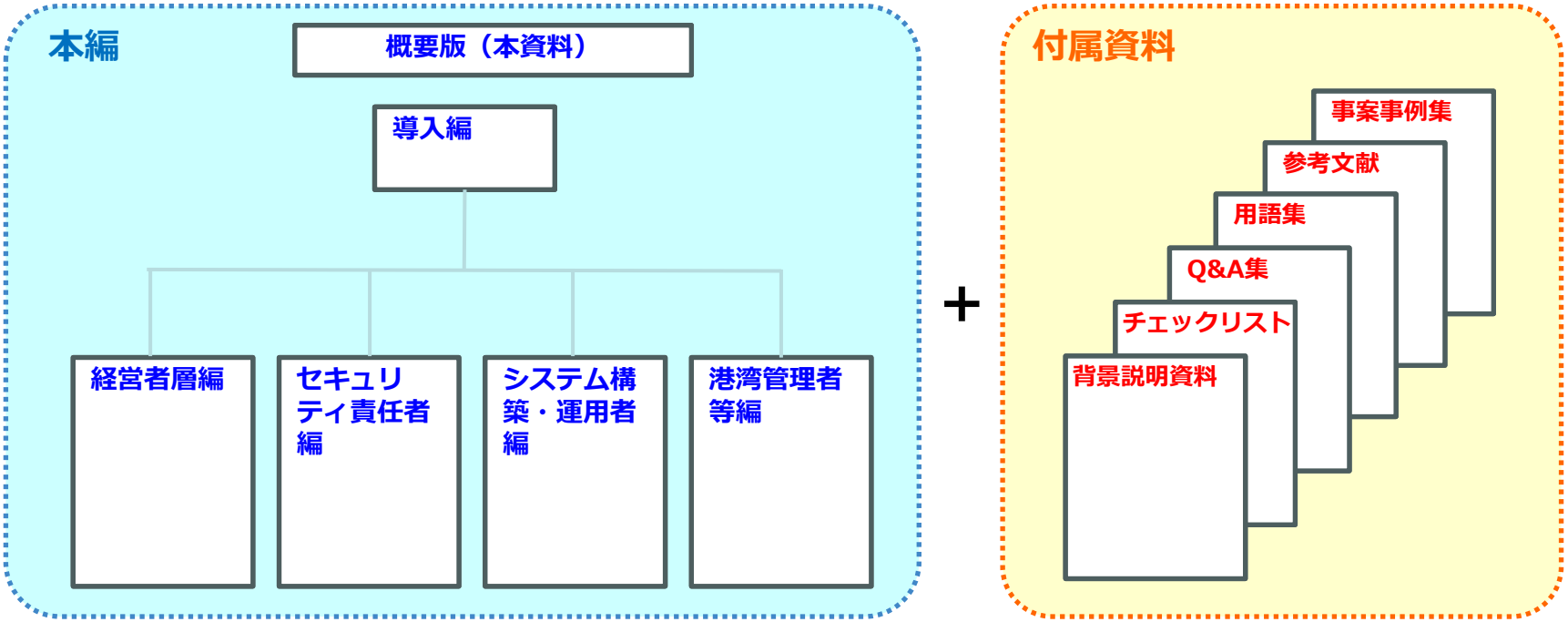
- 本ガイドラインは、令和６年４月に策定しました「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第１版）」を、その後の港湾を取り巻く環境の変化等を踏まえて、**「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第２版）」として改訂**したものです。
- また、本ガイドラインは、関係法令に準じて国が定める「ガイドライン」として、（強制要件ではなく）**推奨事項を列挙**しているものであり、事業分野の特性に鑑み、重要インフラ事業者等をはじめ、全国の港湾関係事業者等の皆様に、**自らのセキュリティ対策を実施する際の参考資料として活用することを想定**しています。
- ただし、本ガイドラインに掲載の一部の項目については、**港湾運送事業法に基づき、一定の一般港湾運送事業を営む際の事業計画において遵守すべき事項**とされている項目もありますので、法令等の遵守に当たり遺漏のないようにお願いします。
- 本ガイドラインの本文は、「導入編」、「経営者層編」、「セキュリティ責任者編」、「システム構築・運用者編」、「港湾管理者等編」の５編に分けるとともに、チェックリストやＱ＆Ａ等の付属資料によって構成されており、**各編で想定する読者それぞれの目的に応じて、どの部分を読めばいいのかがわかるように構成を見直し**ています。
- 本概要版のＰ６「はじめに～」からＰ24の「５．対策項目」においては、**本ガイドライン全体の構成を理解していただく観点**から、**第１版時の目次構成を基本に、第２版の各編との関係性（どこに記載があるのかなど）がわかるように整理**しています。

安全ガイドラインの資料構成

国土交通省

- ✓ 本編と付属資料で構成しています。
- ✓ 本編は、導入編、経営者層編、セキュリティ責任者編、システム構築・運用者編、港湾管理者等編で構成しています。
- ✓ 付属資料は、背景説明資料、チェックリスト、Q&A集、用語集、参考文献、事案事例集で構成しています。

第2版の文書構成



安全ガイドラインの目次構成（1）

国土交通省

・本表では、重要インフラ事業者等が実施する各対策について、どの段階で実施することが望ましいかを「事前準備」「平時対策」「インシデント発生時及び事後対応」に分類したうえで、分冊化した各編の記載箇所との関係を整理しています。
・分冊化によって組織内の役割として担当すべき部分を明確にすることは可能になりますが、必ずしも各自の担当する部分のみを読んで理解するのではなく、本表において●印の記載のある項目は、合わせて理解しておくことが望ましいと考えています。

凡例　各読み手の分冊で記載している項目（数字は章・節）
●●「導入編」別紙を参照し、理解しておくことが望ましい項目

本ガイドラインでの主な対策項目			経営者層	セキュリティ責任者	システム構築・運用者
事前準備	方針	• サイバーセキュリティ確保に関する事項の組織方針への組み入れ、サイバーセキュリティ方針を内外に対して宣言	1.1	●	
	体制構築	• セキュリティリスクのリスク評価・管理体制の構築（サイバー保険への加入検討含む）	1.2		
	リスクの識別	• 自組織のサイバーセキュリティ対処態勢の実態把握、外部からの要求事項の整理、自組織の重要インフラサービス継続に係る特性の理解（コンテナ荷役等の停止が経済社会に与える影響、サービス継続に係るシステム機能等）		1.1	
		• システムの機器構成、ネットワーク構成、外部との接続状況等の資産の特定・管理		1.2.1	●
		• セキュリティ対策の運用に関するリスクアセスメントの実施、目標とする将来像の設定		1.2.2～1.2.3	
	対応策の検討・立案	• 将来像と実態とのギャップを埋めるための対策方針の検討、対策の優先順位付け		1.3.2	
		• 対策方針に基づいたリスク対応計画の策定（実施事項、ロードマップ、責任者等）		1.3.3～1.3.5	●
		• 外部委託に伴うサプライチェーン・リスクへの対応検討（事業者間の契約において担うべき役割と責任範囲の明確化）		1.4	●
		• 情報の形態及び格付けに応じた通信セキュリティの確保（ネットワークの分離、暗号技術の活用、ログ監視等）		1.5	●
		• クラウドサービス活用時のセキュリティ要件の確認、契約条項へのセキュリティ要件の盛り込み		1.6	●
		• システムの外部委託先のセキュリティ要件の確認、契約条項へのセキュリティ要件の盛り込み		1.7	●
	インシデント対応	• インシデント発生時の対応手順等を定めた「初動対応計画（コンティンジェンシープラン）」の策定		1.8.1	●
		• 事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP）」等の策定		1.8.2	●
		• インシデントに備えた対処体制の整備（CSIRT（Computer Security Incident Response Team）等）		1.9.1	●
		• インシデント発生時の自組織内の連絡体制の整備（エスカレーション）		1.9.3	●
	物理的保護	• 機器の物理的保護策（免震・耐震設備、非常電源装置等）		●	1.2
	テレワーク	• リモートアクセス環境をテレワークに利用する際の対策基準の策定		●	1.3
平時対策	コミュニケーション	• セキュリティリスク、インシデント等に関する組織内外とのコミュニケーションの推進	2.1	●	
	担当者指名	• セキュリティリスクの管理に関する組織体制の確立、最高情報セキュリティ責任者の任命、担当者の役割・権限の割当て	2.2		
	リソース確保	• 必要となる予算・体制・人材等の継続的確保	2.3		
	監査体制確保	• セキュリティ対策の運用状況の監査・モニタリング体制の確保（外部監査含む）	2.4	●	
	セキュリティ対策の運用管理	• サイバー攻撃等の予兆把握のため平時からのセキュリティ対策の運用管理（機器のログ確認等）		2.1.1	●
		• サイバー攻撃等の予兆を認識した場合、現在の対策で対処可能か確認し、必要に応じて対策の見直し		2.1.2	
		• セキュリティ関連情報の情報収集体制の確立・実施（関係者（専門家含む）との定期的な情報共有等）		2.1.3	
		• 情報漏洩を防止するための適切な従業員の管理（守秘義務の徹底等）、要管理区域の入退出管理		2.1.4	
		• セキュリティ管理策のモニタリング、自己点検、監査の実施、セキュリティ管理策の継続的改善		2.4	
	教育・訓練	• 全従業員に対するサイバーセキュリティに関連する意識啓発・教育		2.2	
		• インシデント対応等の演習・訓練の定期的な実施		2.3	
	モニタリング・監査	• セキュリティ管理策のモニタリング、自己点検、監査の実施、セキュリティ管理策の継続的改善		2.4	
	防御策の実装	• ネットワーク機器、サーバ機器への不正アクセス対策（接続元IPアドレス指定、主体認証機能、複雑なパスワード等）		●	2.1
		• 情報システムのアクセス制御（専用端末の設置、利用場所の限定、アカウントロック機能、専用線接続の場合の対応等）		●	2.2
		• 暗号を活用した情報管理（暗号化機能、電子署名等）		●	2.3
		• システムの負荷分散・冗長化対策、多層防護の導入		●	2.4～2.5
	防御策の運用	• サーバ機器、端末等の資産のセキュリティ運用の実施（機器の変更・更新・廃棄管理、廃棄管理機器、端末の不正運用等の定期的なチェック、適切なデータ保管・管理等）		●	2.6
		• 日常的なマルウェア対策の実施（ネットワーク機器のソフトウェアの確実な更新、通信記録等のログ取得、USBメモリ等外部記憶媒体の取扱いルール、ウイルス対策ソフトの導入・定期的更新、バックアップ保存等）		●	2.7
インシデント発生時及び事後対応	情報開示体制	• インシデント発生時の対応等の情報開示の取組み	3.1	●	
	プラン実行	• インシデント発生時のコンティンジェンシープランの実行（証拠保全、被害の拡大防止、システム障害復旧、原因調査等）	3.2	3.1	3.1
		• 事業継続計画、事業復旧計画の実行	3.2	3.1	●
	関係者との情報共有	• インシデント発生時の関係者との情報共有（自組織内、セキュリティ専門組織、国・港湾管理者、都道府県警察等）		3.2	
	対外説明	• セキュリティ管理状況の対外説明（障害の状況、復旧状況等）		3.3	
	原因究明	• インシデントの原因究明、インシデントで得た教訓等の対策への反映		3.4	●

安全ガイドラインの目次構成（2）

国土交通省

第2版では、新たに「港湾管理者編」を追加。

はじめに ～ 1.「安全ガイドライン」策定の背景（1）

- 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、機能が停止また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ります。
- 国土交通省では、所管する**重要インフラ５分野（鉄道、航空、空港、物流、水道）**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、**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**することとしています。

「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　等

<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

サイバーセキュリティ戦略本部決定の「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
- 事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に**参考資料として活用することを想定**

1.「安全ガイドライン」策定の背景（2）

策定の背景

○「重要インフラのサイバーセキュリティに係る行動計画」（令和6年3月8日サイバーセキュリティ戦略本部改定）

- ✓ 重要インフラにおいて、任務保証の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとするサイバー攻撃等をリスクとして捉え、リスクを許容範囲内に抑制すること及び障害発生時に迅速な復旧を図ることの両面から、強靭性を確保し、重要インフラサービスの安全かつ持続的な提供を実現すること（重要インフラ防護の目的）

○「重要インフラのサイバーセキュリティ確保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）

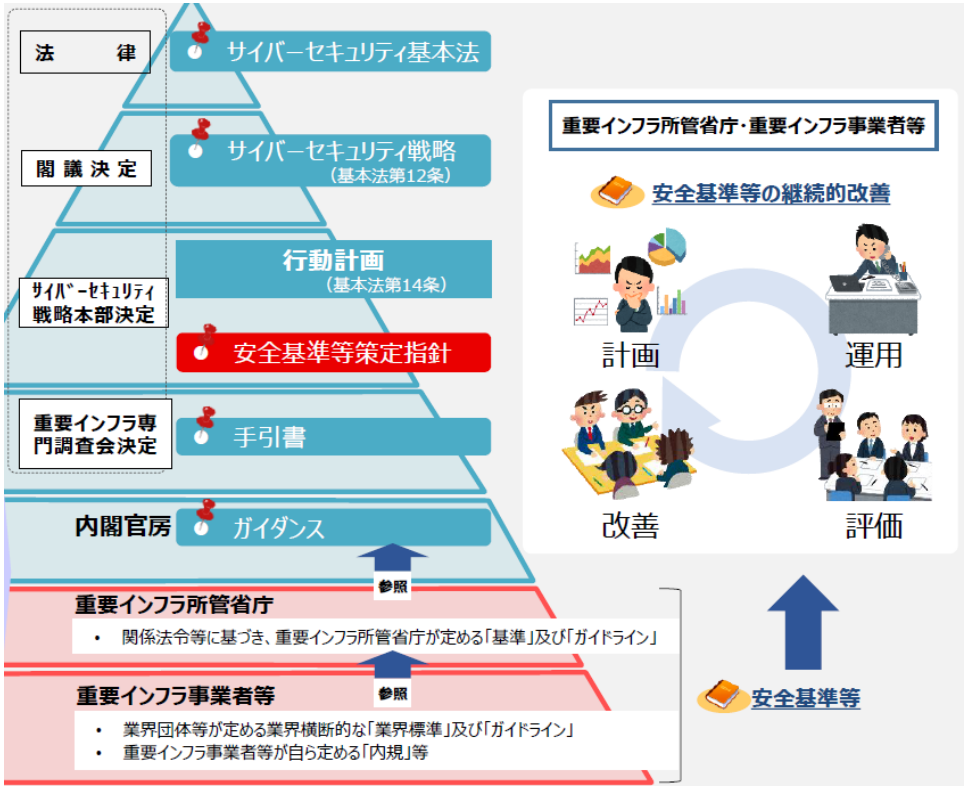
- ✓ 上記行動計画の内容を踏まえ、経営層の責務としてのセキュリティガバナンスや、サプライチェーンを含むリスクマネジメントにおけるサイバーセキュリティ確保、リスクアセスメントを行う際の考慮事項等を整理
- ✓ 構成面では、経営層が取り組む事項とセキュリティ責任者が取り組む事項でそれぞれの項目を作成し、ISO/IEC 27002:2022のセキュリティ管理策や昨今のインシデント事例を踏まえ、対策項目を整理するとともに、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」を新規に作成し、策定指針で示すセキュリティ確保に向けた取組についての参考情報を提供

○その他参照規定の改定を反映

- ✓ 「政府機関のサイバーセキュリティ対策のための統一基準群」（令和5年7月4日サイバーセキュリティ戦略本部決定）
- ✓ 「サイバーセキュリティ経営ガイドライン Ver3.0」（令和5年3月24日経済産業省・独立行政法人情報処理推進機構改訂）

1.「安全ガイドライン」策定の背景（3）

- ✓ 港湾運送事業者等は、サイバーセキュリティ基本法が規定する重要インフラ事業者（重要社会基盤事業者）として、「任務保証の考え方」を踏まえ、港湾運送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す。
- ✓ 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や対策を実施し、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ます。



※「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.nisc.go.jp/pdf/policy/infra/cip_policy_abst_2022.pdf

2. 港湾分野における「安全ガイドライン」の概要

～「安全ガイドライン」の対象範囲～

国土交通省

導入編

- ✓ 港湾分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システムは、第一に、コンテナターミナルにおける**ターミナルオペレーションシステム（TOS）**が挙げられます。
- ✓ また、**TOSと同様に、システム停止によるサービス障害が、社会経済活動等に多大な影響を与えるシステムについても、保護対象**となります（重要インフラ事業者等の責任において、当該システムを検討・抽出する必要があります）。
- ✓ 重要インフラ事業者等は、上記のTOS等システムに対して、**外部からのサイバー攻撃**のみならず、**内部犯行や過失、システム障害（自然災害含む）**等を念頭に置き、セキュリティ管理策を実施することが求められます。

港湾分野における主要システム

主要システム	主要な機能
ターミナルオペレーションシステム（TOS）	貨物取扱システム コンテナドキュメント管理システム オペレーションシステム ゲートシステム

港湾分野における重要インフラサービス障害の例

重要インフラサービス	システムの不具合から引き起こす重要インフラサービス障害の例
TOSによるターミナルオペレーション	荷捌きの効率低下、停止によるコンテナ貨物の搬入・搬出の停滞、停止

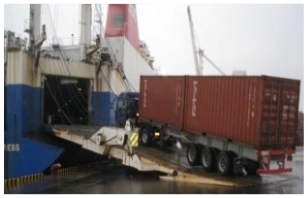
本ガイドラインの対象とするターミナル種類、リスク事象

	外部からのサイバー攻撃	内部犯行、過失、システム障害(自然災害含む)
コンテナターミナル	ガイドラインの対象	
コンテナターミナル以外		

参考：ターミナル種類

（コンテナターミナル）

（フェリー・ROROターミナル）



（バルクターミナル）

3. 組織統治におけるサイバーセキュリティ（1）

国土交通省

経営者層編

～組織方針とサイバーセキュリティ、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

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】

✓ **リスクを許容水準まで低減**することは、重要インフラ事業者等として果たすべき**社会的責任**であり、その実践は**経営層としての責務**です。

【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】

✓ 組織内のガバナンスや内部統制、その他の**リスクマネジメントにおけるコミュニケーションの一部として**、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設けることを求めます。

組織方針とサイバーセキュリティ

事業者へ求めること

経営者層は、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

経営者層の会議等においてサイバーセキュリティリスクを取り扱い、適切にリスク管理することを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（2）

～責任及び権限の割当て情報開示～

国土交通省

経営者層編

ガイドラインの記載内容

【責任及び権限の割当て】

✓ 全ての者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることでサイバーセキュリティは実現されます。そのため、それらの**権限と責務を明確**にし、**必要となる組織・体制を確立**することが望ましい。

✓ 特に、**サイバーセキュリティ責任者や最高情報セキュリティ責任者（CISO）を任命すべき**です。

【情報開示】

✓ 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な範囲で開示**することは、ステークホルダーの信頼・安心感の醸成に繋がります。

責任及び権限の割当て

事業者へ求めること

経営者層は、情報セキュリティ対策の推進の責任者（役員クラスが相当）として最高情報セキュリティ責任者（CISO）を指定するとともに、情報セキュリティ担当者を指定し、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

- ❒ 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

経営者層は、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。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）

3. 組織統治におけるサイバーセキュリティ（3）

～資源の確保、監査・モニタリング～

ガイドラインの記載内容

【資源の確保】

- ✓ 必要な予算・体制・人材等の**経営資源を継続的に確保**し、**リスクを考慮して適切に配分**すること。
- ✓ 十分な資源の確保が難しい場合には、中小企業向けのサイバーセキュリティ対策の導入・運用の支援を目的とした、**サイバーセキュリティお助け隊サービス制度*等の活用を検討**すること。

*https://www.ipa.go.jp/security/sme/otasuketai-about.html

【監査・モニタリング】

- ✓ サイバーセキュリティは、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、**リスクマネジメントとセキュリティ対策が整合する取組となるように留意**すること。
- ✓ セキュリティ対策の実施状況について、**組織による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を定期的に実施**すること。

セキュリティ対策の監査の実施例

<サイバーセキュリティ確保の取組全般に対する内部監査担当者>

- 監査の基本的な方針として、年度情報セキュリティ監査計画を整備
- 監査実施計画を立案し、監査を実施。実際の運用がサイバーセキュリティ関係規程に準拠しているかを確認
- 監査結果については、報告書として文書化

<最高情報セキュリティ責任者*>

- 報告書の内容を踏まえ、指摘事項に対する改善計画の策定等をサイバーセキュリティ責任者に指示

<サイバーセキュリティ責任者>

- 必要な措置を行った上で改善計画を策定
- 措置結果及び改善計画を最高情報セキュリティ責任者に報告

● 情報セキュリティ対策の推進の責任者（役員クラスが相当）として最高情報セキュリティ責任者（CISO）を指定すること。CISO は、情報セキュリティ対策を推進する上での最終決定権及び責任を持つこと

- ✓ 経営者層は、監査の結果等により、目標未達や進捗遅延、セキュリティ管理策の**要改善点等が確認された場合は、改善指示を行うこと。**
- ✓ これらを**繰り返し実施し、サイバーセキュリティの取組の効果を高めること。**

4. リスクマネジメントの活用と危機管理（1）

～組織状況の理解～

ガイドラインの記載内容

【組織状況の理解】

- ✓ 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す。
- ✓ **貨物輸送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**

内部状況・外部状況の理解

事業者へ求めること

情報セキュリティ責任者（CISO等）は、組織内部及び外部の現状をサイバーセキュリティの視点から理解する

内部状況の例

- ❒ 組織体制、経営戦略、セキュリティ方針
- ❒ リスクマネジメント戦略、リスク許容度
- ❒ 貨物輸送サービス等に係る各種システム、データ
- ❒ セキュリティ投資が可能な資源状況
- ❒ リスク分析や対応に必要な技術や人的資源
- ❒ セキュリティリスクに対する、部署や立場による認識の差異
- ❒ 従業員のセキュリティリテラシー

外部状況の例

- ❒ 関連する法令の改正状況（事業法、個人情報保護法等）
- ❒ 所管省庁や規制当局における基準の策定、改正状況
- ❒ 関連団体における基準やガイドラインの策定、改正状況
- ❒ 重要インフラサービスの利用者に与える影響
- ❒ 国内外におけるセキュリティインシデントの発生事例や、その報道等による社会からのセキュリティ認識の広まり
- ❒ 外部取引先との契約における、セキュリティに関する要求事項
- ❒ 任務保証を達成するために必要な他の重要インフラサービス
- ❒ 自組織と他組織の相互依存関係

重要インフラサービス継続に係る特性の理解

事業者へ求めること

情報セキュリティ責任者（CISO等）は、自組織の重要インフラサービス継続に係る特性を理解する

重要インフラサービス継続に係る特性

- ❒ コンテナ荷役等の停止が経済社会に与える影響
- ❒ サービス継続に係る重要なシステムや機能
- ❒ 重要なシステムや機能を支える業務
- ❒ 業務を支える資源及び知識（予算、人員、設備、技術、資産の脆弱性情報）
- ❒ 他の重要インフラとの相互依存関係
- ❒ 貨物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
- ❒ 自動運転、ドローン配送、AGV（無人搬送型ロボット）、AMR（自律走行型ロボット）、その他IoTデバイスの活用などによる、自動化に伴うリスクの増大

重要インフラ事業者等の役割

- ● 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、重要インフラ所管省庁への連絡を行う。なお、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

4. リスクマネジメントの活用と危機管理（2）

～リスクアセスメントの実施、目標とする将来像の設定～

国土交通省

セキュリティ責任者編

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**を実施すること。

✓ **制御システムについても適切にリスクアセスメント**を実施すること。

【目標とする将来像の設定】

✓ リスクアセスメントの結果や、自組織の目標、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、**目標とする将来像を決定**すること。

リスクアセスメントの実施

事業者へ求めること

情報セキュリティ責任者（CISO等）は、組織の状況や特性（前スライド参照）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（次スライド参照）

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

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

情報セキュリティ責任者（CISO等）は、リスクアセスメントの結果や、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

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（3）

～リスクアセスメントの実施～

ガイドラインの記載内容

✓ 具体的なプロセスについては、NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0 版」等を参考にしながら、リスクの特性に応じたリスク分析手法によってリスクを評価すること。

リスクアセスメントプロセス	
①リスクアセスメントの対象の特定	絶えず変化する自組織を取り巻く状況及び関係主体等のニーズを踏まえ、重要インフラサービスの提供に必要な業務の範囲・水準等を明らかにするとともに、当該業務の遂行に必要な情報システム等の経営資源を特定する。また、その過程で自組織のリスクに対する態度・リスク許容度を分析する
②リスク特定	情報システム等の経営資源に対する「サイバーセキュリティリスク」を特定する
③リスク分析	リスクに対する態度・リスク許容度等を考慮しつつ、「事象の結果によるサービス・業務への影響度合い」や「事象の発生可能性」等を評価軸として策定されるリスク基準を活用して、特定されたリスクの大きさを確認する。重要インフラサービスの継続提供を不確かなものとするシナリオを作成し、リスク分析を実施することが望ましい。重要インフラサービスの継続的提供を不確かなものとするリスクとしては、自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化、感染症やテロ・戦争、システム障害、労災・事故、内部不正等があり、リスクの特性に応じたリスク分析手法を選択する
④リスク評価	基準値以上の大きさのリスクを抽出するとともに、個別事情も考慮してリスク対応の対象とするリスクを抽出する

✓ 抽出した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（共有）」、「保有（需要）」のいずれかの具体的な対応を決定すること。

4. リスクマネジメントの活用と危機管理（4）

～サイバーセキュリティリスク対応～

国土交通省

セキュリティ責任者編

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】

- ✓ 環境変化や日々のセキュリティ対策の運用状況に応じて適宜見直さなければ、新たな脅威に対応できません。そのため、**セキュリティ対策の運用においてリスクアセスメント**を行うこと。
- ✓ **システム運用中**も、サイバー攻撃に関する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、**本来あるべき状況や要件を検討・目標とする将来像を決定**することが重要です。

サイバーセキュリティリスク対応

事業者へ求めること

情報セキュリティ責任者（CISO等）は、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

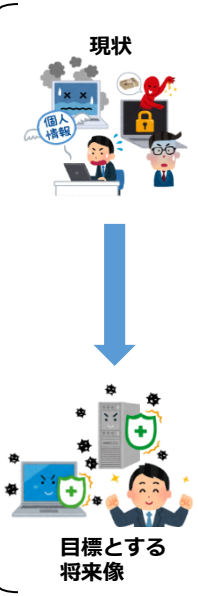
個別方針の策定

❒ 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
- ✓ 目標とする将来像
- ✓ 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%で報告率が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

現状に対して、目標とする将来像の設定の例

❒ 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

サイバーセキュリティに係る取組が自らのサイバーセキュリティに限らない**既存の各種計画等と整合的なものになるようにする**とともに、監査やリスクアセスメント等の**個々の取組を既存の計画等の中に位置付けたり、紐付けたりする**ことを通じて、**サイバーセキュリティに係る取組が持続可能なものとなるように留意**すること

4. リスクマネジメントの活用と危機管理（5）

～サプライチェーンリスクマネジメント、情報共有～

国土交通省

セキュリティ責任者編

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**すること。

【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

情報セキュリティ責任者（CISO等）は、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

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（次スライド参照）
情報セキュリティ責任者（CISO等）は、セキュリティベンダー、セキュリティ専門機関、都道府県警察等と平時から情報交換等を行う

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

予兆・ヒヤリハットや法令等で報告が義務付けられていない事象を国土交通省に報告することで、政府機関からの指導等に繋がるのではないかといった懸念を払拭できず、情報共有の活性化を阻害する一因ともなっていたと考えられることから、重要インフラ事業者等が国土交通省に直接報告する形態に加え、法令等で報告が義務付けられていない事象については、セプター事務局経由で情報連絡元の匿名化等を行った上で国土交通省に報告することも可能としている

4. リスクマネジメントの活用と危機管理（6）

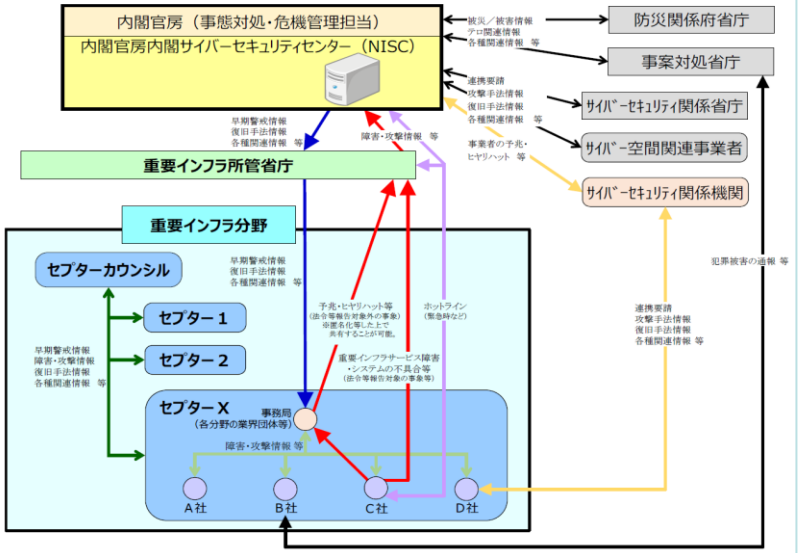
～情報共有～

国土交通省

セキュリティ責任者編

「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)

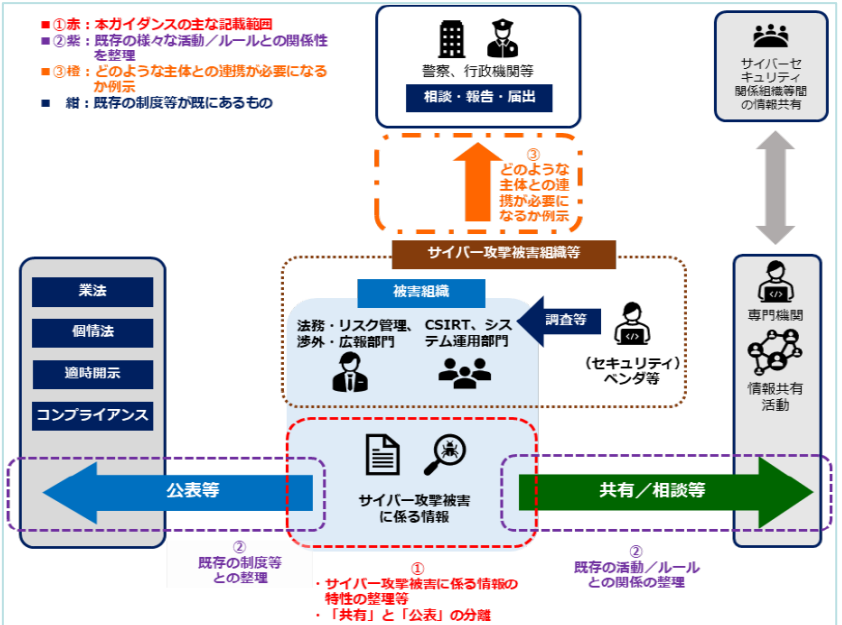


別紙４－３　情報共有体制における各関係主体の役割

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、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣ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、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房（ＮＩＳＣ）	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ＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣ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（7）

～人材育成・意識啓発、CSIRT等の整備～

国土交通省

セキュリティ責任者編

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）」**との考え方の下、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**を行います。

【CSIRT等の整備】

✓ **CSIRT（または同等の機能をもつ組織）を重要インフラ事業者等内に整備し、役割分担や対応手順等について、あらかじめ関連部門と合意しておく**ことが重要です。

人材育成・意識啓発

事業者へ求めること

情報セキュリティ責任者（CISO等）は、全ての従業員に対して、サイバーセキュリティに関連する教育・訓練を行うとともに、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

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

情報セキュリティ責任者（CISO等）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。
サイバー攻撃に迅速に対処する観点から、セキュリティ専門機関や都道府県警察等を含めた社内外の対処態勢を平時から整備しておくことが望ましい

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）

～マルウェアからの保護、バックアップ～

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、他への情報システムの再感染を引き起こす可能性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性等、**他者に対するセキュリティ脅威の原因となり得る**。このため、**マルウェア対策を行うことが重要**です。

【バックアップ】

✓ 緊急事態発生時には、通常業務に**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す。

マルウェアからの保護

事業者へ求めること

システム構築・運用者は、マルウェア感染の回避を目的とし、取扱者に対する日常的実施事項を定める。
外部接続するネットワーク機器、及びTOS等ネットワーク内のサーバ機器等に係る適切なマルウェア対策を講じる。
外部記憶媒体（USB）を利用する際には、マルウェア感染回避のための、適切な運用ルールを定め実施する

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

バックアップ

事業者へ求めること

システム構築・運用者は、システム障害やサイバー攻撃発生に備え、バックアップを適切に取得する。
取得したバックアップは、現用システムとは切り離した場所に保存する

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

*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

5. 対策項目（人的／物理的対策）（1）

～リモートアクセス管理、セキュリティ確保が求められる領域～

国土交通省

セキュリティ責任者編　システム構築・運用者編

ガイドラインの記載内容

【リモートアクセス管理】

✓　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**を定める必要があります。

【セキュリティ確保が求められる領域】

✓　情報処理設備を含む領域を保護するために、**セキュリティ境界を明確に定め**、**適切な入退管理策**によって**セキュリティの保たれた領域（要管理対策区域）を保護**することが望ましい。

リモートアクセス環境（人的対策）

事業者へ求めること

システム構築・運用者は、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

情報セキュリティ責任者（CISO等）は、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）

❒ 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（人的／物理的対策）（2）

～利用者アクセスの管理、主体認証機能～

ガイドラインの記載内容

【利用者アクセスの管理】

✓ 外部との接続機器、システム内部の機器については、予め許可された者のみがシステムへの接続が可能となるよう、技術的な安全管理措置を講じる必要があります。

【主体認証機能】

✓ 外部との接続機器、システム内部の機器については、主体認証を行う機能を設ける必要があります。

利用者アクセスの管理

事業者へ求めること

システム構築・運用者は情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、データに対する技術的な安全管理措置を講ずる。
外部との接続に係るVPNルータ等のネットワーク機器については、接続元IPアドレスの指定等予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講ずる。
システム内部のサーバ機器及びネットワーク機器については、管理者用パスワードの適正な管理等予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講ずる

具体例

- ❒ 情報システムや情報等へアクセスする利用者とそのアクセス権を管理する
- ❒ ユーザアカウントに管理権限を割り当てず、管理権限も用途ごとに設定する
- ❒ 離職者のアカウント管理として、全てのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有する全てのユーザアカウントと、組織情報へのアクセスを無効にする
- ❒ 共有アカウントを使用せざるを得ない制御システム等については、セグメントの分割や端末の制限といった対策を活用し、アクセス権を利用する利用者を管理する

主体認証機能

事業者へ求めること

システム構築・運用者は、情報システムについて、情報の格付けに従って、識別及び主体認証を行う機能を設ける。
外部との接続に係るVPNルータ等のネットワーク機器については、外部ユーザに対する主体認証を実施する。
システム内部のサーバ機器及びネットワーク機器については、管理者に対する主体認証を実施する

具体例

- ❒ 知識（パスワード等、利用者本人のみが知り得る情報）による認証
- ❒ 所有（電子証明書を格納するIC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証
- ❒ 生体（指紋や静脈等、本人の生体的な特徴）による認証

5. 対策項目（技術的対策）

～情報システム等のアクセス制御、多層防御～

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】

- ✓ どの主体がどの情報にアクセスすることが可能なのかを**情報毎にアクセス制御**する必要があります。
- ✓ 全ての情報システムについて、**アクセス制御を行う必要性の有無を検討**して、アクセス制御を行う機能を設けることが重要です。

【多層防御】

- ✓ 従来型の境界防御のみでは侵入を検知することが困難であるため、**複数の対策を組み合わせ、一つの対策で防御できなくても次の対策で防御または検知**するという考え方の下、セキュリティ対策を検討することが重要です。

情報システム等のアクセス制御

事業者へ求めること

システム構築・運用者は、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。外部との接続に係るVPNルータ等のネットワーク機器については、アカウントロック機能等により、外部からのアクセスを適切に制御する

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

システム構築・運用者は、重要業務を行う端末、ネットワーク、システムまたはサービスには、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）

～クラウドサービス、委託先管理～

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）等、**新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意**することが重要です。

【委託先管理】

✓ 重要情報の漏えいや不正アクセス等のリスクは、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。このことから、外部委託先に係る管理において、**委託先の適切な選定、責任分界点の明確化、重要インフラサービス障害発生時の対処態勢等を整備**すること。

クラウドサービス

事業者へ求めること

情報セキュリティ責任者（CISO等）は、インターネットを介したサービス（クラウドサービス）を利用する場合には、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
クラウドサービスを利用してTOS等の機能を実現している場合においても、マルウェアからの保護や不正アクセス対策を実施するとともに、情報保管管理等のセキュリティ要件をクラウドサービスに求め、契約内容にも含める

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

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

情報セキュリティ責任者（CISO等）は、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）

- ❒ 情報セキュリティ責任者（CISO等）は、TOS等の開発・保守等を外部委託する際は、委託先の選定手続・選定基準、及び委託先が具備すべき要件を整備する
- ❒ 情報セキュリティ責任者（CISO等）は、外部委託に係る業務遂行に際して、委託先に実施させるセキュリティ対策やシステム障害に対する対処手順等を、調達仕様書等に定め、委託の際の契約条件とする

情報システムに関する業務委託

- ❒ 情報セキュリティ責任者（CISO等）は、整備されている選定手続、選定基準及び委託先が具備すべき要件に基づき、委託先を選定し、外部委託を実施する際にセキュリティ対策要件等を含む外部委託契約を取り交わす
- ❒ 外部委託の終了時に、仕様書等定められた検査手続に従い、サイバーセキュリティに係る要件が満たされていることを確認する

6. 港湾管理者等の対策項目

- ✓ ひとたび１つの港湾のターミナルがサイバー攻撃を受ければ、港全体での道路混雑や滞船等の利用障害が懸念されるだけでなく、背後圏や国際サプライチェーンへの影響も懸念されます。
- ✓ 情報セキュリティ確保に係る対策は、一義的には重要インフラ事業者等が実施するものですが、港湾の重要インフラ事業者等の場合、他の分野の事業者と比べ必ずしも事業規模が大きくないことから、事業者単独では対策に限界が生じることも予想されます。
- ✓ そのため、港湾分野においては、当該港湾全体としてのサイバーレジリエンス体制の強化に向けて、港湾管理者あるいは港湾運営会社等が、重要インフラ事業者等の取り組みが円滑かつ適確に実施されるように支援することが求められています。

港湾におけるサイバーレジリエンス体制強化に向けた取組

港湾管理者等へ求めること

港湾管理者等は、当該港湾全体としてのサイバーレジリエンス体制の強化に向けて、重要インフラ事業者等の取組が円滑かつ適確に実施されるように支援する

【事前準備】

情報セキュリティに関する会議体の設置

❒ 港湾関係者・都道府県警察・セキュリティ専門機関等からなる情報セキュリティに関する会議体を設置する

休日・夜間を問わない連絡体制の構築

❒ インシデント発生時に迅速な情報連絡・情報共有を行えるように、休日・夜間を問わない連絡体制を構築する

インシデント発生時における対処要領の策定

❒ 港湾関係者間でインシデント発生時の対処方針や共有・報告すべき情報を予め策定（マスコミ窓口、役割分担など）する

【平時対策】

インシデント発生時の情報伝達訓練や机上対処訓練の実施

❒ 港湾関係者からなるインシデント発生時の情報伝達訓練や机上の対処訓練を実施する

情報セキュリティ対策に関する研修などの人材育成

❒ 最近の情報セキュリティに関する動向や発生事案についての情報の共有や研修の実施など、港湾関係者の対処能力向上への支援を図る

【インシデント発生時及び事後対応】

インシデントの情報収集（リエゾンの派遣等）

❒ インシデント発生時には、当該事業者へのリエゾンの派遣や、同様の事案が発生していないか他の事業者への状況確認など自ら情報収集を行う

道路混雑や滞船などの港湾の利用障害の情報発信

❒ インシデントに起因する船舶の滞船や道路混雑等の利用障害に関する情報発信を行う

インシデントの原因究明への協力

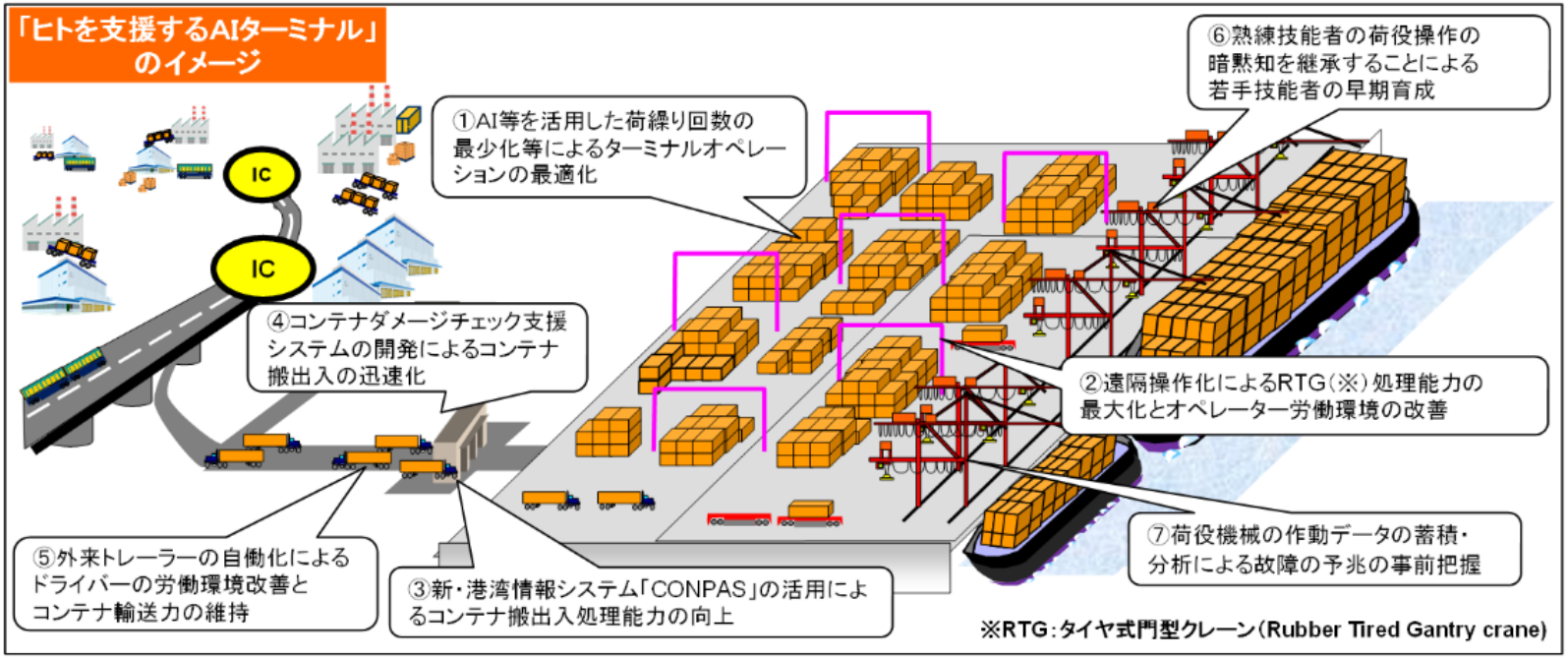
❒ 事態収束後に重要インフラ事業者等が行うインシデントの原因究明や改善策検討に関し、重要インフラ事業者等の求めに応じ、協力を行う

港湾分野特性から求められる取組の例

国土交通省

《物流の自動化》
物流業界は今後、**自動運転やドローン配送、AGV（無人搬送型ロボット）、AMR（自律走行型ロボット）、その他IoTデバイスの活用**が見込まれ、**制御システムのセキュリティ対策が重要**となります。そのため、制御システムのセキュリティ対策やリスクマネジメントを強化する必要があります。

従来から使用しているハンディターミナルにも、近年では汎用OSを活用されているなど、一般的な情報システムやサーバ装置と同様にセキュリティ対策が求められる。港湾における特定用途機器においても同様の対策を実践することや、インターネットと接続されていないシステムであっても、物理的、人的なセキュリティ管理策を実践することが望ましい。



出典-国土交通省　報道発表資料
https://www.mlit.go.jp/kowan/kowan_00001.html