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）

背景説明資料

令和７年３月

国土交通省港湾局

目次

（１）何を守るのか（本ガイドラインの保護対象）

- 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）**が挙げられる。
- 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**となる（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・抽出の必要あり）。
- 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る。

【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）

（２）どうやって守るのか（サイバーセキュリティのリスクマネジメント）

- 重要インフラ事業者等は、重要インフラサービスの安全かつ持続的な提供の実現に向けて、**サービス停止のリスクを許容範囲内に抑制する**ことが求められている。一方、各事業者はマルウェア感染や外部からの攻撃を防止する対策を実施しているが、昨今の複雑・巧妙化する**サイバー攻撃全てを防ぐことは難しい状況**にある。
- そのため、港湾分野における情報セキュリティ確保にあたっては、リスク抑制に向けて、重要インフラ事業者等において**経営層を含めた組織全体での対応**を一層促進するとともに、自組織の特性を明確化し**リスクマネジメント**を通して自組織に最も適した防護対策を実施する必要がある。
- また、リスクマネジメントによる事前対応と危機管理の組合せにより、**障害対応体制を強化**する必要がある。

【「重要インフラのサイバーセキュリティに係る行動計画」の基本的考え方・要点】

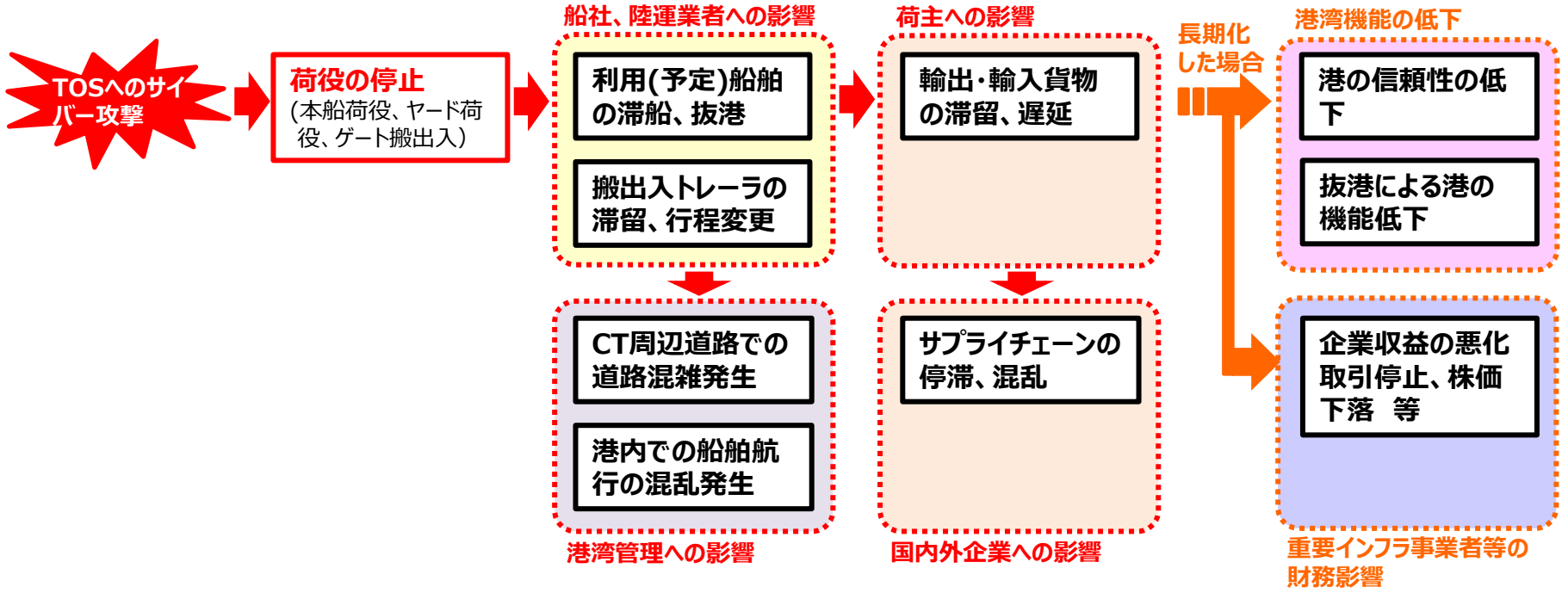
「重要インフラ防護」の目的	重要インフラにおいて、任務保証の考え方を踏まえ、 ①重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること ②重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。
基本的な考え方	• 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。 • 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。 • 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。
障害対応体制の強化に向けた取組	• リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。 • 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を明確にする。 • サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

出典：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（2024年3月、内閣サイバーセキュリティセンター）

（３）守らないとどういうことになるのか（サイバー攻撃による影響想定）

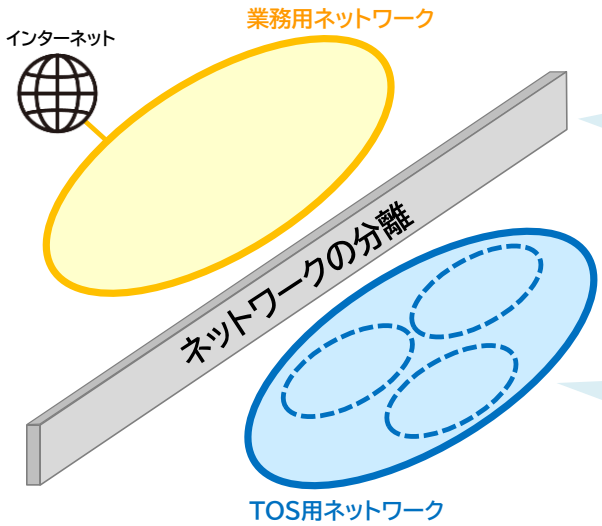
- TOS等へのサイバー攻撃の目的としては、ランサムウェア攻撃による金銭目的や、荷役妨害による社会的混乱の発生、貨物情報・荷役情報の盗聴・偽造による不正物資等の密輸や船舶へのテロ攻撃などが想定される。
- いずれの目的においても、荷役が停止すれば、その影響は、直接の利用者である**船社、陸運事業者への影響**のみならず、周辺**道路混雑や滞船等船舶航行混乱**の発生、さらには、**背後圏産業の生産活動の停止、国際的なサプライチェーンの停止・遅延**といった事態が想定される。
- また、システム復旧に時間がかかることや、何度もサイバー攻撃を受けたりすれば、当該ターミナルのみならず**当該港の信頼性低下**にもつながり、船社・荷主等は他港利用へシフトするといった事態も想定され、**当該港の機能・サービス低下**が懸念される。**当該事業者においては財務影響**も懸念される。

【TOS等へのサイバー攻撃による港湾機能等への影響想定】



（４）本ガイドラインにおける対策の要点（重要インフラ事業者等の対策）

要点①ネットワークの分離



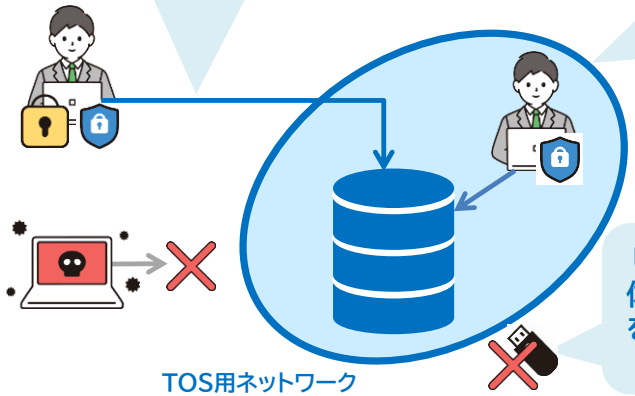
マルウェアに感染させたくないエリアを分割する

利用形態に応じ、ネットワークをセグメント化する

要点②アクセス制御

外部からのアクセスを限定する（接続IP限定、多要素によるユーザー認証等）

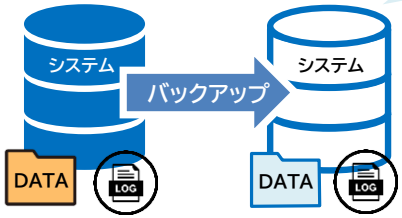
内部アクセスにおけるユーザー管理を行う（ユーザー認証、アクセス権限管理等）



USBメモリ等外部記憶媒体の利用を禁止する。やむを得ず利用する場合は、事前に安全性の確認を行う

要点③バックアップ

許容される荷役停止時間等を踏まえて、バックアップ対象、バックアップ頻度を設定する



現用ネットワークとは切り離された場所で、バックアップを保管する

要点④インシデント対応体制・手順の整備

組織内のインシデント対応体制（CSIRT等）を整備する

関係省庁、警察機関、セキュリティ専門組織、港湾管理者等との連絡・相談体制を整備する

インシデント対応手順、連絡網を文書化する

（１）ガイドラインの位置付け①他の法制度との関係

- 「コンテナターミナルにおける情報セキュリティ対策等委員会 取りまとめ」（令和６年１月）（以下、「取りまとめ」と称す）で示された、３つの制度的措置について、それぞれ取組が進展。
- 港湾運送事業法については、改正・施行済み（令和６年３月）。港湾運送事業者は、事業計画においてTOSのサイバーセキュリティの確保に関する事項を届出が必要（令和７年３月31日までに届出）。
- 経済安全保障法については、法改正済み（令和６年5月）、制度具体化に向けた審議中。
- サイバーセキュリティ基本法については、重要インフラ分野に「港湾分野」が位置付けられ（令和６年３月）、あわせて、令和６年４月に、**「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）」を公表済み**。

【３つの制度的措置の概要】

制度的措置　　TOS：ターミナルオペレーションシステム

港湾運送事業法の観点

✓ 法改正済み
✓ 事業計画の届出必要(～令和7年3月31日)

○コンテナターミナルにおいて一般港湾運送事業者が使用するTOSについて、①TOSの情報セキュリティ対策の状況を的確に把握し、②TOSの情報セキュリティ対策の強化・底上げを図ることが必要。

○港湾運送事業への参入等に際して審査を受ける必要がある事業計画にTOSの概要や情報セキュリティの確保に関する事項の記載を求める。

➡ **TOSの情報セキュリティ対策の確保状況を国が審査する仕組みの導入**

サイバーセキュリティ基本法の観点

✓ 重要インフラとして指定済み
✓ ガイドライン（第1版）を策定・公表済み

○「重要インフラのサイバーセキュリティに係る行動計画」を改定し、重要インフラ分野に「港湾分野」を位置づける方向で検討する。

○コンテナターミナルにおけるTOSを含む港湾分野に焦点を当てた情報セキュリティガイドラインを作成する。

➡ **官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進**

経済安全保障の観点

✓ 制度具体化に向けて審議中

○コンテナターミナルにおいて一般港湾運送事業者に使用されるTOSの機能が停止・低下し、荷役作業に支障が生じた場合、影響が甚大となるおそれがある。

○経済安全保障推進法の趣旨も踏まえ、TOSを使用して役務の提供を行う一般港湾運送事業を経済安全保障推進法の対象事業とすることが必要であると考えられる。

➡ **経済安全保障の観点からも国として積極的に関与**

出典：コンテナターミナルにおける情報セキュリティ対策等委員会取りまとめ「名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策および情報セキュリティ対策等の推進のための制度的措置について（概要）」（令和6年1月）

（１）ガイドラインの位置付け②ガイドラインの性格、第1版からの改定理由

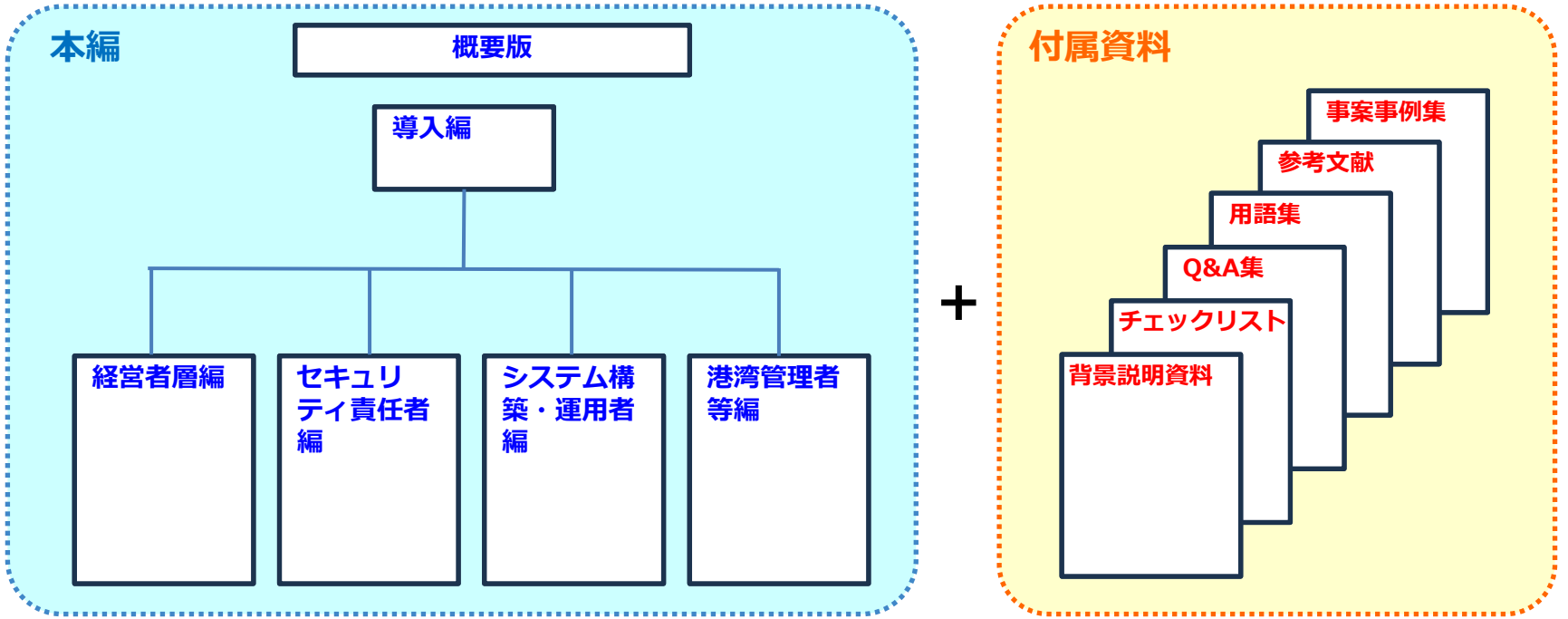
- 本ガイドラインは、重要インフラサービスの継続性維持に向けて、重要インフラ事業者等がサイバーセキュリティ確保に向けて、自主的に取組、対策の実施や検証にあたっての目標を定めることを目的として策定したものであり、国が定める「ガイドライン」として**推奨事項を列挙しているもの**。
- 今回、以下の理由により、第1版から第2版へ改定した。

  - ガイドライン（第1版）では、名古屋港事案を踏まえた港湾特有の課題については記載されているものの、「取りまとめ」における対応策については盛り込まれておらず、これまでの**港湾分野の知見が十分に反映されたものとはなっていない**。
  - 情報セキュリティ対策の実施にあたっては各組織が組織的に対応することが求められ、ガイドラインも様々な立場の者が読み手となるが、ガイドライン（第1版）では、全体の分量が多く、文章も丁寧な記述が多いため、**読み手それぞれの目的に応じて、どの部分を読めば良いかが分かりづらい**。
  - 港湾運送事業者等からみれば、港湾運送事業法での事業計画の申請項目は、対策が必須の内容（強制要件）であるのに対し、ガイドライン（第1版）は推奨事項としての位置付けであり、**ガイドラインと港湾運送事業法上の事業計画の申請項目との関係が分かりづらい**。
  - ガイドライン（第1版）は、TOS等のシステム使用者を対象としたガイドラインであるが、名古屋港事案にみるように、インシデント対応や事業継続対応等において、港湾管理者等が果たす役割も期待されることから、**港湾管理者等向けの内容を追記することが望まれる**。
  - ガイドライン（第1版）では、ガイドライン本体のみの文書構成となっているが、ガイドラインを周知・徹底していく上では、**簡潔な概要資料やチェックリスト、Q&A集等の実践的なツールの提供が求められる**。

（２）ガイドラインの構成①文書構成

- 本文と付属資料で構成。
- 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点。
- 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、事案事例集の６点。

第2版の文書構成



（２）ガイドラインの構成②本文の内容構成

- 本文では、各対策項目について事業者に求める事項を、**【事業者に求めること】**として四角囲みで記述している。
- 事業者に求めることの下に、**〔解説〕**として、対策の必要性や考え方等を記述し、**〔具体例〕**として、対策の例示を記載している。なお、その対策のうち、港湾運送事業法における事業計画の届け出で必要となる項目（強制要件）については、網掛け（全ての港が対象）、下線（特定の港が対象）を付している。

改定版本文の内容構成

【事業者に求めること】

➢ ・・・・

〔解説〕

・・・・

〔具体例〕

●

・・・

【具体例での港湾運送事業法における強制要件の表記例】

〔具体例〕

●外部との接続に係る不正アクセス対策

VPN、ルータ等のネットワーク機器については、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、以下の措置を執ること。

- ✓ 接続元の IP アドレスを指定することで接続元を限定、明確化する。
- ✓ 知識情報（パスワード等、利用者本人のみが知り得る情報）、所有情報（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）、生体情報（指紋や静脈等、本人の生体的な特徴）のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの（12 文字以上、大小英文字＋数字＋記号を推奨）とする。
- ✓ 識別コードについて、安全な配布方法と運用手順を定めること。
- ✓ アカウントロック機能を実装することが望ましい。
- ✓ 不正ログイン試行を検知する機能（通常とは異なる IP アドレスからシステムへアクセスがあった際にメールで通知等）を実装することが望ましい。

※ 　は、港湾運送事業法では強制要件（全ての港）

※ ___は、港湾運送事業法では強制要件（特定の港（＊注））

＊注：特定の港とは、京浜港、名古屋港、大阪港、神戸港、博多港の5つの港。以下の事項において同様

（3）ガイドラインの骨子①本編（導入編、経営者層編）

国土交通省

導入編

- 導入編では、各編を理解する上で**前提となる考え方**や**港湾分野の特性**、**各編の概要**等を示すもの。主な内容は以下の通り。
  - ✓ 本ガイドラインの目的と位置付け（事業者の任務保証の観点から、重要インフラの防護を目的として、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）
  - ✓ 港湾分野におけるセキュリティ管理策の現状と課題、港湾分野におけるガイドラインの対象（対象者、対象システム（当面はTOS）、対象とする事象（サイバー攻撃、災害を含めたシステム障害等）
  - ✓ 本ガイドラインの構成、各編の概要、本ガイドラインでの各対策項目の整理の仕方、第1版からの改定内容　等

経営者層編

- 経営者層編では、組織統治の観点から、主に以下の内容について、**経営者層として対応・判断すべき事項**、セキュリティ責任者やシステム構築・運用者等に対して**指示、管理すべき事項**とその考え方を示すもの。

【事前準備】
- ✓ 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
- ✓ 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）

【平時対策】
- ✓ 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
- ✓ 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
- ✓ 必要となる予算・体制・人材等の継続的確保
- ✓ 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）

【インシデント発生時及び事後対応】
- ✓ インシデント発生時の対応等の情報開示の取組み

凡例　**新規に作成した項目**　**「取りまとめ」の対策内容を追記した項目**

（３）ガイドラインの骨子②本編（セキュリティ責任者編）

セキュリティ責任者編

- 主に以下の内容について、**情報セキュリティ責任者として対応すべき事項**、TOS等システムの実装・運用に関して、**システム構築者、システム運用者に対して指示、管理すべき事項**とその考え方を示すもの。

【事前準備：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）
- ✓ 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
- ✓ 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

【事前準備：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
- ✓ 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）
- ✓ 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）
- ✓ 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）
- ✓ 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
- ✓ 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

【事前準備：インシデント対応手順、業務継続計画の策定】

- ✓ 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
- ✓ 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）」、平時のサービス水準までの復旧方針等を定めた「事業復旧計画」の策定
- ✓ インシデントに備えた対処体制の整備（CSIRT（Computer Security Incident Response Team）等）
- ✓ 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）

凡例　**新規に作成した項目**　**「取りまとめ」の対策内容を追記した項目**

（３）ガイドラインの骨子②本編（セキュリティ責任者編）

セキュリティ責任者編（つづき）

【平時対策：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）
- ✓ 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
- ✓ 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）
- ✓ 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

【平時対策：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
- ✓ インシデント対応等の演習・訓練の定期的な実施

【平時対策：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

【インシデント発生時及び事後対応】

- ✓ 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）
- ✓ 事業継続計画、事業復旧計画の実行
- ✓ 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）
- ✓ 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）
- ✓ 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

凡例　**新規に作成した項目**　**「取りまとめ」の対策内容を追記した項目**

（３）ガイドラインの骨子③本編（システム構築・運用者編）

国土交通省

システム構築・運用者編

- 主に以下の内容について、経営者層やセキュリティ責任者の指示に基づき、TOS等のシステムを構成する機器、ソフトウェア等の各種資源の**設計、実装、運用等の実務を担う担当者（外部委託先含む）として対応すべき事項**とその考え方を示すものとする。

【事前準備】
- ✓ 機器の物理的保護策（免震・耐震設備、非常電源装置等）
- ✓ 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

【平時対策：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）
- ✓ 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）
- ✓ 暗号を活用した情報管理（暗号化機能、電子署名等）
- ✓ システムの負荷分散・冗長化対策、多層防護の導入

【平時対策：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）
- ✓ 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）

【インシデント発生時及び事後対応】
- ✓ 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）

凡例　**新規に作成した項目**　**「取りまとめ」の対策内容を追記した項目**

（３）ガイドラインの骨子④本編（港湾管理者等編）

- 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こととなるが、港湾分野においては、他の分野の事業者と比べて、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る。
- 一方、港湾分野においては、例えばコンテナターミナル（CT）では、それぞれのCTでターミナルオペレーターが異なり、1つの港湾内に複数の重要インフラ事業者等が存在している。また、ひとたび１つのCTがサイバー攻撃を受ければ、同一のアクセス道路及び航路を利用している他のCT及びCT以外の施設においても、道路渋滞や滞船等の影響を受けることになる。また、背後圏経済、国際物流・国際サプライチェーンの影響も懸念される。
- そのため、港湾分野においては、重要インフラ事業者等のみに情報セキュリティ確保の取組を委ねるのではなく、**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は、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組が円滑かつ適確に実際されるように支援**する必要があると考えている。
- また、港湾管理者等としては、自然災害時と同様に、**サイバー攻撃事案発生時においても、港湾機能の維持・早期回復に向けて、港湾BCP協議会のようなまとめ役的な役割を担う必要があると考えている。**

港湾におけるサイバーレジリエンス体制強化の考え方

- 港湾分野全体あるいは地域（港）全体としてのサイバーレジリエンス体制の強化にあたっては、本ガイドライン等の活用を通して、重要インフラ事業者等の個々の組織でリスクマネジメント体制の構築・強化を図るとともに、インシデント発生時には、被害軽減、早期復旧、事業継続等に向けて、関係者間で協力して対処にあたることができる体制を平時から構築しておくことが重要。

（３）ガイドラインの骨子④本編（港湾管理者等編）

港湾管理者等編

- 主に以下の内容について、港湾管理者等が、**港湾全体を管理・運営する立場として対応すべき事項**とその考え方を示すもの。

【事前準備】
- ✓ 港湾関係者からなる情報セキュリティに関する会議体の設置
- ✓ インシデント発生時に、休日・夜間を問わない連絡体制の構築
- ✓ 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）

【平時対策】
- ✓ 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の実施
- ✓ 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

【インシデント発生時及び事後対応】
- ✓ インシデントが発生時の情報収集（リエゾンの派遣、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）
- ✓ 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
- ✓ 事案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・対策検討への協力

凡例　**新規に作成した項目**　**「取りまとめ」の対策内容を追記した項目**

（３）ガイドラインの骨子⑤付属資料（概要資料、チェックリスト）

概要資料

新規に作成

- サイバーセキュリティ関連業務に初めて携わる者や一般の従業員等向けに、港湾分野でのサイバーセキュリティ対策に関する意識啓発に向けて、セキュリティ**対策の必要性**や**対策の要点**等を示すもの。主な内容は以下の通り。
  - ✓ 港湾分野で想定されるサイバーセキュリティリスクと、サイバー攻撃を受けた場合に想定される影響（名古屋港の例等）
  - ✓ 港湾分野におけるサイバーセキュリティ対策の取組概要（サイバーセキュリティ基本法、港湾運送事業法、経済安全保障推進法）と、ガイドラインの位置付け
  - ✓ ガイドラインにおけるサイバーリスクマネジメントの考え方、ガイドラインの構成
  - ✓ 事業者に求める個別のセキュリティ対策（推奨事項）の概要（マルウェア対策、不正アクセス対策、インシデント対応手順策定等） 等

チェックリスト

新規に作成

- 各事業者が対策の取組みを進めていくうえでの補助的な資料として、サイバーセキュリティ対処態勢の**実態把握**、**将来目標**の設定、実態と目標とのギャップ、ギャップ改善に向けた取組みの進捗状況を**自ら確認**できるもの。主な内容は以下の通り。
  - ✓ 現状の評価（実施済み、進行中、未着手）
  - ✓ １年後の目標（実施済み、進行中、未着手）
  - ✓ 備考欄（取組方針等を記入してもらう）

表　チェックリストのイメージ（案）

	対策	現状の評価	1年後の目標	備考
経営者層	①サイバーセキュリティ方針の策定・宣言	☐ 実施済み ☑ 進行中 ☐ 未着手	☑ 実施済み ☐ 進行中 ☐ 未着手	現在策定中。 今年度内に策定し、組織内外に宣言予定。
	②			

- チェックリストは、**重要インフラ事業者等用と、港湾管理者等用の２種類**を用意する。

（３）ガイドラインの骨子⑥付属資料（Q&A集、用語集）

Q&A集

新規に作成

- ガイドラインの**法的位置付けや港湾行政上の位置付けの理解**を深めるとともに、各事業者が具体的に**対策実施するにあたって想定される困りごとや疑問点等への助言**的な内容を示すもの。主な内容は以下の通り。
  - ✓ 本ガイドラインの法的位置付け、港湾行政上の位置付けに関するQ&A（港湾運送事業法、経済安全保障推進法との関係含む）
  - ✓ 経営者層編の取組み事項に関するQ&A（サイバー事案発生時の責任のあり方、最高情報セキュリティ責任者等に求める資質・資格要件、外部監査の依頼先　等）
  - ✓ セキュリティ責任者編の取組み事項に関するQ&A（リスクアセスメントの実施方法、対策の優先順位付けの考え方、インシデント対応手順での留意事項、効果的な演習・訓練の実施方法・内容　等）
  - ✓ システム構築・運用者編の取組み事項に関するQ&A（マルウェア対策の種類・内容、不正アクセス対策の種類・内容、外部委託先との契約における留意事項　等）

用語集

第1版の本文より移動・加筆

- サイバーセキュリティに関する**技術的な専門用語について、簡潔な解説**を示すもの。

  ex. セキュリティ対策技術に関する用語（多要素認証機能、アカウントロック機能、ゼロトラストセキュリティ、EDP、サイバーハイジーン　等）

  . ソフトウェアの脆弱性に関する用語（SQLインジェクション脆弱性、OSコマンドインジェクション脆弱性　等）

  . サイバー攻撃に関する用語（マルウェア、ランサムウェア、標的型攻撃、DDoS攻撃、パスワードリスト攻撃　等）

（３）ガイドラインの骨子⑦付属資料（参考文献、事案事例集）

参考文献

第1版の本文より移動

- 「共通編」「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」で提示した各対策項目の参考文献を示すもの。
  - ✓ NISCの指針・基準、JISQ27001・27002 等

事案事例集

新規に作成

- サイバー攻撃の手口や、サイバー事案発生時の影響の大きさ等の周知を図るうえで、国内外の港湾及び重要インフラにおけるサイバー事案の代表的な事例について、**事案概要（攻撃方法、システム停止期間、社会経済への影響等）**を示すものとする。主な事案事例は以下の通り。
  - ✓ 名古屋港の事例（ランサムウェア攻撃、システム停止3日間、部品組立工場一時操業停止）
  - ✓ ベルギー・アントワープ港の事例（オイルターミナル運営会社への攻撃、石油製品積込停止。混乱１ヶ月以上継続）
  - ✓ 米国コロニアルパイプラインの事例（ランサムウェア攻撃、システム停止7日間、身代金支払い、市場燃料枯渇）
  - ✓ 日本政府e-Govの事例（DDoS攻撃、システム停止1.5日間、システムによる手続き停止）
  - ✓ ウクライナ停電の事例（標的型攻撃、システム停止6時間、停電により22万5千人に影響）
  - ✓ 米国SolarWindsの事例（SolarWinds製品の世紀のアップデートを通じた米国政府機関や大手IT企業へのサプライチェーン攻撃、システム修正までに約10ヶ月、被害概要未だ不明）　等