サイバーセキュリティ基本法に係る
安全ガイドラインの改定に向けた準備状況について

令和６年11月

国土交通省港湾局

目次

（１）港湾における情報セキュリティ対策推進に向けた制度的措置の取組状況

国土交通省

- 「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、省令等改正・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）。
- 経済安全保障推進法については、法改正済み(令和６年5月)、制度具体化に向けて検討中（本検討会）。
- 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

✓ 省令等改正済み
✓ 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検討中

○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）港湾における情報セキュリティ対策推進に向けた制度的措置の取組状況

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」の概要】

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 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

NISCによる総合調整

重要インフラ所管省庁

- 金融庁
  ［金融］
- 総務省
  ［情報通信、行政］
- 厚生労働省
  ［医療］
- 経済産業省
  ［電力、ガス、化学、クレジット、石油］
- 国土交通省
  ［航空、空港、鉄道、水道、物流、港湾］

重要インフラ(全１５分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾

関係機関等

- サイバーセキュリティ関係省庁
  ［総務省、経済産業省等］
- 事案対処省庁
  ［警察庁、防衛省等］
- 防災関係府省庁
  ［内閣府、各省庁等］
- サイバーセキュリティ関係機関
  ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者
  ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

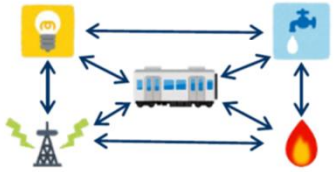
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

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8日、サイバーセキュリティ戦略本部決定）

（２）現行のガイドライン（第１版）の概要

① 国土交通省所管重要インフラの他分野（鉄道、航空、空港、物流）のガイドライン改定と同時期（令和6年4月）に公表。**国交省所管他分野と同じ構成・内容で作成**（一部、港湾特性を踏まえた記述有り）。

② NISCの指針改定（＊注）にあわせて、**リスクマネジメントの観点から構成・内容を整理**。章立てとして、経営層が取組む事項とセキュリティ責任者が取組む事項、個別の管理策を整理。

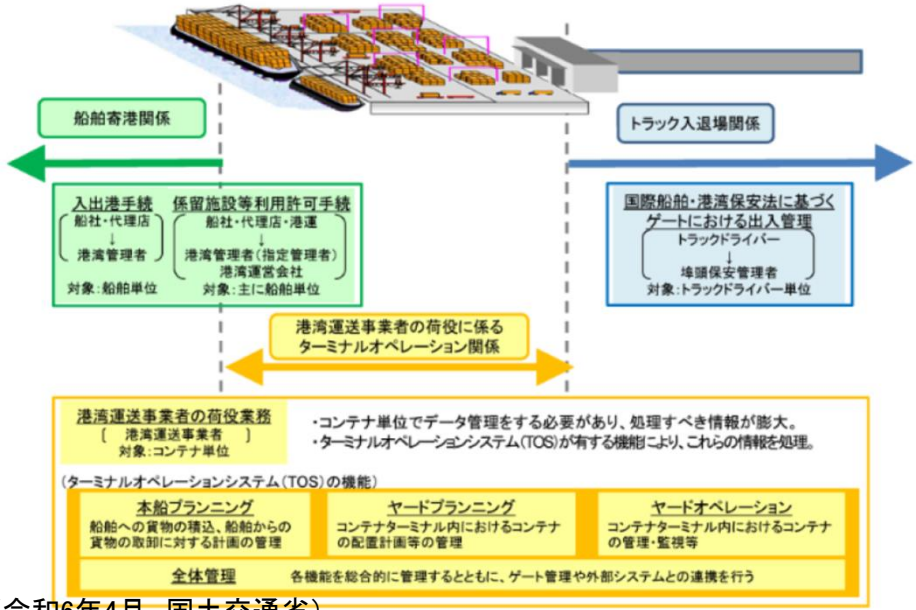
＊注：「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（令和5年7月４日)、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント手引書」（令和5年7月４日）

③ 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（港湾運送事業者等）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**。

【港湾分野の重要インフラサービス/システム（例）】

コンテナ荷役サービス

ターミナルオペレーションシステム



出典：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）（令和6年4月、国土交通省）

（２）現行のガイドライン（第１版）の概要

国土交通省

【ガイドライン（第1版）の目次構成】

はじめに
1．「安全ガイドライン」策定の背景

2．港湾分野における
「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

出典：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）（令和6年4月、国土交通省）

（３）ガイドライン（第1版）を改定する理由

- 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**。

- 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**。

- 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**。

- 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**。

- 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**。

（１）改定の方針

方針１

「取りまとめ」※の対策内容を盛り込む。　※コンテナターミナルにおける情報セキュリティ対策等検討委員会取りまとめ

- ✓ 対策の具体例部分に、「取りまとめ」の内容を追加する。
- ✓ また、港湾運送事業法による強制要件との関係を記載する。

方針２

港湾管理者等用の分冊を作成する。

- ✓ インシデント対応や、平時の情報共有体制等に関して、港湾管理者等が対応すべき内容を記載する。
- ✓ ガイドライン（第1版）には、港湾管理者等向けの内容は無いため、新規に作成する。

方針３

各項目で、**要求事項（事業者に求めること）を明確**にする。

- ✓ 「事業者に求めること」を各項目の最初に記載（枠囲み等で強調）し、その下に、解説を記載し、さらに具体例を列挙する。

方針４

事業者組織内の**読み手別に分冊**とする。

- ✓ ガイドライン本文は、導入編と、読み手別（①経営層編、②セキュリティ責任者編、③システム構築・運用者編）に分ける。

方針５

概要資料やチェックリスト、Ｑ＆Ａ集等の**付属資料を作成**する。

- ✓ 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向けに、対策の要点を示した、概要資料を作成する。
- ✓ ガイドライン（第1版）に記載されている専門用語集及び参考文献を、付属資料に移動する。
- ✓ 自組織のサイバーセキュリティ対策現状のみならず、将来目標も設定することで、今後の対応が必要なところが一目でわかるチェックリストを作成する。
- ✓ ガイドラインの取扱いや、対策実施にあたり想定される疑問点等に対応した、Q&A集を作成する。
- ✓ 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事例集を作成する。

（１）方針１：「取りまとめ」の対策内容①

国土交通省

【「取りまとめ」における対応策（概要）】

→ガイドライン改定(案）での該当部分

◆ 名古屋港事案の検証

【感染経路】
保守用VPNを通じて物理サーバにランサムウェアが侵入し、サーバ情報が暗号化されたものと考えられる一方で、VPN経由以外での侵害の可能性についても精査すべき

【主な問題点】
○保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたこと
○サーバ機器及びネットワーク機器の脆弱性対策が不十分であったこと
○バックアップの取得対象と保存期間が不十分であったこと
○システム障害発生時の対応手順が未整備であったこと　等

【主な評価点】
○事案発生から丸2日半という短期間で復旧が図られたこと
○システムを使用せずにマニュアル作業で船舶との間の荷役が継続されたこと　等

◆ ターミナルオペレーションシステムに必要な情報セキュリティ対策

○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把握　→「セキュリティ責任者」資産の特定・管理
○サーバやネットワーク機器の外部接続に関する設定の見直し →「システム構築・運用者編」 運用の管理
○セキュリティ対策ソフトの導入、ソフトウェアの定期的な更新 →「システム構築・運用者編」運用の管理
○システムログを含むバックアップの取得と適切な取得頻度・保存期間・保存場所の設定 →「システム構築・運用者編」 運用の管理
○外部委託を行う場合の情報セキュリティの確保　等 →「セキュリティ責任者編」委託先管理

◆ コンテナターミナルの運用に必要な情報セキュリティ体制

○最高情報セキュリティ責任者及び情報セキュリティ担当者の指定 →「経営者層編」 責任及び権限の割当て
○セキュリティインシデント対応手順の策定及びセキュリティインシデント対応訓練の実施 →「セキュリティ責任者編」演習・訓練
○情報連絡体制の構築、システム障害を想定した事業継続計画の策定→「セキュリティ責任者編」 事業継続計画等の作成
○情報セキュリティに関する情報の収集 →「セキュリティ責任者編」 モニタリング及びレビュー
○関係者の情報セキュリティ意識の向上及び情報セキュリティ教育・訓練等の実施 →「セキュリティ責任者編」 人材育成・意識啓発
○脆弱性や設定不備の検査及び情報セキュリテイ対策の監査の定期的な実施　等→「セキュリティ責任者編」 モニタリング及びレビュー

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）方針１：「取りまとめ」の対策内容②

- 本文は、第1版の内容を、【事業者に求めること】、〔解説〕、〔具体例〕に再整理し、「取りまとめ」の対策内容を追加。

改定版本文の内容構成（案）

【事業者に求めること】

➢ ・・・・

〔解説〕

・・・・

〔具体例〕

●

・・・

（作成方法）

- ガイドライン（第1版）概要版より。概要版に無い項目については、第1版の対策項目の内容を要約。
- 文末は、「～する」とする。（「～すること」とはしない）

- ガイドライン（第1版）での、【対策の指針】、【対策項目】、【実施項目】の文章を、基本的には踏襲。

- ガイドライン（第1版）での具体例（表囲み）の内容を、基本的には踏襲。

- 「取りまとめ」の「３．ターミナルオペレーションシステムに必要な情報セキュリティ対策」及び「４．コンテナターミナルの運用に必要な情報セキュリティ体制」について、第1版の該当項目部分に盛り込み。

（1）方針1：「取りまとめ」の対策内容③

国土交通省

【本文の内容構成の例（第1版との対比）】

ガイドライン（第1版）

5.4　技術的対策

5.4.1 不正アクセス等の脅威への対策

【対策の指針】

重要インフラサービス障害の原因となる不正アクセス等の脅威への対策として、利用者アクセスの管理、主体認証機能及び権限管理機能についてのセキュリティ管理策を記載する。

また、制御システム等は、一律に脆弱性対処ができない場合があるので、サイバーセキュリティ上のリスクを評価し把握した上で適切な対策をとることが望ましい。

5.4.1.1　利用者アクセスの管理

【対策項目】

サイバーセキュリティ責任者は、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ことが重要である。

【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。
  - ✓ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。
  - ✓ 利用者アクセス権を定期的にレビューする。
- ユーザー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（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 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ーアカウントと、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。（【5.4.2 情報システム等のアクセス制御】参照）

ガイドライン（第1版改訂（案））

2　平時対策

2.1　不正アクセス等の脅威への対策

2.1.1 利用者アクセスの管理

赤字は「取りまとめ」の対策内容を追加した部分

【事業者に求めること】

- システム管理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。

～（省略）～

●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

●TOS 等ネットワーク内のサーバ機器、ネットワーク機器に係る不正アクセス対策

サーバ機器及びシステム内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

- 管理者の認証に当たっては、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。

※ ___は、港湾運送事業法では強制要件として、管理者用の初期 ID 及びパスワードの変更等の適切な管理が必要。加えて、簡単に推測されない複雑なパスワードが必要。（全ての港）

～（省略）～

（1）方針2：港湾管理者等用の分冊作成

- 名古屋港事案に係る港湾管理者の対応内容、事案後の取組動向等を踏まえ、港湾の情報セキュリティ対策において、**港湾管理者等に求められる役割等の内容（推奨事項）を記述**する。
- なお、本ガイドラインは港湾管理者等が所有するシステムに対して取るべき措置ではなく、港湾運送事業者が所有するシステムが攻撃を受けた場合に、港湾管理者等が取るべき行動をまとめたもの。
- 内容としては、**関係者間の情報共有体制の構築支援**や、**インシデント対応時の対処**（情報発信、道路混雑等の対処等）、**関係事業者が行う対策の実施支援**等を盛り込む。

港湾管理者等編の目次（案）

【事例：コンテナターミナルのサイバーセキュリティ対策強化に向けた港湾管理者等の対応】

名古屋港

- ✓「NUTSシステムサイバーセキュリティ対策連携会議」設置。管理者内部に「NUTSシステムサイバーセキュリティ等対策本部」立ち上げ。
- ✓ システム復旧費と今後のサイバーセキュリティ強化対策費用に対する補助金を創設
- ✓ 国内外のサイバーセキュリティ演習等に積極的に参加　等

東京港

- ✓ 各コンテナターミナルにおけるセキュリティ対策の状況について緊急の実態調査、専門家が調査結果を確認、ターミナル毎に必要な対策等を個別にフィードバック。
- ✓ 重点的に実施すべきセキュリティ対策等に関する説明会を実施。
- ✓ 警視庁と合同で、コンテナターミナル借受者等を対象とした「サイバーセキュリティ対策連絡会」を開催　等

ロサンゼルス港

- ✓ CRC（サイバーレジリエンスセンター）を設置し、複数のコンテナターミナルとMOUを締結し、通信ログを監視し、異常検知した場合には関係ステークホルダーに報告。
- ✓ 各コンテナターミナルのサイバーセキュリティ対策費の財政支援（政府の補助金獲得含む）　等

（１）方針３：要求事項の明確化①

- 本文は、第1版の内容を、【事業者に求めること】、〔解説〕、〔具体例〕に再整理し、「取りまとめ」の対策内容を追加。

改定版本文の内容構成（案）

（作成方法）

【事業者に求めること】

➢ ・・・・

〔解説〕

・・・・

〔具体例〕

●

・・・

- ガイドライン（第1版）概要版より。概要版に無い項目については、第1版の対策項目の内容を要約。
- 文末は、「～する」とする。（「～すること」とはしない）

- ガイドライン（第1版）での、【対策の指針】、【対策項目】、【実施項目】の文章を、基本的には踏襲。

- ガイドライン（第1版）での具体例（表囲み）の内容を、基本的には踏襲。

- 「取りまとめ」の「３．ターミナルオペレーションシステムに必要な情報セキュリティ対策」及び「４．コンテナターミナルの運用に必要な情報セキュリティ体制」について、第1版の該当項目部分に盛り込み。

（1）方針3：要求事項の明確化②

【本文の内容構成の例（第1版との対比）】

ガイドライン（第1版）

5.4　技術的対策

5.4.1 不正アクセス等の脅威への対策

【対策の指針】

重要インフラサービス障害の原因となる不正アクセス等の脅威への対策として、利用者アクセスの管理、主体認証機能及び権限管理機能についてのセキュリティ管理策を記載する。

また、制御システム等は、一律に脆弱性対処ができない場合があるので、サイバーセキュリティ上のリスクを評価し把握した上で適切な対策をとることが望ましい。

5.4.1.1　利用者アクセスの管理

【対策項目】

サイバーセキュリティ責任者は、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ことが重要である。

【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。
  - ✓ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。
  - ✓ 利用者アクセス権を定期的にレビューする。
- ユーザー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（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 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ーアカウントと、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。（【5.4.2 情報システム等のアクセス制御】参照）

ガイドライン（第1版改訂（案））

4　技術的対策

4.1　不正アクセス等の脅威への対策

4.1.1 利用者アクセスの管理

【事業者に求めること】

- ➢ システム管理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。

〔解説〕

重要インフラサービス障害の原因となる不正アクセス等の脅威への対策として、利用者アクセスの管理、主体認証機能及び権限管理機能についてのセキュリティ管理策を記載する。

また、制御システム等は、一律に脆弱性対処ができない場合があるので、サイバーセキュリティ上のリスクを評価し把握した上で適切な対策をとることが望ましい。

システム管理者は、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ことが重要である。

〔具体例〕

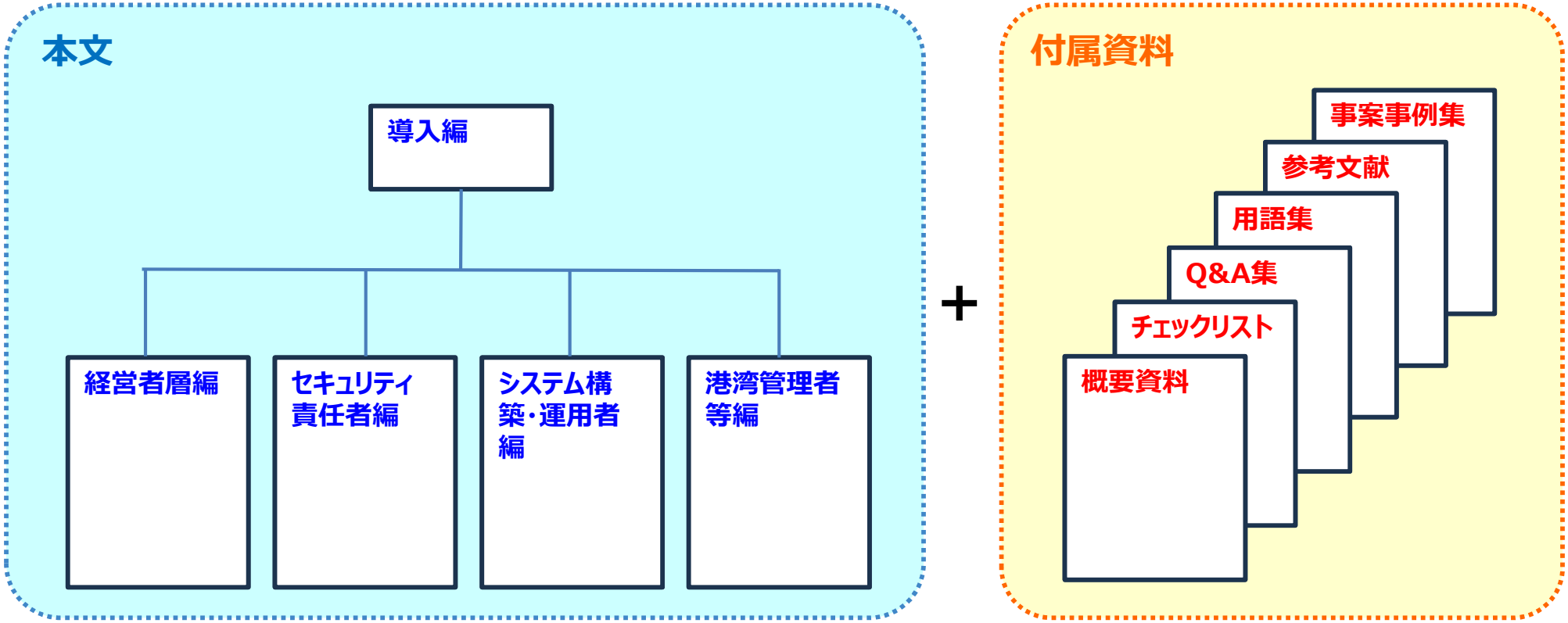
●利用者アクセスの管理（例）

- 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。
  - ✓ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。
  - ✓ 利用者アクセス権を定期的にレビューする。
- ユーザー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（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 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ーアカウントと、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。（【5.4.2 情報システム等のアクセス制御】参照）

（１）方針４・５：読み手別に分冊化・付属資料の作成

- 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、概要資料、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。

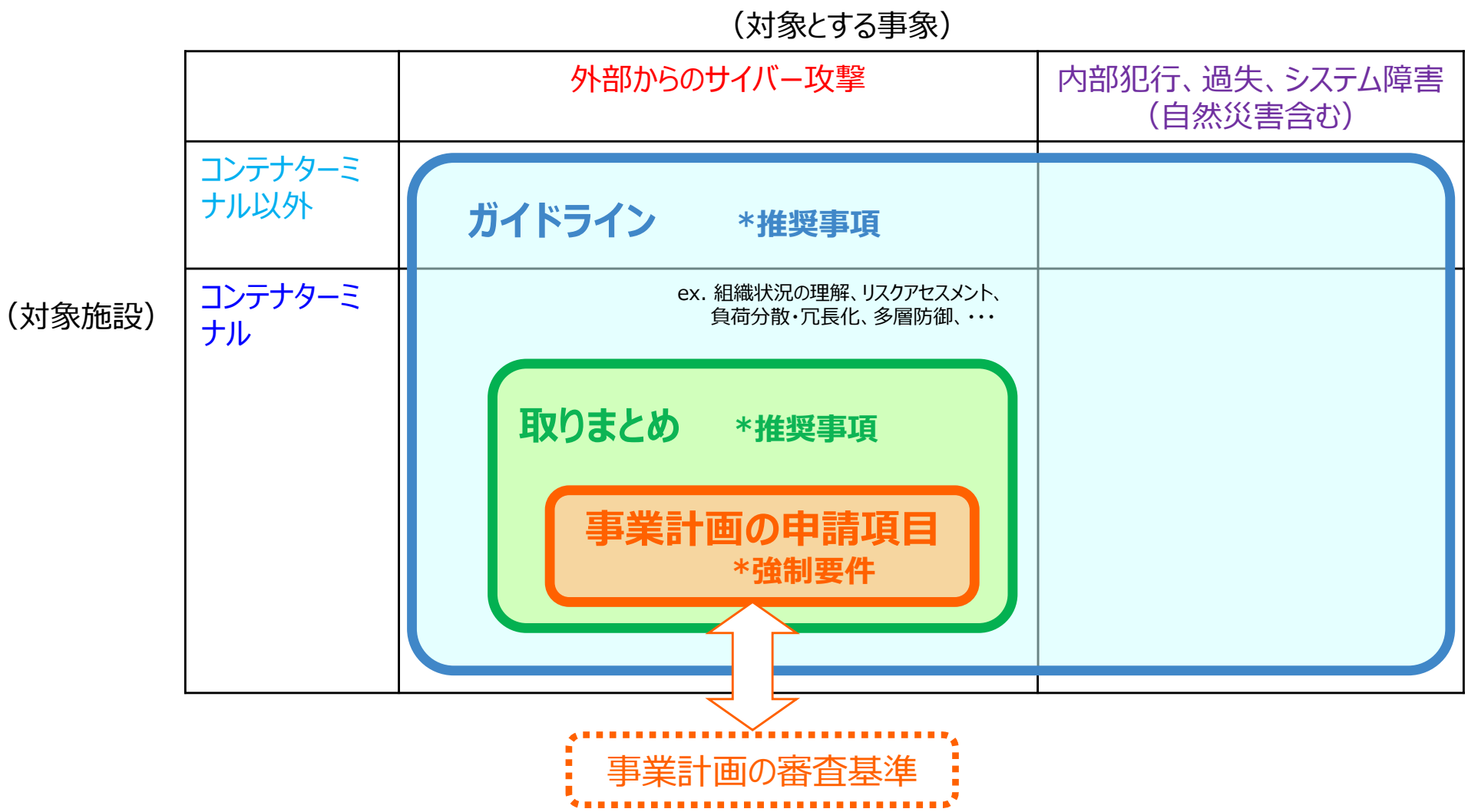
改定版の文書構成（案）



（１）ガイドラインの想定される読み手と利用方法

国土交通省

【ガイドラインと「取りまとめ」及び港湾運送事業法の事業計画申請項目との関係】



（２）本文で記載する内容（案）①

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**等を示すものとする。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（重要インフラ事業者の任務保証の観点から、重要インフラ防護を目的として、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とする。

【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**

（２）本文で記載する内容（案）②

セキュリティ責任者編

- 主に以下の内容について、**サイバー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とする。

【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**

（２）本文で記載する内容（案）③

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
- ✓ 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

【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**

（２）本文で記載する内容（案）④

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**

（２）本文で記載する内容（案）⑤

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とする。

【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。
- ✓ 事案収束後のインシデントの原因究明・対策のための有識者、港湾関係者からなる検討会の設置。

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）付属資料で記載する内容（案）①

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**等を示すものとする。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**できるものとする。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用（港湾運送事業者等用）と、港湾管理者等用の２種類**を用意する。

（3）付属資料で記載する内容（案）②

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とする。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）
- なお、Q&A集は、今後予定している港湾運送事業者等へのガイドラインの説明会や、アンケート調査・ヒアリング調査での意見も踏まえ、適宜内容を追加する予定。

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**を示すものとする。

  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）付属資料で記載する内容（案）③

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とする。
  - ✓ 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
- この他、最新のトピックを含めて、港湾及び重要インフラへの攻撃事案を紹介予定。

4. 今後のスケジュール（案）

国土交通省

- 改定案（素案）作成後、サイバーセキュリティ**専門家への意見聴取**を行う予定。また、主要港の**港湾運送事業者・港湾管理者等へのアンケート調査・ヒアリング調査も並行して行う。**
- それらで出されて意見を踏まえて、年度内に改定（最終案）を作成し、京浜港・阪神港等において、関係者への**説明会**を実施予定。
- **年度末には、ガイドライン（第1版改定）として公表予定。**

ガイドライン改定に向けた今後のスケジュール（案）