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）

～港湾管理者等編～

令和７年３月28日

国土交通省港湾局

目次

はじめに
1　港湾分野における「安全ガイドライン」の概要 1
1.1　港湾分野におけるセキュリティ管理策の現状 1
1.2　「安全ガイドライン」の対象範囲 1
1.3　本ガイドラインの構成・読み方 2
2　港湾のサイバーレジリエンス強化の考え方 4
2.1　港湾分野におけるセキュリティ強化に向けて 4
2.1.1　情報セキュリティ強化に向けた 3 つの制度的措置 4
2.1.2　港湾のサイバーセキュリティ強化の考え方 5
2.2　サイバーレジリエンス強化における港湾管理者等の関与のあり方 6
2.2.1　サイバー事案が発生した場合に想定される港湾機能への影響想定 6
2.2.2　港湾管理者等に求められる役割 6
3　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対応 8
3.1　事前準備 8
3.1.1　情報セキュリティに関する会議体の設置 8
3.1.2　休日・夜間を問わない連絡体制の構築 10
3.1.3　インシデント発生時における対処要領の策定 11
3.2　平時対策 12
3.2.1　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 12
3.2.2　情報セキュリティ対策に関する研修などの人材育成 13
3.3　インシデント発生時及び事後対応 15
3.3.1　インシデントの情報収集（リエゾンの派遣等） 15
3.3.2　道路混雑や滞船などの港湾の利用障害の情報発信 16
3.3.3　インシデントの原因究明への協力 17

はじめに

〔港湾管理者等編が想定する読者〕

港湾分野の重要インフラ事業者等においては、任務保証の観点から、TOS によるターミナルオペレーション等の安全かつ持続的な提供が求められる。コンテナ荷役の提供を不確かなものとするリスクを許容水準まで低減することは、港湾事業者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ある。

本ガイドラインの「港湾管理者等編」では、主に港湾管理者・港湾運営会社等において危機管理を担う部署・担当職員を対象にしており、港湾の管理・運営の観点及び港湾におけるサイバーレジリエンス強化の観点から、港湾管理者等として対応すべき事項とその考え方を示している。なお、本編は、当該港における重要インフラ事業者等の TOS 等システムが攻撃を受けた場合等の対応を示したものであり、港湾管理者等が所有・運用するシステムが、重要インフラサービスに該当する場合には、「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」をそれぞれ参照して対応する必要がある。

〔港湾分野における情報セキュリティ〕

港湾分野においては、令和５年７月の名古屋港における情報セキュリティ事案を受けて、「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））において、緊急に実施すべき対応策が示されるとともに、同取りまとめで示された3つの制度的措置（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それぞれの制度的措置）を進めている。

本ガイドラインは、サイバーセキュリティ基本法に基づき、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である。なお、本編は、当該港における重要インフラ事業者等の TOS 等システムが攻撃を受けた場合等の対応を示したものである。

港湾管理者・港湾運営会社等の危機管理担当部署・職員においては、本編を閲読し、理解した上で、必要な措置を講じることが求められる。

〔本ガイドラインの読み方〕

本ガイドラインの「港湾管理者等編」では、各対策項目について港湾管理者等に求める事項を、【港湾管理者等に求めること】として四角囲みで記述している。なお、それら事項は、本ガイドラインの性格上、あくまでも推奨事項である。

なお、本ガイドラインでは、対策項目を、港湾 BCP 等にならい、対策のフェーズ（「事前準備」、「平時対策」、「インシデント発生時及び事後対応」）で整理している。

1　港湾分野における「安全ガイドライン」の概要

1.1　港湾分野におけるセキュリティ管理策の現状

港湾分野における、国民生活や社会経済活動に影響を及ぼし事業継続の取り組み対象となるような重要システムは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（以下「TOS」という。）である。

TOS に障害が生じた場合でも、緊急の対応としてマニュアル作業で荷役を行うことも考えられるものの、代替運用時においては作業効率が著しく低下することや、大規模な港湾では取扱うコンテナ貨物量が膨大であるため、遅延の発生や搬入・搬出への支障の発生が予想される。

TOS は、コンテナターミナル内におけるコンテナの管理を主目的としたシステムであり、陸上輸送によるコンテナの搬入・搬出、コンテナターミナル内におけるコンテナの一時保管、海上輸送のための船舶へのコンテナの積卸しまで一貫してコンテナのデータを管理しているので、サイバー攻撃を受けて停止した場合、当該港湾におけるコンテナの搬入・搬出が止まる等大規模な重要インフラサービス障害につながる可能性がある。

港湾分野においては、令和 5 年 7 月の名古屋港における情報セキュリティ事案をはじめ、世界各国で、多くの事業者に影響を与える港湾事業に対するサイバー攻撃がここ数年起きており、復旧が遅れた場合、物流へ大きな影響を与える可能性があるため、多角的な対策の検討が必要である。

港湾分野の重要インフラ事業者等は、マルウェア感染や外部からの攻撃を防止する対策については各々実施している。しかし、パスワードリスト攻撃や標的型攻撃、ランサムウェア攻撃等をはじめとする昨今の複雑・巧妙化するサイバー攻撃全てを防ぐことは困難である。また、外部ネットワークと内部ネットワークとの境界による防御には限界があることから、従来の境界型のセキュリティ管理策に加え、内部ネットワークにも脅威が存在しうることを前提としたゼロトラストの考え方に基づき、データや機器等の単位でのセキュリティ管理策が必要である。

また、多くの重要インフラ事業者等で、セキュリティ管理策の継続的改善の実施が不十分であるという課題認識があることから、それぞれの事業者が目標とするセキュリティ水準に向けたセキュリティ管理策の継続的改善の実施が必要である。

1.2　「安全ガイドライン」の対象範囲

本ガイドラインにおける保護対象は、「重要インフラのサイバーセキュリティに係る行動計画（令和 6 年 3 月 8 日）」別紙1に掲げる「対象となる重要インフラ事業者等と重要システム例」及び同別紙2に掲げる「重要インフラサービスとサービス維持レベル」等の内容を踏まえ、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及び情報資産である。

港湾分野においては重要インフラサービス障害の発生によって荷役の遅延やコンテナの搬入・搬出の停止等物流に大きな影響を及ぼすターミナルオペレーションシステム（TOS）及びその中で利活用される情報資産[1]が挙げられる。

なお、例示されたシステム以外についても、事業者の責任において検討し抽出する必要がある。

[1] NISC「重要インフラのサイバーセキュリティに係る行動計画」別紙2 重要インフラサービスとサービス維持レベル　参照。
https://www.nisc.go.jp/policy/group/infra/siryou/index.html

港湾分野における、主要なシステムは以下の通りである。

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

港湾分野において、システムの不具合が引き起こす重要インフラサービス障害の例は以下の通りである。

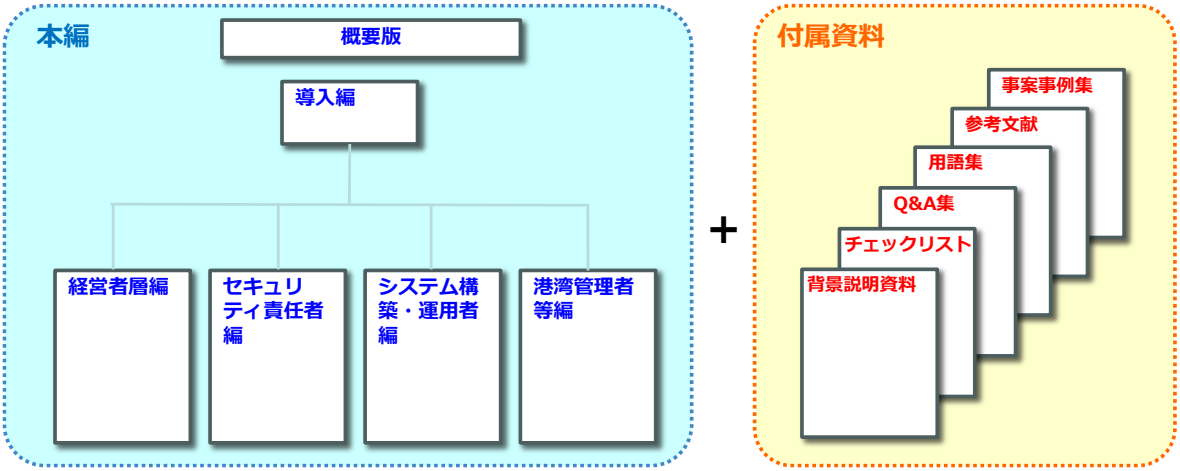
重要インフラサービス	システムの不具合が引き起こす重要インフラサービス障害の例
TOS によるターミナルオペレーション	荷捌きの効率低下、停止によるコンテナ貨物の搬入・搬出の停滞、停止

1.3 本ガイドラインの構成・読み方

本ガイドラインは、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等を整理した導入編と、TOS 等システムの安全管理と実施するための統制・管理について、重要インフラ事業者等の自組織内で想定される読者類型ごとに、「経営者層編」、「セキュリティ管理者編」、「システム構築・運用者編」の4編から構成する。加えて、重要インフラ事業者等のシステムがサイバー攻撃を受けた場合等に、港湾を管理・運営する立場である港湾管理者・港湾運営会社等が取るべき行動として「港湾管理者等編」をとりまとめている。

また、本ガイドラインの理解を深め、本ガイドラインに沿った対策を実施するための実践的なツール等の各種資料を「付属資料」として用意している。

【本ガイドラインの構成】



本「港湾管理者等編」では、主に港湾管理者・港湾運営会社等において危機管理を担う部署・担当

職員を対象にしており、港湾の管理・運営の観点及び港湾におけるサイバーレジリエンス強化の観点から、港湾管理者等として対応すべき事項とその考え方を示している。なお、本編は、当該港における重要インフラ事業者等の TOS 等システムが攻撃を受けた場合等の対応を示したものであり、港湾管理者等が所有・運用するシステムが、重要インフラシステムに該当する場合には、「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」をそれぞれ参照して対応する必要がある。

2　港湾のサイバーレジリエンス強化の考え方

2.1　港湾分野におけるセキュリティ強化に向けて

2.1.1 情報セキュリティ強化に向けた３つの制度的措置

港湾分野においては、令和５年７月の名古屋港における情報セキュリティ事案を受けて、当該事案の原因究明を行うとともに、同種事案の再発防止に向け、必要な情報セキュリティ対策や関連法令における港湾の位置付け等について整理・検討を行うため「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」を設置した。同検討委員会のとりまとめ「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）では、コンテナターミナルにおいて緊急に実施すべき対策とともに、港湾分野における情報セキュリティ強化に向けて、３ つの制度的措置（サイバーセキュリティ基本法の観点、港湾運送事業法の観点、経済安全保障の観点）が提言され、それぞれの取組を進めている。

サイバーセキュリティ基本法の観点では、「重要インフラのサイバーセキュリティに係る行動計画」において、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８日）、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）」を公表済みである。これにより、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している。なお、本ガイドライン（第２版）は、第１版の改訂版である。

港湾運送事業法の観点では、改正港湾運送事業法施行規則を施行（令和６年３月 31 日）し、港湾運送事業者に対し、一般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ている。これにより、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を導入している。

経済安全保障の観点では、改正経済安全保障推進法が公布され（令和 ６ 年 ５ 月 17 日）、TOS を使用して役務の提供を行う一般港湾運送事業が経済安全保障推進法の対象事業に追加された。これにより、当該設備（システム）の導入等に際して事前審査を行い、港湾運送の役務の安定提供の確保を図ることとしている。

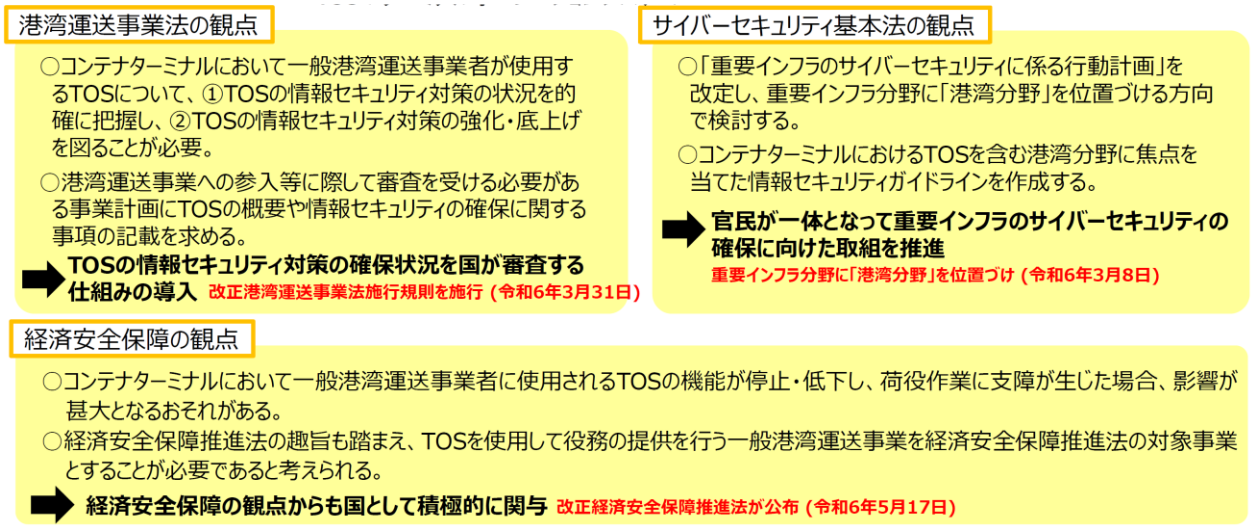


図　港湾分野における情報セキュリティ対策等推進のための3つの制度的措置

2.1.2 港湾のサイバーセキュリティ強化の考え方

サイバーレジリエンスとは、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によれば、「サイバーリソースを含むシステムに対する悪条件・ストレス・攻撃、または侵害を予測し、それに耐え、そこから回復・適応する能力」であるとされている。サイバーインシデント発生時には、セキュリティ担当者はその被害の封じ込め、復旧対応のために現場から経営者層までさまざまな部署の担当者と円滑に連携し、組織一体となって、サイバーレジリエンスを実現していくことが求められる。

一方で、サイバーレジリエンスの実現にあたっては、同じ企業の中の部署であっても、それぞれの部署がもつ専門性や文化の違いからサイバーインシデント対応において必要な連携の中でコミュニケーションエラーが発生しやすい可能性があり、また、サイバーインシデントを体験したことがある担当者が限定的であるため、対応のために必要なコミュニケーションスキルに個人差がある可能性があるといった課題が指摘されており、インシデント対応の演習・訓練等を通して、インシデント対応時のコミュニケーション能力の向上を図ることが求められる。

港湾分野においても、重要インフラ事業者等において、情報セキュリティ確保に関する知識や、インシデント対応時の経験を有する者が限定的と想定されることから、組織一体となってサイバーレジリエンスの実現に向けた取組を進めることが必要になる。さらに、事業者単独での対応には一定の限界があると予想されること、令和 5 年 7 月の名古屋港における情報セキュリティ事案にみるように、サイバー攻撃の影響が周辺地域だけでなく、国際物流及び国際的なサプライチェーンにも及ぶことから、重要インフラ事業者等のみならず、港湾管理者等港湾物流に係る関係者を含めた港湾分野全体あるいは地域（港）全体として、サイバーレジリエンス体制の強化を図ることが期待される。

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である。また、こうした関係者間の体制を、定期的な情報共有・交換や、共同での演習・訓練の実施等を通して、体制が自律的な仕組み（エコシステム）として機能させていくことが重要である。

2.2　サイバーレジリエンス強化における港湾管理者等の関与のあり方

2.2.1 サイバー事案が発生した場合に想定される港湾機能への影響想定

TOS 等システム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、あるいは、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、重要インフラ事業者等における重要インフラサービスの任務保証が実現できないばかりでなく、令和 5 年 7 月の名古屋港における情報セキュリティ事案にみるように、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、サイバー攻撃を受けた事業者においてシステム復旧に時間がかかること、何度もサイバー攻撃を受けることなどが生じた場合、当該ターミナルの信用の低下のみならず、当該港の信用低下にもつながることも懸念される。信用が低下すれば、当該港を利用していた船社・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、当該港湾の機能・サービス低下が懸念される。

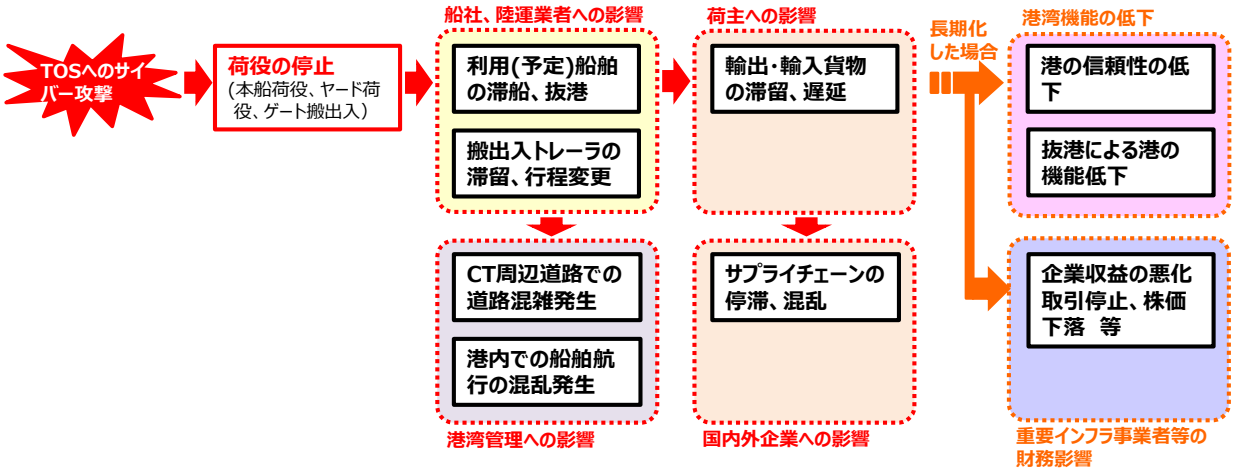


図　TOS 等へのサイバー攻撃による港湾機能等への影響想定

2.2.2 港湾管理者等に求められる役割

本ガイドラインでは、重要インフラ事業者等を対象に、「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」を作成している。重要インフラ事業者等は、本ガイドライン等を参考に、重要インフラの担い手としての意識に基づいて自主的に情報セキュリティ対策に取り組むことが求められている。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。

一方で、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る状況にあり、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た場合には、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、前述のとおり、背後圏経済、国際物流・国際サプライチェーンへの影響も懸念される。

以上のことから、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ことが求められている。

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ことも求められている。

本編では、重要インフラ事業者等が個別に実施するよりも、港湾管理者等が主導して合同で実施した方が効率的な取組内容や、インシデント発生時等において港湾を管理・運営する立場として港湾管理者等が実施すべき内容等について抽出し、事前対策、平時対策、インシデント発生時及び事後対応に区分して、港湾管理者等に求められる対応を記述している（3.1～3. 3）。なお、本編は、他編と同様に、推奨事項を列挙したものである。

コラム

COLUMN

サイバー攻撃を含めた緊急事態への対応計画策定に関する港湾管理者等の取組事例

近年、自然災害や犯罪やテロリズム、ミサイルや戦争・紛争、情報流出やサイバー攻撃、ネット炎上、感染症パンデミック等のあらゆる危機を対象にした危機管理として、ひとつの組織行動原則（オールハザード・アプローチ）で対応するという考え方が注目を集めている。

港湾においても、港湾活動に重大な危機が発生するおそれがあるハザードの1つとしてサイバー攻撃を位置付け、港湾管理者等の危機管理対応計画を策定していくことも考えられる。

◆名古屋港管理組合の「危機管理推進要綱」

- 名古屋港では、名古屋港において社会的影響の大きい危機が発生し又は発生する恐れがある緊急の事態に、迅速かつ的確に全庁をあげて統一的に対処する危機管理体制（機動的な編成）や基本的事項を定め、名古屋港における危機管理を推進し、もって名古屋港における港湾活動への被害の防止・軽減を図ることを目的として、2023 年 8 月に「名古屋港管理組合危機管理推進要綱」が制定されている。
- 同要綱における危機の定義として、「名古屋港に係るサイバー攻撃」が最初に例示されており、他では、港湾の整備・管理に支障を来す事件・事故、油流出及び大量漂流物による海洋汚染を伴う事故、クルーズ船における事件・事故、にぎわい施設における事件・事故があげられている。
- 同要綱では、組合内の危機管理体制、危機発生時の対処体制フロー、危機発生時の組合内連絡体制フロー、平時の対策、危害発生時の対策、収束時の対策等が記載されている。

3　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対応

3.1　事前準備

3.1.1 情報セキュリティに関する会議体の設置

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等に対して、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としている(【セキュリティ責任者編 1.9.インシデントに備えた組織体制(CSIRT 等)の整備】参照)。また、セキュリティインシデントが発生した場合には、自組織内の情報共有を行うとともに、専門組織への情報共有、国・港湾管理者等への情報共有、都道府県警察への通報を行うとしている(「セキュリティ責任者編」3.2 参照)。加えて、TOS 等の情報セキュリティに関するグッドプラクティスやヒヤリハットを各 TOS 等の情報セキュリティ担当者間で共有する枠組みを構築することが望ましいとしている(【セキュリティ責任者編 2.1.3 情報共有】参照)。

令和 5 年 7 月の名古屋港における情報セキュリティ事案における対応において、「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)では、グッドプラクティスとして、日頃より情報セキュリティ研修等の場を通じて愛知県警と名古屋港運協会との関係が構築できていたことにより、事案発生時の相談、対応がスムーズになされた点があげられている。その一方、初動対応時にサイバーセキュリティ専門家の意見を聞く場面がなかったことが課題としてあげられている。

上記の点を踏まえ、港湾管理者等は、港湾のサイバーセキュリティ強化に向け、重要インフラ事業者等の社内外の情報共有体制の構築を事業者のみに委ねるのではなく、港湾管理者等が主導するかたちで、当該港内の各重要インフラ事業者等、都道府県警察、国の機関、地方港運協会、セキュリティ専門機関(JPCERT 等)等が一堂に会し情報共有・情報交換する会議体(協議会等)を設置して、インシデント発生に備えて、平時から関係者の顔が見える関係を築くことが望ましい。

会議体の設置にあたっては、都道府県警察が設置する「サイバーテロ対策協議会」等に、重要インフラ事業者等及び港湾管理者等が参加することも有効な方法の1つではあるが、「サイバーテロ対策協議会」等は他分野の重要インフラ事業者等も含まれることから、港湾分野に特化した会議体を別途設置することが望ましい。

また、港湾分野においては、港湾管理者及び港湾において活動を行う様々な関係者から構成される会議体として、港湾 BCP 協議会や、港湾 BCP(感染症対策)協議会、港湾保安委員会等が、既に組織化されており、それら既存の協議会等の枠組みを参考とすることも有用である。なお、既存の会議体を活用する場合には、情報セキュリティを担当する者がメンバーであるかなど、適切なメンバーであるかの確認は必要である。

〔具体例〕

●情報セキュリティに関する会議体(例)

＜名古屋港の例＞

・ 名古屋港管理組合は、令和 5 年 7 月の情報セキュリティ事案に係るシステム復旧後、名古屋港運協会と連携協力し、「NUTS システムサイバーセキュリティ対策連携会議」を設置。連携会議では、以下の内容について討議。
  - ✓ 危機事案発生時における情報共有・連絡体制等の構築
  - ✓ 更なるセキュリティ強化に向けた対策
  - ✓ 今後の名古屋港管理組合の支援・協力のあり方 等
・ また、組合内部では、効率的な対策を迅速かつ的確に講じるため、「NUTS システムサイバーセキュリティ対策本部」を立ち上げ、上記連携会議と両輪で機能しながら必要な対策を推進。

＜東京港の例＞
・ 東京都港湾局は、2024 年 7 月に、警視庁と合同で各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。
・ 会議では、以下の内容を実施。
  - ✓ 令和 5 年 7 月の名古屋港における情報セキュリティ事案の概要を説明
  - ✓ 警視庁担当者からサイバー攻撃の情勢や対策等について講演
  - ✓ 実際のサイバー攻撃がどのように進んでいくかを示す実演
  - ✓ 個別相談会の実施 等

3.1.2 休日・夜間を問わない連絡体制の構築

【港湾管理者等に求めること】

- 港湾管理者等は、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。
- 構築した連絡体制を、連絡体制図・連絡表等として文書化し、文書を関係者間で共有する。

〔解説〕

本ガイドラインでは、重要インフラ事業者等に対して、セキュリティインシデントが発生した場合には、自組織内の情報共有を行うとともに、専門組織への情報共有、国・港湾管理者等への情報共有、都道府県警察への通報を行うこととしている(【セキュリティ責任者編 3.2 重要インフラサービス障害発生時の情報共有】参照)。また、自組織内では、エスカレーションとして、従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにすることとしている(【セキュリティ責任者編 1.9.3 エスカレーション】参照)。

港湾管理者等においても、休日、夜間を問わず、事案発生時に連絡のとれる体制とすることが望ましい。連絡体制として、部署名、担当者名(複数名)、平日連絡先(電話番号、E メールアドレス)、休日・夜間連絡先(携帯電話番号等)を記載した連絡先リストとともに、情報疎通の経路・内容を示した連絡体制図を作成し、関係者間で共有しておくことが望ましい。また、担当者異動等の際には随時更新することが望ましい。

3.1.3インシデント発生時における対処要領の策定

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等に対して、セキュリティインシデントが発生した場合には、自組織内の情報共有を行うとともに、専門組織への情報共有、国・港湾管理者等への情報共有、都道府県警察への通報を行うこととしている(【セキュリティ責任者編 3.2 重要インフラサービス障害発生時の情報共有】参照)。また、障害の状況や復旧等の外部への情報共有・情報発信において、港湾管理者と事前に役割分担をしておくことも有効であるとしている(【セキュリティ責任者編 3.3 セキュリティ管理状況の対外説明】参照)。

重要インフラ事業者等が迅速・円滑・適切に関係者と情報共有を行うためには、インシデント発生時に、重要インフラ事業者等以外の各機関がどのような役割を果たすことになるかを重要インフラ事業者等が理解しておくことも重要である。

そのため、港湾管理者等は、インシデント発生時の対処方針の決定方法や、インシデント発生時における関係者の役割分担を明確にし、関係者間で共有・報告すべき情報内容(事案の種類ごとの報告・共有すべき情報)、外部への情報発信窓口(マスコミ対応含む)における役割分担等について事前に定め、これらをインシデント発生時の対処要領として策定しておく。

策定した対処方針は、文書化し、関係者に共有するとともに、関係者間での周知・徹底を図る。

〔具体例〕

●インシデント発生時の対処要領の策定の考え方(例)

- 「港湾の事業計画策定ガイドライン(改定版)」(令和２年５月)では、緊急時に必要な対応を確実に実施するためには、あらかじめ手順を整理し、定めておくことが重要であるとしている。
  - ✓ 緊急時の連絡体制
  - ✓ 関係者の役割・責任
  - ✓ 指揮命令系統
  - ✓ 権限委譲や、代行者及び代行順位 等
- また、初動段階で実施すべき具体的な対応のうち、手順や実施体制を定め、必要に応じてチェックリストや記入様式などを用意し、これらの対応の実施について時系列で管理ができる全体手順表(アクションシート)や個々の行動の詳細内容、責任部署(者)、行動に必要な資材の在処等を項目ごとに１ ページに記した行動手順書(アクションカード)なども用意しておくとよいとしている。

3.2 平時対策

3.2.1 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

【港湾管理者等に求めること】

> ➢ 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等は、セキュリティインインシデント対応手順の確認等を行う訓練を定期的に実施することとしている。また、システム障害やサイバー攻撃を想定したものを含むBCP(事業継続計画)に関する訓練を定期的に実施することとしている(【セキュリティ責任者編 2.3 演習・訓練】参照)。

港湾のサイバーセキュリティ強化に向けては、重要インフラ事業者等の自組織内のインシデント対応手順の訓練に加えて、インシデント発生時に実際に情報連絡・情報共有することになる関係者も参加した合同の演習・訓練が効果的である。

港湾管理者等は、3.1.1 の会議体を活用する等により、港湾管理者等が主導して、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定期的に企画・実施することが望ましい。また、NISC や都道府県警察等外部機関が実施するサイバーセキュリティ演習に、関係者合同で参加することも有用である。

〔具体例〕

●インシデント対応訓練(例)

＜米国国土安全保障省の例＞

- 米国国土安全保障省(DHS)と国土交通省港湾局との共催により、日本の港湾でサイバー攻撃が発生した際の影響や対策について理解を深めるために、ディスカッションを主とする机上演習を実施(令和 6 年 8 月 21～22 日)。当日は演習シナリオを基に、日本の政府関係機関や港湾関係者が対応を議論し、米国側出席者と意見交換を行うなど、活発な演習が行われた。
- 演習参加者は以下の通り(オブザーバーを含む)

日本　政府関係機関　:国土交通省(港湾局、総合政策局)、海上保安庁、内閣官房(国家安全保障局、内閣サイバーセキュリティセンター)、警察庁等
港湾関係者　:港湾管理者、港湾運送事業者、警察本部、システム関係企業等
米国　:国土安全保障省、沿岸警備隊、サイバーセキュリティ・インフラストラクチャセキュリティ庁、在日米国大使館 等

●サイバーセキュリティ演習への参加(例)

＜名古屋港の例＞

- 名古屋港管理組合は、NISC が提供する 2023 年度分野横断的演習疑似体験プログラムに、名古屋港運協会とともに参加。
- また、シンガポールマリタイムウィーク期間中(シンガポール海事港湾庁(MPA)主導で発足)に開催された、サイバーセキュリティ演習に参加。

3.2.2 情報セキュリティ対策に関する研修などの人材育成

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等は、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・訓練を行うこととしている(【セキュリティ責任者編 2.2 人材育成・意識啓発】参照)。

サイバー攻撃が複雑化・巧妙化する中、重要インフラ事業者等が任務保証を実現するためには、組織全体を通じたサイバーセキュリティへの意識の底上げと組織内の適切な連携が重要となる。「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・意識啓発を行うことが求められる。

港湾管理者等は、港湾のサイバーレジリエンス強化に向けて、重要インフラ事業者等が行う、従業員等の情報セキュリティに関する意識向上やインシデント対処能力向上の取組に対する支援を行うことが望ましい。支援の内容としては、例えば、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発信や、情報セキュリティ対策に関する研修・セミナーの実施(外部講師の招へい含む)、都道府県警察等が実施するセミナーの案内等が考えられる。また、3.1.1 で設置する会議体の定期的な開催等を通じて、TOS 等の情報セキュリティに関するグッドプラクティスやヒヤリハットを各 TOS 等の情報セキュリティ担当者間で共有することも有効である。

〔具体例〕

●セキュリティ対策に関する説明会の実施(例)

＜東京港の例＞

- 東京都港湾局では、令和 5 年 7 月の名古屋港における情報セキュリティ事案を受けて、東京港内の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実態調査を行い、調査結果等を踏まえ、東京港において特に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。
  - ✓ 実態調査は、東京都デジタルサービス局と連携し、専門的な観点から分析
  - ✓ 社名等を秘匿した上で、専門家が調査結果を確認し、ターミナル毎に必要な対策等を個別にフィードバック

コラム

COLUMN

重要インフラ事業者等との協働によるリスク兆候の検知体制の高度化事例

海外港においては、リスク兆候の検知体制の高度化に向けて、港湾管理者等（ポートオーソリティ）が重要インフラ事業者等（港湾運送事業者等）と協働して、事業者の通信ログを解析し、リスク兆候検知を行っている事例がある。港湾管理者等は、より関心の高い重要インフラ事業者等に対して、事業者と協働しながら、こうした更なる高度化メニューを今後提供していくことも考えらえる。

◆ロサンゼルス港CRC（サイバー・レジリエンス・センター）

- CRC （Cyber Resilience Center）は、サプライチェーンエコシステム（ターミナルオペレーター、船会社、鉄道会社、トラック会社等のステークホルダー）のサイバーリスクを軽減するため、2023 年に設置（ロサンゼルス港湾局の独自財源で対応）。IBM により運営。
- 物流に大きな影響を与える恐れのある悪意あるサイバーインシデントの検出と同種のインシデントからの防護のため、ステークホルダーへの早期警報システムとして、インシデントに関する情報共有や制御方法の調整を実施。CRC のサービスは無料。
- CRC と各ステークホルダーは MOU（覚書）を締結しており、ステークホルダーは自主的にサイバーセキュリティ関連情報のログを提供。CRC が異常を検知した場合は、速やかに関係ステークホルダーに報告。

3.3 インシデント発生時及び事後対応

3.3.1 インシデントの情報収集(リエゾンの派遣等)

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等は、セキュリティインシデントが発生した場合には、自組織内の情報共有を行うとともに、専門組織への情報共有、国・港湾管理者等への情報共有、都道府県警察への通報を行うこととしている(【セキュリティ責任者編 3.2 情報インフラサービス障害発生時の情報共有】参照)。

港湾管理者等は、港湾内の状況把握の観点から、インシデント発生情報を入手した際には、当該重要インフラ事業者等に対して、システム障害の内容や港湾荷役業務への影響等について自ら情報収集(事業者へのリエゾンの派遣含む)を行うことが望ましい。あわせて、インシデントが発生した事業所以外から、同様のことが発生していないか、影響が発生していないか、今後影響が発生するおそれはないかなどの情報を収集することが望ましい。

3.3.2 道路混雑や滞船などの港湾の利用障害の情報発信

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等は、セキュリティインシデントが発生した場合には、情報共有や情報発信を行うにあたり、情報提供及び問合せ対応の窓口を設定することとしている。また、港湾管理者等と事前に役割分担をしておくことも有効であるとしている(【セキュリティ責任者編 3.3 セキュリティ管理状況の対外説明】参照)。

令和５年７月の名古屋港における情報セキュリティ事案では、システム障害により港湾荷役が停止したことで、コンテナターミナル(CT)周辺の道路では、CTへの搬出入待ち車両による渋滞が発生し、利用者からの苦情やマスコミからの問い合わせが港湾管理者に殺到した。また、荷役スケジュールに影響が生じた船舶は 37 隻に及び、最大 24 時間程度の遅延が発生した。搬入・搬出に影響があったコンテナ約２万本(推計)の他、トヨタ自動車の愛知県と岐阜県にある４つの拠点の稼働停止、アパレルメーカーにおける衣類の入荷遅延等の経済活動への影響も報道されている。

上記の事態を踏まえ、港湾管理者等は、港湾を管理・運営する立場から、港湾荷役の停止・遅延によって生じる、当該施設周辺の道路混雑や、当該施設利用予定船舶の滞船等の船舶航行の混乱に対し、関係省庁と連携し、情報収集及び混雑等緩和に向けた適切な情報発信を行うことが望ましい。

また、情報発信にあたっては、情報発信及び問合せ対応の窓口担当者を予め複数指定しておくとともに、情報発信内容について重要インフラ事業者等との間で役割分担を決めておくことが望ましい。

なお、港湾管理者等は、港湾荷役の停止が数週間継続する場合や、事態終息後にも当該港の信用・評判が回復しない場合(レピュテーションリスク)等には、当該港の信頼維持・回復に向けて、適切な情報発信を行うことが望ましい。

また、荷役停止の長期化が見込まれる場合には、代替港利用の選択肢が発生する可能性もあり、そのような場合には、既存の港湾 BCP における港湾間の連携スキームを活用する等、必要に応じ、円滑な代替港利用に向けた支援を行うことが望ましい。

3.3.3 インシデントの原因究明への協力

【港湾管理者等に求めること】

- 港湾管理者等は、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。

〔解説〕

本ガイドラインでは、重要インフラ事業者等は、セキュリティインシデントが発生した場合には、策定したコンティンジェンシープラン及び事業継続計画等を実行し、早急にその状況を把握し、被害の拡大防止、早期復旧のための対策を講ずることとしている(【セキュリティ責任者編 3.1 コンティンジェンシープラン及び BCP の実行】参照)。また、発生したインシデント管理として、既存のセキュリティ管理策の運用を通じて得た経験等を分析し、今後の運用に活用することとしている(【セキュリティ責任者編 3.4 インシデント管理】参照)。

令和 5 年 7 月の名古屋港における情報セキュリティ事案における対応において、「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)では、改善点として、原因究明やシステム復旧後のシステムのセキュリティ対策状況が適切であるかどうか確認するためにも、情報セキュリティ事案発生時にサイバーセキュリティ専門家と直ちに相談できるよう、日頃から関係を構築しておくことが望ましいとしている。

事態収束後のインシデントの原因究明は、一義的には当該重要インフラ事業者等が行うものであるが、港湾の重要インフラ事業者等の場合、他の分野の重要インフラ事業者と比べて、必ずしも事業規模が大きくないことから、事業者単独では原因究明に限界が生じることも予想される。そのため、港湾管理者等は、港湾機能の維持に向けたサイバーセキュリティリスクの軽減のため、重要インフラ事業者等の求めに応じ、事業者が行うインシデントの原因究明や事後検証、対策の改善、改善策の有効性のモニタリング等に関して、国とともに協力を行うことが望ましい。

〔具体例〕

●有識者、港湾関係者による検討会(例)

＜国土交通省港湾局の例＞

- 国土交通省港湾局では、令和 5 年 7 月の名古屋港における情報セキュリティ事案を受けて、当該事案の原因究明を行うとともに、同種事案の再発防止に向け、必要な情報セキュリティ対策や関連法令における港湾の位置付け等について整理・検討を行うため「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」を設置した。
  - ✓ 委員会メンバーは、有識者、港湾関係事業者(港湾運送事業者、港湾管理者、業界団体等)、行政関係者(NISC、国土交通省合政策局、国土交通省港湾局等)
- 検討委員会での討議内容は以下の通り。
  - ✓ 事案の検証(事案の概要及び対応状況、感染経路、問題点の抽出と改善点、グッドプラクティス)
  - ✓ 緊急に実施すべき対応策(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、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) 等

コラム

COLUMN

港湾地域におけるサイバーセキュリティに係るコミュニティの形成事例

海外港においては、港湾地域産業のサイバーレジリエンス強化に向けて、港湾管理者や警察機関、地元自治体等公的機関と、立地企業や民間事業者から構成される、サイバーセキュリティに関するコミュニティを形成している事例がある。

港湾管理者等は、当該港において設置する情報セキュリティに関する会議体を、単に情報共有・連絡体制構築の場とするのみならず、更に発展させて、人材育成や演習・訓練、脆弱性評価、原因究明等を包括的に行う地域コミュニティの形成を促していくことも考えられる。このようなコミュニティが形成されることで、本ガイドラインの効果的な運用とともに、港のサイバーレジリエンス体制が自律的な仕組み(エコシステム)として機能していくことが期待される。

◆ロッテルダム港 FERM

- ロッテルダム港では、港湾地域産業のサイバーレジリエンス強化に向け、「FERM」という組織を設立している。設立にあたり、ロッテルダム港湾会社、警察、ロッテルダム市等公的機関が出資し、FERM のサービスを受ける民間事業者がパートナーとして参加している(参加費用を支払い)。
- 港湾地域産業には、オイル・化学(石油精製及びプロセス産業)、一般貨物(コンテナ物流及びブレークバルク貨物)、バルク貨物(ドライバルク及びタンク貨物)のサプライチェーンと、主要セクターとして、物流サービス提供者、産業サービス提供者が含まれる。
- FERM のサービスとして、最新で関連性の高い脅威情報の提供や、共同でのサイバー演習(年 1 回以上)、年次レポートの発行、トレーニング及び教育プログラムの提供、ペネトレーションテストや組織固有の脅威情報分析等セキュリティサービスの共同調達(追加サービス)を実施している。
- このほか、年数回、「ポートサイバーカフェ」を開催し、ロッテルダム港湾地域におけるサイバーセキュリティの最新トピックについて、専門家との議論を実施している。
- 業界の ISAC とも協力関係にあるが、ISAC は参加企業が限定されており、情報共有が自動化されていないのに対し、FERM はより多くの組織にアクセスし、レジリエンス向上のためのサービスを提供している。情報共有においても、特定の脅威情報を収集・分析し、それを分かりやすく説明する積極的な取組を行っている。