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）

～導入編～

令和７年３月28日

国土交通省港湾局

目次

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。また、重要インフラはその性質上、安全かつ持続的なサービス提供が求められていることから、その防護に当たっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を可能な限り減らすとともに、障害発生の早期検知や、障害の迅速な復旧を図ることが重要である。

国土交通省では、これまで、所管する4分野（鉄道、航空、空港、物流）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、「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」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きた。

昨今、新型コロナウィルス感染症の影響により、我が国の社会・経済活動は大きな打撃を受け歴史的な変革を求められており、テレワークや WEB 会議、クラウドサービス、IoT 等の ICT を活用することによる緊急事態発生時での事業継続、働き方改革への対応、事業者が行うデジタルトランスフォーメーション（DX）及び Society 5.0 への対応等、従来のサイバーセキュリティモデルでは十分賄えない新たな課題が生まれている。このような加速度的に進んでいるサイバーセキュリティを取り巻く環境変化に対応するため、関連する最新の基準、ガイドライン等に基づき、新たに重要インフラの分野として位置づけられた港湾についても「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」を策定したものである。

本ガイドライン（第2版）は、令和 6 年 4 月に策定した第 1 版の内容に、「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）で提言されている対策内容を盛り込むとともに、重要インフラ事業者等（港湾運送事業者等）が所有するシステムがサイバー攻撃を受けた場合等に、当該港の港湾管理者・港湾運営会社等に求められる対応内容を追記し、再整理したものである。

1 「安全ガイドライン」策定の背景

1.1 「安全ガイドライン」の目的と位置づけ

1.1.1「安全ガイドライン」の目的

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、「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)」に記載された「任務保証(【1.1.5「安全ガイドライン」における用語の定義(10)】参照)の考え方」を踏まえ、サービスの提供に必要な情報システム(【1.1.5「安全ガイドライン」における用語の定義(5)】参照)のセキュリティを確保するなど、必要な対策に取り組むことが重要である。具体的には、サイバーセキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を実現することなどであり、特に、経営者層(【1.1.6 責任者・組織等の役割(1)】参照)が積極的に関与し、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付け、サイバーセキュリティに係るリスクマネジメントの実施等により、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要となっている。

このため、それぞれの事業分野において、その特性に応じたセキュリティ管理策の水準を示し、個々の重要インフラ事業者等が、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取り組み、対策の実施や検証に当たっての目標を定めることが「安全ガイドライン」の目的である。

1.1.2「安全ガイドライン」の形態

各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。

このことを踏まえ、「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」(以下、「指針」と称す)においては、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「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

※安全基準等に該当する文書類は、「安全(Safety)」の実現のために作成されたものに限定されないことに留意。

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り、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している。

1.1.3「安全ガイドライン」の位置づけ

「安全ガイドライン」には、重要インフラ分野においてサービス提供継続及び重要インフラ利用者（【1.1.5「安全ガイドライン」における用語の定義（3）】参照）の信頼性に応えるとの観点から、サイバーテロ対策を始めとして、災害や非意図的要因などサービス提供に影響を及ぼす可能性のある様々な事象を念頭に置き、セキュリティ管理策を実施する場合に何らかの対処がなされていることが望ましい項目、及び対処すべき内容を列挙する。

また、それぞれの事業分野の特性に応じて重要インフラ事業者等が活用し易い基準等とするとの視点から、各事業分野の特性や現状をもとにした、想定事象、対処方針等について記述する。

このため、「安全ガイドライン」における対策項目は、「指針」で示されている文書構成に沿って、「指針」及び以下に示す「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」を始めとした国内外で用いられるベストプラクティスやスタンダード（基準）等を基に、各分野において必要と想定される事項を補足して構成する。

（1）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

重要インフラにおける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の実現を図る観点から、安全基準等において規定が望まれる項目を整理・記載したもの。

なお、サイバーセキュリティ確保に向けて取り組む際の重要事項が、組織統治におけるサイバーセキュリティ、リスクマネジメントと危機管理、対策項目の構成で記載されている。

令和５年７月４日にサイバーセキュリティ戦略本部決定されている。

（2）政府機関等のサイバーセキュリティ対策のための統一基準群

国の行政機関や独立行政法人等（以下「政府機関等」という。）の情報セキュリティ水準を向上させるための統一的な枠組みであり、政府機関等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定したもの。統一基準群の運用により、政府機関等それぞれの組織において適切なセキュリティ管理策の実践、見直し、改善を行い、政府機関等全体としてのサイバーセキュリティの確保を図ることとしている。サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 25 条第1項第2号に基づき、現在、令和５年７月４日に令和５年度版がサイバーセキュリティ戦略本部決定されている。

（3）情報セキュリティ管理基準

経済産業省が策定し、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実践規範であり、情報セキュリティ監査において、評価判定基準として用いられる。情報セキュリティに係るマネジメントサイクル確立のための標準規格である JIS Q27001:2014 及び JISQ27002:2014 との整合を取る形で構成されている。

平成 15 年に初版を策定後、平成 28 年３月１日に平成 28 年改正版が策定されている。

（4）事業継続ガイドライン

内閣府の取り組みとしての事業継続計画の普及、促進のため、中央防災会議「民間と市場の力を

活かした防災力向上に関する専門委員会」の下に設置された、「企業評価・業務継続計画ワーキンググループ」において作成されたガイドライン。
平成 17 年 8 月 1 日に第一版が発行されており、令和 5 年 3 月に最新の改訂版が発行されている。

(5) 個人情報の保護に関する法律についてのガイドライン(通則編)
個人情報の保護に関する法律の第7条第1項の規定に基づき定められた「個人情報の保護に関する基本方針」(平成 16 年 4 月 2 日閣議決定)を受け、事業者が個人情報の適正な取扱い確保に関して行う活動を支援すること、及び当該支援により事業者が講ずる措置が適切かつ有効に実施されることを目的として、個人情報の保護に関する法律(平成 15 年法律第 57 号)第 4 条、第 8 条及び第 60 条に基づき具体的な指針を定めたガイドライン。

(6)その他参考となるガイドライン
・ISO/IEC27000 ファミリー
情報セキュリティマネジメントシステム(ISMS)に関する国際規格であり、要求事項を規定した規格と、ISMS 実施の様々な側面に関する手引きを規定した規格から構成されている。

・IEC 62443 シリーズ
産業用オートメーション及び制御システム(IACS:Industrial Automation and Control System)のセキュリティを確保するための国際標準規格である。IEC 62443 は 2024 年 8 月時点で 18 分冊が提案、開発、または発行されている。規格の内容は ISA(International Society of Automation)内の規格開発グループである Workgroup 99(ISA99)と共同で開発されている。IEC 62443 が活用されている分野は、化学、石油、ガス、パイプライン、機器製造、電力分野などでセキュリティ対策の標準規格の一つとして参照されており、鉄道、ビルオートメーション、医療機器分野などでも注目されている。

・制御システムのセキュリティリスク分析ガイド
重要インフラや産業システムの基盤となっている制御システムのセキュリティリスク分析を事業者が実施できるようにするため、IPA(独立行政法人情報処理推進機構)セキュリティセンターが作成している。

・サイバーセキュリティ経営ガイドライン
経済産業省と IPA が、サイバー攻撃から企業を守る観点で、経営者が認識すべき「3原則」及び経営者が最高情報セキュリティ責任者(CISO)(【1.1.6 責任者・組織等の役割(2)】参照)に指示すべき重要項目をまとめ、公開している。

・重要インフラのサイバーセキュリティを向上させるためのフレームワーク
米国国立標準技術研究所(NIST)が、サイバーセキュリティの効果的・効率的なリスク低減を

実現するために「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能から、適切なサイバーセキュリティ対策のあり方を示し、2014 年に公開している。

2024 年 2 月には、サイバーセキュリティフレームワークバージョン 2.0(CSF2. 0)が発表されている。CSF2.0 への改訂では、中小企業を含むジあらゆる企業や組織での利用が進むように再設計され、従来の5つの機能に加え、新たに「ガバナンス」機能が追加されている。また、サプライチェーンのリスク管理に必要な対策項目が大幅に追加されている。

・海事分野におけるサイバーリスク管理のガイドライン

IMO(国際海事機関)は海事分野におけるサイバーセキュリティに関する取組を段階的に強化している。2004 年に採択された ISPS コード(国際船舶・港湾施設保安コード)は、直接的にサイバーセキュリティ対策を求めるものではないが、リスク評価や対処計画において、コンピュータシステムやネットワークの脆弱性への対処ならびに電子形式の機密情報の保護に関する手順の確立を求めている。

2017 年には、船舶の安全管理システムにサイバーリスク管理を組み込むことを推奨する決議がなされ(MSC.428)、その実施を支援するため、船舶運航におけるサイバーリスク管理に関するガイドラインが承認されている(MSC FAL.1/Circ.3)。

また、2022 年 6 月には、同ガイドラインにおける参考ガイダンスの1つとして、IAPH(国際港湾協会)の「港湾及び港湾施設のためのサイバーセキュリティガイドライン」が組み込まれている。

※国際規格や各国が定めたガイドラインではないが、さらに参考として、一般社団法人運輸総合研究所が発行しているサイバーセキュリティに関する各種手引き等もある。

(7) 内部統制システムとサイバーセキュリティとの関係

組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。経営者層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各組織が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各組織において決定されるべきである。また、組織の意思決定機関は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定することでもよい。

1.1.4「安全ガイドライン」の見直し

セキュリティの脆弱性は、事業や情報資産(【1.1.5「安全ガイドライン」における用語の定義(7)】参照)を取り巻く加速度的な環境の変化の影響を受けるものであることから、「安全ガイドライン」についてはセキュリティを取り巻く環境の変化や関連する各種規格、国内外のベストプラクティス等に応じ、継続的な改善を行うことが必要である。

よって、国土交通省及び所管する重要インフラ分野の事業者等は、相互に協力し、各重要インフ

ラ分野における重要インフラサービス障害(【1.1.5「安全ガイドライン」における用語の定義(2)】参照)の発生状況等を踏まえ、「安全ガイドライン」が適宜適切なものとなるよう、随時検討を行っていく。

また、重要インフラ事業者等において有効な障害対応体制の構築がなされているかを精緻に把握することを目的に、国土交通省は、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段について調査分析し、各施策の改善に活用する。

1.1.5「安全ガイドライン」における用語の定義

本ガイドラインにおいて使用する用語の定義は、次の各項に定めるところによる。

(1)重要インフラ事業者

サイバーセキュリティ基本法第 12 条 2 項第 3 号に規定する重要社会基盤事業者(国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生じるものに関する事業を行う者)であり、港湾の場合、主要な港湾運送事業者や港湾管理者等である。

(2)重要インフラ事業者等

本ガイドラインでいう、“等”には、港湾関係全ての港湾運送事業者、港湾管理者等を意味している。

(3)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。

(4)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。

(5)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(経営者層や幹部など)、委託先の関係者などを含む。)をいう。

(6)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。

(7)制御システム

社会インフラや工場・プラントの監視・制御や生産・加工ラインにおいて、他の機器やシステムを

管理・制御するために用いられている機器群をいう。

(8)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

(9)重要システム
重要インフラサービスを提供するために必要な情報システム及び制御システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者等ごとに定めるもの。港湾分野においては、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が該当する。

(10)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、各々の組織の経営者層・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。

(11)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。

(12)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)。

(13)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。

(14)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。

(15)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者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。

1.1.6 責任者・組織等の役割

各重要インフラ事業者等内における責任者・組織等の役割を以下のとおり定義する。

なお、該当する責任者・組織等そのものが存在しない場合、同様の役割を担っている役割・組織等に読み替えること。

(1) 経営者層

経営者層は、重要インフラ事業者等の社会的責任として、サイバーセキュリティを確保するよう取り組むこと。また、自らがリーダーシップを発揮し、任務保証の考え方を踏まえて対応すること。

なお、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)に示されたように、組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した経営者層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。

また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営者層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

個人情報の漏えい等によって第三者が損害を被ったような場合、経営者層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う点についても留意する必要がある。

(2)最高情報セキュリティ責任者(CISO)

最高情報セキュリティ責任者は事業者内における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)であり、対策を推進する上での最終決定権及び責任をもつこと。

組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮すること。

(3)情報セキュリティ委員会

情報セキュリティ委員会は、情報セキュリティ対策に関する事業者内基準を策定し、必要に応じて見直しを行うこと。

また、適切な責任及び資源配分によって、組織内におけるセキュリティを推進すること。

さらに、情報セキュリティに対する意識を醸成し、保つために、幹部をはじめとした全ての取扱者等が情報セキュリティの重要性を認識し、対策を理解し実践するために必要な教育・訓練等を計

画的に実施すること。

（4） 情報セキュリティ担当者

情報セキュリティ担当者は、セキュリティ管理策の運用が可能となる組織のまとまりごとの取りまとめの責任者（組織のまとまりの単位が事業部である場合、事業部長クラスが相当）であり、所管する組織のセキュリティ管理策を推進及び運用するため、組織内の体制整備及び事務を行うこと。

また、組織内の実施手順を策定するとともに、セキュリティ管理策の運用実態を十分踏まえ、実務レベルでの管理の仕組みを確立し、全ての取扱者への責務の周知や教育を行う等、個別対策を機能させる環境を整備すること。

（5） 情報セキュリティ責任者（CISO 等）

本ガイドラインでは、最高情報セキュリティ責任者（CISO）及び情報セキュリティ担当者、監査責任者等情報セキュリティ安全管理の実務を担う担当者を、「情報セキュリティ責任者（CISO 等）」と呼ぶ。

（6） システム構築・運用者

システム構築・運用者は、主管する単位における情報システムにおいて、企画、開発、運用、保守等のライフサイクル全般を通じて必要となるセキュリティ管理策の責任を持つこと。また、セキュリティ管理策の技術的事項について補佐する者を必要に応じて選任すること。

（7） セキュリティリスクアセッサー（評価者）

業務観点及びシステム観点でのセキュリティリスク評価（文書レビュー、脆弱性診断等）を実施する主体。セキュリティリスク評価結果や是正対応の推奨策をシステム構築・運用者へ進言すること。また、システムのセキュリティリスク対応状況をモニタリングし、セキュリティ上問題がある場合、システム構築・運用者や情報セキュリティ責任者に対して勧告、提言を行うこと。

（8） CSIRT（Computer Security Incident Response Team）

CSIRT は、組織において発生したセキュリティインシデントに対処するため設置する体制のことで、インシデント関連情報、脆弱性情報、攻撃予兆情報等を収集、分析し、対応方針や手順の策定などの活動をすること。

（9） 取扱者

取扱者は情報セキュリティ委員会等が作成した基準、規程等のルールを認識・理解し、これを遵守すること。テレワークやクラウドサービスの普及により、取扱者も使用する端末の管理や設定、認証情報の管理などに責任をもつこと。

1.2 「安全ガイドライン」の運用について

1.2.1 重要インフラ事業者等の担う範囲

重要インフラ分野では、国民生活や社会経済活動に重大な影響を及ぼさないように、重要インフラサービス障害に対するサイバーセキュリティの確保を適切に行うことが重要である。

その中で重要インフラ事業者等の保有する重要なシステム等に係るサイバーセキュリティの確保については、各重要インフラ事業者等が自らの管理下にある情報資産に責任を持ち、それぞれの事業形態や情報システムの形態に適応したセキュリティ管理策を講じていくことが原則である。

したがって、重要インフラ事業者等には、「安全ガイドライン」を適切に参照しながら、自己の対策が十分であるかを自己検証しつつ、必要に応じてセキュリティ管理策の改善を図ることが求められる。

また、情報及び情報システムの取扱いに関しては、法令及び規制等(以下「関連法令等」という。)においても規定されているため、セキュリティ管理策を実践する際には、関連法令等を遵守する必要がある。

なお、公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保のために、重要インフラに関与するあらゆる組織が、経済社会活動の相互依存関係の深化が進みリスクが高度化・複雑化していることを認識しつつ、サプライチェーン全体を俯瞰し責任ある行動をとることが期待される。

このため、重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者についても、サイバーセキュリティ基本法第7条(サイバー関連事業者その他の事業者の責務)の責務が認識され、責任ある行動がとられるよう取り組む。

1.2.2 適用状況の評価について

重要インフラ事業者等は、「安全ガイドライン」に対する適用状況等を定期的に点検し、必要に応じて対策の改善を行う必要がある。

重要インフラ事業者等が自身のセキュリティ管理策の妥当性を確認したい場合は、以下を例とする第三者認証制度を活用することを推奨する。

(1) ISMS 適合性評価制度

重要インフラ事業者等の組織が情報を適切に管理し、機密を守るための包括的な枠組みである。コンピュータシステムに係るセキュリティ管理策だけでなく、情報を扱う際の基本的な方針としてのセキュリティ方針や、それに基づいた具体的な対策の計画・実施・運用、及び見直しまでを含んでいる。

一般財団法人 日本情報経済社会推進協会(JIPDEC)が、事業者の ISMS が JIS Q27001:2014 に準拠していることを認証する「ISMS 適合性評価制度」を運営している。

(2) プライバシーマーク制度

一般財団法人 日本情報経済社会推進協会(JIPDEC)が管理する、個人情報取り扱いに関する認定制度である。

個人情報について JIPDEC の定める基準を満たして適正に管理していると認定されれば、使用許諾を得ることができる。審査基準は基本的に JIS Q15001(個人情報保護マネジメントシステム―要求事項)に準拠している。

(3) IT セキュリティ評価及び認証制度 (JISEC)

IT 関連製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて第三者(評価機関)が評価し、その評価結果を認証機関が認証する制度である。本制度は主に政府調達において活用されている。

(4) 情報セキュリティ監査制度

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、評価結果をもって保証を与えあるいは助言を行う活動のことである。

2　港湾分野における「安全ガイドライン」の概要

2.1　港湾分野における現状と課題

2.1.1 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。

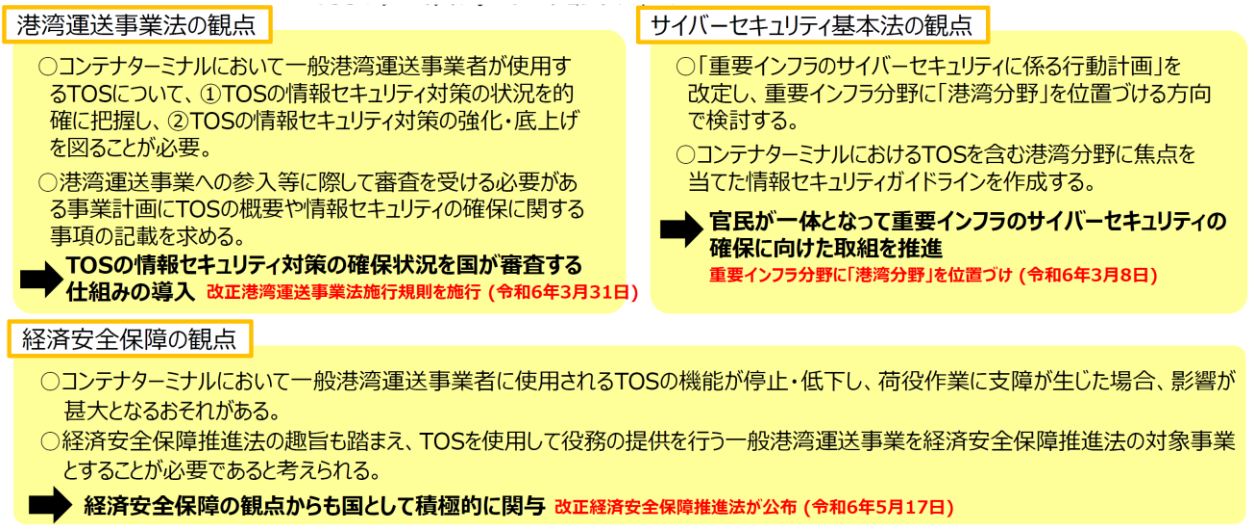


図　港湾分野における情報セキュリティ対策等推進のための3つの制度的措置

また、物流の 2024 年問題に対し、物流の総合的な環境整備の一環として、デジタル技術を活用した見える化、効率化を推進する政策が検討されている。今後、情報システムや新技術の導入がより浸透していくことが予想される港湾分野においては、セキュリティ管理策の徹底に加え、サイバーセキュリティに関する新たなリスクにも対応していかなければならない。

以下、サイバーセキュリティ・インシデント事例(コラム参照)で掲載したように、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。

コラム
港湾におけるサイバーセキュリティ・インシデント事例

◆2023 年 11 月 DP ワールド・オーストラリア

オーストラリアの海上物流の 40%の取り扱いを行う港湾運営会社である同社システムへのサイバー攻撃の疑いから、システムを遮断した。このため主要な 4 港(メルボルン、シドニー、ブリスベン、フリーマントル)のコンテナターミナルの運行に影響が生じ、3 日の操業停止、1 週間程度の混乱が起きた。(出典:ロイター他)

◆2023 年 10 月 米国 Estes Express Lines 社

米国大手貨物自動車運送会社でありバージニア州リッチモンドに本拠を置く同社は、大規模サイバー攻撃を受け IT インフラが停止した。ターミナルとドライバーは手動に切り替えて貨物の集荷と配達を継続した。同社は、X(旧 Twitter)上にフォームを設置したり、重要な情報を伝達するために従業員の個人携帯電話を使用したりするなど、顧客との双方向コミュニケーションを促進するために代替チャネルを使用するという手段を行った。また、どのシステムを最初にオンラインに戻すかについて的確に判断することが可能であったため、一か月近くかかったが早期の復旧が可能となったと言われている。

(出典:Center for Strategic & International Studies, 全米自動車貨物交通協会(NMFTA))

◆2023 年 7 月 名古屋港

名古屋港のコンテナターミナルで発生したシステム障害について、名古屋港運協会は「ランサムウェア」に感染していたことを明らかにした。(次ページに詳細)

◆2022 年 2 月 米国 Expeditors 社(物流会社)

NASDAQ 上場企業であるエクスペディターズ・インターナショナルは、2022 年 2 月 20 日に標的型サイバー攻撃の対象となったと判断したと発表。このインシデントを発見した後、同社はグローバル・システム環境全体の安全を管理するために、ほとんどのオペレーティング・システム(統合情報管理システム)を世界中でシャットダウンした。システムがシャットダウンされている間、貨物の発送の手配や荷物の通関や流通活動の管理等の業務を行う能力が制限された。同社のサービスには、航空及び海上貨物の混載または転送、通関仲介、ベンダー混載、貨物保険、時間指定輸送、注文管理、倉庫保管および配送、カスタマイズされた物流ソリューションが含まれる。

同社によると、調査と修復のためのサイバー攻撃に関連する費用を負担しており、今後もこの種の費用が発生し続けることが予想されること、また同社の業務停止の長さに応じて、サイバー攻撃の影響が道社の事業、収益、業績、評判に重大な悪影響を与える可能性があることを投資家向け広報で明らかにした。(出典:Expeditors 社の IR プレスリリースより)

◆2017 年 6 月 オランダ ロッテルダム港

ロッテルダム港がランサムウェア攻撃を受け、2 つのコンテナターミナルの活動が麻痺。マースクは 4,000 台のサーバと 45,000 台の PC のネットワークを再構築する必要があり、数億ドルの費用がかかった。(出典:ENISA)

【2023 年 7 月 名古屋港】

2023 年 7 月 4 日、名古屋港の 5 つのコンテナターミナル及び集中管理ゲートで運用されている名古屋港統一ターミナルシステム(以下「NUTS」という。)が、大規模なサイバー攻撃を受けて停止し、約 3 日間にわたり名古屋港のコンテナの搬入・搬出が止まる等物流に大きな影響を及ぼした。日本における港湾施設にとって初めてとなる大規模サイバー攻撃の事例である。

＜被害＞

物理サーバ基盤及び全仮想サーバが暗号化され、以下の影響を与えた。

- 荷役スケジュールに影響が生じた船舶 37 隻
  (NUTS の停止によりマニュアル作業で荷役を行うが、最大 24 時間程度の遅延。)
- 搬入・搬出に影響があったコンテナ約 2 万本(推計)

その他、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。

＜感染経路＞

サーバ内のデータが全て暗号化されておりログを解析することが困難なため、感染経路を断定することはできない。しかしながら、サーバ部への直接的な攻撃が行われた可能性が高く、VPN 機器からの侵入が行われたと考えられる。

NUTS の保守用 VPN には緊急時に即時に対応するため外部から接続する IP アドレスに制限をかけておらず、ID とパスワードさえ合致すればインターネット上で誰からでもアクセス可能な状態にあったこと、VPN 機器及び物理サーバに関して数か月前から脆弱性が公表されていたものの、これら脆弱性への対応が未対応であったことが確認されている。

＜対応＞

7 月 4 日、6:30 頃、NUTS システムが停止したことを確認したことによりインシデントが発覚。システム保守会社及びシステム開発会社へ調査を依頼した。

9:00 頃、愛知県警察本部サイバー攻撃対策隊に連絡。インシデント発生後早い段階で、名古屋港運協会幹部の指示の下、同ターミナル部会が招集された。復旧までの間、事実上の意思決定機関として機能し、港湾での物流を早期に再開させるために、システムの復旧を優先するように決定した。

7 月 6 日、7:15 頃 バックアップデータから NUTS システムの復旧を完了。

14:15 頃 データと実在庫情報の整合性の確認を開始。準備が整ったターミナルより順次再開した。

尚、システムが停止した間も、マニュアル作業により船舶との間の荷役が継続された。

(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検討委員会資料)

2.1.2 港湾分野のセキュリティ管理策における課題

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難しい状況にある。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。

重要インフラサービスを提供する上では、制御システムも重要な資産となり得る。制御システムは従来独自の規格で構成され稼働していたが、昨今汎用化が進み、国際標準の通信規格等が使われることが多くなっている。そのため、情報システムと同等の脆弱性対策が求められるが、安全性・可用性が最優先される制御システムにおいてはウィルス対策ソフトの導入や、パッチ適用等の脆弱性対応が難しい実態にある。一般的に制御システムは耐用年数が長く長期間使用されるため、内部で使用される汎用ソフトウェアは修正パッチの提供対象外となることも少なくない。また、可用性の観点からソフトウェアのバージョンアップが保守対象外となるケースもあり、セキュリティ対策が不十分になりやすい事を認識する必要がある。

2.2　本ガイドラインの保護対象と対策の要点

2.2.1 本ガイドラインの保護対象

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 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。

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

- ターミナルオペレーションシステム（TOS）

  港湾運送事業において、船舶への貨物の積込、船舶からの貨物の取卸しに対する計画の管理、コンテナターミナル内におけるコンテナの配置計画等の管理、コンテナターミナル内におけるコンテナの管理・監視、各機能を総合的に管理およびゲート管理や外部システムとの連携を行うシステムが重要な役割を担っている。

  港湾運送事業では、コンテナ単位でデータ管理をする必要があるため、膨大なデータ処理が必要である。ターミナルオペレーションシステムが有する機能により、こうしたデータの処理を効率的に行うことができる。

  標準的なターミナルオペレーションシステムの機能には以下のものがある。

  ①　本船プランニング

[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

船舶への貨物の積込、船舶からの貨物の取卸しに対する計画の管理

② ヤードプランニング
コンテナターミナル内におけるコンテナの配置計画等の管理
ゲートシステム

③ ヤードオペレーション
コンテナターミナル内におけるコンテナの管理・監視等

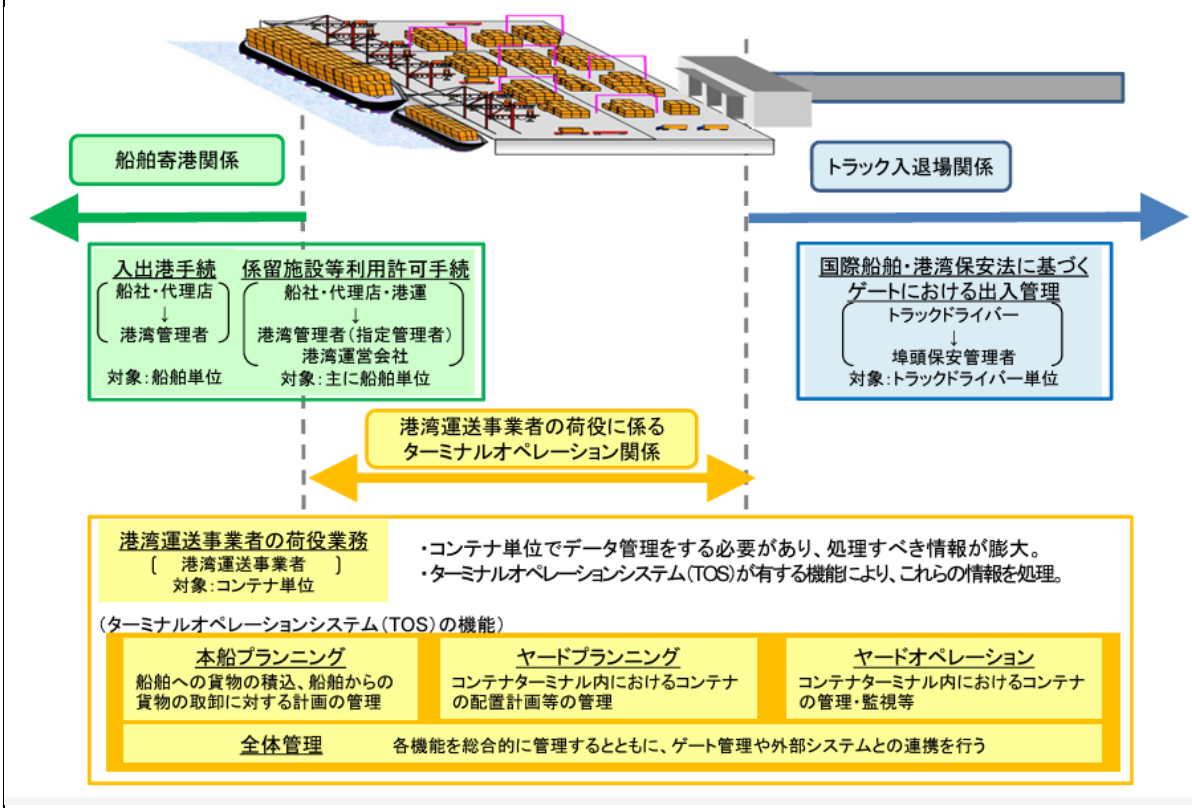
④ 全体管理機能
各機能を総合的に管理するとともに、ゲート管理や外部システムとの連携を行う

ターミナルオペレーションシステムにおいて、取り扱うデータは、コンテナのマスターデータ、履歴、在庫データ等である。サーバシステムはターミナル内のサーバやデータセンターに設置するオンプレミスで保存されていることが多いが、今後はクラウドサービス等の利用の増加も考えられる。データのバックアップ管理について注意を払う必要があると考えられる。専門性の高いシステムであるため、保守に関しては外部委託を利用する機会が多いと考えられるため、保守に関する記録管理等も注意を払う必要がある。

（写真出典：コンテナターミナルにおける情報セキュリティ対策等検討委員会資料）

コンテナターミナルの機能提供に必要なシステムについて

コンテナターミナルでは、港湾運送事業者の荷役に係るターミナルオペレーション関連業務が行われており、船舶輸送業、倉庫業、自動車運送業等多くの事業者との物品・データのやり取りが行われている。



（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検討委員会資料）

2.2.2 本ガイドラインにおける対策の特徴、要点

本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え港湾分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめた。具体的には、昨今のサイバー攻撃動向や港湾分野の事業特性に応じた脅威という観点から、標的型攻撃対策、パスワードリスト攻撃対策等を示した。

また、本ガイドラインの第 1 版改訂にあたり、「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）で提言されている対策内容を盛り込むとともに、重要インフラ事業者等が所有するシステムがサイバー攻撃を受けた場合等に、当該港の港湾管理者・港湾運営会社等に求められる対応内容を追記した。

本ガイドラインにおいて、重要インフラ事業者等に求める対策の要点としては、以下の4点である。

- ✓ 要点①ネットワークの分離
- ✓ 要点②アクセス制御
- ✓ 要点③バックアップ
- ✓ 要点④インシデント対応体制・手順の整備

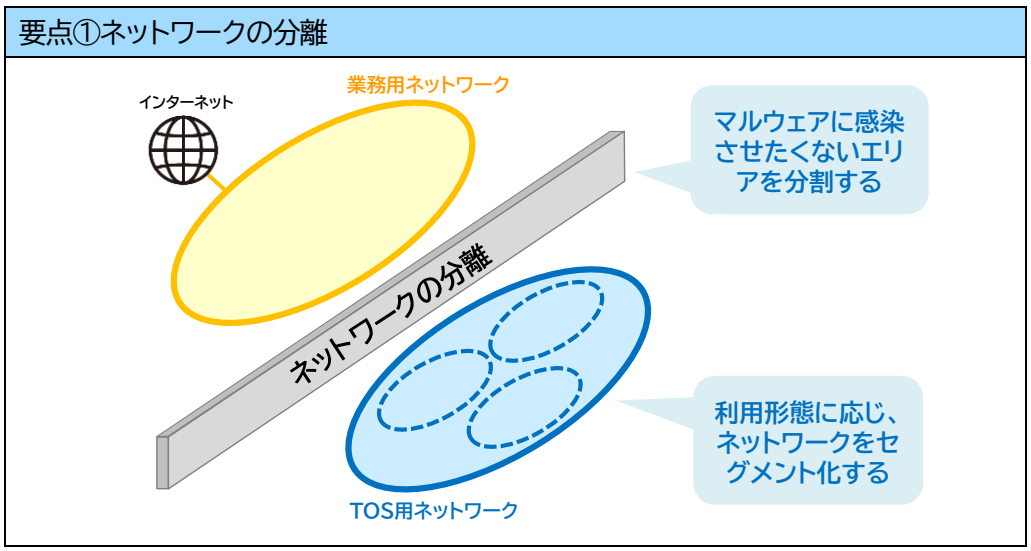


図 本ガイドラインで重要インフラ事業者等（港湾運送事業者等）に求める対策のポイント（1／2）

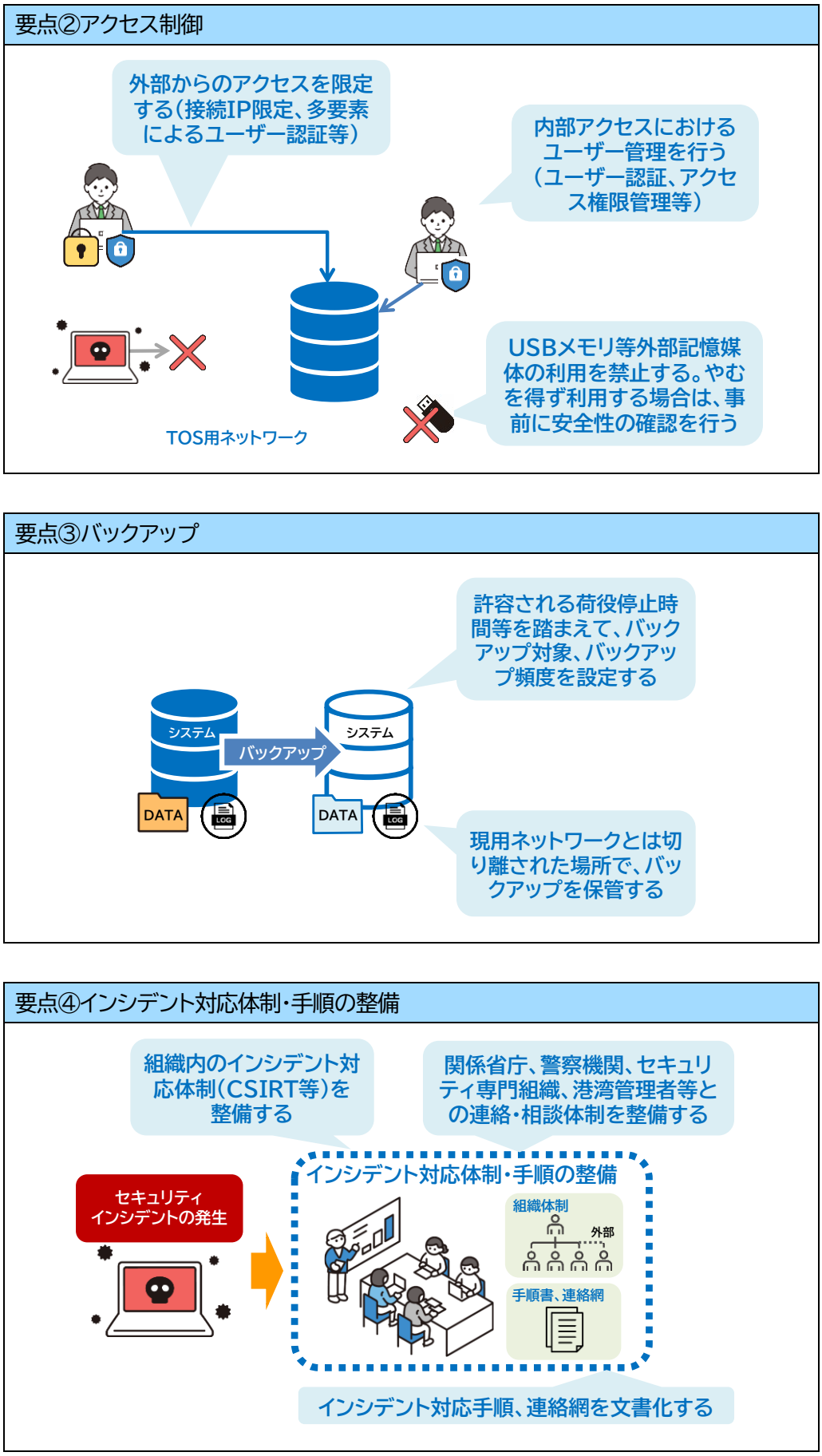


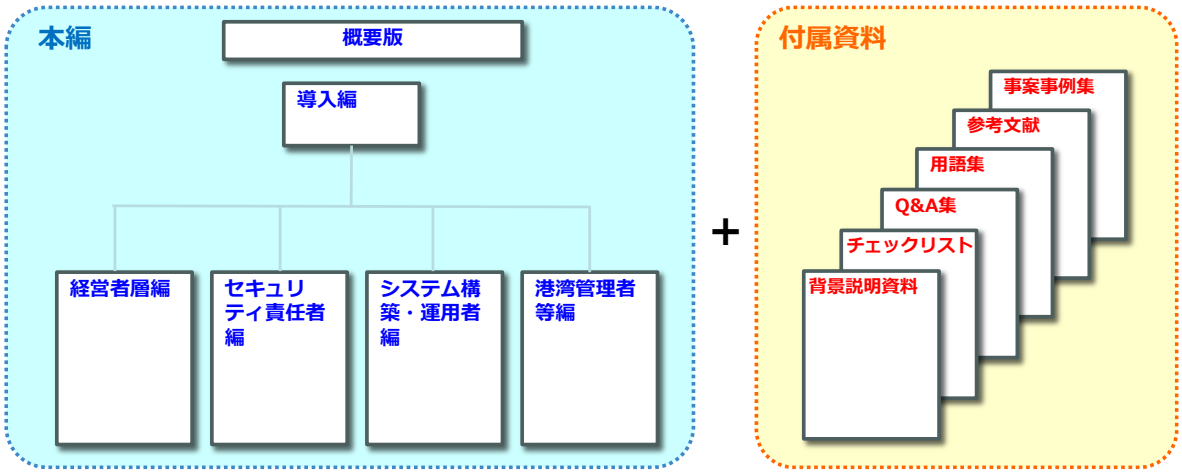
図　本ガイドラインで重要インフラ事業者等（港湾運送事業者等）に求める対策のポイント（2／2）

2.3　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】



2.3.1 各編の目的・概要

「導入編」では、本ガイドラインの目的や対象、港湾分野の特性に加え、各編を理解する上で前提となる考え方等を示している。

「経営者層編」では、主に重要インフラ事業者等において組織の経営方針を策定し、意思決定を担う経営者層を対象にしており、組織統治の観点から、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している。

「セキュリティ責任者編」では、主に重要インフラ事業者等において TOS 等システムの安全管理及びセキュリティリスクの管理の実務を担う担当者（責任者）を対象にしており、リスクマネジメントの観点から、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している。

「システム構築・運用者編」では、重要インフラ事業者等において TOS 等システムの実装・運用の実務を担う担当者を対象としており、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として対応すべき事項とその考え方を示している。なお、TOS 等システムの実装・運用においては、システムベンダー等に外部委託することも考えられるため、委託事業者においても本編を参照の上、

重要インフラ事業者等と協働する必要がある。その際、業務や役割、責任分担のあり方については、あらかじめ両者で取り決めておくことが必要になる。

「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。

2.3.2 本ガイドラインの読み方

「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。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。

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出で必要となる項目(強制要件)については、下線を付している。

また、「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」においては、対策内容によっては、読み手間で重複する内容があるため(【2.3.3 第１版との関係 表1】参照)、対策の全体像の把握及び対策に関係する主体がどのような対応を実施しているのかを理解するために、関連する他編の章・節を合わせて理解しておくことが望ましい(表 1 において●印の記載のある項目)。

「港湾管理者等編」では、上記と同様に、【港湾管理者等に求めること】として四角囲みで記述し、その下に〔解説〕、〔具体例〕を記述している。なお、港湾管理者等者に求めることの内容は、あくまで推奨事項である。

2.3.3 第１版との関係

本ガイドライン(第2版)は、第１版(令和６年４月)の内容に、「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)における対策内容を盛り込み再整理し、読者類型毎に分冊化(「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」)するとともに、新たに、港湾の管理・運営の立場からの対応として「港湾管理者等編」を追加したものである。また、付属資料を新たに追加したものである。

なお、本ガイドラインでは、第１版での対策項目を、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」)で再整理している。

表1　本ガイドラインの読み手別の重複関係　凡例 各読み手の分冊で記載している項目（数字は章・節）　● 関連する項目（他の読み手の分冊を参照し、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	●