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
1　「安全ガイドライン」策定の背景 1
1.1　「安全ガイドライン」の目的と位置づけ 1
1.1.1　「安全ガイドライン」の目的 1
1.1.2　「安全ガイドライン」の形態 1
1.1.3　「安全ガイドライン」の位置づけ 2
1.1.4　「安全ガイドライン」の見直し 4
1.1.5　「安全ガイドライン」における用語の定義 5
1.1.6　責任者・組織等の役割 7
1.2　「安全ガイドライン」の運用について 9
1.2.1　重要インフラ事業者等の担う範囲 9
1.2.2　適用状況の評価について 9
2　港湾分野における「安全ガイドライン」の概要 11
2.1　港湾分野における現状と課題 11
2.1.1　港湾分野におけるセキュリティ管理策の現状 11
2.1.2　港湾分野のセキュリティ管理策における課題 15
2.2　本ガイドラインの保護対象と対策の要点 16
2.2.1　本ガイドラインの保護対象 16
2.2.2　本ガイドラインにおける対策の特徴、要点 19
2.3　本ガイドラインの構成、読み方 21
2.3.1　各編の目的・概要 21
2.3.2　本ガイドラインの読み方 22
2.3.3　第１版との関係 22

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。

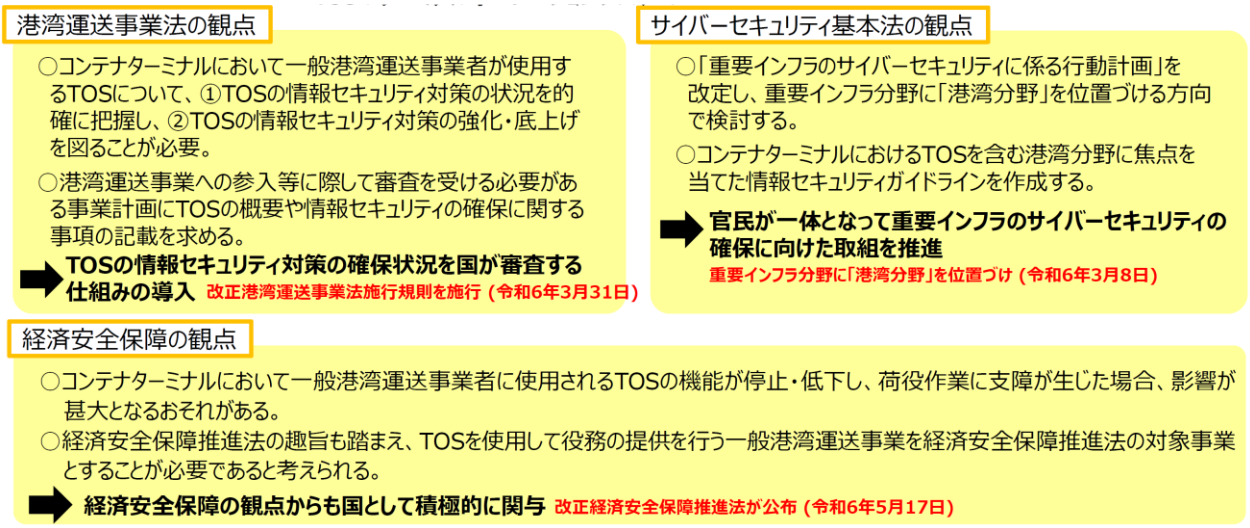


図　港湾分野における情報セキュリティ対策等推進のための3つの制度的措置

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

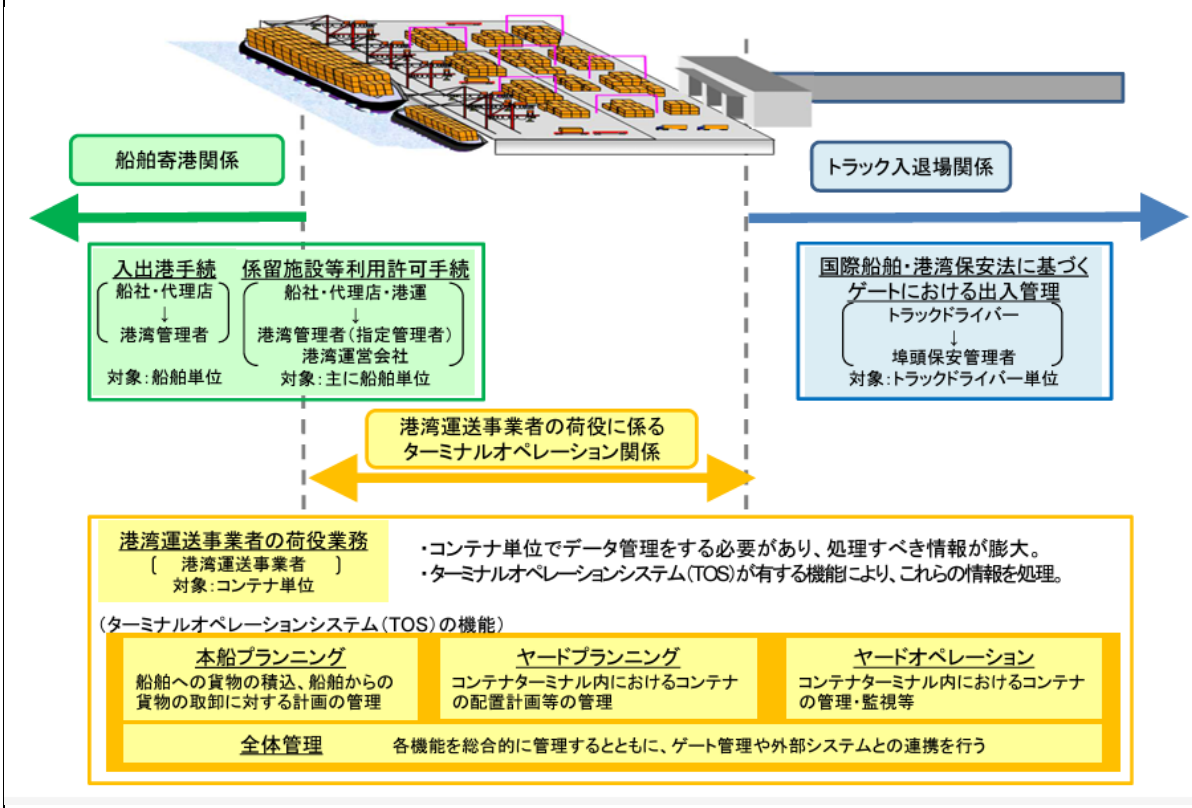
④ 全体管理機能
各機能を総合的に管理するとともに、ゲート管理や外部システムとの連携を行う

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

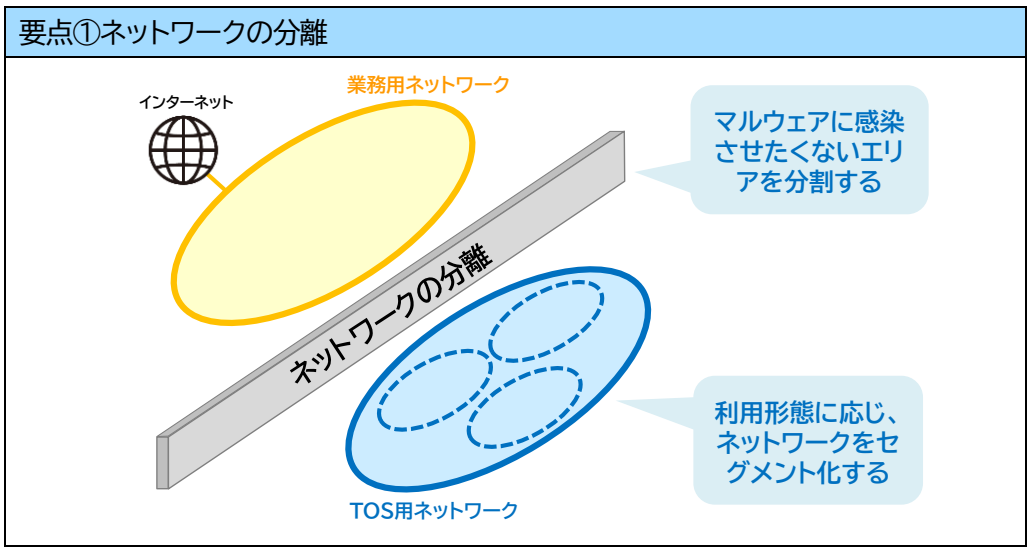


図 本ガイドラインで重要インフラ事業者等（港湾運送事業者等）に求める対策のポイント（1／2）

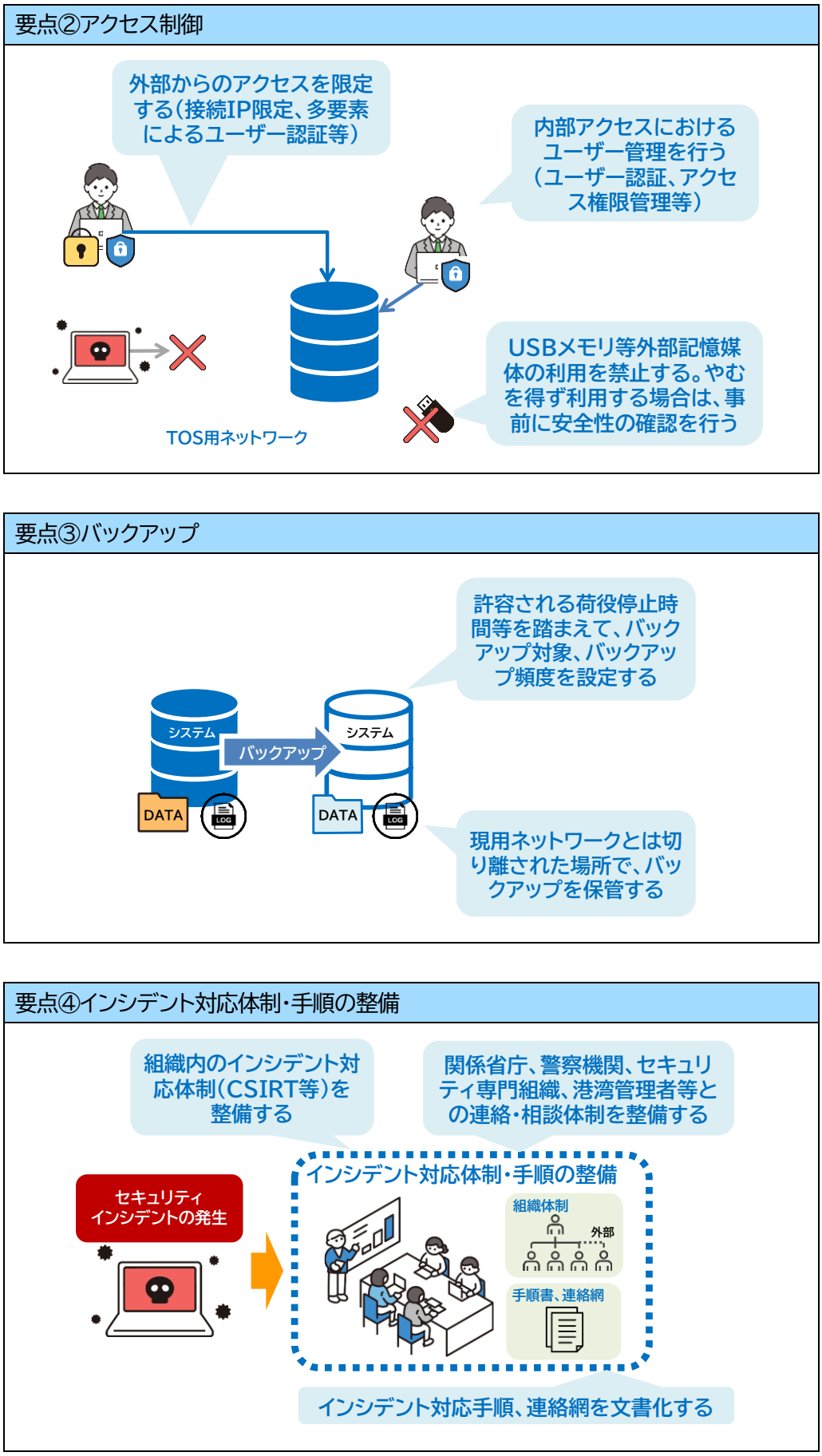


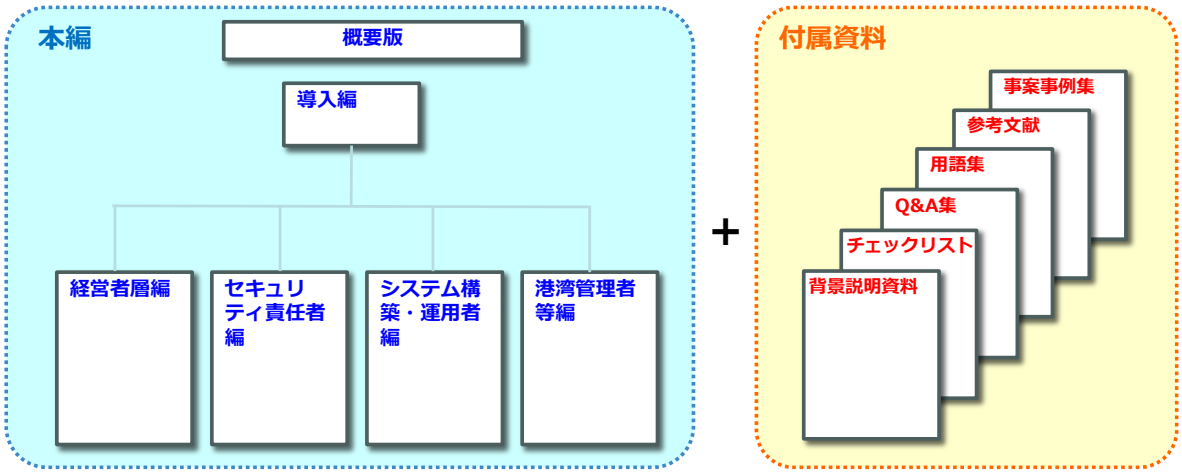
図　本ガイドラインで重要インフラ事業者等（港湾運送事業者等）に求める対策のポイント（2／2）

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	●

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）

～経営者層編～

令和７年３月28日

国土交通省港湾局

目次

はじめに
1　事前準備 1
1.1　組織方針 1
1.1.1　組織方針とサイバーセキュリティ 1
1.1.2　サイバーセキュリティ方針 3
1.2　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 4
2　平時対策 6
2.1　組織内外のコミュニケーション 6
2.2　責任及び権限の割当て 8
2.2.1　情報セキュリティ責任者の任命 8
2.2.2　責任者・組織などの役割 10
2.2.3　役割の分離 12
2.3　資源の確保 13
2.4　監査・モニタリング 14
2.4.1　セキュリティ対策の運用状況の把握 14
2.4.2　セキュリティ対策の監査 15
3　インシデント発生時及び事後対応 16
3.1　情報開示 16
3.2　インシデント対応及び事業継続対応 17

はじめに

〔経営者層編が想定する読者〕

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、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、その実践は経営者層としての責務である。

本ガイドラインの「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。

〔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。

重要インフラ事業者等の経営者層においては、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「経営者層編」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。

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（【導入編２. 3.3 第１版との関係】の表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（【導入編】表 1 において●印の記載のある項目）。

1　事前準備

1.1　組織方針

1.1.1 組織方針とサイバーセキュリティ

【事業者に求めること】

- 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る。
- 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。

〔解説〕

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や、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、当該事業者における財務影響が懸念される。

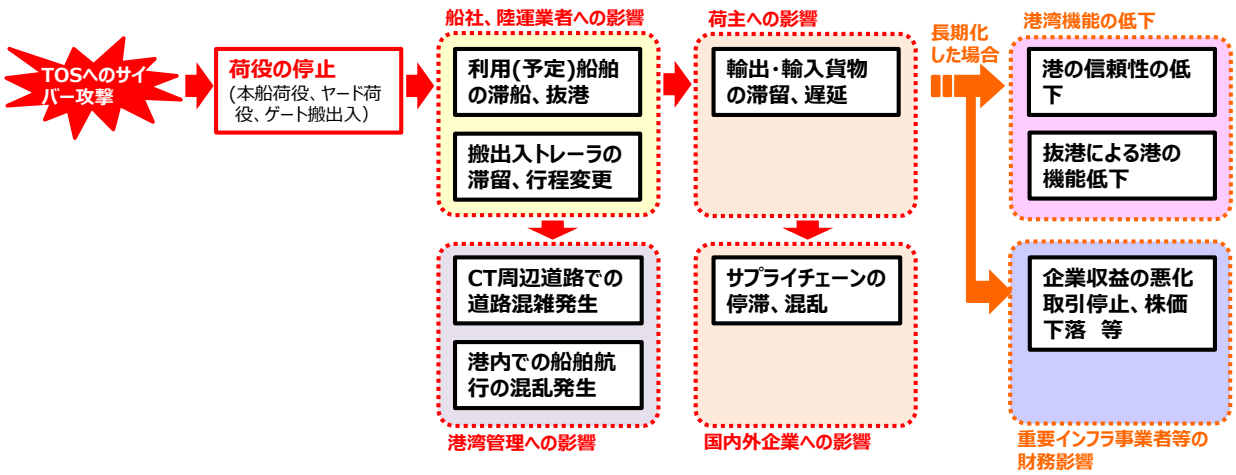


図　TOS 等へのサイバー攻撃による港湾機能等への影響想定

経営者層は、サイバー空間からのリスクは任務保証を阻害しうるものであることを踏まえ、組織全体でサイバーセキュリティ確保に努めるため、取締役会等においてサイバーセキュリティリスクも取扱い、適切にリスク管理をすることとし、組織方針においてその実践を明記し、宣言する。

また、任務保障を果すために維持するサービスの範囲・水準を組織方針に組み入れることが望ましい。

〔具体例〕

●組織方針に組み入れる事項(例)

- 「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」
- 「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」
- 「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」
- 「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」
- 「ゼロトラストセキュリティの考え方を組み入れたセキュリティ管理策の実施」

●維持するサービス水準の望ましい水準(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〇〇時間以内」等を記載する。」
  （例）コンテナ荷役　〇〇時間
- 復旧目標の設定にあたっては、当該港・ターミナルにおいて、どの程度の期間サービスを停止したら顧客が逃げてしまうか等を勘案することが重要である。
- 対外的な情報発信の意味でも、復旧目標を設定することが望ましい。

1.1.2 サイバーセキュリティ方針

【事業者に求めること】

- 経営者層は、セキュリティ対策に取り組むことをサイバーセキュリティ方針等に含め、組織の内外に対して宣言する。

〔解説〕

重要インフラ防護のためには、セキュリティ管理策における根本的な考え方(以下、「サイバーセキュリティ方針」という。)を示す必要がある。

経営者層は、セキュリティ対策に取り組むことをサイバーセキュリティ方針等に含め、組織の内外に対して宣言する。

最高情報セキュリティ責任者は、重要インフラ防護の目的、目指す方向、セキュリティ対策にて守るべき対象等を明らかにし、サイバーセキュリティへの取組姿勢をサイバーセキュリティ方針として規定する。

最高情報セキュリティ責任者は、1.1.1. の組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定する。

- ✓ セキュリティ対策の目的や方向性
- ✓ 関係主体等からの要求事項への対応
- ✓ 経営者層によるコミットメント

サイバーセキュリティ方針には、方針の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規定すること。

また、サイバーセキュリティ方針が妥当かつ有効であることを定期的な間隔で確認するとともに、自組織 を取り巻く状況に大きな変化が発生した場合にも確認する。

1.2　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

【事業者に求めること】

- 経営者層は、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を明確にした上で、リスク管理体制を構築する。

〔解説〕

組織全体のリスクマネジメントの一部として、サイバーセキュリティリスク及びそれが事業運営に及ぼす影響について経営者層が理解し評価できる体制を整備する。

1.1.1.の組織方針を踏まえ、経営者層は、サイバーセキュリティを確保できないことによって組織の情報システム及び情報を活用する事業、事業者としての信頼、その他の経営リスクがどのような影響を受けるのかといった視点からもリスクを管理し、個々の情報システム及び情報自体のセキュリティに関する視点においてもリスクを分析する。また、自組織にとどまらず、ビジネスパートナーや委託先等、サプライチェーン全体にわたるセキュリティ対策への目配りを行う。

経営者層は、重要インフラサービスの提供に不可欠な情報システムは何か、それらがどのようにサイバー脅威にさらされる可能性があるか、どのようなセキュリティ対策をとるべきかを理解することを念頭に、サイバーセキュリティリスクについて理解を深めることが望ましい。[1]

トップマネジメントの観点からは、顧客をいかに逃さないかが関心事であり、そのためには、サイバー攻撃によってどの程度システム及び重要インフラサービス(荷役)が停止する可能性があるか、その結果、顧客にどれだけの影響を与えることになるか等のリスク評価・分析について理解を深めることが望ましい。

また、金融庁の「金融分野におけるサイバーセキュリティに関するガイドライン」(令和６年10月４日)においては、「取締役等の役員は、民法、会社法その他各業法等の規定に基づく責務を負うため、自組織の規模、特性又はサイバーセキュリティリスクに鑑みてサイバーセキュリティ管理態勢が不十分なことに起因して自組織や第三者に損害が生じた場合、善管注意義務違反や任務懈怠による損害賠償責任を問われ得る点に留意が必要である」としており、港湾運送事業者においても留意が必要である。

〔具体例〕

●TOS 利用契約時における責任分界、保険加入の検討

TOSの障害によりコンテナターミナルの機能が停止し、船舶運航会社、荷主等に追加費用や損害が発生した場合、損害賠償請求を受けることが想定される。

TOS の所有者と利用者である港湾運送事業者が異なる場合、両者の間での責任分界について予め整理しておくことが望ましい。また、サイバー攻撃等の外的要因によるシステム障害発生に備えて、サイバー保険に加入しておくことも有効である。

---

[1] 参考となる取組みとして、以下の資料を参照のこと。
経団連「サイバーリスクハンドブック」、2019 年、p.25 図3、p.26-28 、p.36
https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.pdf
経済産業省「グループ・ガバナンス・システムに関する実務指針」2019 年、p.92-94
https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/pdf/20190628_group_gov.pdf

●必要に応じたサイバー保険への加入の検討

- リスク対応の考え方の一つとして、他社へのリスクの移転がある。発生可能性は低いが発生した際の影響度が高い場合に選択させることが多い対策である。自組織の中核事業への影響を鑑み、サイバー保険への加入を検討することも対策の選択肢の一つである。サイバー保険は賠償損害への備えだけでなく、保険会社が提供する総合的な事故対応サポートも有益であると判断できる場合もある。
- グループ企業内での加入を推進する取組みを行っている事業者もある。特に中小規模のグループ会社は有事への備えが不十分であることが多い一方、親会社のサポートには限りがあるため、保険会社やそのパートナー企業のサポートで補完する形を取り、対策を行うケースもある。

●サイバーセキュリティリスク管理(例)

- CISO[2]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。

[2] CISO (Chief Information Security Officer)：最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。(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」2022 年より)

2 平時対策

2.1 組織内外のコミュニケーション

【事業者に求めること】

- 経営者層は、組織内外のコミュニケーションにおいて、サイバーセキュリティリスク、インシデント等の情報を取り扱う。

〔解説〕

組織におけるリスクマネジメントにおいて、コミュニケーション体制の整備は重要である。

有事の際に、エスカレーション（上位の者に報告・相談し指示を仰ぐこと）を円滑に行うためにも、平時から情報開示、情報共有、双方向コミュニケーション、情報収集等、ガバナンスとして行っている様々なコミュニケーション体制において、一つのトピックとしてサイバーセキュリティを取り扱うことが望ましい。

〔具体例〕

●組織内外のコミュニケーション（例）

- 経営者層は、サイバーセキュリティに関してステークホルダー[3]の信頼・安心感を醸成する観点から、平時におけるサイバーセキュリティ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等に取り組む。
- 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、経営者層と担当者層との間で定期的な対話の機会等を設ける。
- セキュリティ・バイ・デザインを共通の価値として認識し、製品・サービス企画時等の内部協議プロセスの関係者にサイバーセキュリティを担当する部署を加えることが望ましい。
- 組織内外の関係者間でサイバーセキュリティに関する役割、責任分担、情報共有の体制等について意見交換を行うことが望ましい。
- グループ企業[4]において、グループ全体の組織ガバナンスを浸透するため、規程類を統一させることが望ましい。

[3]「ステークホルダー」は、株主・経営者・従業員・顧客・取引先のほか、金融機関、行政機関、各種団体など企業のあらゆる利害関係者を指す言葉であるが、ここではサイバーセキュリティに関するリスクが直接影響を及ぼす可能性のある関係者を指している。

[4] グループ企業とは、親会社、子会社、関連会社を含めた関係性のある会社全体を意味する。

コラム COLUMN

リスクコミュニケーションに関する優良事例

◆2019 年 3 月 ノルウェー Norsk Hydro ASA（アルミニウム製造会社）

2019 年 3 月 19 日、ランサムウェアに感染。IT の生産管理システムなども感染したことから、拠点のほとんどが一時的に操業停止に陥った。

＜被害＞

ランサムウェア『LockerGoga』の被害を受け、40 か国 160 の拠点で半数近い PC 及びサーバが感染。そのうち半数が暗号化された。多くはメール、発注や顧客情報管理のコンピュータ等と言われているが、製造用のコンピュータも被害を受けたと推定され、長期間にわたり手作業による製造を強いられた。同社の財務的被害は数十億円にのぼったが、身代金の支払いは一切拒絶した。

＜感染経路＞

2019 年 2 月、攻撃者はある業務端末に設置したバックドアを通じて新たな攻撃用ツール Cobalt Strike を投入し、特権の取得やネットワークアカウント情報などを取得した。さらに、入手したサーバドメインコントローラの管理者権限を用いて攻撃可能範囲を情報システムだけではなく制御端末や生産管理サーバなど制御システムに拡大。ランサムウェアを配布し、3 月 19 日の午前 2 時頃、ほぼ同時期に起動させ、コンピュータ内のファイルを次々に暗号化した。同社の米国本社が発端となり、異なる事業部門へと拡大し、全社的にランサムウェアに感染した。

＜対応＞

被害を緩和し食い止めるため、ネットワークを全面停止した。（この決定は日頃の訓練と事前に定義されたシナリオに基づいた、組織の現場レベルで行われた決断であり、その権限は、事前に（担当者に）与えられていた。）

インシデント発生後、即座に危機管理チームを発足し、「情報開示は頻繁で、オープンで、透明性の高いものであるべき」を原則として広報活動することに合意した。それを受け、インシデント発覚の数時間後、証券取引所が開く午前 9 時前に最初の記者会見を行い、インシデントの公表を行った。同日の 15 時にはライブストリーミングで記者会見を行い、全世界から状況をフォローできるようにしている。その後もプレスリリース及びライブストリーミングを伴う記者会見を頻繁に行っている。

さらに、事態の概況がつかめるまで、情報の発信及び外部からの問い合わせといった全ての広報はオスロ本社に一元化している（1 週間半程度）。このことから、常に矛盾のないメッセージを外部に発信することができた。また、社員に対しても情報共有を適切に実施した結果、各拠点の社員は顧客に対して社内の状況を的確に伝えることができた。このような頻繁でオープンで透明性の高い情報発信は、顧客の理解につながった。

クライシスコミュニケーション戦略では、広報活動の拠点として活用される予定となっていた Web サイト用サーバも暗号化され使用できなくなった。そこで、同社は WhatsApp や Twitter、Facebook 等の代替チャンネルを導入し社内と社外への連絡手段として利用した。

（出典：IPA「制御システム関連のサイバーインシデント事例 5」、Norsk Hydro web 等）

2.2 責任及び権限の割当て

2.2.1 情報セキュリティ責任者の任命

【事業者に求めること】

- 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。

〔解説〕

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る。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。

重要インフラ事業者等は、組織の幹部の関与を明確にするとともにその責任の所在を明確にするため、関係組織の長、情報システムを主管する者及びサイバーセキュリティに関する専門的知識を有する者などで構成する組織(本ガイドラインでは、以下「情報セキュリティ委員会」という。)を設け(既存の類似する組織でも可)、セキュリティを統括する長として最高情報セキュリティ責任者(CISO 等)、セキュリティ対策を進める単位ごとに情報セキュリティ担当者を定めること。

情報セキュリティ責任者(CISO 等)は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと直接コミュニケーションできる者として位置付けられるべきであり、経営者層に相当する者の中から任命されることが望ましい。

〔具体例〕

●最高情報セキュリティ責任者等の指定

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。

※ ＿＿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

●責任者・組織の設置(例)

セキュリティ管理策を推進するにあたり、以下の責任者・組織を設置する。

- 最高情報セキュリティ責任者
- 情報セキュリティ委員会
- 情報セキュリティ担当者
- システム構築・運用者
- CSIRT

●サイバーセキュリティに関する資格(例)

- 情報処理安全確保支援士
- 情報セキュリティマネジメント試験

- CISSP
- CISM

2.2.2 責任者・組織などの役割

【事業者に求めること】

- 経営者層は、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。

〔解説〕

組織・体制を確保するにあたっては、責任者・組織を設置し、責任及び役割を定めることが望ましい。経営者層及び最高情報セキュリティ責任者（CISO）は、以下の具体例のような業務担当者を指揮するものとする。また、必要に応じて外部専門家の登用や、サイバーセキュリティに関する資格保持者の配置を検討することが望ましい。

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となる CSIRT（Computer Security Incident Response Team）の設置にあたっては、一般社団法人 JPCERT コーディネーションセンターの「CSIRT マテリアル」や、一般社団法人日本シーサート協議会の「CSIRT 人材の定義と確保」などが参考となる。

〔具体例〕

●情報セキュリティ責任者（CISO 等）の役割

情報セキュリティ対策の検討及び実施並びに情報セキュリティ事案発生時における対応を主導する情報セキュリティ担当者を指定すること。情報セキュリティ担当者の役割例を以下に示す。情報セキュリティ担当者は、複数名にて役割分担しても構わない。

- 脅威情報等の収集及び関係主体との情報共有
- セキュリティインシデントの管理（CSIRT 等）
- 事業継続計画（BCP）等の実行
- 情報セキュリティ対策の取組全般に対する内部監査
- TOS のシステム開発会社やシステム保守会社における情報セキュリティ対策取組の管理
- セキュリティ人材の職能要件の管理及び教育・研修
- 情報システム（ネットワークを含む）の運用
- 各資産（情報システム、ソフトウェア、情報等）の管理
- 物理的セキュリティが要求される施設の管理
- 制御システム等が運用される環境保有時には制御システム等関連部門の担当

※ は、港湾運送事業法では強制要件（全ての港）

●サイバーセキュリティ管理における役割、業務担当者（例）

- 脅威情報等の収集及び関係主体との情報共有担当
- セキュリティインシデントの管理担当（CSIRT 等）
- コンティンジェンシープラン及び事業継続計画等の実行担当
- サイバーセキュリティに係る取組全般に対する内部監査担当
- サプライチェーン（サプライヤー、委託先等）におけるセキュリティ管理策の取組の管理担当
- セキュリティ人材の職能要件の管理及び教育・研修担当
- 情報システム（ネットワークを含む）の運用担当

- 各資産(情報システム、ソフトウェア、情報等)の管理担当
- 物理的セキュリティが要求される施設の管理担当
- 制御システム等が運用される環境保有時には制御関連部門の担当

2.2.3 役割の分離

【事業者に求めること】

- サイバーセキュリティに係る職務については分離に関する規程を設ける。

〔解説〕

サイバーセキュリティに係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、サイバーセキュリティが確保されていることが確認、証明されたことにはならない。サイバーセキュリティを確立するためには、兼務してはいけない役割が存在するため、サイバーセキュリティに係る職務については分離に関する規程を設ける必要がある。

〔具体例〕

●サイバーセキュリティに係る職務の分離（例）

- 情報セキュリティ委員会は、サイバーセキュリティの運用において、「承認又は許可事案の申請者とその承認者又は許可者」及び「監査を受ける者とその監査を実施する者」の職務について同じ者が兼務しないよう規程を整備すること。

2.3 資源の確保

【事業者に求めること】

- 経営者層は、情報システムの構築・運用及び当該方針の実行に必要な予算・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。

〔解説〕

経営者層は、セキュリティ対策に必要な資源（予算・人材等）について、事業継続性や企業・組織価値を維持・増大していく上で、組織活動におけるコストや損失を減らすために必要不可欠な投資であるとの考え方のもとで配分する。

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[5]等の活用を検討する。

[5] IPA「サイバーセキュリティお助け隊サービス制度」
https://www.ipa.go.jp/security/sme/otasuketai-about.html

2.4 監査・モニタリング

2.4.1 セキュリティ対策の運用状況の把握

【事業者に求めること】

- セキュリティ対策の運用状況について、経営者層の責任において把握する。

〔解説〕

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。これらが整合するようサイバーセキュリティを経営者層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営者層も関与した全社的な体制の下でセキュリティ管理策に取り組む必要がある。

情報セキュリティ責任者(CISO 等)は、セキュリティ対策の導入・運用に伴うリスクの状況変化(事象の発生頻度の変化や、事象の結果の影響度の変化等)を定期的に確認する。また、サイバーセキュリティ方針に基づき設定した目標の達成状況、サイバーセキュリティ方針・各種計画の有効性・妥当性等について、定期的に、又は状況変化に応じて確認する。

〔具体例〕

●セキュリティ対策の運用状況の把握(例)

- 情報セキュリティ責任者(CISO 等)は、サイバーセキュリティの運用状況や対応状況を定期的に経営者層に報告すること。
- 経営者層は、定期的にリスク管理の取組状況を確認し、関係主体等のコミュニケーションを通じて改善を行う。また、サイバーセキュリティリスク管理に関する有効性を検証すること。
- 経営者層は、サイバーセキュリティ確保の取組が、適切及び有効であることを確実にするために、システム監査その他のリソースを活用して、レビューを実施する。レビュー結果は文書化するとともに改善や見直しを指示すること。

2.4.2 セキュリティ対策の監査

【事業者に求めること】

- 経営者層は、セキュリティ対策の実施状況について、定期的な監査体制(内部監査、外部監査)を確保する。

〔解説〕

サイバーセキュリティの確保のためには、本ガイドラインに準拠した対策が適切に策定され、かつ運用されることによりその実効性を確保することが重要であり、その準拠性、実効性及び対策の妥当性が確認されなければならない。そこで、独立性を有する者による情報セキュリティ監査を実施することが必要である。

サイバーセキュリティ確保の取組が適切な状態で維持していることを確認するため、内部監査人による定期的な監査を実施する。実施に当たっては必要に応じて、外部の専門知識を有する者の支援を受けて状況確認をする。

監査責任者は、必要に応じて、監査プロセスに従い、監査方針及び監査計画を作成し実施する。

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。

〔具体例〕

●情報セキュリティ対策の監査

情報セキュリティの確保のためには、情報セキュリティに関する組織内の基準の妥当性、対策の妥当性、体制等の実効性の有無を確認する必要がある。そのため、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。

※ ＿＿は、港湾運送事業法では強制要件(特定の港)

3　インシデント発生時及び事後対応

3.1　情報開示

【事業者に求めること】

- 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。

〔解説〕

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・安心感の醸成につながる。

サイバーセキュリティに関する次の情報を開示することが望ましい。なお、情報開示はステークホルダーとのコミュニケーションの一部という側面があり、ガバナンスとしてサイバーセキュリティに関する取組のみを情報開示することが正しいとは限らないことに留意する。開示する情報は機密情報推測のリスクや、その他の要素を踏まえ経営判断に委ねるべきである。

情報セキュリティ責任者（CISO 等）は、重要システムの停止・低下により、コンテナ荷役の遅延・停止が発生した際等、重要インフラ利用者が安心して対応が行えるよう情報提供を行う。

〔具体例〕

●セキュリティインシデントが発生した場合の情報発信

システム障害等により業務への影響が生じた場合、TOS 等の利用者等の関係者に対して、提供しているサービスの状況、復旧見込み等について適切な情報提供・公表を行うこと。

●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（平時における取組に対する姿勢）

- 組織方針・サイバーセキュリティ方針
- 維持するサービス範囲・水準
- リスク管理体制
- 情報セキュリティ責任者（CISO 等）の知見
- 資源の確保
- リスクの把握とリスクへの取り組み方針
- 緊急対応体制・事業継続／IT-BCP に関する取り組み内容／体制
- 重大なインシデントの発生状況及び対応状況

3.2 インシデント対応及び事業継続対応

【事業者に求めること】

- 経営者層は、インシデントの発生に備え、平時から組織体制（CSIRT 等）や事業継続計画等の整備を情報セキュリティ責任者（CISO 等）に指示するとともに、インシデント発生時には事業継続計画等に沿ったインシデント対応、事業継続対応を指示する。

〔解説〕

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際に、経営者層や職員等がまず実施すべき対応を明確にし、迅速に行動することが求められる。そこで、初動対応（緊急時対応）の方針、手順、態勢等を定めた「コンティンジェンシープラン」の策定が必要となる。

また、重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となる。そこで、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：Business Continuity Plan）」及び、平時のサービス水準までの復旧対応の方針等を定めた「事業復旧計画」に、サイバー空間からの脅威にも備えられるよう、サイバーセキュリティを組み入れる。

重要インフラサービス障害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、IT-BCP（情報システムの事業継続計画）又は BCP 等を実行し、規定に沿った事業継続を進めるとともに、早期復旧に向けた対応を行う。

経営者層は、インシデントの発生に備え、平時から組織体制（CSIRT 等）や事業継続計画等の整備を情報セキュリティ責任者（CISO 等）に指示するとともに、インシデント発生時には事業継続計画等に沿ったインシデント対応、事業継続対応を指示する。

情報セキュリティ責任者（CISO 等）は、重要インフラサービス障害の状況や復旧等の情報提供については、策定した IT-BCP 又は BCP 等に沿って、情報に基づく対応の 5W1H の理解の下、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う

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）

～セキュリティ責任者編～

令和７年３月28日

国土交通省港湾局

目次

はじめに
1　事前準備 1
1.1　組織状況の理解 1
1.1.1　内部状況・外部状況の理解 1
1.1.2　関係主体からの要求事項の理解 4
1.1.3　重要インフラサービス継続に係る特性の理解 5
1.1.4　現在プロファイルの特定 6
1.2　リスクアセスメント 7
1.2.1　資産の特定 7
1.2.2　リスクアセスメントの実施 9
1.2.3　制御システムのリスクアセスメント 11
1.2.4　目標とする将来像の設定 12
1.3　サイバーセキュリティリスク対応 15
1.3.1　サイバーセキュリティ方針の策定 15
1.3.2　リスク対応の決定 16
1.3.3　個別方針の策定 17
1.3.4　リスク対応計画の策定 20
1.3.5　サイバーセキュリティ関係規程の策定 21
1.4　サプライチェーン・リスクマネジメント 22
1.4.1　サプライチェーン全体のリスクマネジメント 22
1.4.2　供給者管理 24
1.5　通信のセキュリティ 26
1.6　クラウドサービス 27
1.7　委託先管理 32
1.7.1　業務委託（共通事項） 32
1.7.2　情報システムに関する業務委託 34
1.7.3　委託先に係る人的安全管理措置 36
1.8　事業継続計画等 37
1.8.1　コンティンジェンシープランの作成 37
1.8.2　事業継続計画等の作成 40
1.8.3　本社等重要拠点の機能の確保 43
1.9　インシデントに備えた組織体制（CSIRT 等）の整備 44
1.9.1　CSIRT 等の整備、関連部門との役割分担等の合意 44
1.9.2　重要インフラサービス障害発生時の体制の整備 46
1.9.3　エスカレーション 47

2　平時対策 49
2.1　平時の運用 49
2.1.1　セキュリティ対策の導入、運用プロセスの確立・実行 49
2.1.2　サイバー攻撃の予兆 51
2.1.3　情報共有 52
2.1.4　従業員の管理 56
2.1.5　要管理対策区域における入退出管理 58
2.2　人材育成・意識啓発 60
2.3　演習・訓練 63
2.4　モニタリング及びレビュー 65
2.4.1　モニタリング実施計画の策定と実施 65
2.4.2　セキュリティ対策の自己点検 67
2.4.3　監査計画の策定と実施 69
2.5　継続的改善 72
3　インシデント発生時及び事後対応 73
3.1　コンティンジェンシープラン及び BCP の実行 73
3.2　重要インフラサービス障害発生時の情報共有 75
3.3　セキュリティ管理状況の対外説明 79
3.4　インシデント管理 80

別紙1. 情報の取扱い・個人情報保護 81
1 情報の取扱いについての規定化 81
1.1 情報の格付け 81
1.2 情報のライフサイクルにおけるセキュリティ管理策 82
1.3 個人情報保護に関わる対策 88
1.4 個人情報に関わる管理 89
1.5 不正アクセスのための脅威への対策 93
1.6 内部関係者による脅威への対策 96
1.7 個人情報漏えい発生時の対応策の整備 98

はじめに

〔セキュリティ責任者編が想定する読者〕

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、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、その実践は経営者層としての責務である。

本ガイドラインの「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情報セキュリティの安全管理の実務を担う担当者（最高情報セキュリティ責任者、情報セキュリティ担当者等）（※注）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・判断すべき事項、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。

※注：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。

〔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、港湾運送事業者等（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。

港湾運送事業者等における最高情報セキュリティ責任者、情報セキュリティ担当者等においては、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「セキュリティ責任者編」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。

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（【導入編 2. 3.3 第１版との関係】の表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（【導入編】表 1 において●印の記載のある項目）。

1　事前準備

1.1　組織状況の理解

1.1.1 内部状況・外部状況の理解

【事業者に求めること】

> ➢ 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。

〔解説〕

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ある。コンテナ荷役等継続の強靭性を確保するため、港湾の特性を理解するとともに、以下に例示する、現段階におけ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

自組織の内部状況、外部状況及び関係主体の要求事項等について把握した情報は、従業員のセキュリティ意識向上の観点から、整理したものを組織内に共有する。

〔具体例〕

●理解すべき組織内部の状況（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情報システム、制御システム、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

●理解すべき外部状況（例）

- 自組織が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[1]
- 景気、為替、経済リスクが与えるセキュリティ投資への影響
- 国外に拠点のある事業者における現地の法令、情勢等の状況
- セキュリティ投資による優遇措置や市場競争におけるイニシアチブ

---

[1] 港湾分野における外部状況として以下の状況が考えられる。

・国外の法令の改正状況

港湾分野はその事業特性から、個人情報保護に関する法令や規制等の改正状況を把握しておく必要がある。また、国際物流に携わる事業者は、海外の規制状況も把握する必要がある。（【1.1.3「安全ガイドライン」の位置づけ(6)参照】

- （コーポレートガバナンスコードに基づく開示や、有価証券報告書においてサイバーセキュリティへの取組や、セキュリティ投資を宣言することによる株主、市場からの評価向上）
- 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
- 自組織が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

港湾分野の関係主体(例)

ステークホルダー	内訳	役割	内容
所轄省庁・局	国土交通省　港湾局 地方運輸局 地方整備局	許認可、監督、インシデントの通知	許認可、インシデントの通知
港湾管理者等	港湾管理者	許認可、港湾管理	港湾施設の使用許可、港湾の管理
	港湾運営会社	港湾運営	港湾運営の一元化・効率化
港湾ターミナル事業者	港湾ターミナル事業者	港湾ターミナルの運営	本船荷役、ヤード内の作業、受け渡し計画を主に実施
港湾運送事業者	船内荷役作業員	荷役作業	船舶への貨物の積込み、取卸し
	沿岸荷役作業員	荷役作業	沿岸での船舶の積込み、取卸し
船舶関連企業	船舶会社/船員	輸送サービス	船舶運航
	船舶・海事関連運送会社	港湾施設利用	海上・陸運における貨物輸送手配
	フェリー・クルージング会社	港湾施設利用	港湾施設利用の場合
	漁業船	港湾施設利用	港湾施設利用の場合
港湾倉庫	貨物保管	貨物の保管	船舶より取卸した貨物を保管
陸運関連企業	後背地関連企業	後背地関連企業	道路、鉄道、河川等の内陸輸送
関連企業(警備、その他)	保安警備会社	保安警備	民間企業
	港湾インフラ維持管理会社	維持管理	港湾インフラ維持管理
	水道	水道供給	水道供給
	電気	電気供給	電気供給
	ガス	ガス供給	ガス供給
	ICTサービス供給	通信サービス提供	通信サービス供給
	海事保険	損害保険の締結	船舶・ターミナル事業・積荷・輸送に関して生じた損出に対する保険
	サイバー保険会社	保険サービス提供	サイバー事故に関する補償、各種支援
	顧問弁護士	法律サポートサービス提供	サイバー事故に関する法的リスクのアドバイス等
	その他認証機関等(該当する場合)	個人情報やデータ保護の認証)	個人情報やデータ保護に関するプライバシーマーク制度、ISMS、GDPRに関連するインシデント報告等
関連機関(税関、警察)	税関	税関	国内・国際法に基づく税の徴収、特に港湾内の倉庫保管等の輸出入・移動に対する課税を担当。
	警察 県警 最寄り警察署 (必要に応じ、警視庁サイバーテロ対策協議会等)	インシデントの通知、捜査、対処	インシデント発生時の通知
	出入国管理	入国管理	入国管理
	沿岸警備隊	沿岸警備	沿岸警備
	外国船舶監督官(PSC)	検査	自国の港に入港する外国船舶の船に対してその国が行う、船内警備や乗組員の資格などの安全に関する立入検査
	海難救助(海上保安庁)	海難救助	海難救助
事業者団体・協会	交通ISAC	インシデントの通知	他の交通団体へ通知
	物流団体	インシデントの通知	インシデント対応に関する相談、情報提供や報告の受付、対応依頼
	JPCERT/CC	インシデント対応に関する報告、相談	コンピュータウイルス・不正アクセス・脆弱性情報に関する発見・被害の届出や情報提供の受付
	情報処理推進機構(IPA)	不正アクセス等に関する相談	重要システムの導入・保守・運用、緊急時の連絡
その他、業務・立地等要件に考慮すべきステークホルダー			
陸運関連企業	後背地関連企業	後背地関連企業	道路、鉄道、河川等の内陸輸送

1.1.2 関係主体からの要求事項の理解

【事業者に求めること】

- 情報セキュリティ責任者（CISO等）は、関係法令や契約等に規定された義務や、サプライヤーや委託先が提示する制限事項等も含め、関係主体、顧客、サプライチェーンからの要求事項を整理する。

〔解説〕

重要インフラ事業者等のセキュリティ対策の取組（重要インフラサービス障害発生時の初動対応や復旧対応等も含む。）にあたっては、各事業分野の関係法令や契約等に規定された義務や、サプライヤーや委託先が提示する制限事項等も含め、関係主体、顧客、サプライチェーン（サプライヤー、委託先等）からの要求事項を整理する必要がある。

その際、サプライチェーンと自組織の「依存関係」について、重要インフラサービスの提供に係る各種業務の抽出・分析等を通じて、正確に把握することが特に重要となる。（例. 通信事業者の障害により各種許認可の申請業務が滞り、コンテナ荷役サービスに影響がある等）

なお、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は、サイバーセキュリティ基本法第 7 条に規定するサイバー関連事業者その他の事業者に当たる。サイバー関連事業者その他の事業者は、サイバーセキュリティ基本法第７条の規定に基づき、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努める責務を有する。

1.1.3 重要インフラサービス継続に係る特性の理解

【事業者に求めること】

- 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。

〔解説〕

内部状況及び外部状況を踏まえ、次に例示するような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。

〔具体例〕

●港湾における重要インフラサービス継続に係る特性(例)

- 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

●重要インフラサービス継続に係る特性の整理方法(例)

重要な業務に関し、その業務に関わるシステムを把握

まだ重要業務の設定、その業務に関わるシステムを整理していない場合は、下記の表のように整理する方法もある。システムの事業への影響度と範囲を把握することが効果的な対策には必要である。

重要業務	システム1	システム2	システム3
業務 I	○		○
業務 II		○	○
業務 III			○

1.1.4 現在プロファイルの特定

【事業者に求めること】

- 情報セキュリティ責任者(CISO等)は、現段階における自組織のサイバーセキュリティ対処態勢の実態把握を行う。

〔解説〕

現段階における自組織のサイバーセキュリティ対処態勢等(現在プロファイル)を把握する。現段階における自組織のサイバーセキュリティ対処態勢等の実態を把握するに当たり、一例として、現在プロファイルの特定が考えられる。

〔具体例〕

●現在プロファイルの特定方法(例)

- 現在プロファイルの特定に当たっては、米国国立標準技術研究所(NIST)サイバーセキュリティフレームワーク(CSF)、英国サイバーアセスメントフレームワーク(CAF)、サイバーセキュリティ能力成熟度モデル(C2M2)、CIS Controls 等が参考となる。
- NIST CSF では、サイバーセキュリティの確保に当たり、コアと呼ばれる5つの区分(特定・防御・検知・対応・復旧)のセキュリティ対策と、ティアと呼ばれる対策の程度を例示している。
- 経済産業省のサイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)は、NIST CSF など国外の主要な規格との整合性を確保しており、国外の規格を踏まえた各国の認証制度との相互承認を進めていくことができる内容となっている。

●把握すべきサイバーセキュリティ対処態勢の内容(例)

- サイバーセキュリティに関する役割・責任が明確であるか
- 情報共有体制が整備され、定期的に見直されているか
- 重要サービスを支える資産の脆弱性を把握しているか
- サイバー攻撃を検知できる体制にあるか
- 従業員に対するセキュリティトレーニングの実施状況
- サイバーインシデント発生時に、意思決定に必要な情報を把握できるか
- インシデントへの対応計画と復旧計画が策定されているか

1.2 リスクアセスメント

1.2.1 資産の特定

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報システム、制御システム、ソフトウェア、情報等の資産を特定し、システム構成、ネットワーク構成、外部との接続状況、システム外の機器(未管理機器)の接続状況等を把握しておく。

〔解説〕

セキュリティ管理策のリスクアセスメント及び対策立案にあたっては、重要インフラサービスに係る情報システム、制御システム、ソフトウェア、情報等の資産を特定し、それら各資産の管理責任者や利用制限等を明確化しておくとともに、システム構成、ネットワーク構成等を把握しておく必要がある。

情報セキュリティ責任者(CISO 等)は、システム構築・運用者と協力して、各資産の管理責任者や利用制限等を明確化した資産台帳やネットワーク構成図を作成・維持管理する。

情報システムの構成要素は、それぞれ保持する情報や使われ方等性質が異なるため、構成要素個別のセキュリティ対策を実施することが重要である。構成要素を以下に区分し記載する。

- ✓ 端末
- ✓ サーバ装置
- ✓ 通信回線・通信回線装置
- ✓ 複合機及び IoT 機器を含む特定用途機器

〔具体例〕

●資産の管理

TOS 等がコンピュータウイルスへの感染や外部からの不正侵入等のサイバー攻撃を受けた際の侵入経路やシステムに与える影響の範囲等の情報セキュリティリスクを推定し対策を検討するために、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、システム外の機器(未管理機器)の接続状況等を把握しておくこと。

これらの情報は、実際にサイバー攻撃を受けた際の侵入経路の特定等にも資する。

※ は、港湾運送事業法では強制要件(全ての港)

●TOS 等と連携している外部機器への影響

TOS 等と連携している外部機器が存在する場合、TOS 等から当該外部機器の制御権を取得できるかどうか確認の上、取得できる場合は必要な対策を執ること。

●資産の管理(例)

- 情報システム、制御システム、ソフトウェア、情報等の資産を特定し、各資産の管理責任者や利用制限等を明確化した資産台帳[2]を作成・維持管理する。

[2] NISC「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第１版）改定版」別紙３を参照
https://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

- 情報システム又はその運用を外部サービスによって代替する場合には、利用する外部サービスの一覧を作成・維持管理する。
- 全てのシステム・ネットワーク構成を記載した文書(システム・ネットワーク構成図)及びデータの流れ図等を作成し、維持管理する。制御システムについても同様の文書を作成する。構成図は定期的なレビューと更新を実施する。
- 重要な機器やサービス業務の機能維持・レジリエンス向上のため、全ての重要な資産の現在の詳細構成を記述した文書を策定し、維持管理する。
- 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする等、組織の情報資産の可視性を高める。技術的に可能な場合、承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する。
- 未承認の資産がネットワークに接続・運用されていないか監視し、対処する。
- システムの可用性維持と脆弱性対策のため、ハードウェア保守体制と EOS(End of Sale/Support)を管理する。
- 通信の監視や許可した機器のみを利用可能とする仕組み等を設け、シャドーIT を検出する。

●ネットワーク構成図の作成時の確認事項

- ネットワーク構成図の作成においては、以下の内容について漏れなく整理するようにする。
- 外部事業者に委託した場合は、入手したネットワーク構成図を適切に管理し、変更等が生じた場合は適時修正する。

対象	種別	確認事項
回線関連	通信事業者	通信事業者名 (キャリア名)
	回線種別	回線の種別・サービス名・スピード
	電話番号/アドレス	電話番号、IP アドレスなどのアドレス識別情報
機器関連	機能	ルータ、ONU、モデムなどの機能名称
	機種名	ハードウェア機種名、型番
	設置場所	機器設置場所
	アドレス	IP アドレスなどのアドレス識別情報

1.2.2 リスクアセスメントの実施

【事業者に求めること】

- 情報セキュリティ責任者(CISO等)は、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。

〔解説〕

サイバーセキュリティ確保のための仕組みは、セキュリティリスクに関する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ない。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必要がある。

1.1 の組織状況を踏まえ、重要インフラサービスの安全かつ持続的な提供に影響を与えるセキュリティリスクを適切に管理すべく、リスクアセスメントを実施する。

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ある。

リスクアセスメントで抽出したサイバーセキュリティリスクに対し、具体的な対応方法を決定すること。リスク対応の選択肢には、「低減」、「回避」、「移転(共有)」、「保有(受容)」があり、「事象の結果による業務への影響度合い」や「事象の発生可能性」等を踏まえて、適切と考えられるものを選定すること。

〔具体例〕

●リスクアセスメントプロセス[3](例)

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。

[3] 詳細については、以下の資料を参考とすること。

- リスクアセスメントの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。
- 自組織の事業の特性や環境等によっては、他の手引書等の手法を適用することが有効な場合も考えられる。例えば IPA の「制御システムのセキュリティリスク分析ガイド」では、資産ベースと事業被害ベース（シナリオベース）を組み合わせたリスク分析手法および実効的なセキュリティ対策のための具体的な作業手順などが記載されている。

●リスクアセスメントにあたっての留意点

- リスク分析に当たっては、任務保証の考え方を踏まえ、貨物輸送サービス等の障害等が社会に与える影響を念頭に分析することが重要である。
- 貨物輸送サービス等の安全かつ持続的な提供のためには、セキュリティリスクに加えて、HSE[4]等の観点からのリスクも特定し、分析・評価を行う事も求められる。
- HSE 等の観点として、例えば、貨物輸送サービス等の提供を担う従業員等の労働安全・衛生の確保や、重要インフラサービスの利用者の安全・健康の確保、貨物輸送サービス等に伴う環境負荷の低減等が考えられる。
- 上記手法においてリスク対応の対象として抽出しなかったリスクも管理が必要である。所管部署の責任において当該リスクを管理させる場合には、各部署の管理状況(セキュリティ管理策の導入有無等)を適時確認可能とする仕組みを整備する。
- リスクアセスメントの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。
- AI 技術等を重要業務において活用している場合は最新の技術動向に係るサイバーリスクの把握に努める。

●多様なリスクへの対応

- 近年、日本を取り巻く地政学リスクが高まっており、サイバー空間における地政学リスクへの対応を強化する必要も考えられる。このため、サイバーセキュリティインテリジェンス活動の一環として、ハッカーやハクティビストなどの脅威活動をモニタリングするサービスの導入等、必要に応じ、脅威情報の入手に務めることが望ましい。DoS/DDoS 攻撃や標的型攻撃の他、発見されたばかりの脆弱性を狙った攻撃は、組織的に実行されることがしばしばあり、インテリジェンス活動により攻撃に対する準備ができる場合があるため、組織のリスクマネジメント上有益と考えられる。

[4] 健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.2.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。　（NISC「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」より）

1.2.3 制御システムのリスクアセスメント

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、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。

〔解説〕

制御システムに汎用機器が用いられ、また、遠隔監視・制御等のために外部と接続される場合がある。コンテナ荷役等の重要サービスを提供するため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適切にリスクアセスメントを実施する。

〔具体例〕

●制御システムのリスクアセスメントの考え方

制御システムにおいては IPA「制御システムのセキュリティリスク分析ガイド」、ISO/IEC 62443「制御システムセキュリティに関する国際規格」、NIST-SP 800-82「産業用制御システム(ICS)セキュリティガイド」等を踏まえ、資産ベースに加え、事業被害ベースの脅威を想定したリスクアセスメントを実施する。

- ✓ 制御システム関連のインシデント事例について情報収集し、リスクを評価することが重要である。
- ✓ 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。
- ✓ 制御システムに関する責任者を設置し、情報システムと制御システムの担当者間で適切なコミュニケーションをとる。
- ✓ セキュリティリスクを考慮し外部ネットワークに接続していない環境で運用していても、災害、自然故障、管理不良等により制御システムの可用性が低下するリスクがある。
- ✓ 自動運転・ドローン等の最新技術[5]を活用している場合には、制御システムの技術動向に係るサイバーリスクの把握に努める。

[5] 国土交通省 ヒトを支援する AI ターミナル　https://www.mlit.go.jp/kowan/kowan_00001.html

1.2.4 目標とする将来像の設定

【事業者に求めること】

- 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。

〔解説〕

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、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。

目標とする将来像を決定するに当たり、1.1.4 の現状把握と同様に、一例として目標プロファイルの作成が考えられる。これは、サイバーセキュリティに関する成熟度を参考とし、自組織が目指すべきサイバーセキュリティ対処態勢を定める方法である。

〔具体例〕

●目標プロファイルの作成(例)

- 現在プロファイルの特定と同様、目標とするティアを設定する。目標とするティアは、自組織の方針に見合うものであり、任務保障の観点からサイバーセキュリティのリスクを自組織にとって許容可能な程度まで低減できるものである必要がある。
- 発生した障害等への対応については、障害等の発生の予防・検知と比べて多くの費用、人材等を要する傾向にあることから、予防・検知の徹底が重要となる。

●目標とする将来像(例)

- 重大なインシデント発生時に、○○時間以内に経営者層までエスカレーションすること
- 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

- 現状プロファイルの特定に当たっての参考文書(【1.1.4 現状プロファイルの設定】参照)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。

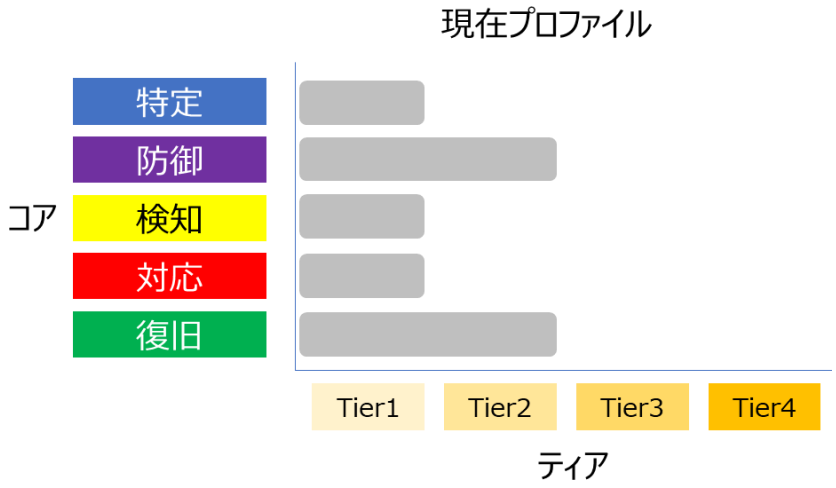
  (例)

  ✓ 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。

●米国国立標準技術研究所(NIST)のセキュリティフレームワークを用いたプロファイルの特定(例)

- セキュリティ対策の状況把握について、NIST CSF ではプロファイルという考え方が説明されている。
- プロファイルには対策の区分であるコアと、対策の程度を示すティアの2つの要素があり、プロファイルを特定するためには、まずこれらを自組織用に整理する必要がある。



図：現在プロファイルの特定の概念図

- NIST CSF にはコアを細分化した 23 のカテゴリ及び 108 のサブカテゴリが例示されている。これらのカテゴリ全てについて対応するのではなく、自組織にとって必要な項目を採用し、整理を行う。
- 対策の程度を示すティアについても4つの段階が例示されているが、ティアの段階についても自組織向けに設定できる。適切なティアを判断するに当たり、成熟度モデル等、既存のガイダンスの活用を検討することが考えられる。また、リスクの許容度がティアに反映される場合もある。
- 成熟度モデルは、組織において現在取り組んでいる対策や手法等に能力レベルを評価し、目標や改善のための優先順位を設定するためのベンチマークとなる。

（代表的な成熟度モデル）

- ✓ サイバーセキュリティ能力成熟度モデル(C2M2)
- ✓ サイバーセキュリティ成熟度モデル認証(CMMC)

表:ティア(対応の程度)の例

Tier1	**・セキュリティ対策が未対応の状態。** ・リスクマネジメントの枠組みが定められておらず、リスク対処は場当たり的。 ・セキュリティリスクに関して意識が不足している。 ・情報共有のプロセスが存在しない。 ・ステークホルダーとは協力関係にない。

Tier2	**・セキュリティ対策は整備しているが、運用化まではできていない。** ・リスクマネジメントの枠組みは経営者層に承認されているが、組織全体のポリシーにはなっていない。 ・サプライチェーン・リスクは把握しているものの対応はできない。
Tier3	**・セキュリティ対策は整備できており、定期的に見直しができる状態。** ・リスクマネジメントの枠組みが自組織のポリシーとなっており、また定期的に見直されている。 ・従業員は割り当てられた役割と責任を果たすための知識とスキルを持っている。 ・セキュリティ担当の役員と他の役員が定期的に他の役員とコミュニケーションを取っている。 ・ステークホルダーと協力関係にある。 ・サプライチェーン・リスクの対処ができる。
Tier4	**・セキュリティ対策は整備できており、適時に見直しができる状態。** ・組織全体のサイバーセキュリティマネジメントのアプローチが確立されている。 ・セキュリティリスクマネジメントが組織文化の一部となっている。 ・役員が示したビジョンを実践し、システムレベルでリスク分析を行っている。 ・事業目的、ミッションの変更に迅速かつ効果的に対処できる。 ・サプライチェーン・リスクをリアルタイムに近い情報で対処している。

出典: NIST CSF
NISC「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」2023 年

1.3 サイバーセキュリティリスク対応

1.3.1 サイバーセキュリティ方針の策定

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、サイバーセキュリティへの取組姿勢をサイバーセキュリティ方針として規定する。

〔解説〕

重要インフラ防護のためには、セキュリティ管理策における根本的な考え方(以下、「サイバーセキュリティ方針」という。)を示す必要がある。

経営者層は、セキュリティ対策に取り組むことをサイバーセキュリティ方針等に含め、組織の内外に対して宣言する。

情報セキュリティ責任者(CISO 等)は、重要インフラ防護の目的、目指す方向、セキュリティ対策にて守るべき対象等を明らかにし、サイバーセキュリティへの取組姿勢をサイバーセキュリティ方針として規定する。

情報セキュリティ責任者(CISO 等)は、「経営者層編」1.1. の組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定する。

- ✓ セキュリティ対策の目的や方向性
- ✓ 関係主体等からの要求事項への対応
- ✓ 経営者層によるコミットメント

サイバーセキュリティ方針には、方針の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規定すること。

また、サイバーセキュリティ方針が妥当かつ有効であることを定期的な間隔で確認するとともに、自組織を取り巻く状況に大きな変化が発生した場合にも確認する。

1.3.2 リスク対応の決定

【事業者に求めること】

- 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。

〔解説〕

1.2.4 の目標とする将来像と実態のかい離を埋めるために実施すべきセキュリティ対策を検討する。セキュリティ対策の程度については、成熟度モデルを活用しつつ、自組織における評価基準等をもって優先順位付けする。

〔具体例〕

●ギャップ分析と優先順位付け(例)

- 現在プロファイルと目標プロファイルの差異について分析する。
- 差異を解消し、目標プロファイルに近づけるための取組について、組織方針に基づく動機、リスク、セキュリティ対策の費用対効果等を踏まえ、優先順位付けを行う。
- リスク対応により、重要インフラサービス障害の発生を抑止するのみならず、発生した障害が経済社会に与える影響を許容範囲内に抑制するための検知・対応・復旧の各機能を実現する。

1.3.3 個別方針の策定

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、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。

〔解説〕

1.3.2の優先順位付けを踏まえ、現在プロファイルと目標プロファイルの差異に対して実施すべき取組において遵守すべき行為や判断基準を個別方針としてまとめる。

本ガイドラインにおいては、TOS 等システムのセキュリティ管理策の対策内容に関しては、システム構築・運用者編で記載しており、情報セキュリティ責任者(CISO 等)は、それら対策の方針を策定する必要がある。システム構築・運用者編で記載している対策項目は以下の通り。

【事前準備】

- ✓ 機器の物理的保護策
- ✓ 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
- ✓ 情報システムのアクセス制御
- ✓ 暗号を活用した情報管理
- ✓ 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
- ✓ 日常的なマルウェア対策の実施

【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

また、サイバーセキュリティ確保のための仕組みに関する違反による損害を最小限に抑えるため、並びにそのような違反を監視してそれらから学習するため、セキュリティ違反を適切な連絡経路をとおして、できるだけ速やかに報告することが必要である。また、セキュリティ違反を犯した取扱者に適用する正式な懲罰手続を確立することが望ましい。

〔具体例〕

●個別方針の策定(例)

- ・ リスク対応の中で決定した個々のセキュリティ対策において遵守すべき行為や判断等の基準を個別方針(例:アクセス制御方針、情報分類方針等)としてまとめ、組織内へ伝達する。
- ・ 必要に応じて委託先等に対しても伝達する。

●現状に対して目標とする将来像の設定(例)

＜現状のサイバーセキュリティ対処態勢の実態＞

- 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%。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＞

- 執行役員として専任で 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[6]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。

●内規の策定・見直しの内容(例)

- 策定・見直しをしたサイバーセキュリティ方針に基づき、個々のセキュリティ管理策を体系化した上で、実施に係る考え方、ルール等について策定、見直しを行う。
- また、内規の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても策定、見直しを行う。
- 内規の策定・見直し結果については、関係者に内容を周知・共有を行う。

●違反と例外措置(例)

＜違反への対応＞

- 情報セキュリティ委員会は、セキュリティ関係規定への重大な違反事故に係る報告手続、サイバーセキュリティ確保のための改善措置の実施に係る手続、及び取扱者の懲戒手続を整備すること。

＜例外措置＞

- 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者を定め、審査手続を整備すること。
- 審査者は、例外措置の適用の申請を、定められた手続に従って審査し、許可の可否を決定すること。また、決定の際には、例外措置の審査記録を整備し、保管すること。

●例外措置の適用申請に含まれる項目(例)

- 申請者の情報(氏名、所属、連絡先)
- 例外措置の適用を申請するサイバーセキュリティ関係規程の適用箇所(規程名と条項等)

[6] 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

- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容(講ずる代替手段等)
- 例外措置により生じるサイバーセキュリティ上の影響と対処方法
- 例外措置の適用を終了したときの報告方法
- 例外措置の適用を申請する理由

1.3.4リスク対応計画の策定

【事業者に求めること】

- 情報セキュリティ責任者(CISO等)は、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。

〔解説〕

情報セキュリティ責任者(CISO 等)は、方針の策定・見直し等に基づき、サイバーセキュリティの具体的な達成目標を定め、達成までの大まかなスケジュールであるロードマップ及びロードマップに基づき詳細化した計画を作成し、サイバーセキュリティに係る取組を進めること。

優先順位付けを踏まえ、現在プロファイルと目標プロファイルの差異に対して実施すべき取組をまとめたリスク対応計画[7]を作成し、実施する。

システム構築・運用者は、個別方針に基づき、各種の対策を実装・運用する。

〔具体例〕

●サイバーセキュリティに関す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
- 責任者
- 達成期限
- 結果の評価方法

[7] IPA「情報セキュリティ対策ベンチマーク活用集　第3章　情報セキュリティ対策ベンチマークからISMS認証取得へ」
https://www.ipa.go.jp/archive/security/sme/benchmark/benchmark-katsuyou.html

1.3.5 サイバーセキュリティ関係規程の策定

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、サイバーセキュリティ方針に準拠したサイバーセキュリティ関係規程の策定を行う。

〔解説〕

情報セキュリティ責任者(CISO 等)は、情報セキュリティ委員会における審議を経て、サイバーセキュリティ方針に準拠したサイバーセキュリティ関係規程の策定、見直しを行うこと。

なお、内規の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規程に含めること。

関係規程の策定にあたっては、独立行政法人情報処理推進機構が公表する「中小企業の情報セキュリティ対策ガイドライン第3.1版」の付録5.情報セキュリティ関連規程(サンプル)が参考となる。

1.4　サプライチェーン・リスクマネジメント

1.4.1 サプライチェーン全体のリスクマネジメント

【事業者に求めること】

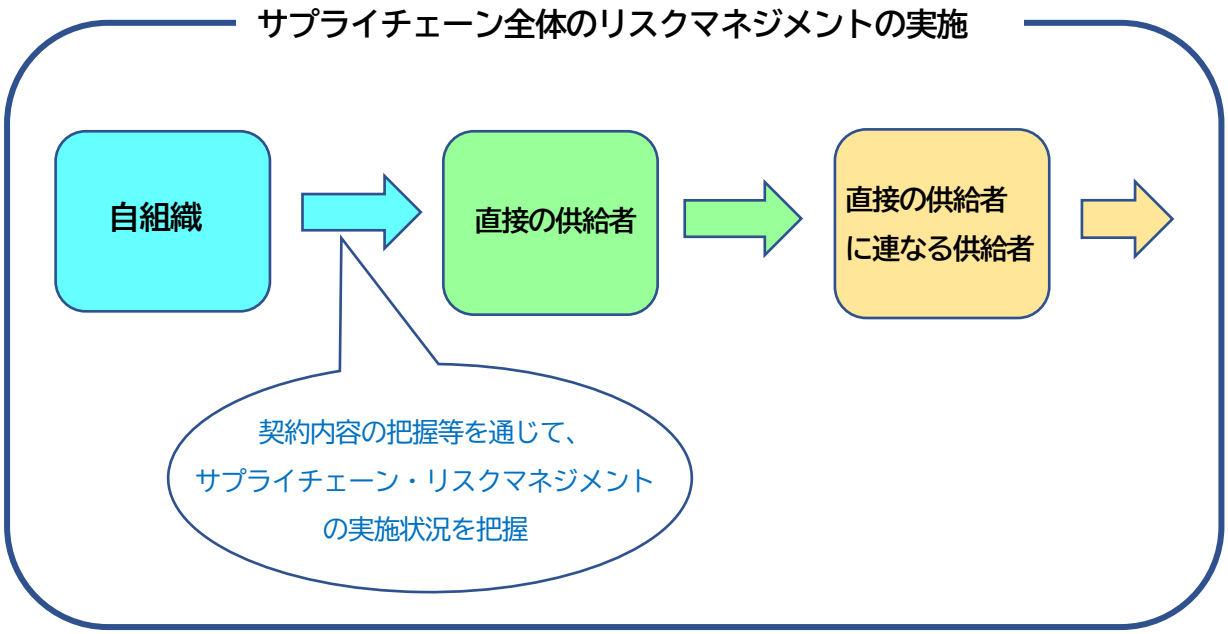
> ➢ 情報セキュリティ責任者（CISO 等）は、直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。

〔解説〕

セキュリティ対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めることが重要である。なお、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどカントリーリスクが高い国が関連する場合、その他関連する法律を参照すること[8]。

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。具体的には自組織の法務部等と連携し、サイバーセキュリティの確保に資する条項を検討の上、契約に含める。

港湾運送事業においては、港湾管理者、港湾運営会社、港湾運送事業者など多くの関係者と連携する必要があり、これら外的要因によるリスクの影響も受けやすい。また、港湾運送事業者の多くは中小事業者であり、セキュリティ対策が十分に実施されていないリスクがあるため、サプライチェーン・リスクマネジメントを強化することが求められる。今後、持続可能な物流サービスを推進するため、共同配送など他者との協業が拡大する動きも考えられるため、アライアンスパートナーを含めたサプライチェーン・リスクマネジメントについても検討することが望ましい。



[8] 参照法律：経済安全保障推進法

〔具体例〕

●対応すべき代表的なサプライチェーンに係る脅威

- 不正機能等の埋め込み
- サービスの供給途絶
- 外部サービスにおける情報の不適切な取扱い
- 海外拠点、グループ組織、取引先等を経由したサイバー攻撃
- 内部犯による情報流出やサービス途絶

＊NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」が参考になる。

●代表的なサプライチェーンに係る脅威への対策の検討（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

●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。

1.4.2 供給者管理

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。
- 海外拠点については、現地の法令、文化等も踏まえた対応を行う。

〔解説〕

事業者は「任務保証」の観点から、システム等の供給者管理においても必要な対策に取り組むことが重要である。また、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどカントリーリスクが高い国が関連する場合、その他関連する法律を参照すること。[9](【1.4 サプライチェーン・リスクマネジメント】参照)

各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。

〔具体例〕

●サプライチェーン・リスクマネジメント(例)

- 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行うこと。
- サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。海外拠点については、現地の法令、文化等も踏まえた対応を行うこと。
- 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。
- 製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理すること。

<リスク管理策例>

- 調達過程における一貫した品質管理が担保できることの選定基準への盛り込み
- 指定したセキュリティ要件が実装されているか、不正プログラムが混入していないかを確認する検査体制の構築
- 委託先が再委託先を監督し責任を負うことが可能な体制であるかの確認
- 再委託の禁止、又は再委託前に委託元の許可を得ることの契約要件への盛り込み
- 部品の供給役務の継続提供の担保
- 供給者の事業計画や提供実績等の確認
- 委託先の事業実施場所の確認、立地条件の考慮
- 外部サービスにおける情報の取扱いに係る脅威に対応する。
- 信用できるサービスの選定
- 情報の返却や抹消などに係る確認手段の設定
- 第三者による評価検証結果の活用

[9] 参照法律：経済安全保障推進法

- サプライチェーンとのネットワーク接続点におけるセキュリティの確認
- 発注者となる組織においては、独占禁止法及び下請法を考慮したパートナーシップ体制を構築する。

●供給者が提供するサービスの変更管理における要求事項(例)

- 供給者やその再委託先等が重要インフラ事業者等の資産にアクセスするリスクを低減するためのセキュリティ要求事項を整理し、あらかじめ供給者と合意すること。
  (例)保守作業において供給者が資産に対してリモートアクセスしたり、機器を接続する際のセキュリティ要求事項
- 供給者のサービス提供に係る契約等の合意事項について定期的に確認するとともに、供給者が作成した報告書のレビューや監査等を実施すること。
- 供給者が提供するサービスの変更に対する管理を行うこと。
- 供給者が提供するサービスにおけるインシデント発生時や、機器の脆弱性を把握した際に、供給者と速やかに情報を共有し対応できる体制を構築すること。

1.5 通信のセキュリティ

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、運搬・送信する情報の形態及び格付けに応じた適切な運搬・送信手段を選択できるように対策を整備する。

〔解説〕

業務においては、その事務の遂行のために他者又は自身に情報を運搬・送信する場合がある。運搬・送信の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部記録媒体の運搬及びPC、紙面に記載された情報の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の運搬・送信により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになるため、適切な情報の運搬・送信に係る措置を講ずることが望ましい。

情報セキュリティ責任者(CISO 等)は、情報を運搬・送信することにより発生するリスクに対応するため、運搬・送信する情報の形態及び格付けに応じた適切な運搬・送信手段を選択できるように対策を整備すること。

〔具体例〕

●通信のセキュリティ(例)

- 重要インフラサービスの提供に係る重要情報等を、電子メールや電子データ交換、インスタントメッセージ及び物理的な運搬等の通信手段を活用して情報転送する場合には、あらかじめ機密性や完全性等のセキュリティ確保に係る取組方針や手順を整理するとともに、それらについて転送相手となる関係主体等の合意を図る。
- 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知等によってネットワークのセキュリティを確保する。
- 重要な情報を通信手段により転送するにあたり、セキュリティ確保に係る取組方針や手順を整理し、転送相手と合意する。
- 転送中のデータを保護するために、適切な TLS 暗号化を導入する。非推奨や、脆弱な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行う。
- 暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照する。なお、暗号技術に係る国内外の法令及び規制の存在について留意する。
- システム構築・運用者は、サービス不能攻撃(DoS/DDoS 攻撃)対策を講じた情報システムについては、監視方法及び監視記録の保管期間を定め、サーバ装置、端末、通信回線装置及び通信回線を監視し、その記録を保存すること。
- 港湾分野においては無線を活用することが多いため、認証(RADIUS 等)、暗号化(WPA2 等)、アクセスコントロール(IP アドレス、MAC アドレス制御等)といった、無線 LAN 設備に対するセキュリティ対策を実施すること。

1.6 クラウドサービス

【事業者に求めること】

- 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。

〔解説〕

システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うこと。事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど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ある。

クラウドサービスでは、クラウド事業者が提供する動作環境を活用していることから、利用者が制御できない環境や領域が存在する。 そのため、クラウド事業者の作業によってインシデントが発生する場合もあり、利用者はクラウド事業者から Web サイトへの公開等により提供される情報の把握や変更管理などを適切に行うことが望ましい。

クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断することが望ましい。クラウドサービスを活用する際は、自組織とクラウドサービス事業者や関係する委託先等ステークホルダーの把握及び、それぞれの責任範囲を明確化することが重要である。

また、以下の具体例に示す参考とするガイドライン・評価制度の例を参考に、クラウドサービス利用における必要な対策を講ずることが望ましい。

〔具体例〕

●クラウド利用時の対策

- 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、「システム構築・運用者編」で示す対策を実施するとともに、以下を例とする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こと。
  - ✓ アクセスログ等の証跡の保存及び提供
  - ✓ 委託先による情報の管理・保管の実施内容の確認
  - ✓ 脆弱性対策の実施内容の確認
  - ✓ 情報の確実な削除・廃棄 等

●クラウドサービス活用にあたっての留意点

- クラウドサービスの選定
- 設定不備や脆弱性に係る診断
- 運用体制の確保
- 仕様変更に対する十分な対応

・ サービス利用約款の把握

●クラウドサービスを利用する際の考慮事項(例)

＜クラウドサービスの選定＞

・ 利用するクラウドサービスの仕様を確認し理解を深める。
・ 責任共有モデルを理解し、クラウドサービス提供者との責任範囲等を明確にする。
・ 情報公開等の設定にミスがないか確認する。
・ サービス仕様が変わる際には影響を確認する。
・ 委託先による情報の管理・保管の実施内容を確認する。
・ データの保管場所(海外など)やデータ越境移転の有無について確認する。

＜法的な考慮＞

・ クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定する。必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。

＜サービスの中断や終了時＞

・ クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。
・ クラウドサービスを利用する際には、①情報の格付けに応じたサービス中断時の復旧要件及び②情報の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法を仕様に含めることが望ましい。
・ クラウドサービスの利用終了時に、クラウドサービス上のデータの取扱い(情報の確実な削除・廃棄)について確認すること。

＜セキュリティ要件＞

・ 多岐にわたるステークホルダーを把握し、情報共有体制・インシデント対応体制を構築する。
・ クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。
  - ✓ アクセス制限(IP アドレス等)
  - ✓ アクセスログ等の証跡の保存及び提供
  - ✓ インターネット回線とクラウド基盤の接続点の通信の監視
  - ✓ データの所在地を含む委託先による情報の管理・保管の実施内容の確認
  - ✓ 脆弱性対策の実施内容の確認
  - ✓ ウイルス対策の実施
  - ✓ 多要素認証の導入
  - ✓ 情報に係る復旧時点目標(RPO)等の指標
  - ✓ 情報の暗号化(保存データの暗号化及び通信回線の暗号化)

- ✓ 情報の確実な削除・廃棄
- ✓ 情報開示請求に対する開示項目や範囲の明記

●クラウドサービス利用における設定不備の対策(例)

- ・ 事業部門等が、情報セキュリティ責任者(CISO 等)が知らないままクラウドサービスを利用することがないよう条件付きで許可するなど、クラウドサービスの利用におけるルールを明確にする。
- ・ クラウドサービス利用におけるユーザーアカウントの管理において、パスワード設定の厳格化や多要素認証の設定を必須とすることを推奨する。
- ・ 設定不備を防ぐため、作業規則や作業手順書を整備し、定期的な内容の見直し等を行う。
- ・ クラウドサービスの設定項目の洗い出し、チェックリスト作成を行い、設定項目の把握やレビュー等に活用する。
- ・ クラウドサービスの設定を定期的にチェックし、不備がある場合は対処する。
- ・ クラウドサービスの機能追加や仕様変更に対しては、定期的ではなく特別に注意してチェック及び対応を行う。

●参考とするガイドライン・評価制度

<参考ガイドライン例>

- ・ 政府機関等の対策基準策定のためのガイドライン(令和５年度版)4.2 クラウドサービス 参照(内閣サイバーセキュリティセンター)
- ・ クラウドサービスの利用・提供における適切な設定のためのガイドライン(総務省 2022.10)[10]
- ・ クラウドを利用したシステム運用に関するガイダンス(詳細版)(内閣官房内閣サイバーセキュリティセンター 重要インフラグループ 2022 年４月５日)[11]
- ・ 中小企業のためのクラウドサービス安全利用の手引き(独立行政法人情報処理推進機構 セキュリティセンター 最終更新日:2021 年３月 10 日)[12]
- ・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン(2013 年度版)(経済産業省)[13]

<評価制度例>

- ・ 政府情報システムのためのセキュリティ評価制度(ISMAP)[14]
- ・ The Federal Risk and Authorization Management Program(FedRAMP[15])

[10] https://www.soumu.go.jp/main_content/000843318.pdf

[11] https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf

[12] https://www.ipa.go.jp/files/000072150.pdf

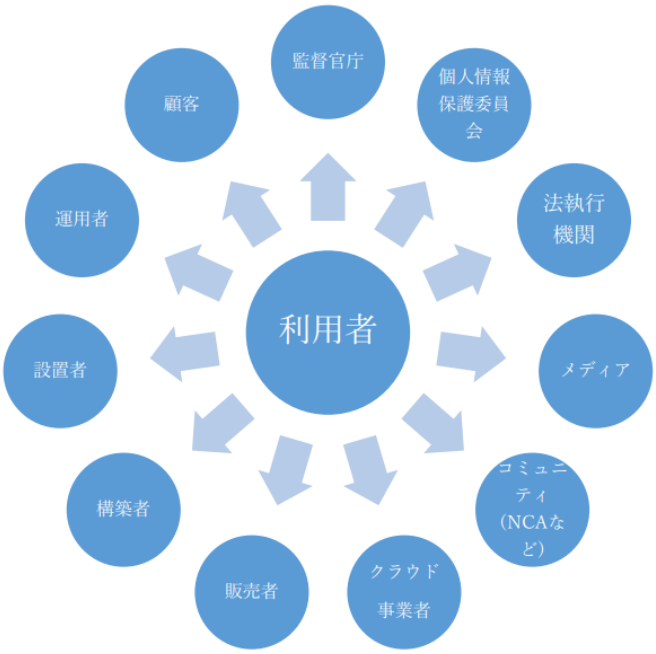
[13] https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

[14] https://www.ismap.go.jp/csm

[15] https://www.fedramp.gov/

●クラウド利用時のインシデント発生時のステークホルダー[16]

- インシデント発生後は、【1.1.1 内部状況・外部状況の理解】で示した港湾分野の関係主体(例)中のステークホルダーに加え、監督官庁や法執行機関、(個人情報の漏えい・滅失・毀損に関する場合は)個人情報保護委員会などとの連携が加わる。また、メディアからの問合せや法的解釈が求められる場合に備え、広報や法務に関係する部門や担当者とも連携を行う。
- このため、クラウド事業者や運用者などの窓口把握に加え、自組織の広報や法務に関係する窓口についても事前に把握し、いつでも連携できる体制を整備する必要がある。
- さらに、自組織やシステムの関係者だけではなく、国内外の研究者や技術者から連絡を受けることにより、インシデントが発見される場合がある。状況によってはこのようなステークホルダーとの連携が追加されることも認識しておくことが大切である。



○インシデント発生時の対応

＜サイバー攻撃の場合＞

- 影響範囲に応じて、システムの停止を検討する。
- クラウド事業者からログの取得を行い、クラウドサービスの利用者や運用者又は他の調査機関で分析を行う。 個人情報の漏えい・滅失・毀損に関する場合は、速やかに監督官庁や個人情報保護委員会に報告する。

＜脆弱性や設定不備の場合＞

- 上記、サイバー攻撃の場合に加えて、以下のようなポイントを追加して検討、対応すること。
  - ✓ クラウド事業者のサポート(サービス)情報を確認し、最新の情報を確認する。
  - ✓ クラウド事業者からガイドや FAQ などが公開されている場合は、参照する。
  - ✓ 特にゼロデイ攻撃の場合、緩和策や回避策があるか確認し、公開されている場合は、組

[16] クラウドを利用したシステム運用に関するガイダンス(詳細版) 内閣官房内閣サイバーセキュリティセンター重要インフラグループ

織内で対応を実施するか検討する。

✓ 新たなモジュールやパッチが公開されたら、できる限り速やかに適用や更新を行う。

・ その他、前述のクラウドサービス利用における設定不備(例)も参照すること。

出典:クラウドを利用したシステム運用に関するガイダンス(詳細版) 内閣官房内閣サイバーセキュリティセンター

1.7 委託先管理

1.7.1 業務委託(共通事項)

【事業者に求めること】

- 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。

〔解説〕

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。

外部委託は、以下の内容が想定される。

- ✓ 情報システムの開発及び構築業務
- ✓ アプリケーション・コンテンツの開発業務
- ✓ 情報システムの運用・保守業務
- ✓ 業務運用支援業務(統計、集計、データ入力、媒体変換等)
- ✓ プロジェクト管理支援業務
- ✓ 調査・研究業務(調査、研究、検査等)
- ✓ 情報システム(クラウドサービス等を含む)、データセンター、通信回線等の賃貸借

さらに、委託先に係る人的対策であるセキュリティ教育及び重要インフラサービス障害発生時の協力に関して合意しておく事が重要である。

なお、港湾における TOS 等の開発、保守等は、外部委託であるケースが多い。これらのような任務保証の上で必須となる業務においては、委託先に対するリスク管理をすることが望ましい。

情報セキュリティ責任者(CISO 等)は、委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準、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(委託事業従事者に対するセキュリティ対策の実施を含む。)を整備すること。

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の内容を整備し、調達仕様書等に定め、委託の際の契約条件とすること。

委託先の選定基準及び契約時に明示する項目には、以下【具体例】を例とする条件を含めることが望ましい。

委託業務でクラウドサービスを利用する場合は、委託先においてもクラウドサービス特有のリスクがあることから、1.6 クラウドサービスで規定する内容についても委託先への要求事項に含める必要がある。

〔具体例〕

●外部委託を行う場合の情報セキュリティの確保

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予め整備の上、これらに基づき委託先を選定すること。また、委託先に請け負わせる業務における情報セキュリティ対策、機密保持(情報の目的外利用の禁止を含む。)、システム障害に対する対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む契約を取り交わすこと。

※ は、港湾運送事業法では強制要件(全ての港)

●委託先に適用するサイバーセキュリティ確保の仕組みの整備(例)

- 委託先に提供する情報の委託先における目的外利用の禁止
- 委託業務における情報の適正な取扱いのためのセキュリティ管理策
- 委託先におけるセキュリティ管理策の実施内容及び管理体制
- 委託先企業又はその従業員、再委託先、もしくは第三者による意図しない変更が加えられないための管理体制
- 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性(サイバー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提供
- 委託先における重要インフラサービス障害に対する対処方法
- 委託先におけるセキュリティ管理策その他の契約の履行状況の確認方法
- 委託先におけるセキュリティ管理策の履行が不十分な場合の対処方法
- 情報セキュリティインシデント発生時の対処方法や報告体制
- 監査の受け入れやサービス品質の保証(取り扱う情報や業務内容等を勘案し必要な場合)
- セキュリティ脅威に対処するための継続的なリスク評価(取り扱う情報や業務内容等を勘案し必要な場合)
- 業務委託終了時の対策(情報が返却、破棄又は抹消されたことの確認等)

1.7.2 情報システムに関する業務委託

【事業者に求めること】

- 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。

〔解説〕

情報システム、アプリケーション・コンテンツの開発、情報システムの保守等を外部委託する際は、委託先選定、委託の実施において必要な対策を講ずることが望ましい。

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、委託先を選定すること。

情報セキュリティ責任者(CISO 等)は、外部委託を実施する際に以下の項目を含む外部委託契約を取り交わすこと。

- ✓ 委託先に請け負わせる業務におけるセキュリティ対策
- ✓ 機密保持(情報の目的外利用の禁止も含む。)
- ✓ 重要インフラサービス障害に対する対処手順
- ✓ セキュリティ対策の履行が不十分である場合の対処手順

外部委託の実施における手続としては、以下【具体例】の対策を講ずることが望ましい。

情報セキュリティ責任者(CISO 等)は、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こと。

重要インフラサービス障害が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。このため、委託先に請け負わせる業務における重要インフラサービス障害に対する対処手順を明確に定めておくことが重要である。

〔具体例〕

●外部委託の実施における手続の遵守(例)

<情報セキュリティ責任者(CISO 等)による対策>

- 外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先におけるサイバーセキュリティの確保のための取組の遵守方法及び管理体制に関する確認書を提出させること
- 委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対してサイバーセキュリティが十分に確保されるよう、本項に規定するセキュリティ対策の実施を委託先に担保させること
- 情報システムの構築・保守等を外部委託する場合には、委託先が実施すべき対策事項を検討し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。また、当該対策による情報システムの変更等を速やかに報告させること。
- 委託先によって情報システムに意図しない変更が加えられないための対策を検討すること。

・ 情報システムの開発の段階や保守の段階等において、脆弱性の混入を防止するための対策を検討すること。
・ 委託先の資本関係や役員情報、委託事業の実施場所、委託事業従事者の専門性や国籍情報等を確認すること。

＜取扱者による対策＞

・ 委託先に提供する情報を必要最低限とし、委託先が取り扱う情報の格付けに従って、適切なセキュリティ管理策を講ずること

●委託先における重要インフラサービス障害発生時の対応策の整備（例）

・ 情報セキュリティ責任者（CISO 等）は、委託先に請け負わせる業務において重要インフラサービス障害を認知した場合の対処手順を整備すること。

1.7.3 委託先に係る人的安全管理措置

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、委託先の情報取扱者に対し、NDA(機密保持契約)締結や教育・訓練等の適切な人的安全管理措置を講じることが望ましい。

〔解説〕

情報セキュリティ責任者(CISO 等)は、取扱者に対する、業務上秘密と指定された情報の NDA の締結や教育・訓練等を行うことが望ましい。

〔具体例〕

●委託先に係る人的安全管理措置(例)

- 雇用契約時及び委託契約時における NDA の締結。
- 取扱者に対する内部規程等の周知・教育・訓練の実施。
- 重要インフラサービスに係る業務の外部委託選定の際には、事業場の要求事項に加えて、アクセスされる情報の分類や認識されたリスク等を考慮すること。
- 自組織と委託先との業務委託契約書等には、以下の項目についても記載すること。
  - ✓ 委託先が自組織のセキュリティの要求を満たすセキュリティ対策に取り組む責任
  - ✓ 従業員に対する意識向上の教育・訓練を実施する責任
  - ✓ 委託終了後もなお有効なセキュリティに関する責任及び義務
- 継続的に取り組むリスクアセスメントの結果次第では、契約文言の見直しが必要な場合も想定されるため、セキュリティ部門や法務部門等による情報交換の場を定期的に設けることが期待される。
- 委託期間中においては、委託先に対するセキュリティに関する要求事項が確実に遂行されるよう、委託先の取組状況を定期的に確認し、必要な改善を求めること。
- 委託先との契約書等に、委託先の従業員に関する要求事項や委託終了後も遵守すべき事項を盛り込むこと。
- 委託先の取組状況を定期的に確認し、必要な改善を求めること。

1.8 事業継続計画等

1.8.1 コンティンジェンシープランの作成

【事業者に求めること】

- 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が発生した場合の初動対応(証拠保全、被害の拡大防止、システム障害復旧、原因調査等)の方針、手順、態勢等を定めた「コンティンジェンシープラン」を策定する。

〔解説〕

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際に、経営者層や職員等がまず実施すべき対応を明確にし、迅速に行動することが求められる。そこで、初動対応(緊急時対応)の方針、手順、態勢等を定めた「コンティンジェンシープラン」の策定が必要となる。策定にあたり、「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 【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照とすることが望ましい。

重要インフラサービス障害を認識した場合に備え、被害の拡大を防ぐとともに、重要インフラサービス障害から復旧するために必要な手順(重要インフラ事業者等外との情報共有含む。)を整備すること。

事前に重要インフラサービス障害について取扱者からの報告手順及び障害発生時の対応手順を整備することが望ましい。

〔具体例〕

●セキュリティインシデント対応手順の策定

サイバー攻撃等のセキュリティインシデントが発生した場合に備え、証拠保全、被害の拡大防止、システム障害復旧、原因調査等に必要な報告や対応の手順等を予め整理しておくこと。

なお、ランサムウェアによる攻撃を受けた場合は、攻撃元の要求に応じて金銭の支払いを行うことは厳に慎むこと。

サイバー攻撃等のセキュリティインシデントが発生した場合に適切な対応が取れるよう、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。

※ ＿＿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

●コンティンジェンシープランに含まれる事項(例)

- 一般的な脅威シナリオ及び自組織固有の脅威シナリオに対応するセキュリティインシデント対応手順を策定すること。制御システムを保有する場合は制御システムも対象とした脅威シナリオにも対応したセキュリティインシデント対応手順を策定する。
  - ✓ 何がセキュリティインシデントに相当するか、基準に従ったセキュリティ事象の評価
  - ✓ インシデントの管理責任者
  - ✓ セキュリティ事象及びインシデントの監視、検知、分類、分析及び報告(エスカレーション)
  - ✓ インシデントの種類に従った対応、危機管理の発動及び事業継続計画の発動の可能性、インシデントからの復旧、内部及び外部の利害関係者への伝達を含む、セキュリティインシ

デントの終結までの管理

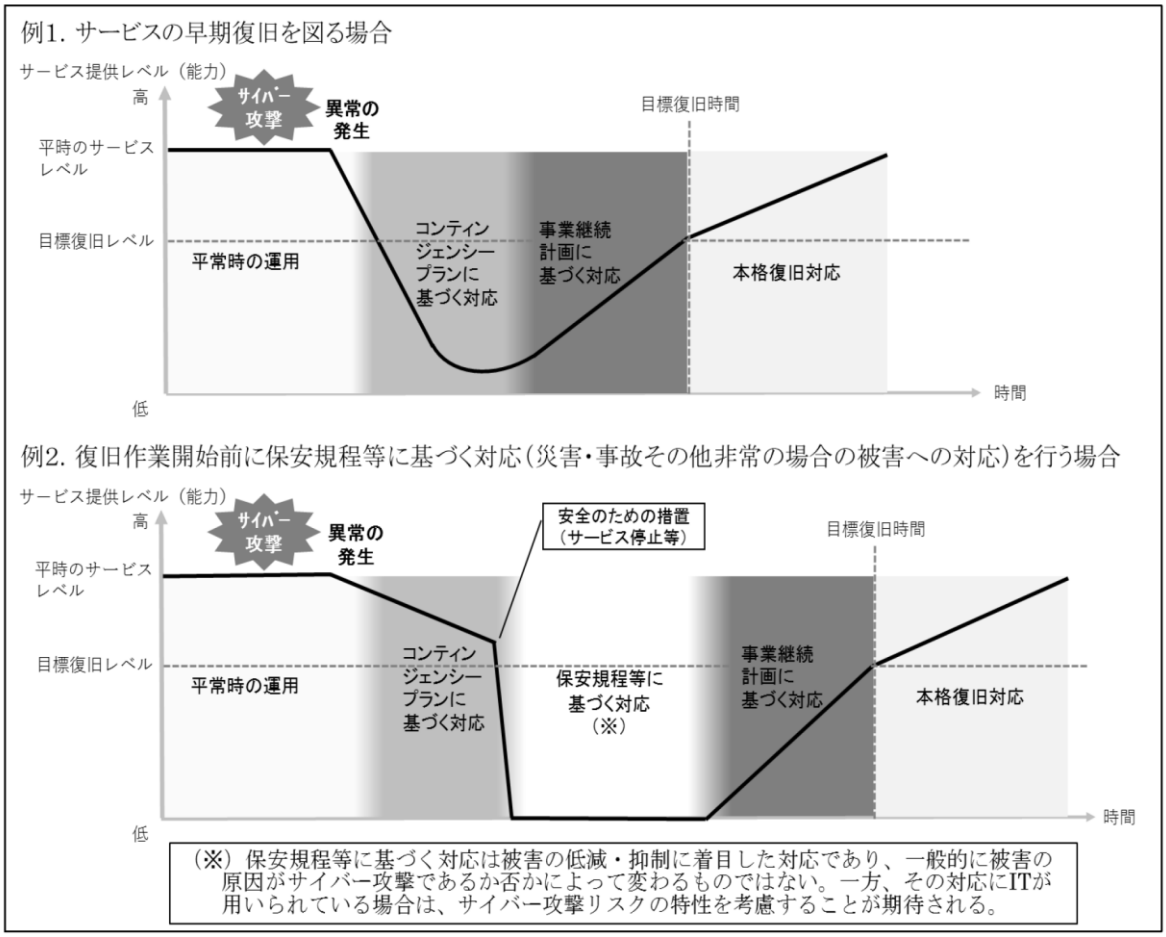
- ✓ 関係当局、供給者、顧客等、内部及び外部の利害関係者との調整
- ✓ 組織内外へのインシデント報告や証拠収集等の手順
- ✓ インシデント管理活動のログ取得
- ✓ 証拠の取扱い
- ✓ 根本原因分析又は事後分析手順
- ✓ 教訓及びインシデント管理手順、セキュリティ管理策についての改善
- ✓ インシデント報告書の作成

・ 策定した対応手順については年 1 回以上訓練を実施し、訓練で得られた教訓をもとにセキュリティインシデント対応計画を更新すること。

●サイバー攻撃の発生から復旧までのフローの例

図１サイバー攻撃の発生から復旧までのフローの例

（下記以外にも様々なフローが存在する。）



上図に示す例(例1及び例2)はいずれもサイバー攻撃により異常が発生し、サービスレベルが時間とともに低下した後、コンティンジェンシープラン(CP)や事業継続計画(BCP)に基づく対応を経てサービスレベルを復旧させる一連のプロセスを表したものである。

例1では、サービスの早期復旧を図るため早いタイミングでBCPに基づく対応を開始している。一方例2では、安全のための措置として意図的にサービスを停止し、保安管理規定等に伴う対応を実施した後にBCPに基づく対応を開始している。いずれの例においてもCP及びBCPは、次頁 以降の特性等を考慮すべき適用対象となる。例2の保安規程等に基づく対応は被害の低減・抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応にITが用いられている場合は、サイバー攻撃リスクの特性等を考慮することが期待される。

出典: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の別紙「対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」

1.8.2 事業継続計画等の作成

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、システム障害やサイバー攻撃を想定したものを含む事業継続計画(BCP)等を策定する。

〔解説〕

重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となる。

そこで、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:Business Continuity Plan)」及び、平時のサービス水準までの復旧対応の方針等を定めた「事業復旧計画」に、サイバー空間からの脅威にも備えられるよう、サイバーセキュリティを組み入れる。策定にあたり、「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 【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照とすることが望ましい。

システムの障害調査やシステムの復旧手順、システムを利用しない荷役手順については、システム構築・運用者の対応の実現性等を踏まえた上で、手順の検討・策定を行うこと。

なお、重要インフラ事業者等全体としての BCP 等とは別のものとして、重要インフラサービスの継続に特化した IT-BCP 等を策定している場合は、BCP 等との整合性の取れた運用の確保が必要である。

港湾関係者が原材料の供給、部品の供給、輸送、生産、販売などに携わる複数の事業者(サプライチェーン)に携わっている場合には、緊急事態発生時に製品・サービスの供給が途絶えてしまう可能性があるため、供給関係にある取引先事業者と、BCP 等の現状について事前に相互理解を深める必要がある。

また、事業継続計画における復旧目標の設定にあたっては、当該港・ターミナルにおいて、どの程度の期間サービスを停止したら顧客を失うか等を勘案することが重要である。仮にサイバー攻撃により TOS が停止した場合には、緊急的にマニュアル作業で荷役を行うことも考えられるが、特に大規模な港湾の場合には、その対応は極めて限定的で、TOS が復旧しない限りは本格的な荷役再開は困難とみられる。一方で、TOS の復旧に要する期間は、その被害の範囲・程度によることになるため、一概に復旧目標時間を設定することは難しい面がある。しかしながら、TOS のネットワーク構成やバックアップ等の対策を検討する際の目標として、また、顧客への対外的な情報発信の意味でも、復旧目標(復旧日数や復旧レベル)を設定することが望ましい。

〔具体例〕

●システム障害やサイバー攻撃を想定したものを含むBCPの策定

事業の継続を目的として、システム障害やサイバー攻撃も想定した上で、優先する業務、必要な対策を決定するまでの過程、事業継続方法、連携を要する関連部門、対外的な情報発信等を規定する BCP を策定すること。なお、自然災害を想定した BCP は多くの TOS 運用者において策定されているものの、システム障害を想定した BCP を策定している事例はほとんど見られなかったことから、システム障害時に特に留意すべき点を以下に示す。

ア. システムの障害調査に係る対応手順

システム障害の原因を調査することは、障害からの復旧のほか、再発防止策の検討のためにも

重要である。システム障害発生時の情報連絡先に加え、調査の方法(委託先等)についても事前に整理しておくこと。調査の委託先については、システム機器の障害の場合等は、TOS 等のシステム保守会社及びシステム開発会社が想定されるが、特に、サイバー攻撃等が疑われる場合は、セキュリティベンダー、セキュリティ専門機関等のサイバーセキュリティ専門家の助言を求めることが望ましい。

なお、システム障害の調査のためには障害発生時の環境を保持しておく必要があることから、システムの復旧作業の開始とトレードオフの関係となりうることに留意する必要がある。

イ. システムの復旧に係る対応手順

システムの復旧に係る対応手順の策定の際には、システムの障害調査に係る対応手順を踏まえた上で検討すること。

システムの復旧に係る対応手順については、実際に復旧作業を行う TOS 等のシステム保守会社やシステム開発会社と事前に共有しておくこと。

また、サイバー攻撃を受けた後に運用を再開する際には、システムが十分な情報セキュリティ対策が取られている状態であるかどうかを確認することが望ましい。

ウ. システムを利用しない荷役等の手順

システム障害発生時の事業継続の手段として、コンテナターミナルの場合は、TOS を利用せずにマニュアル作業によるコンテナの目視確認、データ照合等を行い、本船荷役を実施すること等が想定される。

システムを利用しない場合の荷役等の手順について、取扱貨物量等を踏まえ必要に応じて予め整理しておくこと。

※ は、港湾運送事業法では強制要件(全ての港)

●事業継続計画(BCP)の策定(例)

- 事業継続計画等においては、重要インフラサービス障害発生時における優先業務、必要な対策を決定するまでの過程、事業継続方法、連携を要する関連部門等を規定する。
- 取引先、顧客、取扱者、株主、地域住民、政府・自治体などと情報を共有するため、以下の点を含むことを検討する。
  - ✓ 情報収集・伝達、広報体制を確立すること
  - ✓ 関係当局、地域住民、サプライチェーン等の関係者との連絡体制を構築すること[17]
  - ✓ 通信・情報連絡手段を確保すること
- 規定に際しては、広域災害・複合障害や新型インフルエンザ等の社会全体で対応が望まれる脅威、相互依存関係にある重要インフラからの障害波及、事業継続に必要なデータが特定の都市又は地域に集中している状況等についても考慮する。

[17] 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がグッドプラクティスとして参考となる。
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及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
https://www.mlit.go.jp/kowan/kowan_mn2_000006.html

- 重要インフラサービス障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含む必要がある。
- 事業継続計画等には、サプライチェーンに係る脅威への対応を盛り込む。
- 事業継続計画とあわせて、情報システム及び制御システムに係る記載を詳細化した対応方針(IT-BCP 等)も策定することが望ましい。
- システム障害の影響が組織全体に波及する際、IT-BCP から事業継続計画へ円滑に移行していくことが望ましい。
- システム障害の原因を調査することは、障害からの復旧のほか、再発防止策の検討のためにも重要であるため、システム障害発生時の情報連絡先に加え、調査の方法(委託先等)についても事前に整理しておくことが望ましい。
- システムの復旧に係る対応手順を策定すること。策定の際には、システムの障害調査に係る対応手順を踏まえた上で検討することが望ましい。
- システムを利用しない場合の荷役等の手順について、取扱貨物量等を踏まえ必要に応じて予め整理しておくことが望ましい。

●港湾における BCP 等の検討(例)

- 情報セキュリティ責任者(CISO 等)は、平時から自社に関連のある重要インフラ事業者等の事業継続に関する情報を集めるとともに、自社の BCP 等の現状についてあらかじめ取引先に理解を求めておくこと。
- 製品・サービスの供給関係に関し、BCP 等を検討する際には、以下の点を考慮することが望ましい。
  - ✓ 被災拠点(本社、支店、支社、物流拠点等)を早期復旧する以外に、被災地以外の拠点で代替生産を実施することも検討すること
  - ✓ 拠点の複数化や代替拠点の確保(ただし、複数の拠点における同時被災や、2段階以上先の拠点が同一となり、そこが被災する場合にも留意)
  - ✓ 荷主・拠点との連携(在庫持ち合い、拠点の事業継続能力の把握、BCM 実施要請・支援、事業継続に関する共同訓練の実施、さらに先の拠点企業の事業継続能力の把握要請等)
  - ✓ 同業他社との相互支援協定を利用すること。(特に、拠点が分散していない場合)
- 適正在庫の見直しや在庫場所の分散化による供給継続を検討すること。(特に、代替品のない1社のみが生産している部品材料の場合)

●自然災害を対象とした港湾 BCP における復旧目標の考え方

- 港湾BCPを検討する上では、危機的事象が発生した場合の機能回復に係る目標を設定しておくことが重要であり、どれくらいの時間で復旧させるかを「目標復旧時間」、どの水準まで復旧させるかを「目標復旧レベル」として検討する。
- 具体的には、それぞれの重要機能について、荷主等利用者のニーズを踏まえ、停止(または相当程度の機能低下)が許されると考える時間と必要とされる機能を推定した上で、時間の許容限界より早く目標復旧時間を設定し、機能の許容限界を上回るように目標復旧レベルを設定する。

出典:港湾の事業継続計画策定ガイドライン(改定版)(令和 2 年 5 月、国土交通省港湾局)

1.8.3 本社等重要拠点の機能の確保

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、本社等の重要拠点が被災した場合に備え、重要拠点の機能を確保する。

〔解説〕

本社等の重要拠点が被災した場合に備え、重要拠点の機能を確保し、重要業務を継続するための対策を検討する必要がある。

〔具体例〕

●本社等重要拠点の機能確保(例)

- 情報セキュリティ責任者(CISO 等)は、緊急事態時における対策を検討・指揮するための緊急対策本部を設置すること。
- 本社等の重要拠点の機能の確保に関し、BCP 等を検討する際には、以下の点を考慮することが望ましい。
  - ✓ 被災地での業務の再開以外に、非被災地での業務の継続も検討すること。
  - ✓ 遠隔地の文書・電子データ保存サービスを活用すること
  - ✓ 時差を考慮すること(日本が休日・夜間であっても海外は営業時間であることもあるため海外への情報発信が必要)
  - ✓ 自治体等の各種制度や防災隣組の機能など、地域の資源を活用すること

1.9 インシデントに備えた組織体制(CSIRT 等)の整備

1.9.1 CSIRT 等の整備、関連部門との役割分担等の合意

【事業者に求めること】

- 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(CSIRT 等)の整備を行う。
- CSIRT 等の組織は、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。
- 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。

〔解説〕

サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画等の実行に必要な組織体制として、CSIRT(Computer Security Incident Response Team)(又は同等機能を持つ組織)を重要インフラ事業者等の内部に整備し、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ある。特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応に 制御システム等関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。

また、サイバー攻撃に迅速に対処する観点から、サイバーセキュリティに関連する専門知識を持つ組織を含めた対処体制を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及びサイバーセキュリティ関係機関との連携も有効であると考えられる。

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が重要である。

CSIRT 等の組織は、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ある。 特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応に制御システム等 関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。

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となる CSIRT の設置にあたっては、一般社団法人 JPCERT コーディネーションセンターの「CSIRT マテリアル」や、一般社団法人日本シーサート協議会の「CSIRT 人材の定義と確保」などが参考となる。

〔具体例〕

●インシデント対応の社内外の組織体制の整備

情報セキュリティ事案が発生した際の初動対応時の相談先となりうることから、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ことが望ましい。

※ ＿＿は、港湾運送事業法では強制要件(特定の港)。また、サイバー攻撃が発生した場合等に備え、脆弱性情報などの収集と分析、インシデント発生時の対応、社内外の組織との情報共有や連携を行う体制の整備が必要(特定の港)。

●CSIRT 等の整備の考え方(例)

・ CSIRT を整備し、その役割を明確化すること。

- CSIRT 等は、役割分担や対応手順等を関連部門と合意する。特に、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連携できる体制を整備することが望ましい。
- セキュリティインシデントが発生した際、直ちに CISO への報告が行われる体制を整備すること。
- 職員のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任すること。
- 自社におけ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。
- CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。

●関連部門との役割分担等（例）

- 脅威情報等の収集及び関係主体との情報共有担当
- コンティンジェンシープラン及び事業継続計画の実行担当
- セキュリティ対策の取組全般に対する内部監査担当
- サプライチェーン（供給者、委託先等）におけるセキュリティ対策の取組の管理担当
- セキュリティ人材の職能要件の管理及び教育・研修担当
- 情報システム（ネットワークを含む）の運用担当
- 各資産（情報システム、ソフトウェア、情報等）の管理担当
- 物理的セキュリティが要求される施設の管理担当
- 法務対応・労務管理担当
- コンプライアンス・リスク管理担当
- 個人情報管理担当
- 広報担当

●港湾分野で想定されるインシデント対応体制（例）

- CSIRT
  - ✓ CISO（最高情報セキュリティ責任者）
  - ✓ 統括情報セキュリティ責任者（CISO への報告等、CSIRT 責任者）
  - ✓ インシデントマネージャー（CSIRT 責任者）
  - ✓ CSIRT メンバー（活動メンバー）
- ステークホルダー
  - ✓ 港湾管理者、港湾運営会社
  - ✓ IPA
  - ✓ JPCERT
  - ✓ その他
- CSIRT 支援メンバー
  - ✓ 外部委託業者（SI ベンダー）
  - ✓ 製造ベンダー

1.9.2 重要インフラサービス障害発生時の体制の整備

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、重要インフラサービス障害が発生した際、迅速に検出、防護、回復のための対策を講ずるために、事前に障害発生時の体制を整備することが望ましい。

〔解説〕

重要インフラサービス障害が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた責任者へ報告し、重要インフラサービス障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

〔具体例〕

●障害発生時の体制の整備(例)

- 情報セキュリティ責任者(CISO 等)は、重要インフラサービス障害を認知した場合に備え、被害の拡大を防ぐとともに、重要インフラサービス障害から復旧するために必要な体制を整備すること。
- 業務の遂行のため特に重要と認めた情報システムにおける、担当する責任者の緊急連絡先、連絡手段、連絡項目を含む緊急連絡網を整備すること。

1.9.3 エスカレーション

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、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。

〔解説〕

重要インフラサービス障害の発生及び復旧に関しては、経営者層が意思決定をする必要がある。サイバーセキュリティに担当する部署は、経営者層の意思決定を支援するため、事業にどのような影響があり、どのように対処をしていくのか、初動及び復旧の対応について経営リスクの観点から経営者層へエスカレーションを行うことが重要である。

従業員が発見した又は疑いを持ったセキュリティ事象を、適切なエスカレーションにより速やかに報告するための仕組みを設けることが望ましい。

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。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

インシデントの検知・連絡受付から、組織内情報共有、トリアージ(サイバー攻撃等の事象の影響分析及び対応の優先順位付け)、インシデント対応の基本的な流れについては、JPCERT コーディネーションセンターの「インシデントハンドリングマニュアル」等が参考となる。

〔具体例〕

●インシデント発生の検知方法について

- インシデントの発生を検知するには大きく分けて 2 つの方法がある。
- 1つは、保守作業の中での発見や、あらかじめ設置したセキュリティ機器やシステムによる異常の検知といった、自組織内で検知する方法。
  (例) 監視システムを活用し、不審な挙動を検知
  IT部門・システム管理者が、システムログやネットワークの異常を発見
  従業員・ユーザが不審なEメールを発見
- もう一つは、外部からの通報をもとにしてインシデントの発生を「検知=認知」する方法。
  (例) 外部機関(セキュリティベンダー等)が、脆弱性や攻撃を指摘
  取引先・顧客が、データ漏えいや異常な動作を報告

●トリアージの一般的な流れ(例)

- あらかじめトリアージのための判断基準を明確に定めておく。トリアージの判断基準は、CSIRT にとって「守るべきものは何か」といった基本的な活動ポリシーによって変わる。
- トリアージの一般的な流れ
  ①得られた情報に基づいて、事実関係を確認し、CSIRT が対応すべきインシデントか否かを判断。その際には、必要に応じて、インシデントの報告者やインシデントに関係する可能性のあるサイトの運営者(以降、関係者)と情報をやり取りして詳細を確認。
  ②CSIRT が対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織の

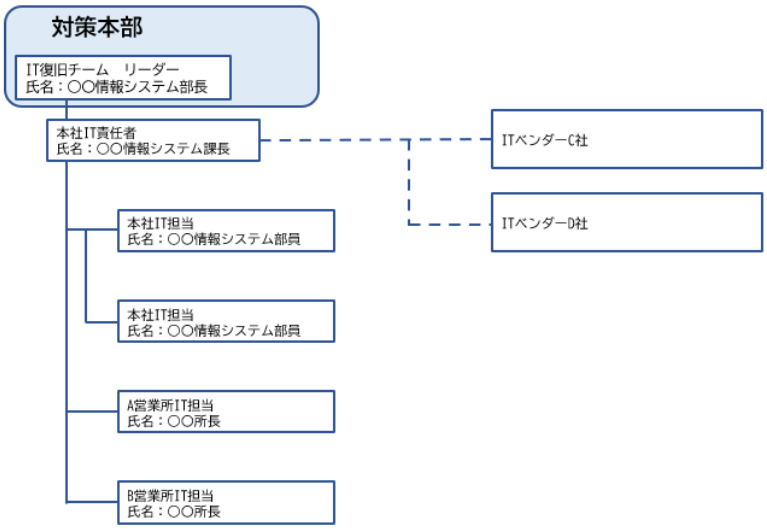
ポリシーなどに照らして可能な範囲で詳細に、報告者や関係者に連絡。

③CSIRT が対応する、しないにかかわらず、関係者に速やかな対応を依頼すべき、または情報提供すべきと判断した場合は、注意喚起などの情報発信を行う。

④CSIRT が対応すべきと判断した場合には、インシデントを「レスポンス（対応）」の対象とする。

●緊急時の連絡体制（例）

・ 緊急時の連絡体制を整備し、各役割を定めておくことが重要である。



緊急時連絡体制（例）

メンバー	役割
リーダー	システムの統括責任者
本社 IT 責任者	情報システムの被害状況の確認と復旧作業、外部ベンダーとの調整
本社 IT 担当	クライアント PC 環境等の被害状況の確認と復旧作業
A 営業所 IT 担当	クライアント PC 環境等の被害状況の確認と復旧作業
B 営業所 IT 担当	クライアント PC 環境等の被害状況の確認と復旧
IT ベンダーC 社	基幹システムの被害状況の確認
IT ベンダーD 社	クラウドサービスの被害状況の確認

2 平時対策

2.1 平時の運用

2.1.1 セキュリティ対策の導入、運用プロセスの確立・実行

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、サイバー攻撃等の予兆を把握するために、システム機器のログ等を定期的に確認する等、平時からセキュリティ対策を導入し運用状況を管理する。
- 情報セキュリティ責任者(CISO 等)は、安全管理について取扱者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認する。

〔解説〕

平時よりリスク対応計画を踏まえ、セキュリティ対策の導入、運用プロセスの確立・実行、 CSIRT 等の運用を行う。重要インフラサービス障害に繋がる可能性のある事象(サイバー攻撃、情報システムの異常状態等)を早期検知する仕組みを構築するとともに、関係部署等との情報共有、トリアージ等の運用プロセスを確立することが望ましい。

情報システムに対するサイバー攻撃等の予兆を把握するために、平時からセキュリティ対策を導入し運用することが重要である。

また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等を通じてセキュリティ対策の水準を維持する。

情報セキュリティ責任者(CISO 等)は、安全管理について取扱者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することが重要である。

システム構築・運用管理者は、システム機器のログを取得し、異常が無いか等を定期的に確認すること。

〔具体例〕

●セキュリティ運用・監視の実施

システム機器のログ等を定期的に確認することによりシステムのセキュリティの状況を定期的に把握するとともに、異常が検知された場合には早い段階で対応し、可能な限り重大なインシデントに発展することを未然に防ぐこと。

●平時におけるリスク対応(例)

- 「リスク対応計画」に基づき、リスク対応において決定したセキュリティ管理策の導入を進めるとともに、それらを効果的かつ確実に運用するためのプロセスを確立し、実行する。
- 重要インフラサービスの提供に係る情報システム等の運用状態を示すデータについて、アラートやログ等の複数の監視結果を相互に組み合わせて、重要インフラサービス障害につながる可能性のある事象(サイバー攻撃、情報システムの異常状態等)を早期検知する仕組みを構築するとともに、検知後に続く関係部署等との事象の共有、トリアージ等の運用プロセスを確立する。
- サイバーセキュリティ関係機関等からの情報提供や収集した脅威情報等を踏まえ、必要に応じて追加のリスクアセスメント及びリスク対応を実施し、重要インフラサービスの強靭化を図る。

●組織的安全管理措置(例)

- 安全管理措置を講ずるための組織体制を整備すること。
- 安全管理措置を定める規程等の整備と規程等に従った運用を行うこと。
- データの取扱い状況を一覧できる手段を整備すること。
- 安全管理措置の評価、見直し及び改善を定期的に実施すること。
- 事故又は違反に対する対処状況を確認すること。
- 情報システム等の運用に関連する手順書を整備すること。
- 手順書を共有し、作業誤りやセキュリティ基準違反を抑止すること。
- 情報システム等の更新に関する事前承認手続きを定めること。
- 運用環境と開発・試験環境を分離すること。
- サイバーセキュリティに関する脅威情報を収集し、分析すること。
- インターネットに接続されたシステムの既知の脆弱性(CVE 情報等)を、重要な資産から優先的にパッチ適用等により緩和すること。
- パッチ適用が不可能もしくは、可用性や安全性を損なうおそれのある制御システムについては、ネットワークの分離や監視等の代替手段を使用し、当該システムがインターネットからアクセスできないようにすること。
- 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。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処すること。

2.1.2 サイバー攻撃の予兆

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施する。

〔解説〕

サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施すること。また、重要インフラサービス障害が発生した場合、事業継続計画等に従った初動・復旧対応を実施すること。

重要インフラサービス障害の発生検知が遅れると、重大な障害となる恐れがある。したがって、重要インフラサービス障害発生時は、迅速に障害の発生を検知するとともに、切り分けの手順を明確化する必要がある。

〔具体例〕

●サイバー攻撃の予兆への対応(例)

- サイバーセキュリティを担当する部署は、初動・復旧対応に関する経営者層の意思決定を支援するとともに、組織内外と情報共有を実施する。
- 重要インフラサービス障害の発生時に、システム構築・運用者が障害の発生や情報システムの状態を迅速に把握できる仕組みを導入することが望ましい。
  - ✓ 設備、機器、サーバ等の障害をアラーム等で通知する仕組み
  - ✓ 設備、機器、サーバ等の状態を画面等で表示、監視できる仕組み
- 重要インフラサービス障害の切り分けについての具体的な手順を内規で定めておくことが望ましい。
  - ✓ 設備、機器、サーバ等における具体的な切り分け手順作成
  - ✓ 切り分けに必要な情報収集手順、報告手順等の明確化

2.1.3 情報共有

【事業者に求めること】

- 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。
- 情報セキュリティ責任者(CISO 等)は、収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行う。
- 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。

〔解説〕

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恐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は、今後の更なる対策の強化を可能とするものである。自組織にとっても、社会全体にとっても望ましい。収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行うことが重要である。

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の別紙４－1～3の体制に従い実施するものとする。具体的な情報共有の手引については「行動計画」に基づく手引書を参照し実施すること。

なお、予兆・ヒヤリハットやシステムの不具合に係る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つな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。

システムの不具合等に関する情報は、以下の関係主体から提供される場合がある。提供された情報が、自組織で保有するシステムに関連する場合には、行動計画で示す情報共有体制に従い、積極的に情報提供を行うものとする。

- ✓ 内閣官房
- ✓ 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
- ✓ サイバー空間関連事業者
- ✓ 国土交通省

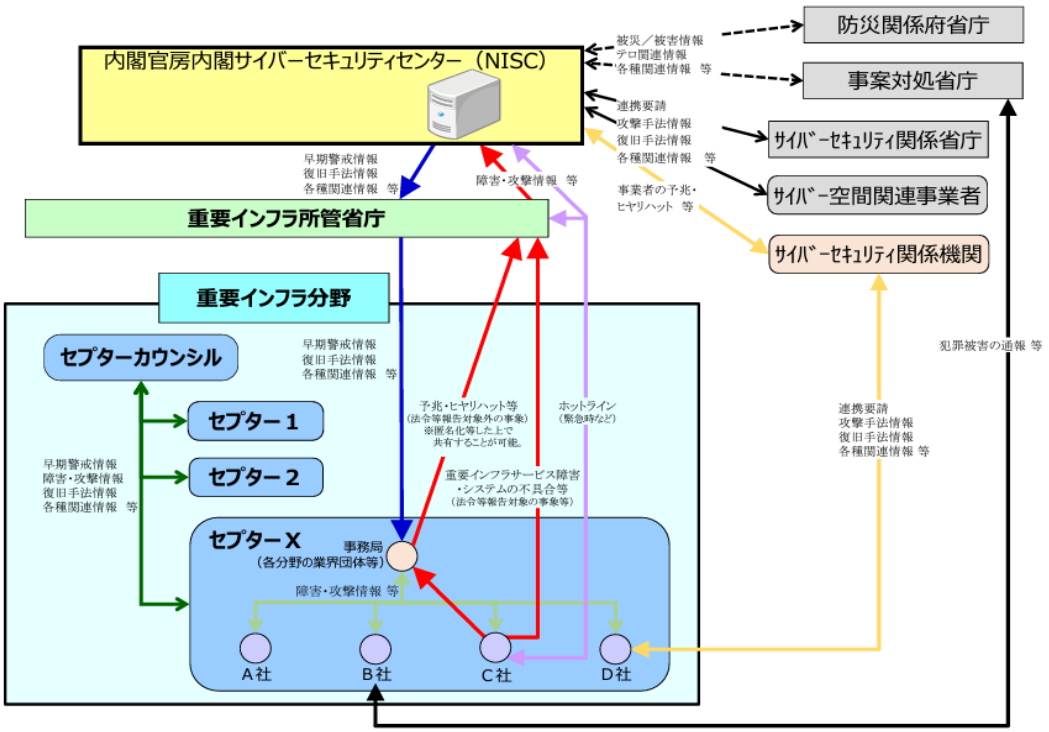
セキュリティ事案が発生した際の初動対応時の相談先となりうることから、セキュリティベンダー、セキュリティ専門機関、都道府県警察等と平時から情報交換等を行うこと。

ISAC[18]・サービス提供者のウェブサイト、JVN iPedia、ニュース等の脆弱性情報を収集し、脆弱性の発生状況、対策状況を把握すること。

[18] Information Sharing and Analysis Center：サイバーセキュリティに係る情報共有及び分析を行うコミュニティ。業種ごとに構成されており、2020 年 4 月に交通 ISAC が設立された。

「行動計画に基づく手順書」での関係者間の情報共有体制(平時)

別紙４－１　情報共有体制(通常時)



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。

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別紙 4-1「情報共有体制(通常時)」

別紙 4-3「情報共有体制における各関係主体の役割

〔具体例〕

●情報セキュリティに関する情報収集

セキュリティインシデントの情報更新速度は非常に速いため、日頃から情報収集を継続的に実施する必要がある。また、情報セキュリティ事案が発生した際の初動対応時の相談先となりうることから、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ことが望ましい。

また、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。

※ ＿＿は、港湾運送事業法では強制要件(特定の港)

●関係主体からの情報提供(例)

- セキュリティホールやプログラム・バグ等に関する情報を入手した場合等であって、他の重要インフラ事業者等においてもその情報に関係する重大な問題を生じるおそれがあると認められる場合。
- サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合。
- そのほか重要インフラ事業者等のサイバーセキュリティの確保に有効と考えられる場合。

●組織内外との情報共有(例)

- ISAC 等の分野専門性の高い情報共有活動に参加し、情報収集すること。
- 連絡体制が最新の情報に更新されているか確認すること。
- 有益な情報を得るには自ら 適切な情報提供を行う必要があることを自覚し必要に応じて[19]、組織内外に情報提供を行うこと。
- リスクマネジメントにおけるコミュニケーション及び協議には、以下に記載する取組を行うことが望ましい。
  - ✓ 分析したリスクについてステークホルダーとの共有や議論
  - ✓ リスクマネジメントの方法や、それに必要な分析に使用する最新の情報を収集すること
  - ✓ リスクの特定や評価を行うためのノウハウの共有
- 国民の安心感の醸成を図る観点から、組織内の既存の情報開示体制を活用し、可能な範囲(情報セキュリティ報告書、CSR 報告書、各種ディスクロージャ資料等)でサイバーセキュリティに関する取組を開示する。サイバーセキュリティに関する次の情報を開示することが望ましい。
  - ✓ 組織方針・サイバーセキュリティ方針
  - ✓ 維持するサービス範囲・水準
  - ✓ リスク管理体制

[19] 情報提供にあたっての判断基準として TLP (Traffic Lights Protocol) がある。TLP に関するガイダンスを一般社団法人 JPCERT コーディネーションセンターが翻訳し公開している。
「TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance – Version 2.0」
https://www.jpcert.or.jp/research/FIRST-TLP.html

- ✓ 情報セキュリティ責任者(CISO 等)の知見
- ✓ 資源の確保
- ✓ リスクの把握とリスクへの取り組み方針
- ✓ 緊急対応体制・事業継続／IT-BCP に関する取り組み内容／体制
- ✓ 重大なインシデントの発生状況(提供しているサービスの状況、復旧見込み等)

・ サイバー攻撃などの意図的な原因、機器等の故障などの偶発的な原因、自然災害などの環境的な原因によるシステム障害が発生し、業務への影響が生じた場合、管轄される地域の地方運輸局等の港運担当課へ情報共有することが望ましい。

●重要インフラ事業者等間の情報共有(例)

・ 重要インフラ事業者等は、所属するセプターにおいて、相互に重要インフラサービス障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の共有を行うこと。

・ 必要に応じて、他分野の重要インフラ事業者等との情報共有にセプターカウンシルを活用すること。

・ ISAC 内でサイバーセキュリティの確保に資する情報の共有・調査・分析、さらには海外の ISAC 等との情報共有等も進められている。ISAC 連携等による自動化を含めた分野間・官民連携の枠組みの整備を検討するなど、ISAC への参画や ISAC 間の情報共有を促進することで、更なる事業者間の情報共有の活発化やサイバーセキュリティの確保に係る積極的な取組を行うことが望ましい。(交通 ISAC [2.2 人材育成・意識啓発]参照)

2.1.4 従業員の管理

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報漏えいを防止するために、記録及び報告、人的安全管理措置、経営者層の訓練及び従業員の管理等の、適切な従業員の管理を講じる。

〔解説〕

PC や外部記録媒体の盗難、紛失及び当該 PC や外部記録媒体からの情報漏えいを防止するための措置や、個人情報を処理するアプリケーションからの情報漏えいを防止するために、適切な従業員の管理を講ずることが重要である。

例えば、港湾関連事業においては、コンテナヤード内に、多くの関連事業者の従業員が立ち入ることから、適切な従業員管理を行う必要がある。

〔具体例〕

●記録及び報告(例)

- リスクマネジメントの検証、改善のため、各プロセスにおいて、記録を作成する。記録の作成に当たっては次の事項を考慮する。
  - ✓ 記録の作成及び維持管理の費用及び労力
  - ✓ 閲覧方法、検索の容易性及び保存媒体
  - ✓ 保有期間
  - ✓ なお、記録を取ることを目的にするのではなく、利用目的に合わせて記録することが重要なことに留意する。
- ステークホルダーとのコミュニケーションの質を高めたり、経営者層の意思決定を補助したりするために報告を実施する。報告に当たっては次の事項を考慮する。
  - ✓ それぞれのステークホルダーに特有の情報の必要性及び要求事項
  - ✓ 報告の費用、頻度及び適時性
  - ✓ 報告の方法
  - ✓ 情報と組織の目的及び意思決定との関連性

●人的安全管理措置(例)

- 情報セキュリティ責任者(CISO 等)は、取扱者に対し、業務上知り得た秘密情報について守秘義務を課すこと及び秘密情報の取り扱いに関する教育・訓練等を行うこと
- 雇用契約時及び委託契約時における NDA(機密保持契約)の締結
- 取扱者に対する内部規程等の周知・教育・訓練の実施

●従業員の管理(例)

- 重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理する。

●経営者層の訓練及び従業員の管理(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の基本的な概念を網羅し、サイバーセキュリティに関する組織内文化を醸成する。
- サイバーセキュリティの基本的なトレーニングに加え、制御システムの運用、維持、保全の担当者は、制御システムに特化したサイバーセキュリティのトレーニングを年 1 回以上実施する。
- 雇用の終了又は変更後も有効なセキュリティに関する責任及び義務を定めて、従業員はその要求事項を遵守する。外部委託等の利害関係者に対しても同様の要求事項を伝達する。

2.1.5 要管理対策区域における入退出管理

【事業者に求めること】

> ➢ 情報セキュリティ責任者(CISO 等)は、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、適切な入退管理策を行う。

〔解説〕

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う資産や情報システムのサイバーセキュリティを確保する必要がある。

例えば、海上における人命の安全のための国際条約(SOLAS 条約)[20]に従い、国際港湾施設に設置が義務づけられている保安設備(保安照明、監視カメラ、不正侵入防止フェンス、ゲート、照明施設等)に対し、物理的な不正侵入対策を行う必要がある。

情報セキュリティ責任者(CISO 等)は、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(以下、「要管理対策区域」という。)を保護することが望ましい。

情報セキュリティ責任者(CISO 等)は、要管理対策区域への訪問者がある場合、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属の提示を求め、立入りを審査するための手続を整備すること。また、要管理対策区域内において、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講じ、必要に応じて取扱者が訪問者に付き添うための措置を講ずることが重要である。

〔具体例〕

●要管理対策区域における職員の入退出管理(例)

- 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。
- 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。
- 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。
- 情報システムを収容する建物の屋根、壁、天井及び床を強固な構造物とし、外部に接する全ての扉を施錠すること。
- 入退室時におけるアクセスカード、生体認証等による認証の仕組みや、警備員、侵入者警報、監視カメラ等による監視システムを構築すること。これにより、 認可された要員だけが管理領域に入

[20] 「海上における人命の安全のための国際条約」2002 年改正、国際海事機関 (IMO)
https://www.mlit.go.jp/seisakutokatsu/solas/index2.html

退できるようにする 。

●要管理対策区域における訪問者及び受渡業者の管理(例)

- 許可されていない者の入室手続きを定めること。
- 悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。
- 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、システム構築・運用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。

2.2　人材育成・意識啓発

【事業者に求めること】

- 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。
- 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。

〔解説〕

規程が適切に整備されているとしても、その内容が取扱者に周知されず、これが遵守されない場合には、サイバーセキュリティの向上を望むことはできない。このため、全ての取扱者が、サイバーセキュリティ教育を通じて、規程への理解を深め、セキュリティ対策を適切に実施することが必要である。

また、リスクに起因する経営・事業上の脅威に対するマネジメントや、経営者層等と緊密な連携を行えるよう、戦略マネジメント層の育成に取り組むことが求められる。さらに、有事のみならず、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といったサイバーセキュリティを確保・維持するための対応が必要である。サイバーセキュリティに係る担当者が変更となってもセキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行うことが重要である。

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。

セキュリティ対策業務に従事する人材を確保するため、キャリアパスの設計や外部人材活用の検討をすること。

情報セキュリティ責任者（CISO 等）は、サイバーセキュリティ関係規程について、取扱者を適切に教育・配置するための計画を立案するとともに、その実施体制及び教育のために必要となる資料を整備し、ノウハウの蓄積に努めること。

〔具体例〕

●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

情報セキュリティ対策の実施に当たっては、システム業務に従事する人材のみならず、システムユーザや PC 操作者に対しても必要な措置（情報セキュリティポリシー等の規程に基づく操作等）を求める必要がある。情報セキュリティ関係規程を組織全体に周知する等、組織内における情報セキュリティ意識の向上を図るとともに、情報セキュリティに係る教育・訓練等も実施すること。

※　　は、港湾運送事業法では強制要件（全ての港）

●サイバーセキュリティに関連する教育（例）

- サイバーセキュリティに関連する教育は、システム業務に従事する人材のみならず、システムユーザーやテレワーク勤務者を含むPC操作者も対象であることから、全社的に行うこと。

- サイバーセキュリティの推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を確保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び賃金政策をあらかじめ検討しておくこと。
- 重要インフラ事業者等においては、サイバーセキュリティに係る取組について海外同業他社や国際会議を通じた海外の動向把握、海外 ISAC[21]等との情報共有等により、多角的・多面的な国際連携に取り組むことが望ましい。

●人材育成・意識啓発(例)

- 情報セキュリティ責任者(CISO 等)は、サイバーセキュリティに関連する教育の計画に従い、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施すること。
- 重要インフラ事業者等の従業員がセキュリティ方針及びセキュリティ管理策の個別方針に基づく義務と責任を果たせるようにするため、従業員に対して、サイバーセキュリティに関連する十分な教育・トレーニングを実施する(必要に応じて委託先にも実施する。)こと。
- セキュリティ対策業務に従事する人材においては、政府機関の人材育成プログラムやセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練への参加、「情報処理安全確保支援士」等の資格取得等を推進すること。これらの取組は人材育成の達成状況を客観的に評価・確認する際にも有効となる。
- 各部門においても、セキュリティ対策を推進するセキュリティ担当者を配置するのが望ましい
- セキュリティ対策が不十分であった場合に生じる影響例を示す等の方法によりセキュリティ対策の重要性について啓発をすること。
- 経営リスクとなっているサイバーセキュリティリスクと他の経営リスクとの差異や、必要な組織体制、サイバーセキュリティ・インシデント対応における経営者層の役割等について可能な限り理解できるよう、経営者層に対してセキュリティ教育を実施すること[22]。
- 制御システムのサイバーセキュリティの確保に当たっては、制御システムを熟知した上でサイバーセキュリティの知見を高めることが重要である。制御システムに関するセキュリティ人材を確保する取組としては、産業サイバーセキュリティセンター(ICSCoE)による中核人材育成プログラムを活用することが考えられる。

●従業員の管理(例)

- セキュリティ対策業務に従事する人材を確保するため、キャリアパスの設計や外部人材活用の検討をすること。
- 重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理する。

[21] 交通 ISAC https://t-isac.or.jp/
[22] NISC では経営者層や DX を推進する部課長向けに、プラス・セキュリティ知識として、参考となるカリキュラムを公開している。
https://security-portal.nisc.go.jp/dx/plussecurity.html

●ノウハウの蓄積(例)

- 情報セキュリティ責任者(CISO 等)は、サイバーセキュリティ関係規程について、取扱者を適切に教育・配置するための計画を立案するとともに、その実施体制及び教育のために以下を例とする資料を整備し、ノウハウの蓄積に努めること。
  - ✓ 情報の取扱い(格付け及び取扱制限)
  - ✓ セキュリティ方針
  - ✓ セキュリティへの脅威と対策
  - ✓ 重要インフラサービス障害発生時の対処手順及び体制

2.3 演習・訓練

【事業者に求めること】

- リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行う。
- 情報セキュリティ責任者(CISO 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。
- 情報セキュリティ責任者(CISO 等)は、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。

〔解説〕

演習・訓練[23]を通じた課題抽出として、新たなリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に鑑みてリスクを特定する。

リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行う。経営者層も交え、組織全体[24]での演習・訓練を実施することが望ましい。また、演習・訓練の実施及びその結果評価(課題の抽出、改善策検討)において、セキュリティ専門機関と連携することが有効である。

また、他の重要インフラ事業者等、サプライチェーンに係る事業者等と合同の演習・訓練、過去のインシデント対応事例の研究等を実施することが望ましい。

〔具体例〕

●セキュリティインシデント対応訓練の実施

サイバー攻撃等のセキュリティインシデントが発生した場合に適切な対応が取れるよう、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(【1.8.1コンティンっジェンシープラン】参照)。

※ ＿＿は、港湾運送事業法では強制要件(特定の港)

●BCPに関する訓練の実施

事業の継続を目的として、システム障害やサイバー攻撃も想定した上で、優先する業務、必要な対策を決定するまでの過程、事業継続方法、連携を要する関連部門、対外的な情報発信等を規定する BCP を策定すること(【1.8.2 事業継続計画等の作成】参照)。

また、BCP に対応するための訓練を定期的に実施すること。

※ 　は、港湾運送事業法では強制要件(全ての港)

●演習・訓練(例)

・ リスクマネジメントによる事前対応と、障害発生時の危機管理の両面から、体制や取組の有効性を

[23] 演習・訓練に関して、日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」が参考となる
https://www.nca.gr.jp/activity/pub_doc/drill_manual.html

[24] 情報システムを共有しているグループ組織を含めた組織全体での視点を持った演習の必要性についても検討する。

検証するため、定期的に演習・訓練を実施する。

- 重要インフラ全体の防護能力の観点からは、同業の重要インフラ事業者等やサプライチェーン、関係主体等との合同での演習・訓練やケーススタディ（他事業者の過去のインシデント対応事例の研究）の実施も期待される。
- セプター訓練[25]を通じて、緊急時における情報連絡体制・手段の検証等、セプターや国土交通省からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有訓練の実現を目指す。重要インフラ事業者等はセプター訓練を通じて課題等を抽出し、改善に繋げることが望ましい。
- 合同での演習・訓練には、内閣サイバーセキュリティセンターが主催する「分野横断的演習」や、重要インフラ所管省庁やサイバーセキュリティ関係機関等の関係主体が主催するものがある。

[25] 行動計画では、各分野におけるセプター及び国土交通省との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施するとしている。

2.4 モニタリング及びレビュー

2.4.1 モニタリング実施計画の策定と実施

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、リスク対応計画の策定において決定した計画に則り、リスク対応を行ったセキュリティ管理策について評価を行うことが望ましい。
- 情報セキュリティ責任者(CISO 等)は、システムの構成機器上で利用するソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認する。

〔解説〕

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。これらが整合するようサイバーセキュリティを経営者層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営者層も関与した全社的な体制の下でセキュリティ管理策に取り組む必要がある。

セキュリティ対策の導入・運用に伴うリスクの状況変化(事象の発生頻度の変化や、事象の結果の影響度の変化等)を定期的に確認する。また、サイバーセキュリティ方針に基づき設定した目標の達成状況、サイバーセキュリティ方針・各種計画の有効性・妥当性等について、定期的に、又は状況変化に応じて確認する。

サイバーセキュリティ確保の取組の効果測定をし、改善を行うため、リスク対応計画や、人材育成の進捗状況等をモニタリングする。継続的に実施するため、モニタリング及びレビューのプロセスを計画に組み込む。

現状のシステムやセキュリティ対策の問題点を検出するために、重要システムに対して脆弱性診断、ペネトレーションテスト等を実施することが望ましい。

情報セキュリティ責任者(CISO 等)は、【1.3.4 リスク対応計画の策定】において決定した計画に則り、リスク対応を行ったセキュリティ管理策について評価を行うことが望ましい。セキュリティ方針や法令の遵守状況といった、コンプライアンスに偏った評価だけでなく、以下の具体例に示す項目についても評価を行うことが望ましい。また、【1.1.4 現在プロファイルの特定】で記載した成熟度モデル等を活用し、目標とした成熟度に達しているかどうか、を軸とした評価方法も参考となる。

〔具体例〕

●脆弱性や設定不備の定期検査

サーバ装置、端末及びネットワーク機器上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認すること。

脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及びネットワーク機器上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用、ソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、適切な措置を講ずること。

※ ＿＿は、港湾運送事業法では強制要件として、外部接続するネットワーク機器上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認することが必要(全ての港)。

●モニタリング実施計画の策定と実施(例)

- インシデントの検知の可否
- インシデント検知に要した時間
- 復旧までの時間(ダウンタイム)
- 経営者層へのエスカレーションフローの正当性
- 経営者層の意思決定に要した時間

※対応するべきインシデントが発生していない場合には、演習・訓練等による想定シナリオへの対応をもとにした評価を行うこともできる。

2.4.2 セキュリティ対策の自己点検

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、自己点検を実施するに当たり、その実施頻度、実施時期、自己点検すべき項目、実施項目の選択等に関する年度自己点検計画を整備する。

〔解説〕

セキュリティ対策の自己点検は、取扱者が自ら実施すべき対策事項の確認だけではなく、組織全体のセキュリティ水準の確認という目的もあることから、適切に実施することが重要である。また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

情報セキュリティ責任者(CISO 等)は、自己点検を実施するに当たり、その実施頻度、実施時期、自己点検すべき項目、実施項目の選択等に関する年度自己点検計画を整備すること。また、セキュリティの状況の変化に応じ、取扱者に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。

〔具体例〕

●セキュリティ対策の自己点検の実施(例)

＜情報セキュリティ責任者＞は、年度自己点検計画に基づき、
取扱者に自己点検の実施を指示する。

⇩

＜取扱者＞は、情報セキュリティ責任者から指示された
自己点検票及び自己点検の手順を用いて自己点検を実施する。

⇩

＜情報セキュリティ責任者＞は、自己点検結果の分析を行い、
評価結果を＜最高情報セキュリティ責任者＞へ報告する。

⇩

＜最高情報セキュリティ責任者＞は、自己点検結果を全体として評価し、
自己点検の結果により明らかになった問題点について、
情報セキュリティ責任者に改善を指示し、改善結果の報告を受ける。

⇩

自己点検の結果は、サイバーセキュリティ関係規程や
サイバーセキュリティ確保のための取組の更新に活用する。

●自己点検の実施計画に含む事が望ましい項目

- 実施頻度:年に2度以上実施することが望ましいが、例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては半年に一度の頻度で実施する等、様々な選択肢が考えられる。

- 実施時期：例えば、当初は毎月10項目ずつ自己点検し、取扱者の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。
- 確認及び評価の方法：自己点検が正しく行われていること、自組織の規程に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った評価とすることが望ましい。例えば、自己点検実施率（対策実施数／自己点検回答数）等の把握が挙げられる。
- 実施項目：例えば、前年度に重要インフラサービス障害が発生した事案や、前年度の自己点検実施率が低かった遵守事項等、様々な選択肢が考えられる。

2.4.3 監査計画の策定と実施

【事業者に求めること】

- 監査責任者は、必要に応じて、監査プロセスに従い、監査方針及び監査計画を作成し実施する。
- 情報セキュリティ対策の点検は、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。

〔解説〕

サイバーセキュリティの確保のためには、本ガイドラインに準拠した対策が適切に策定され、かつ運用されることによりその実効性を確保することが重要であり、その準拠性、実効性及び対策の妥当性が確認されなければならない。そこで、独立性を有する者による情報セキュリティ監査を実施することが必要である。

重要サービスや重要資産に対するサイバーセキュリティ確保の取組が適切に整備、運用されているかどうかを、独立した立場から検証、評価を行うことを目的とし、セキュリティ監査を実施する。監査を行い、自組織のセキュリティ対策が適正か、またどの程度浸透しているのかを検証し見える化することは、信頼性の高さを示すとともに、組織外に対しての説明責任にもつながる。

監査責任者は、必要に応じて、監査プロセスに従い、監査方針及び監査計画を作成し実施する。

〔具体例〕

●独立性を有する者による情報セキュリティ対策の点検

情報セキュリティの確保のためには、情報セキュリティに関する組織内の基準の妥当性、対策の妥当性、体制等の実効性の有無を確認する必要がある。そのため、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。

※ ＿＿は、港湾運送事業法では強制要件（特定の港）

●監査プロセス（例）

1. 監査方針の策定
2. 監査計画の立案
3. 監査の実施
4. 監査報告書の作成

●監査計画書に含める項目と方向性（例）

＜準備＞

監査人[26]の選定を含めた体制整備等

＜監査方針＞

重要インフラサービス提供に係る業務・システム及び設備に対するセキュリティ管理策の実効性を確認する

[26]組織内にセキュリティ監査人を設置することが難しい場合は、内部監査を外部委託することを検討する。公認情報セキュリティ監査人といった認定制度を参考とする。
https://www.jasa.jp/qualification/about/auditor/

＜対象業務＞
　重要インフラサービス提供に係る業務を対象とする
＜監査期間＞
＜監査報告＞
＜監査結果への対応＞
＜フォローアップ＞

●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する。
年度情報セキュリティ監査計画及びサイバーセキュリティの状況に応じた監査の実施指示に基づき、個別の監査業務毎の監査実施計画を立案する。

監査実施計画に従って監査を実施し、事業者内基準が本ガイドラインに準拠しているか、被監査部門における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する。

監査結果は、報告書として文書化した上で、適切な保管・管理を実施する。

＜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情報セキュリティ責任者に指示する。

＜情報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し、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する。
報告結果をサイバーセキュリティ関係規程やセキュリティ対策の更新に活用する。

●年度情報セキュリティ監査計画に含むことが望まれる項目

- 重点とする監査対象及び監査目標（情報漏えい防止、不正アクセス防止など）
- 監査の実施期間
- 監査業務の管理体制
- 外部委託による監査の必要性及び範囲
- 監査に係る予算 等

●監査実施計画に含まれることが望ましい項目

- 監査の実施時期
- 監査の実施場所
- 監査の実施担当者及び割当て

- 準拠性監査(サイバーセキュリティ関係規程に準拠した手続が実施されていることを確認する監査)のほか、必要に応じて妥当性監査(実施している手続が有効なセキュリティ管理対策であることを確認する監査)を行うかについての方針
- 実施すべき監査の概要(監査要点、実施すべき監査の種類及び試査の範囲を含む。)
- 監査の進捗管理手段又は体制

2.5 継続的改善

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、各規程の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

〔解説〕

サイバーセキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、サイバーセキュリティ水準を維持できなくなる。このため、対策の根幹をなすサイバーセキュリティ関係規程は、実際の運用において生じた課題、自己点検、監査の結果等を踏まえて、適時見直しを行う必要がある。

見直しを行う時期については、次の状況を勘案し、セキュリティ対策に支障が発生しないように判断すること。

- ✓ 運用段階における事故等の発生
- ✓ 自己点検・監査の結果
- ✓ 取扱者からの相談等

サイバーセキュリティに関する監査・モニタリングの結果や、最新のセキュリティ動向も踏まえ、組織統治の枠組みの継続的改善を行う。サイバーセキュリティを担当する部署においては、経営者層からの指示、モニタリング・レビュー、危機管理、演習・訓練等を踏まえ、サイバーセキュリティ方針、各種計画等の継続的改善を行う。

改善を継続的に実施することで、サイバーセキュリティも含めたリスクマネジメントの考え方が組織に浸透し、組織風土に定着するよう努めることが望ましい。

〔具体例〕

●セキュリティ管理策の見直しにあたっての留意点

- サイバー空間からの脅威の変化に対応して見直しを実施すること。
- 過去のサイバーセキュリティ・インシデントの特性を踏まえ、セキュリティ方針の有効性について、定期的に見直しを実施すること。
- 実施しているセキュリティ対策の管理策に対する費用対効果について、定期的に見直しを実施すること。
- セキュリティ管理策を刷新することによる効果について、定期的に見直しを実施すること。
- モニタリング及び監査結果から、改善や見直しが必要な箇所を認識する。レビューに際し、内部環境、外部環境の変化や、関係主体からの要求事項も確認する。

3　インシデント発生時及び事後対応

3.1　コンティンジェンシープラン及び BCP の実行

【事業者に求めること】

- 情報セキュリティ責任者（CISO 等）は、重要インフラサービス障害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。

〔解説〕

重要インフラサービス障害が発生した場合には、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必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた責任者へ報告し、障害による影響や範囲をエスカレーションし、二次被害を最小限に抑えることが重要である。

策定したコンティンジェンシープラン、IT-BCP 又は BCP 等を実行し、規定に沿った事業継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、重要インフラサービス障害をもたらした原因への適切な対処を可能とすることが望ましい。

インシデント発生時の対応としては、IPA「中小企業のためのセキュリティインシデント対応の手引き」、JPCERT コーディネーションセンター「インシデントハンドリングマニュアル」等が参考となる。

〔具体例〕

●コンティンジェンシープラン及び BCP の実行（例）

- 情報セキュリティ責任者（CISO 等）は、サイバー攻撃等の事象が発生した際、経営者層の意志決定を支援するため、経営者層が理解できるように事象の内容、影響及び現在の対応状況等を説明する。
- 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析（情報システム等へのフォレンジックを含む。）、関係主体等との情報共有・調整（顧客向け広報活動を含む）、被害拡大の防止、サービスの復旧等の対応を実施する。
- 原因究明等に必要なログ等の電子的記録を収集・分析することにより、重要インフラサービス障害をもたらした原因への適切な対処を可能とする。
- 重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

●インシデント対応フロー（例）

- JPCERT コーディネーションセンターの「インシデント対応マニュアルの作成について」（2021 年 11 月）では、インシデントの対応フローとして、以下が例示されている。
  1. インシデントの発見及び報告
     - ✓　インシデントの発見者からの報告を受け取る
     - ✓　インシデントの報告を受けた者の行動基準を明確にしておく

- ✓ インシデントの取り扱いに関するすべての記録を残す

2. インシデントに対する初動対応
   - ✓ 発生したインシデントに関して、どこまで情報を共有するのかを判断する
   - ✓ 過去の経験を活用できるかどうかを判断する
3. インシデントに関する告知
   - ✓ 組織外に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
   - ✓ 誰に告知をすべきかを判断する
   - ✓ 告知する手段を検討する
4. インシデントの抑制措置と復旧
   - ✓ インシデントの被害を抑制するための検討
   - ✓ 復旧に関する検討
5. インシデントの事後対応
   - ✓ 復旧後の監視を継続する
   - ✓ 再発防止策を検討する
   - ✓ 他の情報資産への影響がないかどうかを評価する
   - ✓ 得られた教訓を従業員やスタッフ等への教育に反映する

●インシデント対応の流れ(例)

・ NISTの「Computer Security Incident Handling Guide Revison2」では、インシデント対応の流れとして、「準備」、「検知・分析」、「封じ込め、根絶、復旧」、「事後の活動」の流れが示されている。

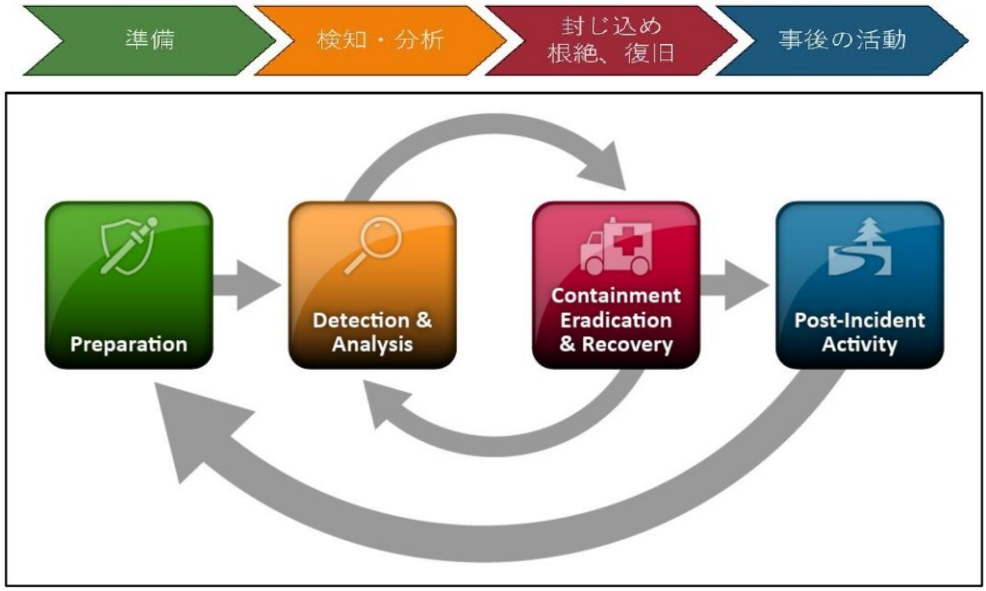


Figure 3-1. Incident Response Life Cycle

・ いわゆる、初動対応は、上図の「検知・分析」から「封じ込め」ぐらいまでを指すことが多い。

3.2　重要インフラサービス障害発生時の情報共有

【事業者に求めること】

- 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。
- 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。

〔解説〕

重要インフラ事業者等は、国民生活及び社会経済活動に影響を与える重要インフラサービス障害が発生し以下のいずれかのケースに該当する場合、国土交通省へ情報連絡を行うものとする。重要インフラサービス障害には、サイバー攻撃などの意図的な原因、機器等の故障などの偶発的な原因、自然災害などの環境的な原因が挙げられる。情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとし、全容が判明する前の断片的又は不確定なものであっても差し支えない。

（システムの不具合等により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。
- ✓ 関係主体が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した場合であって、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。
- ✓ そのほか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。

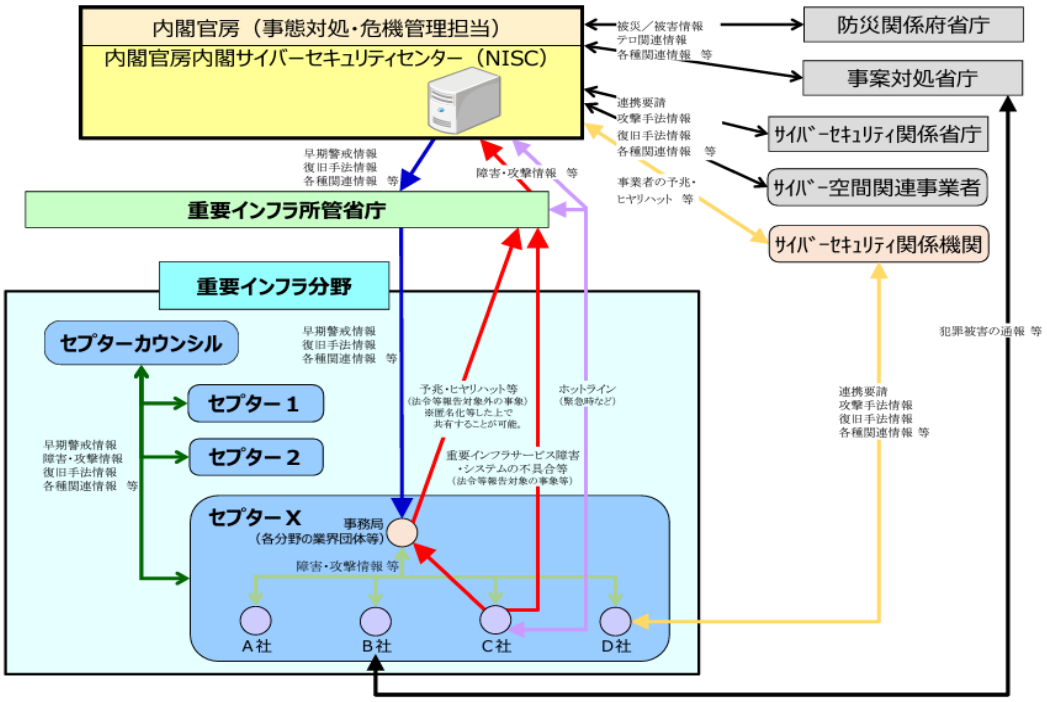
NISC「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和5年3月8日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）を参照の上、組織内外と情報共有を実施することが望ましい。

収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行う。（【1.1.1 内部状況・外部状況の理解】で示した港湾分野の関係主体（例）参照）

また、情報共有や情報発信を行う際は、情報提供及び問合せ対応の窓口を設定すること。なお、問合せが集中する恐れがあることから、複数名を指定しておくことが望ましい。また、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。

「行動計画に基づく手順書」での関係者間の情報共有体制(大規模インフラサービス障害対応時)

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

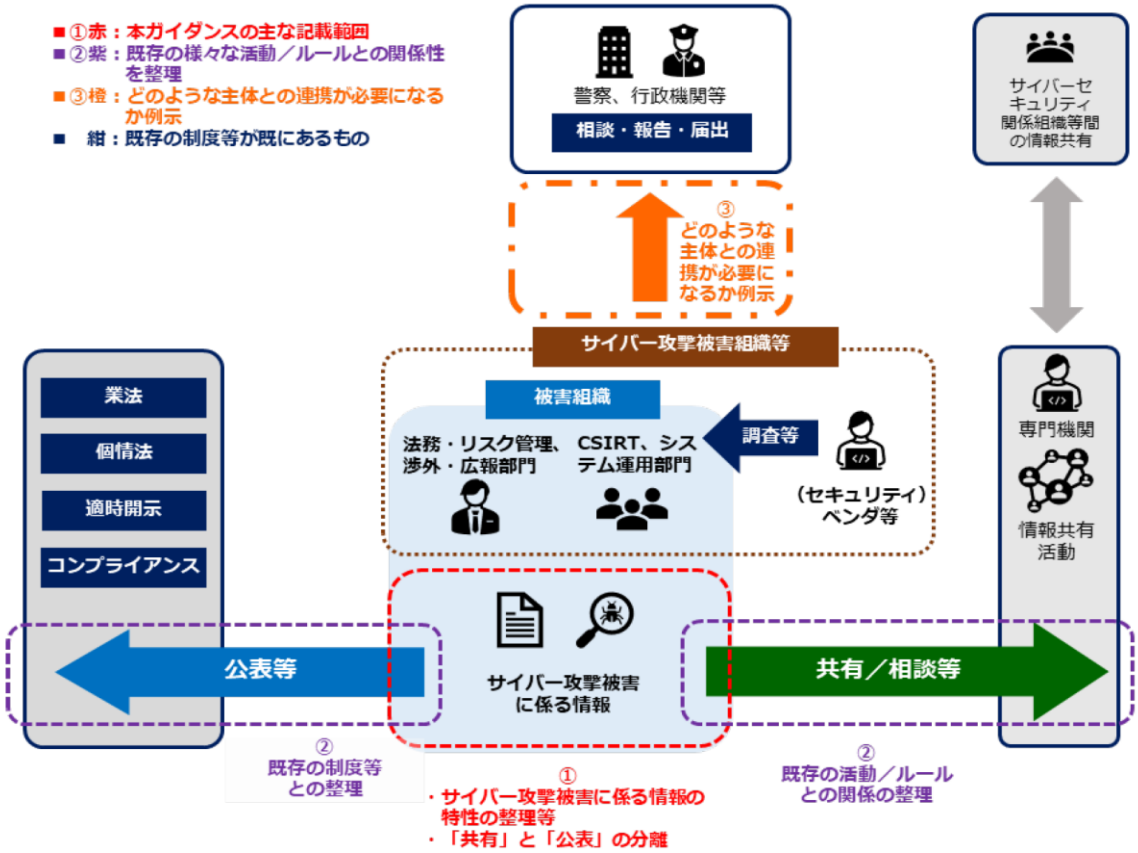
関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における[注]各関係主体の役割
○ 内閣官房 （事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房 （ＮＩＳＣ）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	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。

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別紙 4-1「情報共有体制(通常時)」

別紙 4-3「情報共有体制における各関係主体の役割

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」での情報共有の内容



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

出典:サイバー攻撃被害に係る情報の共有・公表ガイダンス（令和５年３月８日）より抜粋

〔具体例〕

●セキュリティインシデントが発生した場合の情報連絡体制

ア. 自組織内の情報共有

セキュリティインシデントが発生した場合、情報セキュリティ対策の観点から CISO 及び各情報セキュリティ担当者間で速やかに情報共有を行うとともに、事業継続の判断等を行う経営者層に対しても速やかに情報共有を行うこと。

イ. 専門組織への情報共有

サイバー攻撃が発生した場合には、国の法令、制度等に基づき非営利でインシデント対応相談や分析、情報共有活動を行う専門機関やセキュリティベンダーといった専門組織に対して、マルウェア情報等攻撃者による攻撃活動やまたはその痕跡を示す攻撃技術情報を共有することで、攻撃原因や被害範囲の特定を進めることが望ましい。

また、原因の特定を行うにあたり、専門組織に対してセカンドオピニオン的な相談を行うことが望ましい。

ウ. 国、港湾管理者等への情報共有

サイバー攻撃等の意図的な原因、機器等の故障等の偶発的な原因、自然災害等の環境的な原因によるシステム障害が発生し、業務への影響が生じた場合、管轄される地域の地方運輸局等の港運担当課へ情報共有を行う。

また、港湾内の状況把握の観点から、港湾管理者に対しても情報共有を行うとともに、港湾管理者は管轄される地域の地方整備局等の危機管理担当課へ情報共有を行う。

なお、サイバー攻撃が発生した場合には、所轄の都道府県警察に通報を行うこと。

●専門組織への情報共有（例）

- サイバー攻撃が発生した場合には、国の法令、制度等に基づき非営利でインシデント対応相談や分析、情報共有活動を行う専門機関やセキュリティベンダーといった専門組織に対して、マルウェア情報など攻撃者による攻撃活動やまたはその痕跡を示す攻撃技術情報を共有することで、攻撃原因や被害範囲の特定を進めることが望ましい。
- また、原因の特定を行うにあたり、専門組織に対してセカンドオピニオン的な相談を行うことが望ましい。

3.3 セキュリティ管理状況の対外説明

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、重要インフラサービス障害の状況や復旧等の情報提供については、策定した IT-BCP 等又は BCP 等に沿って、対応する。
- 上記の情報共有や情報発信を行う際は、情報提供及び問合せ対応の窓口を設定する。また、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。

〔解説〕

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・安心感の醸成につながる。なお、情報開示はステークホルダーとのコミュニケーションの一部という側面があり、ガバナンスとしてサイバーセキュリティに関する取組のみを情報開示することが正しいとは限らないことに留意する。開示する情報は機密情報推測のリスクや、その他の要素を踏まえ経営判断に委ねるべきである。

重要インフラサービス障害の状況や復旧等の情報提供については、策定した IT-BCP 等又は BCP 等に沿って、情報に基づく対応の 5W1H の理解の下、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う。

- ✓ 重要インフラサービス障害による重要インフラサービスの停止等の情報の提供
- ✓ 重要システムの停止・低下により、輸送の遅延・停止が発生した際等、重要インフラ利用者が安心して対応が行えるよう情報提供を行うこと。

●セキュリティインシデントが発生した場合の情報発信

ア. 対外的な情報発信

システム障害等により業務への影響が生じた場合、TOS 等の利用者等の関係者に対して、提供しているサービスの状況、復旧見込み等について適切な情報提供・公表を行うこと。

イ. 窓口担当者の指定

上記の情報共有や情報発信を行う際は、情報提供及び問合せ対応の窓口を設定すること。なお、問合せが集中する恐れがあることから、複数名を指定しておくことが望ましい。また、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。

3.4 インシデント管理

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、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。

〔解説〕

既存のセキュリティ対策の運用を通じて発見した脅威や脆弱性、及びそれらから生じた事象等を分析し、今後の運用に活用する。また、過去に生じたインシデントへの対応を通じて得た知見を活用することにより、重要インフラサービス障害からの速やかな回復、及び類似障害の再発防止、対策の改善を図る。

既存のセキュリティ管理策の運用を通じて得た以下のような経験等を分析し、今後の運用に活用すること。

- ✓ 新たな脅威や脆弱性
- ✓ 重要インフラサービスへの影響
- ✓ 重要インフラサービス障害のインパクト

また、重要インフラサービス障害の復旧後、類似の障害再発防止ならびに再発時における措置等の改善策の強化を図ることが重要である。また、障害情報の管理方法、項目等の具体的運用方法について内規等で定めることが望ましい。

インシデントの原因究明にあたっては、システム構築・運用者のみならず、セキュリティ専門機関の意見も踏まえつつ、原因究明を行うことが望ましい。

特に、サイバー攻撃被害を受けた場合には、感染経路の特定に加えて内部ネットワークへ侵入された痕跡がないか、侵入された可能性がある場合は横展開され被害範囲が拡大していないか等のフォレンジック調査を行うことが望ましい。フォレンジック調査は、原因究明や再発防止策策定に資するのみならず、フォレンジック調査レポートを公表することで、企業の信頼性の維持や、情報セキュリティに関わる事故により自社が責任を問われることになった場合や不正者を訴えたい場合等の法的措置への対応にも有効となる。

〔具体例〕

●インシデント管理(例)

- 重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。
- 管理、文書化、検知、優先順位付け、分析、伝達及び利害関係者の調整等を含む、自組織がセキュリティインシデントを管理するためのプロセスを確立する。

別紙1. 情報の取扱い・個人情報保護

1 情報の取扱いについての規定化

取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、提供、運搬、送信、消去等といった情報のライフサイクルの各段階における遵守事項、セキュリティ管理策を規定する。

なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みた取扱いを規定する。

【事業者に求めること】

- 重要インフラサービスに係る情報の取扱い手順を整備し、分類・ラベル付けする。

〔解説〕

重要インフラサービスの提供に係る情報及びその他の関連資産を適切に保護するため、情報の取扱い手順を整備する。情報は機密性、完全性、可用性及び関連する利害関係者の要求事項に基づき分類及び情報媒体へのラベル付けを行う。

〔具体例〕

●情報の格付けと取扱の規定化（例）

- 機密性、完全性、可用性の観点から、情報を格付けし、情報媒体（紙、電子）へのラベル付け等により管理する。
- 情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を実施する。
- 自組織の業務上の要求事項に対処できるよう、情報の分類体系はアクセス制御に関する方針と整合させる。
- 自組織が採用した情報分類体系に従って、情報のラベル付けに関する手順を策定し、情報の分類、伝達、処理、管理を適切に行う。ラベル付けは物理的、電子的手段等があるが、デジタル情報についてはメタデータを活用する手法がある。
- 技術的な制約等によりラベル付けが不可能な場合の情報についても取扱いの手順を定める。

1.1 情報の格付け

【事業者に求めること】

- 情報のライフサイクル全体で適切な対策を講じ、情報作成時に格付けや取扱制限を明示し対応する必要がある。

〔解説〕

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての取扱者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、取扱者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び

取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

〔具体例〕

●情報の格付けと取扱制限規定の整備(例)

- 情報セキュリティ委員会は、業務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から情報の格付け及び取扱制限に関する以下を含む規定を整備し、取扱者へ周知すること。
  - ✓ 情報の格付及び取扱制限についての定義
  - ✓ 情報の格付及び取扱制限の明示等についての手続
  - ✓ 情報の格付及び取扱制限の継承、見直しに関する手続

1.2 情報のライフサイクルにおけるセキュリティ管理策

1.2.1 情報の作成・入手

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、共通の情報利用時に認識のずれが生じないよう、作成時に情報の格付けや取扱制限を明示し、適切な管理対策を講じることが求められる。

〔解説〕

業務の遂行のために複数の者が共通の情報を利用する場合がある。この際、取扱者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切なセキュリティ管理策が採られないおそれがあるため、情報を作成し又は入手した段階で、全ての取扱者において認識を合わせるための措置が必要となる。

情報セキュリティ責任者(CISO 等)は、情報を作成又は入手することにより発生するリスクに対応するため、情報の作成又は入手時における格付けの決定と取扱制限の明示方法などについて、定められた手順に従って適切な対策を講ずること。

情報の入手と作成については、以下の対策を規定することが望ましい。

〔具体例〕

●業務以外の情報の作成又は入手の禁止(例)

- 取扱者は、業務の遂行以外の目的で、情報を作成し又は入手しないこと。

●情報の作成又は入手時における格付けの決定と取扱制限の検討(例)

- 取扱者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。
- 取扱者は、事業者外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。
- 取扱者は、入手した情報の格付けおよび取扱制限が不明な場合には、情報の作成元や入手元に確認すること。

●格付けと取扱制限の明示(例)

- 取扱者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。

●格付けと取扱制限の継承(例)

- 取扱者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

●格付けと取扱制限の変更(例)

- 取扱者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。
- 取扱者は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

1.2.2 情報の利用

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、認識不足や対策の不備による情報漏えいや改ざんのリスクを避けるため、情報の格付けに応じた適切な取扱いと対策を徹底する必要がある。

〔解説〕

業務の遂行のために多くの情報を取り扱うが、情報システムの取扱者の認識不足等による情報の不適切な利用や、情報システムの責任者による脆弱性の対策及び不正プログラム対策の不備等の問題により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。情報を不適切に利用すると、情報の漏えい、改ざん、不当な消去、不当な持出し等によって、情報セキュリティを損なうリスクが増大し、事業に何らかの損害を与えることが考えられる。それらのリスクに対応するため、情報を適切に利用しなければならない。

情報セキュリティ責任者(CISO 等)は、情報を利用することにより発生するリスクに対応するため、情報の取り扱い方法などについて、利用する情報の格付けに応じた適切な対策を講ずること。

情報の利用については、以下の対策を規定することが望ましい。

〔具体例〕

●業務以外の利用の禁止(例)

- 取扱者は、業務の遂行以外の目的で、情報システムに係る情報を利用しないこと。

●格付け及び取扱制限に従った情報の取扱い(例)

- 取扱者は、利用する情報に明示された格付け及び取扱制限に従って、当該情報を適切に取り扱うこと。

1.2.3 情報の保存

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報保存に伴うリスクに対応するため、保存情報の格付けに応じた管理方法や保存期間など、適切な対策を講じることが求められる。

〔解説〕

業務においては、継続性を確保するなどの必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続するため、適切に情報を保存する必要がある。

情報セキュリティ責任者(CISO 等)は、システム構築・運用者に対し、情報を保存することにより発生するリスクに対応するため、情報の管理方法、保存期間等について、保存する情報の格付けに応じた適切な対策を講ずるよう指示すること。

情報の保存については、以下の対策を規定することが望ましい。

〔具体例〕

●格付けに応じた情報の保存(例)

- システム構築・運用者は、サーバ装置、端末に保存された情報の格付けに従って、適切なアクセス制御を行うこと。
- 取扱者は、情報の格付けに従って、情報が保存された外部記録媒体を適切に管理すること。
- 取扱者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面について、情報の格付けに従って、適切に管理すること。
- 外部記憶媒体を使用する際は、システムと切り離された端末でウィルスチェックを行うこと。
- 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、暗号化を行う必要性の有無を検討し、必要があると認めたときは、客観的に評価された暗号技術(※)により、情報を暗号化すること。
- 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用する必要性の有無を検討し、必要があると認めたときは、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用するなどの対応を行うこと。
- 取扱者は、情報を保存した機器等について、保存した情報の格付けに従って、盗難及び不正な持ち出し等の物理的な脅威から保護する必要性の有無を検討し、必要があると認めたときは、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。
- 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付

けに従って、暗号化や電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に客観的に評価された暗号技術(※)による暗号化や電子署名を付与すること。
- 取扱者は、情報を外部記録媒体に保存する場合には、保存する情報の格付けに従って、外部記録媒体に保存内容が容易に想定できるようなタイトル表示をしない等の対処を行うこと。
- 取扱者は、電磁的記録又は設計書等の情報システム関連文書について、情報の格付けに従って、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。
- システム構築・運用者は、電磁的記録のバックアップ又は設計書等の情報システム関連文書の複写の保管について、情報の格付けに従って、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること。
- システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うこと。
- 事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど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。
- 個人情報及び認証情報を含む機微なデータは、暗号化して保存され、許可された管理者のみがアクセスできるようにすること。

※「電子政府推奨暗号リスト」に記載された暗号化アルゴリズム

●情報の保存期間(例)

- 取扱者は、サーバ装置、端末又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

1.2.4 情報の運搬・送信

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報運搬・送信に伴うリスクに対応するため、情報の形態や格付けに応じた適切な運搬・送信手段を選択できるよう、対策を整備することが求められる。

〔解説〕

業務においては、その事務の遂行のために他者又は自身に情報を運搬・送信する場合がある。運搬・送信の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部記録媒体の運搬及び PC、紙面に記載された情報の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の運搬・送信により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになるため、適切な情報の運搬・送信に係る措置を講ずる必要がある。

情報セキュリティ責任者(CISO 等)は、情報を運搬・送信することにより発生するリスクに対応するため、運搬・送信する情報の形態及び格付けに応じた適切な運搬・送信手段を選択できるように対策を

整備すること。

情報の運搬・送信については以下の対策を規定することが望ましい。

〔具体例〕

●情報の運搬・送信に関する許可(例)

- 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って、情報セキュリティ責任者(CISO 等)の許可を得ること。

●情報の運搬・送信の選択(例)

- 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って安全確保に留意して、送信又は運搬のいずれによるかを決定すること。

●運搬・送信手段の選択(例)

- 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って安全確保に留意して、当該情報の運搬・送信手段を決定すること。
- 取扱者は、情報の格付けに従って、秘密文書に該当するような機密性の高い情報を運搬・送信する場合には、情報セキュリティ責任者(CISO 等)が指定する方法に従うこと。

●書面に記載された情報の保護対策

- 取扱者は、書面を運搬する場合には、記載されている情報の格付けに従って安全確保のための適切な措置を講ずること。

1.2.5 情報の提供・公表

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報の提供・公表に伴うリスクに対応するため、提供・公表する情報の形態や格付けに応じた適切な情報提供・公表が行われるよう、対策を整備することが求められる。

〔解説〕

業務においては、その業務の遂行のために事業者外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがあるため、適切な情報の提供に係る措置を講ずる必要がある。

情報セキュリティ責任者(CISO 等)は、情報の提供・公表により発生するリスクに対応するため、提供・公表する情報の形態及び格付けに応じた適切な情報提供・公表がなされるように対策を整備すること。

情報の提供・公表については、以下の対策を規定することが望ましい。

〔具体例〕

●情報の公表(例)

- 取扱者は、情報を公表する場合には、公表する情報の格付けに従って公表の可否を決定すること。
- 取扱者は、電磁的記録を公表する場合には、情報の格付けに従って、当該情報の付加情報(更新の履歴、文書のプロパティ等をいう。)等からの不用意な情報漏えいを防止するための措置を採ること。

●他者への情報の提供

- 取扱者は、情報を事業者外の者に提供する場合には、提供する情報の格付けに従って、情報セキュリティ責任者(CISO 等)の許可を得ること。
- 取扱者は、情報を事業者外の者に提供する場合には、提供先において、提供する情報の格付けに従って適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること
- 取扱者は、電磁的記録を提供する場合には、情報の格付けに従って、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を採ること。

1.2.6 情報の消去

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、情報の処分に伴うリスクに対応するため、処分する情報の形態や格付けに応じた適切な処分が行われるよう、対策を整備することが求められる。

〔解説〕

業務において利用したサーバ装置、端末、通信回線装置及び外部記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報の消去を行っていたつもりでも、適切な措置が採られていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されないため、適切な情報の消去に係る措置を講ずる必要がある。

情報セキュリティ責任者(CISO 等)は、情報の処分により発生するリスクに対応するため、処分する情報の形態及び格付けに応じた適切な処分がなされるように対策を整備すること。

情報の消去については、以下の対策を規定することが望ましい。

なお、委託先は、事前に合意した情報の廃棄方法の手順に沿って情報を廃棄すること。

〔具体例〕

●電磁的記録の消去方法(例)

- 取扱者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。
- 取扱者は、サーバ装置、端末、通信回線装置及び外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、全ての情報を復元できないよう抹消すること。

・ 取扱者は、サーバ装置、端末、通信回線装置及び外部記録媒体を他の者へ提供する場合には、保存された情報の格付けに従って、復元が困難な状態にする必要性の有無を検討し、必要があると認めたときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該サーバ装置、端末等の情報を復元が困難な状態にし、残留する情報を最小限に保つこと。

●書面の廃棄方法(例)

・ 取扱者は、情報が記録された書面を廃棄する場合には、廃棄する情報の格付けに従って、復元が困難な状態にすること。

1.3 個人情報保護に関わる対策

【事業者に求めること】

➢ 業務で取り扱う個人情報は、その目的や重要性に応じて適切な対策を講じ、情報セキュリティを確保する必要がある。

〔解説〕

業務で取り扱う個人情報については、その目的、用途及び保管項目により、取扱いに慎重を要する度合いは様々であり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、適切な対策を講ずる必要がある。

〔具体例〕

●個人データ取り扱い台帳の整備(例)

・ 情報セキュリティ責任者(CISO 等)は、個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備し、定期的に内容を更新することで最新状態を維持すること。

●個人情報の類型化(例)

・ 情報セキュリティ責任者(CISO等)は、個人データの適切なレベルでの保護を確実にし、保護の必要性、優先順位、及び程度を示すために、漏えい時の事業への影響度などのリスク評価の結果に応じて分類すること。

●海外の個人情報の取扱い(例)

・ 海外の個人情報の取り扱いに関しては、各国で個人情報保護における法制度が確立されており、国によっては罰則などが適用されるおそれがある。そのため、各国のルールに沿って個人情報を取り扱うため、諸外国の個人情報の規則を必要に応じて参照すること。例えば、EU 域内の個人データ保護を規定する「EU 一般データ保護規則(General Data Protection Regulation:GDPR)等がある。

1.4 個人情報に関わる管理

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、個人情報の入力時の照合・確認、誤り訂正、記録更新・保存期間設定により、個人データを正確かつ最新に保ち、媒体をライフサイクルに基づき適切に取り扱う措置を明示することが求められる。

〔解説〕

業務の遂行のために複数の者が共通の個人情報を利用する場合がある。この際、取扱者により個人情報の取扱いに関する認識が異なると、個人情報に応じた適切なセキュリティ管理策が採られないおそれがあるため、情報を作成し又は入手した段階で、全ての取扱者において認識を合わせるための措置が必要となる。

情報セキュリティ責任者(CISO 等)は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つこと。

また、情報セキュリティ責任者(CISO 等)は、個人情報が記録された媒体を、ライフサイクル(「取得・入力」「運搬・送信」「利用・加工」「保管・バックアップ」「消去・廃棄」)に基づいて適切に取り扱うための措置を明示すること。

ライフサイクルに基づいた個人情報の管理対策を検討する際には、以下の対策を講ずることが望ましい。

〔具体例〕

●取得・入力時における個人情報の管理策(例)

＜作業責任者の明確化＞

- 個人データを取得する際の作業責任者の明確化
- 取得した個人データを情報システムに入力する際の作業責任者の明確化

＜手続の明確化と手続に従った実施＞

- 取得・入力する際の手続の明確化
- 定められた手続による取得・入力の実施
- 権限を与えられていない者が立ち入れない建物、部屋(以下「建物等」という。)での入力作業の実施
- 個人データを入力できる端末の、業務上の必要性に基づく限定
- 個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定(例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。)
- Web 会議で扱われる音声、映像、参加者 ID、参加者のメールアドレス等の様々な個人情報の取扱いに関する適切な手続きの明確化

＜作業担当者の識別、認証、権限付与＞

・ 個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
・ ID とパスワードによる認証、生体認証等による作業担当者の識別
・ 作業担当者に付与する権限の限定
・ 個人データの取得・入力業務を行う作業担当者に付与した権限の記録

＜作業担当者及びその権限の確認＞

・ 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・ アクセスの記録、保管と、権限外作業の有無の確認

●運搬・送信時における個人情報の管理策(例)

＜作業責任者の明確化＞

・ 個人データを運搬・送信する際の作業責任者の明確化

＜手続の明確化と手続に従った実施＞

・ 個人データを運搬・送信する際の手続の明確化
・ 定められた手続による運搬・送信の実施
・ 個人データを運搬・送信する場合の個人データの暗号化等の秘匿化(例えば、公衆回線を利用して個人データを送信する場合)
・ 運搬時におけるあて先確認と受領確認(例えば、簡易書留郵便その他個人情報が含まれる荷物を輸送する特定のサービスの利用)
・ FAX等におけるあて先番号確認と受領確認
・ 個人データを記した文書をFAX等に放置することの禁止
・ 暗号鍵やパスワードの適切な管理

＜作業担当者の識別、認証、権限付与＞

・ 個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
・ ID とパスワードによる認証、生体認証等による作業担当者の識別
・ 作業担当者に付与する権限の限定(例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。)
・ 個人データの移送・送信業務を行う作業担当者に付与した権限の記録

＜作業担当者及びその権限の確認＞

・ 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・ アクセスの記録、保管と、権限外作業の有無の確認

●利用・加工時における個人情報の管理策(例)

＜作業責任者の明確化＞

・ 個人データを利用・加工する際の作業責任者の明確化

＜手続の明確化と手続に従った実施＞

・ 個人データを利用・加工する際の手続の明確化
・ 定められた手続による利用・加工の実施
・ 権限を与えられていない者が立ち入れない建物等での利用・加工の実施
・ 個人データを利用・加工できる端末の、業務上の必要性に基づく限定
・ 個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

＜作業担当者の識別、認証、権限付与＞

・ 個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
・ ID とパスワードによる認証、生体認証等による作業担当者の識別
・ 作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
・ 個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

＜作業担当者及びその権限の確認＞

・ 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・ アクセスの記録、保管と権限外作業の有無の確認

●保管・バックアップ時における個人情報の管理策（例）

＜作業責任者の明確化＞

・ 個人データを保管・バックアップする際の作業責任者の明確化

＜手続の明確化と手続に従った実施＞

・ 個人データを保管・バックアップする際の手続（※）の明確化

※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（OS）やアプリケーションのバックアップも必要となる場合がある。

＜定められた手続による保管・バックアップの実施＞

・ 個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化
・ 暗号鍵やパスワードの適切な管理
・ 個人データを記録している媒体を保管する場合の施錠管理

・ 個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
・ 個人データを記録している媒体の遠隔地保管
・ 個人データのバックアップから迅速にデータが復元できることのテストの実施
・ 個人データのバックアップに関する各種事象や障害の記録

＜作業担当者の識別、認証、権限付与＞
・ 個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
・ ID とパスワードによる認証、生体認証等による作業担当者の識別
・ 作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。）
・ 個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

＜作業担当者及びその権限の確認＞
・ －手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・ アクセスの記録、保管と権限外作業の有無の確認

●消去・廃棄時における個人情報の管理策（例）

＜作業責任者の明確化＞
・ 個人データを消去する際の作業責任者の明確化
・ 個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

＜手続の明確化と手続に従った実施＞
・ 消去・廃棄する際の手続の明確化
・ 定められた手続による消去・廃棄の実施
・ 権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
・ 個人データを消去できる端末の、業務上の必要性に基づく限定
・ 個人データが記録された媒体や機器をリース事業者に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回又は複数回上書きする。）
・ 個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

＜作業担当者の識別、認証、権限付与＞
・ 個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
・ ID とパスワードによる認証、生体認証等による作業担当者の識別
・ 作業担当者に付与する権限の限定
・ 個人データの消去・廃棄を行う作業担当者に付与した権限の記録

＜作業担当者及びその権限の確認＞

- 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管、権限外作業の有無の確認

1.5 不正アクセスのための脅威への対策

【事業者に求めること】

- 情報セキュリティ責任者（CISO 等）は、個人データの漏えい、滅失、き損防止のため、組織的、人的、物理的、技術的な安全管理措置を講じ、リスクに応じた適切な対策を実施することが求められる。

〔解説〕

個人情報が保存されたPCや外部記録媒体の盗難、紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、個人情報を処理するアプリケーションからの情報漏えいを防止するために、適切な対策を講ずる必要がある。

情報セキュリティ責任者（CISO 等）は、取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない。

その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講ずること。

不正アクセスのための脅威への対策を検討する際には、以下の対策を講ずることが望ましい。

〔具体例〕

●組織的安全管理措置（例）

情報セキュリティ責任者（CISO 等）は、安全管理について取扱者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認すること。

- 個人データの安全管理措置を講ずるための組織体制の整備
- 個人データの安全管理措置を定める規程等の整備と規程等に従った運用
- 個人データの取扱い状況を一覧できる手段の整備
- 個人データの安全管理措置の評価、見直し及び改善
- 事故又は違反に対する対処
- サイバーセキュリティに関する脅威情報を収集し、意思決定等に活用できるよう分析する。
- インターネットに接続されたシステムの既知の脆弱性（CVE 情報等）を、重要な資産から優先的にパッチ適用等により緩和する。パッチ適用が不可能もしくは、可用性や安全性を損なうおそれのある制御システムについては、ネットワークの分離や監視等の代替手段を使用し、当該システムがインターネットからアクセスできないようにする。
- 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。報告手段は電子メールや Web フォーム等が一般的である。報告を

受けた場合には、その重大性に応じて適切に対処する。

●人的安全管理措置(例)

情報セキュリティ責任者(CISO 等)は、取扱者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うこと。

- 雇用契約時及び委託契約時における NDA(機密保持契約)の締結
- 取扱者に対する内部規程等の周知・教育・訓練の実施
- 委託先との契約書等に、委託先の従業員に関する要求事項や委託終了後も遵守すべき事項を盛り込む。
- 委託先の取組状況を定期的に確認し、必要な改善を求める。
- 重要インフラサービスに係る業務の外部委託選定の際には、事業場の要求事項に加えて、アクセスされる情報の分類や認識されたリスク等を考慮する。自組織と委託先との業務委託契約書等には、委託先が自組織のセキュリティの要求を満たすセキュリティ対策に取り組む責任、従業員に対する意識向上の教育・訓練を実施する責任、委託終了後もなお有効なセキュリティに関する責任及び義務等について盛り込む。
- なお、継続的に取り組むリスクアセスメントの結果次第では、契約文言の見直しが必要な場合も想定されるため、セキュリティ部門や法務部門等による情報交換の場を定期的に設けることが期待される。
- 委託期間中においては、委託先に対するセキュリティに関する要求事項が確実に遂行されるよう、委託先の取組状況を定期的に確認し、必要な改善を求める。

●技術的安全管理措置(例)

情報セキュリティ責任者(CISO 等)は、個人データ及びそれを取り扱う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、個人データに対する技術的な安全管理措置を講ずること。

- 個人データへのアクセスにおける識別と認証
- 個人データへのアクセス制御
- 個人データへのアクセス権限の管理
- 個人データのアクセスの記録
- 個人データを取り扱う情報システムについての不正ソフトウェア対策
- 個人データの運搬・送信時の対策
- 個人データを取り扱う情報システムの動作確認時の対策
- 個人データを取り扱う情報システムの監視

●物理的安全管理措置(例)

情報セキュリティ責任者(CISO 等)は、入退館(室)の管理、個人データの盗難の防止等の措置を講ずること。

・ 入退館(室)管理の実施
・ 盗難等の防止
・ 機器・装置等の物理的な保護

●個人情報を委託する場合の対策(例)

情報セキュリティ責任者(CISO 等)は、適切な委託先管理を実施するために、個人データの安全管理、取扱い時の報告義務、責任の範囲、及び非開示義務について、委託契約時に明確にすべき内容を規定すること。

契約時に明確にする項目について、以下【具体例】の対策を講ずることが望ましい。

・ 個人データの安全管理に関する事項
  - ✓ 個人データの漏えい等の防止、盗用の禁止に関する事項
  - ✓ 委託契約範囲外の加工、利用の禁止
  - ✓ 委託契約範囲外の複写、複製の禁止
  - ✓ 委託期間
  - ✓ 委託終了後の個人データの返還・消去・破棄に関する事項
・ 個人データの取扱いの再委託を行うに当たっての委託元への報告とその方法
・ 個人データの取扱い状況に関する委託者への報告の内容及び頻度
・ 委託契約の内容、期間が遵守されていることの確認
・ 委託契約の内容、期間が遵守されなかった場合の措置
・ 個人データの漏えい等の事故が発生した場合の報告・連絡に関する事項
・ 個人データの漏えい等の事故が発生した場合における委託元と委託先の責任の範囲

●個人情報を委託する場合の委託先の監督(例)

システム構築・運用者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うこと。その際、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。

1.6 内部関係者による脅威への対策

1.6.1 事業者外での情報処理の制限

【事業者に求めること】

- 情報セキュリティ責任者(CISO 等)は、事業者外での情報処理や情報システム持ち出し時に、情報の格付けに基づいた安全管理措置を整備し、申請者審査の手続きを明確に規定することが求められる。

〔解説〕

業務の遂行のため、事業者外において情報処理を実施する必要が生ずる場合がある。この際、事業者外での実施では物理的な安全対策を講ずることが比較的困難になることから、取扱者は、事業者内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

情報セキュリティ責任者(CISO 等)は、事業者外での情報処理を行う場合、及び情報システムを事業者外に持ち出す場合の安全管理措置について、対象となる情報の格付けに従って、規定を整備すること。この際、申請者を審査するために必要な手続を明確に規定すること。

事業者外での情報処理及び情報システムを事業者外に持ち出す場合について、以下を規定することが望ましい。

〔具体例〕

●事業者外での情報処理と安全管理(例)

- 取扱者は、事業者外で情報処理を行う場合、及び情報システムを事業者外に持ち出す場合は、取扱う情報の格付けに従って、情報セキュリティ責任者(CISO 等)の許可を得ること。
- 取扱者は、事業者外で情報処理を行う場合は、取扱う情報の格付けに従って、必要な安全管理措置を講ずること。

1.6.2 事業者支給以外の情報システムによる情報処理の制限

【事業者に求めること】

- 事業者支給以外の情報システムを利用する場合、セキュリティ確保のため、適切な対策を講じる必要がある。

〔解説〕

業務においては、その遂行のため、事業者支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、重要インフラ事業者等が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できないため、適切な対策を講ずる必要がある。

〔具体例〕

●事業者支給以外の情報システムの安全管理(例)

- 情報セキュリティ責任者(CISO 等)は、事業者支給以外の情報システムにより情報処理を行う場

合に講ずる安全管理措置について、処理の対象となる情報の格付けに従い、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための必要な対策や利用時の措置を講ずること。
・ この際、申請者を審査するために必要な手続を明確に規定すること。

1.6.3 取扱者の管理

【事業者に求めること】

> ➢ 情報セキュリティ責任者(CISO 等)は、個人データの漏えい防止のため、組織的、人的、物理的、技術的措置を講じ、リスクに応じた適切な対策を実施すること。また、取扱者に対して監督・教育を行い、個人データ保護の意識向上を図ることが求められる。

〔解説〕

個人情報の漏えい事故の多くは取扱者などの内部関係者による、内部犯行となっていることから、内部関係者の個人情報保護に対する意識を高め情報漏えいを抑止するために、取扱者の適正な管理を行うことが必要である。

情報セキュリティ責任者(CISO 等)は、取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの保護のため、組織的、人的、物理的及び技術的安全管理措置を講ずること。その際、本人の個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況並びに個人データを記録した媒体の性質等に起因するリスクに応じ、必要かつ適切な措置を講ずること。

また、情報セキュリティ責任者(CISO 等)は、個人データの安全管理が図られるよう、取扱者に対し必要かつ適切な監督をしなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、個人データを取り扱う取扱者に対する教育及び研修等の内容及び頻度を充実させるなど、必要かつ適切な措置を講ずること。

取扱者のモニタリングを実施する際には、以下【具体例】のような対策を講ずることが望ましい。

〔具体例〕

●モニタリング実施に関する規程と管理(例)

・ モニタリングにおいて取得する個人情報の利用目的をあらかじめ特定し、事業者内規程に定めるとともに、取扱者に明示すること。
・ モニタリングの実施に関する責任者とその権限を定めること。
・ モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた事業者内規程案を策定するものとし、事前に事業者内に徹底すること。
・ モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

●雇用管理(例)

情報セキュリティ責任者(CISO 等)は、取扱者を雇用する場合、別紙 1【1.5 不正アクセスのため

の脅威への対策】に規定する各安全管理措置を取扱者に実施させることを契約条件とする等、以下【具体例】を例とする必要かつ適切な措置を講ずること。

- 雇用契約時における情報の守秘や非開示の契約の締結
- 退職後の個人情報保護規定の整備

1.7 個人情報漏えい発生時の対応策の整備

【事業者に求めること】

- 個人情報漏えい発生時には、状況検出後、被害拡大防止と回復対策を講じ、関係者に影響範囲を報告し、現場の混乱を最小限に抑えることが重要。

〔解説〕

個人情報の漏えいが発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた関係者へ報告し、重要インフラサービス障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

〔具体例〕

●個人データ漏えい発生時の対応(例)

情報セキュリティ責任者(CISO 等)は、個人データの漏えい等が発生した場合はまず、漏えい源の特定、漏えい継続の阻止、関係機関への周知、漏えいした情報の拡散阻止等の対策を取ること。その後、個人データ漏えいに至った経緯、原因等の解析を行い、再発防止策を検討し、対策を施すこと。

●本人への通知(例)

情報セキュリティ責任者(CISO 等)は、個人データの漏えい等が発生した場合に、事実関係を本人に速やかに通知するために必要な手続を規定すること。

●事実関係、再発防止策等の公表(例)

情報セキュリティ責任者(CISO 等)は、個人データの漏えい等が発生した場合に、二次被害の防止、類似事案の発生回避等の観点から、可能な限り影響範囲などの事実関係、再発防止策等を公表するために必要な手続を整備すること。

●個人情報保護委員会等への報告(例)

情報セキュリティ責任者(CISO 等)は、個人データの漏えい等が発生した場合に、事実関係を個人情報保護委員会に速やかに報告するために必要な手続(このために国土交通省への報告に必要な手続を含む。)を整備すること。

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）

～システム構築・運用者編～

令和７年３月28日

国土交通省港湾局

目次

はじめに
1　事前準備 1
1.1　災害による障害の発生しにくい設備の設置及び管理 1
1.2　装置の管理 2
1.3　リモートアクセス環境導入に関する対策基準の策定 3
2　平時対策 4
2.1　不正アクセス等の脅威への対策 4
2.1.1　利用者アクセスの管理 4
2.1.2　主体認証機能 6
2.1.3　権限管理機能 8
2.2　情報システム等のアクセス制御 9
2.2.1　アクセス制御機能 9
2.2.2　パスワード管理 11
2.3　暗号を活用した情報管理 12
2.4　負荷分散・冗長化 13
2.5　多層防御 15
2.6　資産のセキュリティ運用 16
2.6.1　情報システムの構成要素の運用 16
2.6.2　情報システムの監視 19
2.6.3　情報システムの更改・廃棄時の措置 20
2.6.4　データ管理 21
2.7　サイバー攻撃等に備えた運用管理 22
2.7.1　マルウェアからの保護 22
2.7.2　バックアップ 25
2.7.3　ログ取得 27
2.7.4　運用ソフトウェアの管理 29
2.7.5　脆弱性の管理 30
2.7.6　電子メール運用時の対策 32
3　インシデント発生時及び事後対応 33
3.1　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 33

別紙1　システムの取得・開発・保守に係るセキュリティ管理策 35
1.1 情報システムの取得・開発・改善における要求事項の確認 35
1.2 情報システムのセキュリティ要件 36
1.3 端末、サーバ装置、複合機及び特定用途機器 37
1.4 アプリケーション 42
1.5 通信回線及び通信回線装置 46

はじめに

〔システム構築・運用者編が想定する読者〕

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、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、その実践は経営者層としての責務である。

本ガイドラインの「システム構築・運用者編」では、主に重要インフラ事業者等において TOS 等システムの実装・運用管理を担う担当者を対象にしており、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（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。

重要インフラ事業者等におけるシステム構築・運用者においては、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「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。また、【具体例】で示している具体的な対策内容については、2024 年時点の対策技術動向をもとにした内容であり、数年で陳腐化するおそれもあるため、その実装にあたっては、最新の脅威動向・対策技術動向を踏まえた内容にアップデートしていくことが重要である。

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（【導入編 2. 3.3 第１版との関係】の表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・節を参照することが望ましい。

1　事前準備

1.1　災害による障害の発生しにくい設備の設置及び管理

【事業者に求めること】

- システム構築・運用者は、重要インフラサービス障害をもたらす原因となる様々な脅威からサーバ装置、端末及び通信回線装置を保護するための物理的な対策を検討することが望ましい。

〔解説〕

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

情報システムの設置環境については、システムが保有する情報の格付けに従って、自然災害、サイバー攻撃等、重要インフラサービス障害をもたらす原因となる様々な脅威からサーバ装置、端末及び通信回線装置を保護するための物理的な対策を検討することが望ましい。

〔具体例〕

●脅威に応じた物理的対策(例)

- 免震・耐震設備を有する施設、免震機能を有したサーバラック、人体・通信装置・環境に対する安全性を考慮した消火設備、無停電電源装置等の非常電源装置等の設置を検討すること
- 全ての外部扉及びアクセス可能な窓を防御し、侵入者の検知システムを設置すること
- 建物は目立たせず、その用途を示す表示は最小限とすること
- 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと
- 火災、洪水、地震等の自然災害や、爆発物、武器等による人的災害についてリスクアセスメントを実施し、災害対策や、ランダムな物品検査を実施すること

1.2　装置の管理

【事業者に求めること】

- システム構築・運用者は、機器・装置等の物理的な保護及び停電や落雷等、電源管理に関する対策を検討する。

〔解説〕

情報システムの装置の管理に関して、情報セキュリティ責任者(CISO 等)は、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う資産や情報システムのサイバーセキュリティを確保する。

また、システム構築・運用者は、社内の情報機器を安全に利用するために、不正侵入に対する防御だけでなく、機器・装置等の物理的な保護及び停電や落雷等、電源管理に関する対策も検討することが重要である。

〔具体例〕

●機器・装置等の物理的な保護(例)

- 重要インフラサービスの提供に係る装置(情報システム等)は、認可されていないアクセスの機会を低減できるように設置するとともに、可用性及び完全性を継続的に維持するため、適切に保守を実施する。
- 書類や取り外し可能な記録媒体について、セキュリティを保って保管し 、不要になった場合にはセキュリティを保った仕組みを使用してそれらを破棄する。記憶媒体を持ち出す場合には認可を要求し持ち出し管理を行う。
- 重要システムの通信・電源ケーブルについて、ケーブル保護のための外装電線管の導入や、点検・終端箇所は施錠可能な部屋又は箱の設置を検討する。
- ケーブル配線の物理的識別及び検査を可能にするため、ケーブルの各端に始点及び終点を示す詳細をラベル付けする。
- モバイル機器など、通信機能がある記憶媒体においては、紛失や盗難時の対策として位置追跡及び遠隔データ消去機能を実装する。

●電源管理(例)

- 傍受や損傷の可能性を考慮して通信・電源ケーブルを配線する。
- 重要システムの通信・電源ケーブルについて、ケーブル保護のための外装電線管の導入や、点検・終端箇所は施錠可能な部屋又は箱の設置を検討する。
- 重要システムが稼働する施設について、雷対策や定期的な計画停電のスケジュールを管理して対応する。
- 重要システムへ供給する電源系統を複数にすることや、無停電電源装置等を使用し可用性を考慮した対策を実施する。

1.3 リモートアクセス環境導入に関する対策基準の策定

【事業者に求めること】

- 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リモートアクセス環境導入に関する対策基準を定めること。

〔解説〕

リモートアクセス環境を利用する際、以下の脅威が想定される。

- ✓ リモートアクセス環境の不正利用
- ✓ 接続されたサーバ装置、端末、通信回線装置等への不正アクセス
- ✓ 送受信される情報の盗聴、改ざん、破壊等
- ✓ リモートアクセスに係るシステムおよび取り扱う情報のセキュリティの低下

これらのことを踏まえ、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る。

〔具体例〕

●リモートアクセス環境をテレワークに導入する場合の対策(例)

- テレワーク勤務者が所有する無線 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テレワーク勤務者に周知すること。
- テレワーク勤務者が無線 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テレワーク勤務者に周知すること。
- 組織の施設外から従業員が作業し、組織内の情報にアクセスする際に行われるテレワークにおいては、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。
  - ✓ テレワークサイトにおける、他者(家族、友人等)からの情報又は資源への認可されていないアクセスの脅威
  - ✓ 公共の場所にいる他者からの情報又は資源への認可されていないアクセスの脅威
  - ✓ 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項、制限事項
  - ✓ 個人所有機器(BYOD:Bring Your Own Device)の使用
  - ✓ ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用
  - ✓ システムを遠隔で制御し初期化するためのセキュリティに配慮した仕組み(リモートワイプ)の導入
  - ✓ テレワークが終了したときの、権限及びアクセス権の失効
  - ✓ 利用開始及び利用停止時の申請手続の整備
  - ✓ 通信内容の暗号化
  - ✓ 通信を行う端末及び利用者の識別又は認証
  - ✓ 主体認証ログの取得及び管理
  - ✓ リモートアクセス中の他の通信回線との接続禁止

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

【事業者に求めること】

- 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。

〔解説〕

情報セキュリティ責任者(CISO 等)は、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対策方針に記載する。

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。

なお、港湾における TOS 等の開発・保守等は、外部委託であるケースが多い。これらのような任務保証の上で必須となる業務においては、委託先に対するリスク管理をすることが望ましい。

システム構築・運用者は、情報セキュリティ責任者が示す対策方針を踏まえ、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〕

●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（特定の港）

※ ……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）

●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。

2.1.2 主体認証機能

【事業者に求めること】

- 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。

〔解説〕

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがあるため、情報システムが取り扱う情報の格付けに従った適切な主体認証を実施することが重要である。

制御システム等においては、システムの停止をしない運用を前提としているため、可用性確保の観点から主体認証への対応が現実的に困難な場合があるため、主体認証機能を実装しない場合には、利用場所の限定、利用者管理の徹底等の代替措置を講ずることが望ましい。

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こと。この際、認可されていないアクセスのおそれを最小限に抑えるため、採用する認証技術や識別コード・主体認証情報の安全管理措置について、適切に設計することが重要である。

情報セキュリティ責任者(CISO 等)は、取扱者が、識別コード及び主体認証情報の使用及び管理について、正しいセキュリティ慣行に従うように、自分自身の責任を認識させること。特にパスワードの使用及び取扱者が利用する端末装置のセキュリティに関して、その責任を十分に認識させること。

取扱者における識別コード・主体認証情報の管理対策としては、以下の具体例の対策を規定することが望ましい。

〔具体例〕

●外部との接続に係る主体認証機能

VPNルータ等のネットワーク機器については、外部ユーザの認証方式として、以下の措置を執ること。(【2.1.1利用者アクセスの管理】参照)

- ✓ 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(特定の港)

●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主体認証機能

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、管理者の認証方式として、以下の措置

を執ること。(【2.1.1利用者アクセスの管理】参照)

- ✓ 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)

●主体認証方式(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

●取扱者の責任(例)

- 取扱者は、自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと
- 取扱者は、自己に付与された識別コードを他者に付与及び貸与しないこと
- 取扱者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと
- 取扱者は、業務のために識別コードを利用する必要がなくなった場合は、システム構築・運用者に届け出ること
- 取扱者は、主体認証情報としてパスワードを設定する場合、以下の要素を考慮して、セキュリティ上の強度が高くなるようパスワードを設定すること
  - ✓ パスワードに用いる文字の種類とその組み合わせ
  - ✓ パスワードの桁数
  - ✓ パスワードの有効期間
- 取扱者は、主体認証情報が他者に使用され又はその危険が発生した場合には、直ちにシステム構築・運用者にその旨を報告すること

2.1.3 権限管理機能

【事業者に求めること】

- システム構築・運用者は、全ての情報システムについて、権限管理を行う必要性の有無を検討し、権限管理を行う機能を設ける。

〔解説〕

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになるため、権限管理を行うことが望ましい。

〔具体例〕

●権限管理機能(例)

- 制御システム等において、可用性確保の観点から主体認証が実装されていない場合は、専用端末を設けるなどにより、利用場所の限定、取扱者管理の徹底等の代替措置を取ること。
- システム構築・運用者は、全ての情報システムについて、権限管理を行う必要性の有無を検討し、権限管理を行う機能を設けること。この際、取扱者への識別コード及び主体認証情報の付与に関する手続を明確に定めること。
- 権限管理について、以下の事項を含む手続を明確にすることが望ましい。
  - ✓ 主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続
  - ✓ 主体認証情報の初期配布方法及び変更管理手続
  - ✓ アクセス制御情報の設定方法及び変更管理手続

2.2　情報システム等のアクセス制御

2.2.1 アクセス制御機能

【事業者に求めること】

- 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。
- TOS 等システムと外部システムとが専用線により接続されている場合であっても、ファイアウォール設置等の措置を講じることが望ましい。

〔解説〕

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、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ごとにアクセス制御する必要がある。

なお、制御システム等においては、可用性確保の観点から主体認証が実装されていない場合は、専用端末を設けるなどにより、利用場所の限定、利用者管理の徹底等の代替措置を取る必要がある。

システム構築・運用者は、情報セキュリティ責任者（CISO 等）が示す対策方針を踏まえ、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ある。また、取扱者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすることが望ましい。

〔具体例〕

●外部との接続に係るアクセス制御対策

VPNルータ等のネットワーク機器については、アクセス制御対策として、以下の措置を執ること。（【2.1.1 利用者アクセスの管理】参照）

- ✓ 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）

●専用線、NATで外部と接続する場合のアクセス制御対策

TOS 等は一部の外部システムとは専用線により接続されている。また、港湾運送事業者から TOS 等に接続する際に NAT（＊注）を使用する例も存在する。これらは比較的安全な接続方法ではあるが、そうであっても万が一の事態に備えファイアウォールを設置する等の措置を執ることが望ましい。

＊注：NAT とは、Network Address Translation（ネットワークアドレス変換）の頭文字を取った略語で、グローバル IP アドレスからプライベート IP アドレスを紐付けて変換する技術。

●情報システム等のアクセス制御の導入（例）

＜アクセス制御機能の導入＞

- 利用時間や利用時間帯によるアクセス制御
- 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
- 主体認証を受けたユーザのみが与えられた権限の範囲でアクセス可能となる制御
- 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。
- 運用上明示的に必要な場合を除き、制御システムはインターネット上には配置しない。例外が存在する場合には承認、文書化し、悪用を防止する措置を具備する。悪用防止の措置として、多要素認証や VPN の活用、ロギングによる動作の監視等が挙げられる。また、OT ネットワークへの接続は、特定の機能のため明示的に許可された通信を除き、全て拒否する。IT と OT 間の必要な通信経路にはファイアウォール等中継装置を設置し、厳密に通信を監視する。中継となるファイアウォール装置の設定、脆弱性についても適切に維持管理する。
- インターネットに接続された情報システムについて、サービス不能攻撃（DoS/DDoS 攻撃）を受けるサーバ装置（IoT 機器を含む。）、端末、通信回線装置又は通信回線から監視対象を特定し、システムが扱う情報の可用性に基づいてサービス不能攻撃の発生を想定し、対応を行う。

＜アカウントロック＞

- 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。

2.2.2 パスワード管理

【事業者に求めること】

- システム構築・運用者は、パスワード攻撃に対応した、適切なパスワード管理の対策を講ずる。

〔解説〕

パスワードリスト攻撃とは、攻撃者が何らかの方法で事前に入手した ID とパスワードのリストを使用し、ログイン機能を持つインターネットサービスに不正にログインを試みる攻撃手法である。もし重要インフラ利用者が ID とパスワードを他のインターネットサービス等で使い回していると、第三者によるなりすましログインを可能にしてしまい、顧客情報の不正操作や情報流出のリスクがある。

港湾分野では、顧客向けのインターネットサービスを提供している重要インフラ事業者等が想定されるため、パスワードリスト攻撃への対策が必要である。

〔具体例〕

●パスワード管理(例)

- ハードウェア、ソフトウェア等を使用する前に、製造元のデフォルトパスワードを変更する。制御システムについても、新規又は将来の全てのデバイスのデフォルト認証情報を変更する方針とする。これは、実現が容易なだけでなく、将来的にサイバー攻撃手法が変化した場合の潜在的なリスクも軽減される。ハードコードされている等、デフォルトパスワードの変更が不可能な場合、代替セキュリティ管理策を実施し、ログインのアクセスログを監視する。
- 自組織の情報資産に対して、パスワードの用途ごとに最小パスワード長及び複雑さを設定する。パスワードの用途は、「ログインパスワード」「パスワードロックされた圧縮ファイルや文書ファイル」「無線アクセスポイントへの接続」等がある。アカウントロックや多要素認証等、他の管理策との組み合わせを考慮して、パスワード長及び複雑さを設定する。
- 自組織のサービスや資産に関して、一意かつ個別のパスワードを設定する。利用者に対し、アカウント、アプリケーション、サービス等でパスワードを再利用させないようにする。
- 多要素認証機能(認証コード、ワンタイムパスワード等)の実装
- ハードウェアベースの多要素認証技術が利用可能な場合は有効にする。利用できない場合にはソフトウェアベースを利用する。SMS による多要素認証は、他の選択肢が可能な場合を除きできるだけ避けるようにする。
- アカウントロック機能の実装
- 不正ログイン試行を検知する機能(通常とは異なる IP アドレスからのアクセス時にメールで通知等)の実装
- ログイン履歴表示機能の実装
- システム構築・運用者は、重要インフラ利用者に ID・パスワードの使い回しをしないなどの注意喚起を行うこと。
- システム構築・運用者は、認証ログを監視し、不正ログイン試行を検知した場合、当該 IP アドレスからの通信を遮断する等の対応を検討すること。
- システム構築・運用者は、長期間利用されていないアカウントについて、停止・削除する等の対応を検討すること。

2.3 暗号を活用した情報管理

【事業者に求めること】

- システム構築・運用者は、情報システムにおいては、暗号化機能及び電子署名の付与機能等を適切に実装する。
- 制御システム等においては、暗号化機能を導入していない場合は、ログや通信の監視等の代替措置を講ずることが望ましい。

〔解説〕

情報システムの利用においては、情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装すること。

制御システム等においては、可用性確保の観点から暗号化への対応ができない場合があるため、暗号化機能を導入していない場合は、ログや通信の監視等の代替措置を講ずることが望ましい。

〔具体例〕

●暗号化機能及び電子署名の付与機能の導入(例)

- システム構築・運用者は、情報システムについて、システムが保有する情報の格付けに従って、暗号化機能(機密性の保護)、及び電子署名の付与機能(電子文書の完全性の保護)の必要性の有無を検討し、必要な機能を導入すること。
- 暗号化又は電子署名の付与に用いるアルゴリズムを選択するに当たっては、その暗号強度、利用条件、効率性等について多角的な検討を行うこと。

●暗号化及び電子署名の付与に係る管理(鍵管理も含む)(例)

- 暗号の利用方針や暗号鍵の管理方針を策定する。システム構築・運用者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存方法の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めること。
- 転送中のデータを保護するために、適切な TLS 暗号化を導入する。非推奨や、脆弱な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行うこと。
- 取扱者は、情報を運搬・送信する場合又は電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
- 取扱者は、情報を運搬・送信する場合又は電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。
- 取扱者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、これを他者に知られないように自己管理すること。
- 取扱者は、暗号化された情報の復号に用いる鍵について、機密性、完全性、可用性の観点から、バックアップの必要性の有無を検討し、必要があると認めたときは、そのバックアップを取得し、オリジナルの鍵と同等の安全管理をすること。

2.4 負荷分散・冗長化

【事業者に求めること】

- システム構築・運用者は、システムの負荷分散や冗長化について検討を行い、必要があると認められる場合は、二重化を図るなど適切に処置を行う。
- TOS 等がサイバー攻撃を受けた際の事業継続にあたっては、必要に応じて、バックアップシステムを用意する。

〔解説〕

重要システムの停止・低下は、国民生活や社会経済活動に重大な影響を及ぼすことから、障害や過度のアクセス等によりサービスが提供できない事態となることを防がなければならない。障害や過度のアクセス等、将来の見通しも考慮し、サービス提供に必要なサーバ装置等を冗長構成にするなどにより可用性を確保する必要がある。

システム構築・運用者は、トラフィックの集中や一部の装置の不具合によるシステム機能停止を予防するため、システムの負荷分散や冗長化について検討を行い、必要があると認められる場合は、二重化を図るなど適切に処置を行うことが重要である。

システム構築・運用者は、情報システムについて、システムが保有する情報の格付けに従って、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

サーバ装置、端末及び通信回線装置について、以下【具体例】を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処することが望ましい。

〔具体例〕

●バックアップシステム

TOS 等がサイバー攻撃を受けた際の事業継続にあたり、必要に応じてバックアップシステム(予備系統)を用意しておくこと。

●負荷分散・冗長化の対策(例)

- パケットフィルタリング[1]
- 3-way handshake[2] 時のタイムアウトの短縮
- Syn Flood、UDP Flood 等の各種 DoS/DDoS 攻撃[3]への防御
- WAF(Web Application Firewall)[4]の導入

---

[1] パケットフィルタリング：フィルタリングの一種であり、ネットワークを行き交うパケットをポリシーに応じて制御する事
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/glossary/06.html

[2] 3-way handshake：TCP（Transmission Control Protocol：インターネットで使用されているプロトコルの一つであり、相手と接続を確立してから通信を行う） などにおいて使用されている、接続（コネクション）を確立するための手順。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/glossary/11.html#t

[3] Dos/DDos 攻撃：分散サービス拒否攻撃。Web サーバやメールサーバなどに対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能する攻撃手法。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/glossary/11.html#t

[4] WAF：Web アプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことで、従来のファイアウォールがネットワークレベルでの管理であるのに対し、WAF は Web アプリケーションのレベルで管理ができる。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/download/kokumin-security_admin.pdf

・ CDN(Contents Delivery Network)[5]サービスの使用

[5] CDN：多数のユーザからの大量のアクセスを処理するための仕組み。キャッシュサーバを活用し、ユーザからのアクセスを分散させることができる。
https://www.soumu.go.jp/main_content/000702974.pdf

その他 DoS/DDoS 攻撃の対策についてはサイバー警察局（https://www.npa.go.jp/bureau/cyber/index.html）及び NISC（https://www.nisc.go.jp/）の注意喚起を参照されたい。

2.5　多層防御

【事業者に求めること】

- 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、システム又はサービスには、多層防御を導入することが望ましい。

〔解説〕

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策(入口対策)、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策)からなる、多重防御のセキュリティ対策体系によって、標的型攻撃に備える必要がある。

サイバー攻撃の高度化により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もと、セキュリティ対策を検討することが重要である。

システム構築・運用者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下【具体例】を例とする対策(入口対策)を講ずること。

システム構築・運用者は、サーバ装置及び端末について、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策)を講ずることが望ましい。

〔具体例〕

●入口対策(例)

- 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(例)

- 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(Endpoint Detection and Response)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。

2.6　資産のセキュリティ運用

2.6.1 情報システムの構成要素の運用

【事業者に求めること】

- システム構築・運用者は、端末、サーバ装置、通信回線・通信回線装置、複合機及び IoT 機器を含む特定用途機器のような情報システムの構成要素の運用においては、個別のセキュリティ対策を実施する。

〔解説〕

端末、サーバ装置、通信回線・通信回線装置、複合機及び IoT 機器を含む特定用途機器のような情報システムの構成要素は、それぞれ保持する情報や使われ方等性質が異なる。そのため、運用においては構成要素個別のセキュリティ対策を実施する事が重要である。

〔具体例〕

●端末の運用時・運用終了時の対策(例)

＜システム構築・運用者による対策＞

- 利用可能なソフトウェアについて定期的に見直しを行うこと。
- 主管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。
- 端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

＜端末を利用する取扱者による対策＞

- 業務の遂行以外の目的で情報システムを利用しないこと。
- システム構築・運用者が接続許可を与えた通信回線以外に端末を接続しないこと。
- 事業者内通信回線に、システム構築・運用者の接続許可を受けていない端末を接続しないこと。
- 端末で利用を禁止するソフトウェアを利用しないこと。また、端末で利用を認めるソフトウェア以外のソフトウェアを業務上の必要により利用する場合は、システム構築・運用者の承認を得ること。
- 端末の設置場所から離れ、第三者による不正操作のおそれがある場合は、端末を不正操作から保護するための措置を講ずること。
- 端末を事業者外に持ち出す場合には、システム構築・運用者の許可を得ること。
- 端末の紛失、盗難がないよう適切に管理すること。
- IC カードやパスワード等、端末の認証情報の漏洩や紛失がないよう適切に管理すること。
- 第三者からののぞき見(ショルダーハッキング)や大声でのオンライン会議による情報漏えい、端末等の盗難等が起きない環境で利用すること。
- 端末に接続される機器やソフトウェア等について、最新のアップデートやパッチ適用を定期的に行うこと。
- 端末(特にスマートフォンやタブレット)に対して許可されていない設定の変更をしないこと。

●サーバ装置の運用時・運用終了時の対策(例)

<システム構築・運用者による対策>

- サーバ装置について、構成管理・変更管理を実施すること。また、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。
- 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)とすること。その際、認証コードの安全な配布と運用手順を定めること。
- サーバ装置に保存されている情報について、情報の格付けに従って、定期的にバックアップを取得すること。また、取得した情報を記録した媒体について、安全管理措置を講ずること。
- サーバ機器のログを定期的に取得するとともに、システム外にバックアップを保存すること。
- サーバ機器に対して基幹 OS の付属品以外のセキュリティ対策ソフトを導入し、ウイルスパターンを常時最新のものにすること。
- サーバ装置のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、定期的に更新を行うとともに、不正行為及び不正利用を含むトラブル事象の発生を検知するための措置を講ずること。
- サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

●通信回線及び通信回線装置の運用時・運用終了時の対策(例)

<システム構築・運用者による対策>

- 通信回線及び回線装置について、構成管理・変更管理を実施すること。
- 通信回線及び回線装置の運用管理について、作業日、作業を行った通信回線・回線装置、作業内容及び作業者を含む事項を記録すること。
- 経路制御及びアクセス制御を適切に運用し、定期的に経路制御及びアクセス制御の設定の見直しを行うこと。また、通信回線や通信要件の変更時にも見直しを実施すること。
- 通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。
- 日常的に、通信回線の通信内容、通信回線及び回線装置のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、通信回線の性能低下、不正行為及び不正利用を含むトラブル事象の発生を推測又は検知するための措置を講ずること。
- 通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体の全ての情報を復元できない状態にすること。

●複合機及び IoT 機器を含む特定用途機器の運用時・運用終了時の対策(例)

<システム構築・運用者による対策>

- 複合機及び IoT 機器を含む特定用途機器等の管理責任が曖昧とならないよう、資産管理者を明確にすること。
- 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視すること。
- 複合機及び特定用途機器について、構成管理・変更管理を実施すること。
- 複合機及び特定用途機器の運用管理について、作業日、作業を行った複合機及び特定用途機器、作業内容及び作業者を含む事項を記録すること。
- 複合機及び特定用途機器が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされている等、不適切な状態にある複合機及び特定用途機器を認識した場合には、改善を図ること。
- 複合機及び特定用途機器のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、不正行為及び不正利用を含むトラブル事象の発生を検知するための措置を講ずること。
- 内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機及び特定用途機器は、当該機能を活用することにより複合機及び特定用途機器内部の情報を抹消すること。当該機能を備えていない複合機及び特定用途機器については、外部委託先との契約時に外部委託先に複合機及び特定用途機器内部に保存されている情報の漏えいが生じないための対策を講じさせる旨を、契約内容に含む等の別の手段で対策を講ずること。
- 特定用途機器のセキュリティ上重要なアップデートを、必要なタイミングで適切に実施する方法を検討し、適用すること。
- 複合機及び特定用途機器内部の脆弱性等のセキュリティ関連情報を収集・分析し、取扱者に対して以下の項目を例とする周知・啓発を行うことが望ましい。
    - ✓ 複合機及び特定用途機器の脆弱性等のセキュリティ関連情報
    - ✓ 複合機及び特定用途機器に対して、セキュリティに留意した設定（パスワード設定、ファームウェア更新、サポート期限確認等）を行うこと
- 複合機及び特定用途機器の不適切な使用方法等により、自身だけでなく、他人への被害や環境への悪影響を与えるリスクがあること。

2.6.2 情報システムの監視

【事業者に求めること】

- システム構築・運用者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に発見・追跡できるように、平時より情報システムの監視を行う。

〔解説〕

不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に発見・追跡できるように、平時より情報システムの監視を行うことが重要である。

〔具体例〕

●情報システムの監視(例)

- システム構築・運用者は、情報システムの運用・保守に際しては、情報システムに実装されたセキュリティ機能を適切に運用すること。
- システム構築・運用者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。
- システム構築・運用者は、情報システムのセキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

2.6.3 情報システムの更改・廃棄時の措置

【事業者に求めること】

・ システム構築・運用者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、移行作業におけるセキュリティ対策及び不要な情報の抹消を適切に実施する。

〔解説〕

システム構築・運用者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、移行作業におけるセキュリティ対策及び不要な情報の抹消を適切に実施すること。

〔具体例

●情報システムの更改・廃棄時の措置(例)[6]〕

・ データ消去用のソフトウェアを利用する
・ 専門業者のデータ消去サービスを利用する
・ ハードディスクや記憶媒体を物理的に破壊する
・ 「暗号化消去」を行う

[6] [6] 総務省「廃棄するパソコンやメディアからの情報漏洩」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_18.html

2.6.4データ管理

【事業者に求めること】

- システム構築・運用者は、システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う。

〔解説〕

システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うこと。

事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど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ある。(【セキュリティ責任者編1.6クラウドサービス】参照)

2.7　サイバー攻撃等に備えた運用管理

2.7.1 マルウェアからの保護

【事業者に求めること】

- 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。

〔解説〕

マルウェアは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の秘密情報や業務上の機密情報を漏えいさせることから機密性に対する脅威ともなる。さらに、マルウェアに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、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など他者に対するセキュリティ脅威の原因となり得る。よって、マルウェア対策を行うことが重要である。

なお、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ことが重要である。

〔具体例〕

●外部接続するネットワーク機器に係るマルウェア対策

TOS がサイバー攻撃を受けた際のシステムへの侵入口となり得るのは、外部との接続部分である。VPNルータ等のネットワーク機器は、港湾運送事業者や TOS のシステム保守会社及びシステム開発会社が外部(自社や自宅等)から TOS に接続する際に利用するものである。

VPN ルータ等のネットワーク機器の脆弱性がサイバー攻撃の対象となり得ることから、ネットワーク機器について以下の措置を執ること。

- ✓ ネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。
- ✓ ネットワーク機器の通信記録等のログを定期的に取得するとともに、システム外にバックアップを保存する。
- ✓ サイバー攻撃を受けた場合、ネットワーク機器が踏み台となっている恐れがあることから、新品と交換する。

※　　は、港湾運送事業法では強制要件(全ての港)

●TOS 等ネットワーク内のサーバ機器等に係るマルウェア対策

TOS がサイバー攻撃を受けた際のシステムへの影響を最小化するため、サーバ機器及びシステム内のネットワーク機器の対策を以下に示す。

- ✓ サーバ機器に対して基幹 OS の付属品以外のセキュリティ対策ソフトを導入し、ウイルス

パターンを常時最新のものに更新する。

- ✓ サーバ機器及びネットワーク機器のログを定期的に取得するとともに、システム外にバックアップを保存する。
- ✓ サーバ機器及びネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。

※ 　は、港湾運送事業法では強制要件(全ての港)

●外部記憶媒体(USB 等)に係るマルウェア対策

荷役を行う船舶と TOS の間でコンテナの情報を共有する際等に USB メモリを使用する例が見受けられる。

情報セキュリティの観点からは、USB メモリ等の外部記憶媒体の利用はできる限り控えることが望ましいが、止むを得ず利用する場合には、事前に TOS とは切り離された端末によりウイルスチェックを確実に行い、異常がないことを確認してから使用すること。

※ ___は、港湾運送事業法では強制要件(特定の港)

●マルウェア対策(例)

<システム構築・運用者による対策>

- マルウェアに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、取扱者にその対処の実施に関する指示を行うこと。
- サーバ装置、端末及び想定されるマルウェアの感染経路の全てにおいてマルウェア対策ソフトウェア等を導入すること。
- マクロ等の埋め込みコードの実行を全ての機器において既定で無効とする。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化で実行できることを承認する仕組みを構築すること。
- ファイアウォール装置等による悪性サイトへの遮断(コンテンツフィルタ)の仕組みを構築すること。
- なりすましメールの添付ファイルによる感染被害防止として、メール運用の対策の実施すること。(電子メール運用時の対策【2.7.6 電子メール運用時の対策】参照)
- 被害が発生した際の、攻撃の拡散に備えた対策として、ネットワークセグメント分割(重要インフラの分離)、IPS/プロキシサーバ(不審な外部通信の遮断)、EDR(影響範囲の特定と被害端末の隔離)等を導入すること。
- 速やかなパッチ適用等による脆弱性対策を講ずること。
- 海外拠点、サプライチェーンを含めて資産管理をすること。
- システムソフトウェア及びデータのバックアップを行い、バックアップから復旧可能なことを定期的に確認すること。
- バックアップデータをネットワークから隔離し保存すること。
- 役割等に基づいてネットワークを分割すること。
- 攻撃を受けた後に調査できるようにログなどを保存すること。

- ベンダーなどの関係者と協力関係を構築すること。
- 攻撃を受けた際は国土交通省や警察に連絡し、逐次時系列で状況を保存すること。
- ランサムウェア攻撃により金銭の要求をされた際には、以降の攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むことが望ましいこと。

2.7.2 バックアップ

【事業者に求めること】

- 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。

〔解説〕

緊急事態発生時でも、重要な情報の参照及び、情報システムを使用できることが求められる。しかし、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ある。

システム構築・運用者は、必要な情報のバックアップを取得し、バックアップ元とバックアップ先が同時に被災しない場所に保存する。特に重要な業務を支える情報システムについては、バックアップ方式やバックアップの取得頻度を設計したバックアップ計画を整備することが重要である。

情報システムのバックアップについては、システム障害や災害だけでなく、サイバー攻撃による被害（バックアップ元とバックアップ先が同時に被害に遭う等）も想定しバックアップ方式を検討すること。具体的には以下を考慮することが望ましい。

〔具体例〕

●バックアップ

TOS 等がサイバー攻撃を受けた際の事業継続や、早期復旧や原因究明のため、以下の点に留意して TOS 等のバックアップを取ること。

- ✓ バックアップを取るべき主な対象として、システムプログラム（開発環境、評価環境を含む）、コンテナ情報等の動的データ、システムログ等が挙げられる。
- ✓ 最後にバックアップを取得した時間から情報セキュリティ事案発生時までの更新情報が失われる可能性を考慮し、バックアップ対象ごとにバックアップの取得頻度を設定すること。
- ✓ コンピュータウイルスの潜伏期間を考慮し、バックアップは直近のもののみではなく、数週間前のものを含めて複数保存しておくこと。
- ✓ バックアップは現用のシステムとは切り離した場所に保存すること。

※ ＿＿は、港湾運送事業法では強制要件として、適切なバックアップ対象の設定、及び適切な頻度でのバックアップの取得が必要（全ての港）

※ ＿＿は、港湾運送事業法では強制要件（全ての港）

●バックアップ方式の検討（例）

- バックアップの対象（システムプログラム（開発環境、評価環境を含む）、コンテナ情報などの動的データ、システムログ等）
- 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電磁的記録媒体等の種類
- 遠隔地の文書・電子データ保存サービスの活用

- 対象ごとにバックアップの頻度、世代管理の方法(コンピュータウイルスの潜伏期間を考慮し、バックアップは直近のもののみではなく、数週間前のものを含めて複数保存すること)
- 使用するバックアップツール
- バックアップデータの秘匿性確保、改ざん防止の方法
- バックアップ先の分散化(ランサムウェア感染対応、オンライン、オフラインを含めた複数の事象を想定し、現用システムとは切り離した場所にも保存すること)
- システムイメージやデータ等に対するバックアップの方針及び手順を整備し、定期的なバックアップリカバリー検査を実施
- 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する。
- 制御システムについては、設定、役割、PLC ロジック、設計図面、ツールについてもバックアップする。
- バックアップからの復旧テストや定期的な訓練(年 1 回程度)を実施する。

●バックアップ取得管理状況の把握(例)

- バックアップ計画において、重要なデータの管理状況を把握することが必要である。管理対策をまだ定めていない場合は、以下の表を参照し、自組織で必要とする管理方法で管理を行う方法もある。

①	②	③	④	⑤	⑥	⑦	⑨	⑩
システム名	**対象データ**	**サイクル（日次、週次、月次、随時、ミラーリング）**	**世代**	**媒体**	**方式（フル、差分）**	**容量**	**方法（データ、イメージ、ファイル）**	**バックアップの保管場所（遠隔地、同一区画、別区画）**
TOS	入出庫、在庫、ロケーション管理	日次	7	LTO（磁気テープ）	フル	1.6TB	ファイル	遠隔地（住所）
防護柵	侵入検出記録	日次	7	LTO（磁気テープ）	フル	1.6TB	ファイル	遠隔地（住所）
その他システム								

- クラウド(SaaS など)を利用する場合は、バックアップの有無をサービス提供事業者に確認する。

＜バックアップの保持期間・世代管理の考え方について＞

- バックアップを取得する目的はリストア(復旧)であるが、どの時点のデータまでリストアできればよいかはシステムの環境により異なるため、サービス再開が可能かどうかの観点で、バックアップの保持期間・世代管理を検討する。過去のデータが不要なシステムな場合は、システムプログラムの復旧を目的とした導入当時のシステムバックアップを取得するのみでよい場合も考えられる。バックアップの取得頻度については、リストア後のデータを整合させるための作業コストと、バックアップするデータサイズを考慮して決定する。

2.7.3 ログ取得

【事業者に求めること】

- システム構築・運用者は、情報システムの正常性の確認及び不正アクセス等の検知を行うことを目的として、必要に応じてログを取得する。
- 外部接続するネットワーク機器の通信記録、TOS 等システム内のサーバ機器等のログを定期的に取得し、システム外にバックアップを保存する。

〔解説〕

情報システムにおけるログは、システムの動作履歴、取扱者のアクセス履歴、その他必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の重要インフラサービス障害(その予兆を含む。)を検知するための重要な情報である。また、情報システムに係るサイバーセキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な情報となる。したがって、情報システムにおいては、仕様通りにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されていることが重要である。

システム構築・運用者は、取得したログを定期的に又は適宜点検及び分析し、その結果に応じて必要なセキュリティ管理策を講じなくてはならない。

〔具体例〕

●TOS 等ネットワーク内のサーバ機器、ネットワーク機器のログの取得

TOS 等システム内のサーバ機器及びネットワーク機器のログを定期的に取得するとともに、システム外にバックアップを保存する。

※ 　は、港湾運送事業法では強制要件(全ての港)

●ログの取得・管理の対策(例)

＜システム構築・運用者の対策＞

- 全ての情報システムについて、情報システムの正常性の確認及び不正アクセス等の検知を行うことを目的として、必要に応じてログを取得すること。
- イベントをログとして記録するにあたり、イベントごとに必要な情報項目を記録するように、情報システムの設計・設定をすること。
- アクセス及びセキュリティ関連のログを、検知及びインシデント対応で使用するために収集し、保存すること。イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知すること。
- ログ機能が非搭載の制御システムについては、制御システムとの間の通信ログを収集すること。
- ログが悪意を持った人物やマルウェア等によって故意に改ざん、消去されないよう管理すること。例えば、ログの性質に応じた定期的な検査によって、ログに対する不正行為の有無を確認すること。
- 収集したログはツールや中央システム(SIEM 等)に一元的に保存され、許可された管理者のみがアクセスできるようにすること。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定すること。

●ログとして記録することが望ましい項目(例)

- イベントの主体である人又は機器を示す識別コード
- 識別コードの発行等の管理記録
- 情報システムの操作記録
- イベントの種類(ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等)
- イベントの対象(アクセスした URL、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等)
- 日付、時刻
- 成功、失敗の区別、イベントの結果
- 電子メールのヘッダ情報、通信内容
- 通信パケットの内容
- 操作員、監視要員及び保守要員等への通知の内容

2.7.4 運用ソフトウェアの管理

【事業者に求めること】

- システム構築・運用者は、情報システム、制御システムの設定や、利用するソフトウェア(クラウドサービス含む。)の個々の設定について可能な限り把握・理解し、安全性の確保に努める。
- 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上で利用しているソフトウェアの情報を定期的に確認し、必要に応じ更新する。

〔解説〕

システム構築・運用者は、情報システムで利用するソフトウェアについて、安全性の確保に努めることが重要であり、ソフトウェアのサポート対象バージョンへの更新を計画的に実施することが重要である。安全に関する要求事項を優先する等の理由により、セキュリティ要求事項を完全には満たしていない場合において、採用するセキュリティ管理策を文書化し、正式に承認を得ることが望ましい。

システム構築・運用者は、情報システム、制御システムの設定や、利用するソフトウェア(クラウドサービス含む。)の個々の設定について可能な限り把握・理解し、安全性の確保に努めることが重要である。

〔具体例〕

●外部接続するネットワーク機器に係る運用ソフトウェアの管理

VPN ルータ等のネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。(【2.7.1 マルウェアからの保護】参照)

※ は、港湾運送事業法では強制要件(全ての港)

●TOS 等ネットワーク内のサーバ機器等に係る運用ソフトウェアの管理

サーバ機器及びネットワーク機器上で利用しているソフトウェアの情報を定期的に確認し、確実に更新する。(【2.7.1 マルウェアからの保護】参照)

●運用ソフトウェアの管理(例)

- ソフトウェアのサポート対象バージョンへの更新を計画的に実施すること。サポート対象バージョンへの更新が困難な場合には、ソフトウェアを利用する情報システムに対する通信監視や、アクセス制御等、補完的な措置を講じること。
- 重要インフラサービスに係る運用ソフトウェアを、セキュリティを保って管理するための手順及び対策を実施すること。
- 運用ソフトウェアの更新は、管理層の認可に基づき適切に実施すること。また、「十分に試験を行ってから導入する」、「開発用コードは使用しない」、「ロールバック計画を作成する」「監査ログを維持する」等の準備を含め、計画的に実行すること。

2.7.5 脆弱性の管理

【事業者に求めること】

- システム構築・運用者は、サーバ装置、端末及び通信回線装置上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認する。
- 制御システムにおいては、ソフトウェアの更新や脆弱性スキャンが難しい側面があり、可用性が担保できないと判断される場合には、制御システムに関する通信を監視する等の代替策を検討し、脆弱性対策を実施する。

〔解説〕

ソフトウェアに関する脆弱性は、その脆弱性を攻撃者に悪用されることにより、サーバ装置への不正侵入、DoS/DDoS 攻撃、マルウェア感染等の脅威の発生原因になるなど、情報システム全体のセキュリティの大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、重要インフラ事業者等の社会的な信用が失われるおそれがある。これらのリスクを回避するため、ソフトウェアに関する脆弱性への対応は迅速かつ適切に行う必要がある。

システム構築・運用者は、サーバ装置、端末及び通信回線装置上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、脆弱性対策の状況を定期的に確認することが重要である。

制御システムにおいては、システムの可用性等の観点からソフトウェアの更新や脆弱性スキャンが難しい側面がある。可用性が担保できないと判断される場合には、制御システムに関する通信を監視する等の代替策を検討し、脆弱性対策を実施する。また、制御システムは動作するプロセスが限定的であることが多いため、ホワイトリストによる動作プロセス制限といった対策も有効である。

〔具体例〕

●脆弱性の管理(例)

＜システム運用・構築者の対策＞

- 運用する情報システムのソフトウェア及びその他の技術に関して、関連する技術的脆弱性を特定し、組織の情報資産とあわせて整理すること。
- 情報システム上で利用するソフトウェアに関連する脆弱性情報の収集に努め、当該情報から情報システムのリスクを分析した上で、脆弱性ごとに対策計画を作成し、適切な対策を講ずること。
- ソフトウェアに関する脆弱性対策計画の作成に当たり、以下について判断することが望ましい。
  - ✓ 対策の必要性
  - ✓ 対策方法
  - ✓ 対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法
  - ✓ 対策方法又は回避方法が情報システムに与える影響
  - ✓ 対策の実施予定
  - ✓ 対策テストの必要性
  - ✓ 対策テストの方法
  - ✓ 対策テストの実施予定

- 定期的な脆弱性スキャンを実施すること。
- 外部から取得した情報システムの場合には、供給者に脆弱性の報告や取扱い及び開示を実施することを要求すること。
- 特定した脆弱性に対しリスクアセスメントを実施し、対応方針を検討すること。
- 情報システムへのパッチ適用に関する作業方針・内容を確立すること。パッチ適用が困難な場合には、情報システムに対する監視を強化するなどの補完的な措置を講じること。
- ソフトウェアの更新やパッチ適用等により修復をする際には、「正当な供給元からのパッチである」、「修復の真正性を検証する仕組みを実装する」、「ロールバックの手順を定める」等、適切な対策を実施すること。
- 適用可能な更新、パッチ等がない又はその他の理由により修復が困難な場合には、次のような管理策を検討すること。
    - ✓ 提供元が提案する回避策の適用
    - ✓ その脆弱性に関係するサービス又は機能の停止
    - ✓ ネットワーク境界におけるアクセス制御
    - ✓ 適切なトラフィックフィルタ（仮想パッチ）の適用による攻撃からの保護
- 実際の攻撃を検知するために、監視を強化すること。

2.7.6 電子メール運用時の対策

【事業者に求めること】

- システム構築・運用者は、電子メール運用時の対策の実施を組織全体に浸透させる。

〔解説〕

組織にとって主要なコミュニケーションツールの一つである電子メールは、簡易な操作でファイルのやりとりが可能であり、送信先がインターネット全体に広がっていることから、攻撃の手法に使われやすい。また、宛先を誤った送信等、人的エラーによる被害も大きくなる場合がある。電子メール利用に関して一定のセキュリティ水準を担保するため、組織全体で対策を行う必要がある。

以下の具体例に示す対策の実施を組織全体に浸透させる。必要に応じて、特定のファイルのやり取りを禁止する対処や、電子メールの無害化など、技術的な対策を行うことも検討する。

〔具体例〕

●電子メール運用時の対策(例)

- 送信者のメールアドレス、件名、本文に不審な点が無いか、総合的に判断する。
- 不審な形式の添付ファイル(.exe、.bat、心当たりのない拡張子 等)を開かない。
- 文書ファイルが添付されていても、業務上不要と考えられる添付ファイルは開かない。
- メールに記載された URL リンクに安易にアクセスしない。
- 完全性が求められる情報を取り扱う情報システムについて、STARTTLS、DMARC といった電子署名の付与及び検証を行う機能を設ける必要性の有無を検討する。

3　インシデント発生時及び事後対応

3.1　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

【事業者に求めること】

- システム構築・運用者は、セキュリティインシデントが発生した場合には、コンティンジェンシープランに従い、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。

〔解説〕

セキュリティインシデントの発生及びそれによる重要インフラサービス障害が発生した場合には、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必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた責任者へ報告し、障害による影響や範囲をエスカレーションし、二次被害を最小限に抑えることが重要である。

策定したコンティンジェンシープラン、IT-BCP 又は BCP 等を実行し、規定に沿った事業継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、重要インフラサービス障害をもたらした原因への適切な対処を可能とすることが望ましい。

インシデント発生時の対応としては、IPA「中小企業のためのセキュリティインシデント対応の手引き」、JPCERT コーディネーションセンター「インシデントハンドリングマニュアル」等が参考となる。

インシデントの原因究明にあたっては、システム構築・運用者のみならず、セキュリティ専門機関の意見も踏まえつつ、原因究明を行うことが望ましい。

〔具体例〕

●コンティンジェンシープラン及び BCP の実行（例）

- 情報セキュリティ責任者（CISO 等）は、サイバー攻撃等の事象が発生した際、経営者層の意志決定を支援するため、経営者層が理解できるように事象の内容、影響及び現在の対応状況等を説明する。
- 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析（情報システム等へのフォレンジックを含む。）、関係主体等との情報共有・調整（顧客向け広報活動を含む）、被害拡大の防止、サービスの復旧等の対応を実施する。
- 原因究明等に必要なログ等の電子的記録を収集・分析することにより、重要インフラサービス障害をもたらした原因への適切な対処を可能とする。
- 重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

●インシデント対応フロー（例）

- JPCERT コーディネーションセンターの「インシデント対応マニュアルの作成について」（2021 年 11 月）では、インシデントの対応フローとして、以下が例示されている。
  1. インシデントの発見及び報告
     - ✓ インシデントの発見者からの報告を受け取る

- ✓ インシデントの報告を受けた者の行動基準を明確にしておく
- ✓ インシデントの取り扱いに関するすべての記録を残す

2. インシデントに対する初動対応
   - ✓ 発生したインシデントに関して、どこまで情報を共有するのかを判断する
   - ✓ 過去の経験を活用できるかどうかを判断する
3. インシデントに関する告知
   - ✓ 組織外に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
   - ✓ 誰に告知をすべきかを判断する
   - ✓ 告知する手段を検討する
4. インシデントの抑制措置と復旧
   - ✓ インシデントの被害を抑制するための検討
   - ✓ 復旧に関する検討
5. インシデントの事後対応
   - ✓ 復旧後の監視を継続する
   - ✓ 再発防止策を検討する
   - ✓ 他の情報資産への影響がないかどうかを評価する
   - ✓ 得られた教訓を従業員やスタッフ等への教育に反映する

●インシデント対応の流れ(例)

・ NISTの「Computer Security Incident Handling Guide Revison2」では、インシデント対応の流れとして、「準備」、「検知・分析」、「封じ込め、根絶、復旧」、「事後の活動」の流れが示されている。

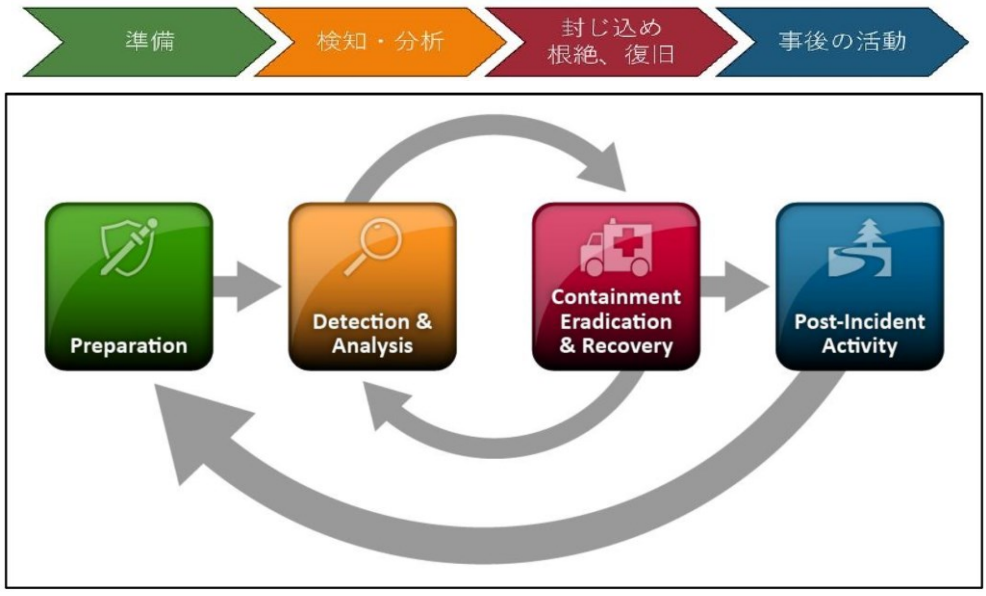


Figure 3-1. Incident Response Life Cycle

・ いわゆる、初動対応は、上図の「検知・分析」から「封じ込め」ぐらいまでを指すことが多い。

別紙1 システムの取得・開発・保守に係るセキュリティ管理策

技術については、サイバーセキュリティを企画・設計段階から確保するための方策を指す「セキュリティ・バイ・デザイン」の考え方を踏まえ、セキュリティ要件に応じて情報システムへのセキュリティ管理策を実装する。その際、セキュリティ管理機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。また、ノウハウの蓄積を考慮し、セキュリティ管理策の実装に係る設計資料を作成する。

運用については、セキュリティ要件に応じてセキュリティ管理策を実装した情報システムの運用設計・手順書化を経て、安定した運用を実現する。また、セキュリティ管理策の有効性を維持するため、認証に要するユーザ登録等の保守をもれなく行う。

また、重要インフラサービスの継続的提供の強靭性の確保を目指すべく、障害対応体制に対してその有効性の検証を行う必要があり、重要インフラ事業者等は、検証目的に応じて、日々の運用、障害対応、診断、テスト、内部・外部監査、演習・訓練等を通じた課題抽出及び改善の取組が求められる。

1.1 情報システムの取得・開発・改善における要求事項の確認

【事業者に求めること】

- 重要インフラサービスの情報システムを新規取得・開発する際や既存システムを改善する際には、セキュリティ要件を検討し、必要に応じて国際標準に基づく第三者認証制度を活用する。

〔解説〕

重要インフラサービスの提供に係る情報システムを新たに取得・開発する際や、既存の情報システムを改善する際には、「セキュリティ・バイ・デザイン」の考え方を踏まえ、システムの要求事項にセキュリティについての要求も含めて検討を行う。重要インフラの分野によっては、情報システムのセキュリティ確保に係る国際標準に則した第三者認証制度が存在するため、必要に応じて、認証された情報システムの活用等も検討する。

〔具体例〕

●情報システム開発時のセキュリティ要件(例)

- 情報システムの取得・開発・改善に係る要求事項にサイバーセキュリティに関する事項を含める。必要に応じて、第三者認証を受けた情報システムや、セキュリティ対策の十分な実績があり対策状況を公開しているといった信頼できる事業者の製品等を活用する。
- 情報システムの取得・開発・改善時にサイバーセキュリティを確保するための手順、環境等を整備する。情報システムの重要度に応じて、情報システムの受け入れ確認時に脆弱性診断を実施する。
- システム開発を外部委託する場合には、サイバーセキュリティに配慮した開発方針の遵守状況を委託先に対して定期的に確認する。
- サイバーセキュリティに配慮した開発や構築を実現するための方針や手順、環境等を整備する。特に、情報システムの受け入れ確認の際には、セキュリティ関連の要求事項の確認に加えて、情報システムの重要度に応じて、脆弱性診断の実施要否を検討する。
- システム開発を外部委託する場合には、サイバーセキュリティに配慮した開発方針の遵守状況を委託先に対して定期的に確認する。

1.2 情報システムのセキュリティ要件

情報システムは、目的業務を円滑に遂行するため、その企画・要件定義、構築、運用・保守、更改・廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはサイバーセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせてセキュリティ管理策を実施する必要がある。

1.2.1 情報システム企画・要件定義

【事業者に求めること】

- システム構築・運用者は、情報システム全体でセキュリティ維持体制の確保を責任者に求めること。

〔解説〕

システム構築・運用者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

〔具体例〕

●情報システムのセキュリティ要件(例)

- システム構築・運用者は、情報システムのセキュリティ要件を決定し、セキュリティ要件を満たすために、機器等の購入(購入に準ずるリースを含む。)及び情報システム開発において必要な対策、機器等の選定基準、サイバーセキュリティに関する機能の設定、セキュリティに関する脅威への対策、並びに情報システムの構成要素についての対策について定めること。
- システム構築・運用者は、情報システムの取扱いに関し、取扱者が理解・遵守するために周知に努め、教育・訓練その他必要な措置を実施すること。

●望ましいセキュリティ管理策(例)

情報システムの企画・要件定義時には、以下【具体例】に示すセキュリティ管理策を講ずることが望ましい。

- システム構築・運用者は、開発する情報システムが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果、及び当該情報システムにおいて取り扱う情報の格付けに応じて、セキュリティ機能(主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等)要件を適切に策定し、仕様書等に明確に記述すること。
- システム構築・運用者は、開発する情報システムが運用される際に利用されるセキュリティ機能についての管理機能要件を適切に策定し、仕様書等に明確に記述すること。
- システム構築・運用者は、開発する情報システムで利用するソフトウェアについて、当該保守期限を考慮するなどして、当該情報システムの次期更改時期まで対策用ファイルの提供が継続されると見込まれるソフトウェアを選定すること。また、適宜入手した保守期限の情報から必要と判断した場合は、後継となるソフトウェアへの更新等の計画を策定すること。
- システム構築・運用者は、情報システムの設計について、そのセキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

・ システム構築・運用者は、開発する情報システムに関連する脆弱性についての対策(情報システムにおいて処理するデータ及び入出力されるデータのセキュリティに関する妥当性を確認する機能等)を仕様書等に明確に記述すること。
・ システム構築・運用者は、開発する情報システムに適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書(ST:Security Target)の ST 評価・ST 確認を受けること。

1.2.2 情報システムの構築

【事業者に求めること】

> ➢ システム構築・運用者は、情報システム構築時にサイバーセキュリティ措置を講じること。

〔解説〕

システム構築・運用者は、情報システムの構築に際しては、サイバーセキュリティの観点から必要な措置を講ずること。

〔具体例〕

●望ましいセキュリティ管理策(例)

情報システムの構築時には、以下に示すセキュリティ管理策を講ずることが望ましい。
・ セキュリティ要件に基づき定めたセキュリティ管理策を行うこと。
・ 構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、サイバーセキュリティの観点から必要な措置を講ずること。
・ 機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、セキュリティ管理策に係る要件が満たされていることを確認すること。
・ 情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、セキュリティ管理策に必要な内容が含まれていることを確認すること。

1.3 端末、サーバ装置、複合機及び特定用途機器

1.3.1 端末

【事業者に求めること】

> ➢ 端末利用時は、取扱者の不適切な利用や過失による不正プログラム感染リスクが高く、持ち出し時には紛失や盗難のリスクも増すため、適切な対策が必要である。

〔解説〕

端末の利用に当たっては、取扱者が専門的知識を有していない場合が多いことから、取扱者の不適切な利用や過失等による不正プログラム感染等のリスクが高い。また、外出時やテレワーク等で事業者外へ持ち出すモバイル端末については、紛失又は盗難のリスクも高くなることから、適切な対策を

講ずる必要がある。

〔具体例〕

●モバイル端末の管理とセキュリティ対策(例)

- システム構築・運用者は、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定め、これを周知すること。
- システム構築・運用者は、端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないように周知すること。
- システム構築・運用者は、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。
- システム構築・運用者は、事業者外へ持ち出すモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。
- システム構築・運用者は、USB メモリ等の外部電磁的記録媒体を用いて情報を取扱う場合は、外部電磁的記録媒体は組織から支給されたものを利用すること。外部電磁的記録媒体による情報のやりとりにおける安全確保のために、情報の取り扱いに関する利用手順を定めるなど必要な措置を講ずること。

●推奨対策項目(例)

また、システム構築・運用者は、以下【推奨対策項目】に示す対策を追加で講じることが望ましい。

- 端末で利用を認めるクラウドサービス及び利用を禁止するクラウドサービスを定め、これを周知すること。
- 端末で利用を認めるハードウェア及び利用を禁止するハードウェアを定め、これを周知すること。
- 端末管理ツールを活用し、利用禁止されているソフトウェアのインストールを制限・警告すること。
- 端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないように周知すること。
- 端末管理台帳を整備し、利用状況(シリアルナンバー、OS 種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等)を必要に応じて管理・把握すること。
- 利用者認証に一定回数失敗した場合、必要に応じ端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定すること。
- 端末における OS をはじめとしたソフトウェアについて、アップデートやパッチ適用を定期的に行い最新の状態に保つように周知すること。

●モバイル端末に対する推奨対策項目(例)

さらに、モバイル端末に対して上記の対策に加え、システム構築・運用者は、以下【具体例】を例とする対策を講ずることが望ましい。

- モバイル端末はできる限り他人と共有しないようにする。共有で使わざるを得ない場合は、業務用のユーザアカウントを別途作成する。
- モバイル端末には必要最小限の権限(例:ユーザ権限)を付与する。

- モバイル端末の内蔵 HDD や USB メモリ等の記録媒体の暗号化を強制し、取扱者で設定を変更できないようにする。
- モバイル端末のファイアウォール(パーソナルファイアウォール)を有効にする。
- モバイル端末を紛失した際に、遠隔から端末の位置情報の把握、端末上のデータ等の削除、端末の初期化等をできるようにする。
- 事業場外のモバイル端末からオフィスネットワーク上のシステムやクラウドサービスに接続するための利用者認証は、多要素認証方式や電子証明書の利用等の技術的基準やパスワードポリシー(長いパスフレーズの利用、使いまわしの禁止等)を明確に定め、適正に管理・運用する。
- テレワーク等で個人所有端末の利用を許可する場合は、利用にあたってのルールの策定や端末へのデータ保存の制限・禁止、セキュリティ対策の実施の確認等を行う。

1.3.2 サーバ装置

【事業者に求めること】

- サーバ装置は大量の情報を保存していることから不正アクセスや感染リスクが高く、機能停止時の影響も大きいため、システム構築・運用者は適切な対策を講ずる必要がある。

〔解説〕

サーバ装置については、当該サーバ装置の内蔵記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。重要インフラ事業者等が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、顧客からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きいことから、システム構築・運用者は、適切な対策を講ずる必要がある。

〔具体例〕

●サーバ装置の安全運用とセキュリティ対策(例)

- サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。
- 障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、将来の見通しも考慮し、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。
- サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアについて、以下を考慮して定めること。
  - ✓ ソフトウェアベンダ等のサポート状況
  - ✓ ソフトウェアと外部との通信の有無及び通信する場合はその通信内容
  - ✓ インストール時に同時にインストールされる他のソフトウェア
  - ✓ その他、ソフトウェアの利用に伴うサイバーセキュリティリスク
- 通信回線を経由してサーバ装置の保守作業を行う場合は、送受信される情報を暗号化する等情

報が漏えいすることを防止するための対策を講ずること。
・ システム運用に不要なサーバアプリケーションについては、機能を無効化して稼動させること。

1.3.3 複合機及び IoT 機器を含む特定用途機器

【事業者に求めること】

- 複合機や IoT 機器などインターネット接続されている特定用途機器は、脆弱性をつかれるリスクがあるため、情報システムの一部として責任者を明確にし、適切な対策を講ずることが重要。

〔解説〕

複合機(プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器)は、事業者内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、重要インフラ事業者等においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。例えば、特定用途機器の中にはインターネットに接続されるいわゆる IoT 機器があるが、近年 IoT 機器の脆弱性をついた攻撃が数多く発生しており、IoT 機器が踏み台となって他の情報システムへの攻撃に利用されるなど、社会的問題になってきている。

したがって、複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

〔具体例〕

●複合機の対策(例)

システム構築・運用者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。システム構築・運用者は以下の項目を例とする運用中の複合機に対する、重要インフラサービス障害への対策を講ずること。

・ 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。
・ 複合機が備える機能のうち利用しない機能を停止する。
・ 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで認証が成功した者のみ印刷が許可される機能等を活用する。
・ 事業者内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。
・ 複合機をインターネットに直接接続しない。
・ リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
・ 取扱者ごとに許可される操作を適切に設定する。

●IoT 機器を含む特定用途機器の対策(例)

システム構築・運用者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じて、以下の項目を例とする対策を講ずること。

- IoT 機器を含む特定用途機器について、利用環境や機器の制約に応じた適切なセキュリティ設定を実施する。
- IoT 機器を含む特定用途機器が備える機能のうち利用しない機能を停止する。
- IoT 機器を含む特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール、暗号化、アクセス制御等の利用により適切に通信制御を行う。
- インターネットに接続されている IoT 機器を含む特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。
- IoT 機器を含む特定用途機器単体だけでなく、IoT システム全体でセキュリティを確保する認証機能を適用する。
- IoT 機器を含む特定用途機器への外部インタフェース経由、物理的アクセスについて対策を講ずる。
- IoT 機器を含む特定用途機器の状態や通信状況を把握して記録する機能、及び記録を不正に消去、改ざんされない対策を講ずる。
- IoT 機器を含む特定用途機器の変更、増設時等には、適切な初期設定が確実に実施される対策を講ずる。

1.3.4 端末、サーバ装置、複合機及び特定用途機器の調達

【事業者に求めること】

- 端末、サーバ装置、複合機、IoT 機器を含む特定用途機器は、運用段階だけでなく、開発や製造過程でもサプライチェーン・リスクが懸念されるため、調達時にはサプライチェーンに関わる事業者も含め、サイバーセキュリティ基本法第 7 条を踏まえた対応が必要である。

〔解説〕

上記に示す端末、サーバ装置、複合機及び IoT 機器を含む特定用途機器は運用段階だけでなく、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクが懸念される。したがって、これらの機器の調達に当たっては、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)の責務があることを踏まえた対応が必要である。

機器調達に関するセキュリティ対策は、政府機関を対象としたガイドライン[7]において以下のような対策が挙げられており、重要インフラ事業者等においてもこれらを参考として対策に活用することが

[7] NISC、「政府機関等の対策基準策定のためのガイドライン(令和5年度版)令和5年7月4日」
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

望ましい。

〔具体例〕

●政府機関等の対策基準策定のためのガイドラインの記載内容（抜粋）

① 統括情報セキュリティ責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を全て含めること。
- 調達した機器等に不正な変更が見付かったときに、必要に応じて追跡調査や立入検査等、機関等と調達先が連携して原因を調査・排除できる体制を整備していること。
- 「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成 30 年 12 月 10 日関係省庁申し合わせ）に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずること。

② 統括情報セキュリティ責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。

③ 統括情報セキュリティ責任者は、機器等の納入時の確認・検査手続には以下を全て含む事項を確認できる手続を定めること。
- 調達時に指定したセキュリティ要件の実装状況
- 機器等に不正プログラムが混入していないこと。

1.4 アプリケーション

1.4.1 電子メール

【事業者に求めること】

- 電子メールは機密性や可用性のリスクのみならず、なりすましなどの第三者リスクも存在するため、適切な管理と利用基準の策定が必要である。

〔解説〕

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、悪意ある第三者等によるなりすまし等に電子メールを利用する取扱者が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要であり、電子メールサーバの管理及び電子メールの利用に関する対策基準を定める必要がある。

〔具体例〕

●電子メールのリスク管理とセキュリティ強化（例）

- システム構築・運用者は、電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について検討すること。
- クラウドによるファイル共有サービスの利用を含む添付ファイルの保護

- 不正中継禁止
- 送受信容量の制限
- 自動転送の制限
- 業務外利用の禁止
- 送信先アドレス漏えいの防止
- 電子署名機能の導入
- 安全性が客観的に評価された暗号技術の利用
- ウィルス対策機能や迷惑メール対策機能、フィッシング対策機能の導入
- 電子メール送信時及び受信時の送信ドメイン認証(SPF 等)の導入
- クラウドによる電子メールサービスを利用する場合は、盗聴を防止するため通信経路を適切に暗号化
- クラウドによるファイル共有サービスを利用する場合は、アクセス制御を適切に設定

1.4.2 ウェブ

【事業者に求めること】

- ウェブサーバは常に情報改ざんやサービス停止、侵入などの攻撃リスクを受けることが考えられるため、適切な対策の実施が必要である。

〔解説〕

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ(ウェブページとして公開している情報)が改ざんされたり、ウェブサーバが利用不能にされたり、又はウェブサーバが侵入されるなどの被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

〔具体例〕

●ウェブサーバの脆弱性対策(例)

- システム構築・運用者は、ウェブサーバを用いて提供するサービスにおいて、システムが保有する情報の格付けに応じて、想定される脅威から保護すべき情報を特定し、対策を行う必要性の有無を検討し、適切な対策を講ずること。
- システム構築・運用者は、ウェブアプリケーションの開発において、以下に示すような既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。
  - a) SQL インジェクション脆弱性
  - b) OS コマンドインジェクション脆弱性
  - c) ディレクトリトラバーサル脆弱性
  - d) セッション管理の脆弱性
  - e) アクセス制御欠如と認可処理欠如の脆弱性
  - f) クロスサイトスクリプティング脆弱性
  - g) クロスサイトリクエストフォージェリ脆弱性
  - h) クリックジャッキング脆弱性

i）メールヘッダインジェクション脆弱性
j）HTTP ヘッダインジェクション脆弱性
k）eval インジェクション脆弱性
l）レースコンディション脆弱性
m）バッファオーバーフロー及び整数オーバーフロー脆弱性

・ システム構築・運用者は、ウェブサーバを用いて提供するサービスにおいて、システムが保有する情報の格付けに応じて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
・ システム構築・運用者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。

1.4.3 ドメインネームシステム（DNS）

【事業者に求めること】

➢ DNS 導入時は、サーバ管理などの適切な対策が必要である。

〔解説〕

ドメインネームシステム（DNS）を導入する際には、サーバの適切な管理などの対策が求められる。

〔具体例〕

●DNS サーバ維持と運用管理（例）

・ システム構築・運用者は、DNS サーバの運用を維持するため、適切な対策を講ずること。

＜DNS 導入時の対策＞

・ 要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置
・ キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置
・ コンテンツサーバにおいて、各重要インフラ事業者等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置

＜DNS 運用時の対策＞

・ コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持
・ コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認
・ キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずる

1.4.4 データベース

【事業者に求めること】

➢ システム構築・運用者は、データベースの不正アクセスや不適切な利用を防ぐため、導入・運用時に必要な対策を講ずることが求められる。

〔解説〕

データベースに保管しているデータが漏えいするリスクがあることから、必要な対策が求められる。システム構築・運用者は、不正アクセス等の外的要因やデータの不適切な利用等の内的要因など、保管するデータの漏えい・改ざんのリスクに対して対策を講じ、データベースの導入・運用時の対策として、以下に挙げる事項を含む必要な対策を講ずることが求められる。

〔具体例〕

●データベースのセキュリティ管理(例)

- 管理者アカウントの適正な権限管理
- データにアクセスした利用者を特定できるような措置
- データの不正な操作を検知、対策
- データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止する対策
- データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化
- クラウドによるデータベースサービスを利用する場合は、通信経路を適切に暗号化

1.4.5 Web 会議

【事業者に求めること】

- Web 会議での通信や情報共有は機密性リスクを伴うため、適切な運用・管理と対策基準の策定が必要である。

〔解説〕

Web 会議での通信や情報共有は情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。このようなリスクを回避するためには、適切な Web 会議の運用・管理が必要であり、利用に関する対策基準を定める必要がある。

〔具体例〕

●Web 会議におけるリスク管理と対策(例)

- システム構築・運用者は、Web 会議におけるセキュリティ上のリスクを軽減するための管理策の必要性について検討すること。
- Web 会議の開催方式を機密性に合わせて適切に選択する。
- Web 会議のサービス提供者を適切に選択する。
- 例えば、海外のサービス提供者が暗号鍵を持つサービスの場合、政府によるサーバのデータの強制収容リスクがあることに注意する。
- Web 会議ソフトウェアを常に最新の状態にアップデートする。
- Web 会議参加者のアクセス権限を適切に設定する。
- Web 会議参加者の確認・認証(会議案内の安全な経路での配布、Web 会議ソフトウェアのセキュリティ機能の利用)

- オンライン会議にアクセスするための URL を正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないよう周知すること
- 録画、スクリーンショット等による情報漏えいの対策を行うこと。(画面共有内容の吟味、会議終了後の録画データ削除等)
- のぞき見、音漏れ等による情報漏えいの防止を行うこと。(サテライトオフィス等の多数の人々出入りする場所等)
- 自宅においては、離席中に子どもが意図せず操作することや、家族が撮影した室内写真に情報が写り込む等の点に十分に注意すること。

1.5 通信回線及び通信回線装置

通信回線の利用については、当該通信回線の不正利用、これに接続されたサーバ装置、端末又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報のセキュリティが損なわれるおそれを有している。また、通信事業者の公衆回線や事業者専用の通信回線の運用主体又は有線回線や無線LAN 回線等の物理的な回線の種類によってサイバーセキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

1.5.1 通信回線共通対策

【事業者に求めること】

- システム構築・運用者は、通信回線のセキュリティを実現・維持するため、適切な対策を講ずること。

〔解説〕

システム構築・運用者は、通信回線構築・運用に係るリスクに対応するため、通信回線におけるセキュリティを実現・維持するために、適切な対策を講ずること。

〔具体例〕

●通信回線の構築時に講ずることが望ましい対策(例)

- 通信回線に論理的に接続する際の審査手続を整備し、承認を受けていない者からの通信を遮断するための対策を講ずること。
- 通信回線のサイバーセキュリティ維持に関する対策として、アクセス制御、経路制御、送受信情報の暗号化、及び物理的セキュリティなどの必要性の有無を検討し、適切な対策を講ずること。
- 通信回線構築によるリスクを検討し、通信回線を構築すること。
- 通信回線に接続されるサーバ装置、端末をグループ化し、それぞれ通信回線上で分離すること。
- グループ化されたサーバ装置及び端末間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。
- 通信する情報の格付けに従って、通信回線を用いて送受信される情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
- 通信する情報の格付けに従って、通信回線に利用する物理的な回線のセキュリティを検討し、必要な対策を講ずること。

- 取扱者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。
- 遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてサイバーセキュリティを確保すること。
- 通信回線装置に存在する公開された脆弱性から通信回線装置を保護するための対策を講ずること。
- 通信回線装置を要管理対策区域に設置すること。
- 電気通信事業者の通信回線サービスを利用する場合には、セキュリティ水準及びサービスレベルを含む事項に関して契約時に取り決めておくこと。
- 事業者内通信回線にインターネット回線、公衆通信回線等の事業者外通信回線を接続する場合には、事業者内通信回線及び当該事業者内通信回線に接続されている情報システムのサイバーセキュリティを確保するための措置を講ずること。
- 通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。

1.5.2 リモートアクセス環境導入時の対策

【事業者に求めること】

- リモートアクセス環境は、不正利用や情報の盗聴、改ざん等のリスクを抱えているため、導入時に適切な対策基準を定める必要がある。

〔解説〕

リモートアクセス環境の利用については、当該通信回線の不正利用、これに接続されたサーバ装置、端末又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報のセキュリティが損なわれるおそれを有している。また、利用する回線や用途により想定される脅威及びリスクが異なる。これらのことを踏まえ、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る。

VPN 回線及び公衆電話網を利用する際は、以下の対策を講ずる必要がある。

〔具体例〕

●VPN 回線利用時の対策（例）

- 利用開始及び利用停止時の申請手続の整備
- 認証コードの安全な配布方法と運用手順の整備
- 通信内容の暗号化
- 通信を行う端末の識別又は認証（特にパスワードを使用する場合は、簡単に推測されない複雑なものとすること）
- リモートアクセス環境を利用する者の認証
- 主体認証ログの取得及び管理
- リモートアクセスにおいて利用可能な通信回線の範囲の制限
- アクセス可能な情報システムの制限

・ リモートアクセス中の他の通信回線との接続禁止

●公衆電話網利用時の対策(例)

・ 利用開始及び利用停止時の申請手続の整備
・ 通信を行う者又は発信者番号による識別及び主体認証
・ 主体認証ログの取得及び管理
・ リモートアクセス経由でアクセスすることが可能な情報システムの制限
・ リモートアクセス中に他の通信回線との接続の禁止
・ 不正ログインを検知する機能の実装

1.5.3 無線 LAN 環境導入時の対策

【事業者に求めること】

➢ 無線 LAN を利用する場合、通信内容の暗号化に加え、サイバーセキュリティ確保のための必要な措置を講ずる必要がある。

〔解説〕

無線 LAN 技術を利用して事業者内通信回線を構築する場合は、通信回線共通対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他のサイバーセキュリティ確保のために必要な措置を講ずる必要がある。

システム構築・運用者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む対策を講ずることが望ましい。

〔具体例〕

●無線 LAN セキュリティ強化の対策(例)

・ SSID の隠ぺい
・ 無線 LAN 通信の暗号化
・ MAC アドレスフィルタリングによる端末の識別
・ 802.1X による無線 LAN へのアクセス主体の認証
・ 無線 LAN 回線利用申請手続の整備
・ 無線 LAN 機器の管理手順の整備
・ 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

1.5.4 IPv6 (Internet Protocol Version 6)通信回線

【事業者に求めること】

➢ IPv6 通信プロトコルは不正アクセスのリスクがあるため、対策を講ずる必要がある。

〔解説〕

インターネットの規格である IPv6 通信プロトコルは、不正アクセスの手口として悪用されるおそれも

あることから、必要な対策を講じていく必要がある。

システム構築・運用者は、IPv6 通信を行う情報システムに係る対策として、以下に挙げる事項を含む必要な対策を講ずることが望ましい。

〔具体例〕

●IPv6 のセキュリティ対策(例)

- IPv6 通信を行う情報システムに係る対策
- 意図しない IPv6 通信の抑止・監視

1.5.5 5G /ローカル 5G 通信回線

【事業者に求めること】

- システム構築・運用者は、5G 通信回線の構築にあたって、従来通信回線共通の対策に加え、ローカル 5G 特有のサイバーセキュリティリスクにも留意し、対策を講ずる必要がある。

〔解説〕

移動通信システムの規格である 5G 通信回線は、4G などの従来の移動通信システムと比較して、「超高速」、「超低遅延」、「多数同時接続」であるという特長を有しており、IoT と組み合わせて様々な分野での利活用が期待されている。

また、通信事業者以外の事業者等が自らの建物や敷地内において、自営で 5G 通信回線を構築し、利用することができるローカル 5G の普及が見込まれている。

5G 通信回線では、前述の通信回線共通の対策が求められるが、ローカル 5G の利用においては特有のサイバーセキュリティリスクがあることに留意し必要な対策を講じていく必要がある。

システム構築・運用者は、ローカル 5G を利用する情報システムに係る対策として、以下に挙げる事項を含む必要な対策を講ずることが望ましい。

〔具体例〕

●ローカル 5G 機器と SIM 認証のセキュリティ対策(例)

- ネットワーク接続の認証に用いられる SIM カードを正規デバイスから不正に窃取し、許可されていない端末に差し込んで使用する不正行為(SIM スワッピング)に対して、端末と SIM カードの組合せにより、真正性をチェックする。
- ローカル 5G 用機器を屋外に固定設置する場合には、第三者が不用意に接触したり取り外したりできないように、機器設置場所への接近の制限、機器をしっかりと固定する等の物理的な対処を施す。
- ローカル 5G 用機器のネットワーク接続状態を常に監視し、予定外の接続状態変更に対してアラーム等が通知される仕組みを用意する。

●参考とするガイドライン例

また、以下に示す参考とするガイドラインの例を参考に、5G/ローカル 5G の構築、利用における

必要な対策を講ずることが望ましい。

＜参考ガイドライン例＞

・ 5G セキュリティガイドライン第 1 版(総務省　2022.4.22)
https://www.soumu.go.jp/main_content/000812253.pdf

・ ローカル 5G セキュリティガイドライン初版(一般社団法人 ICT-ISAC　5G セキュリティ推進グループ　2022.3)
https://www.ict-isac.jp/news/2_Local_5G_Security_Guideline.pdf

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。

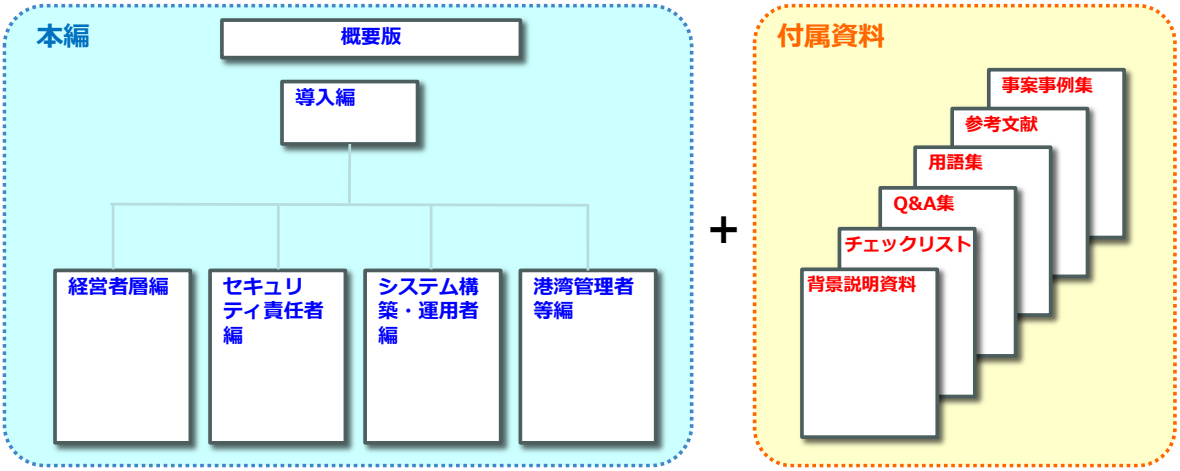
重要インフラサービス	システムの不具合が引き起こす重要インフラサービス障害の例
TOS によるターミナルオペレーション	荷捌きの効率低下、停止によるコンテナ貨物の搬入・搬出の停滞、停止

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。

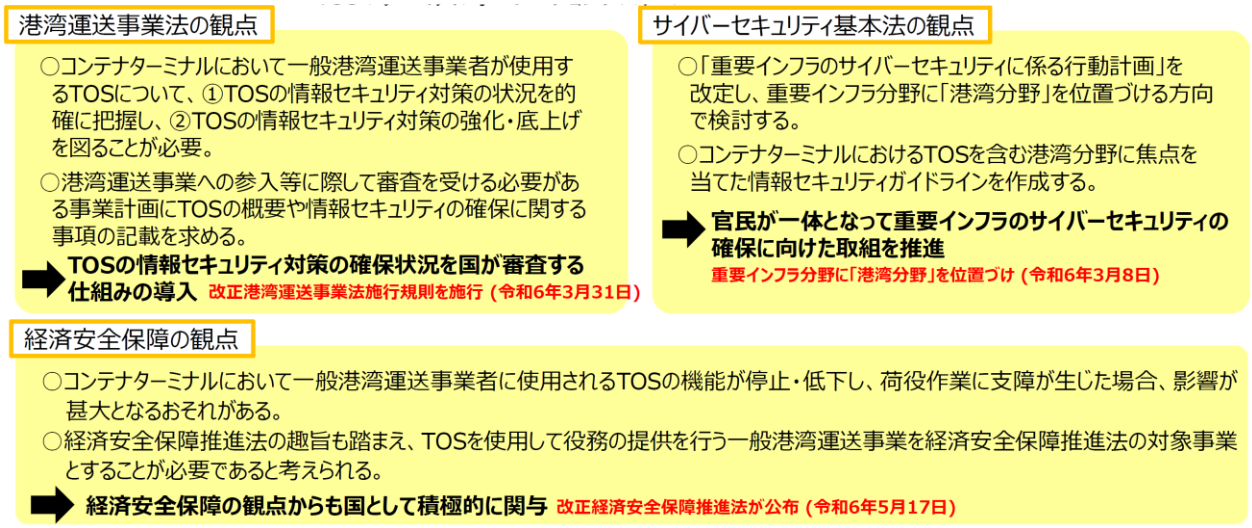


図　港湾分野における情報セキュリティ対策等推進のための3つの制度的措置

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。

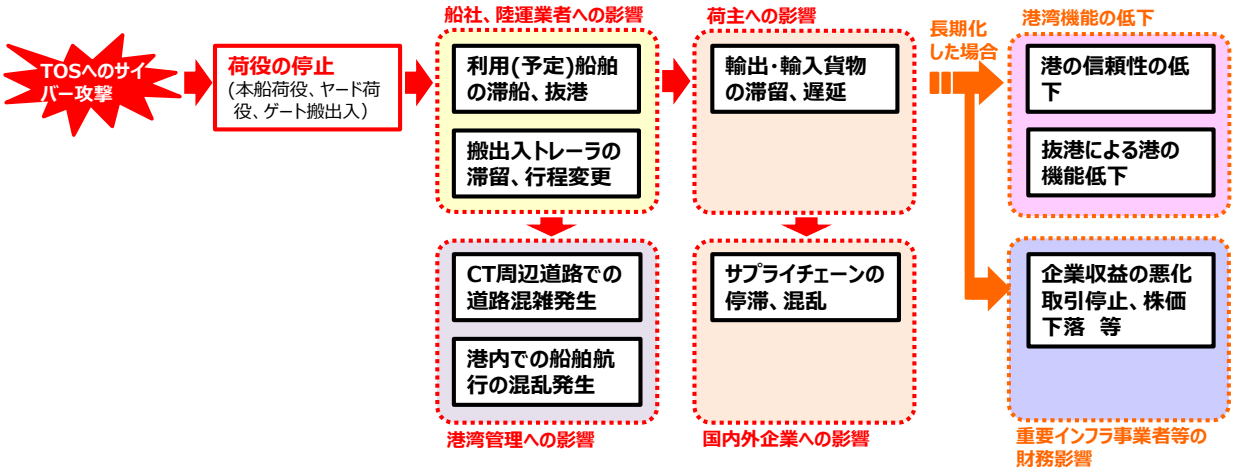


図　TOS 等へのサイバー攻撃による港湾機能等への影響想定

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。