# 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

〔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。

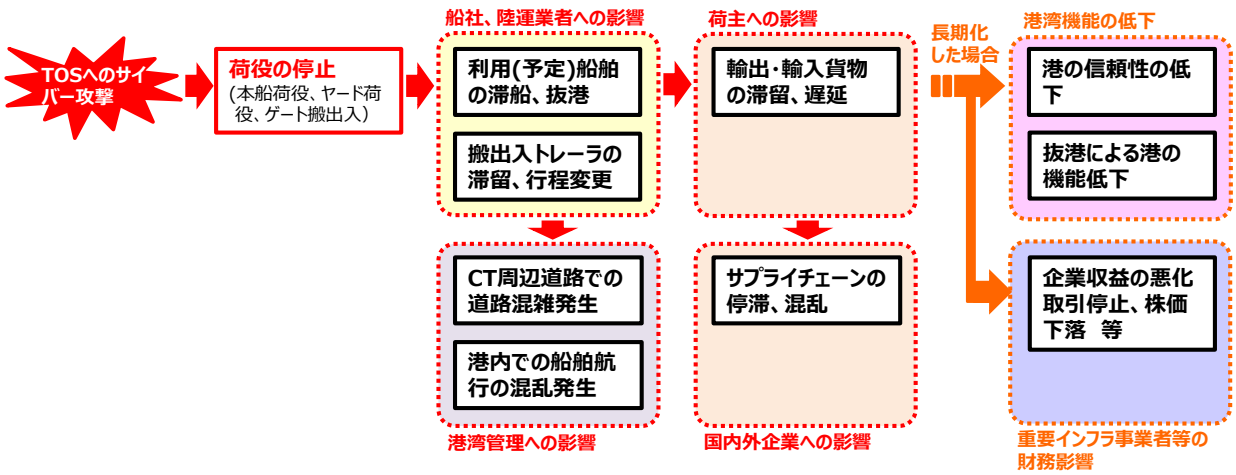


図　TOS 等へのサイバー攻撃による港湾機能等への影響想定

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