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

〔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。

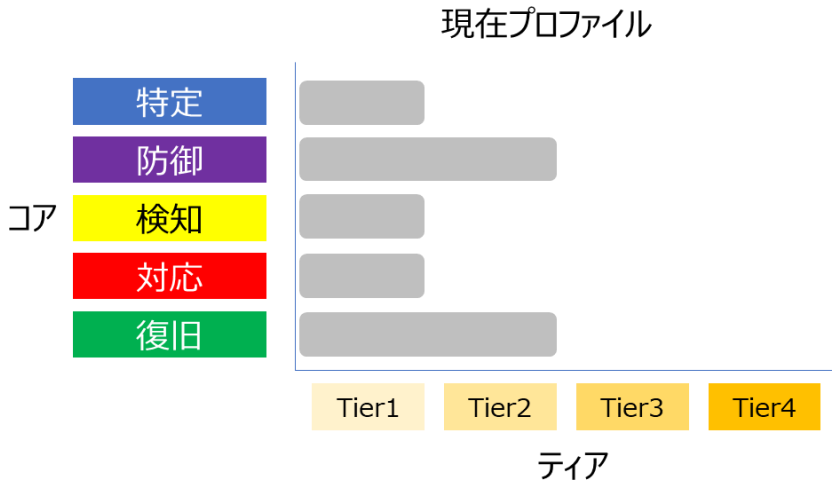
  (例)

  ✓ 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】

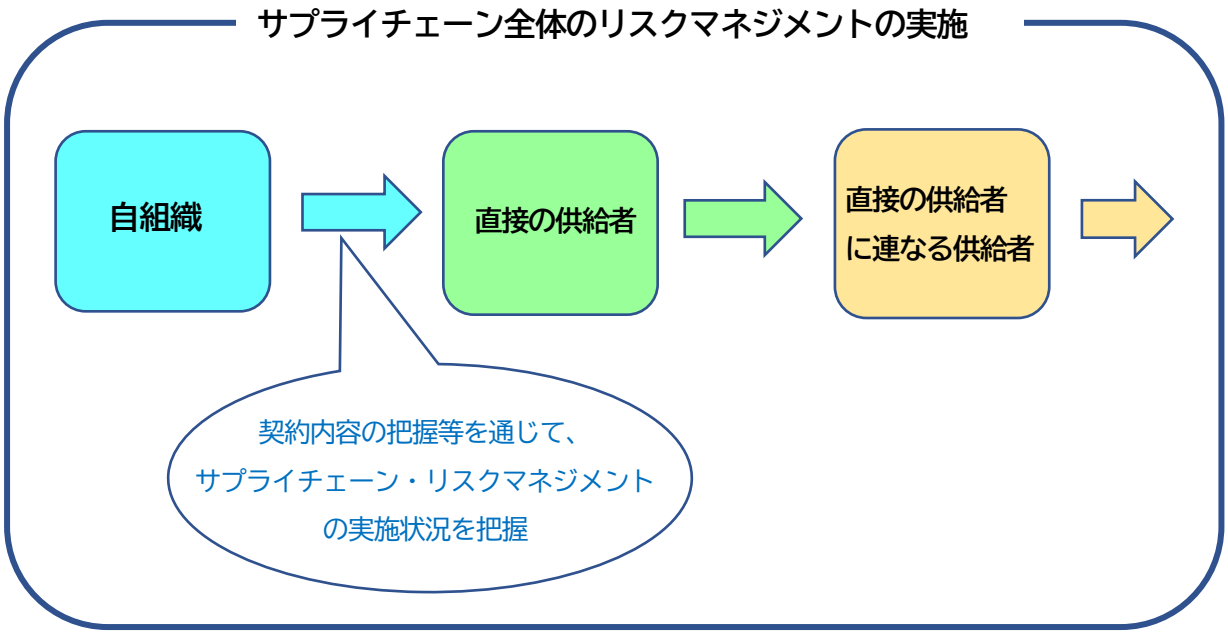
> ➢ 情報セキュリティ責任者（CISO 等）は、直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。

〔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

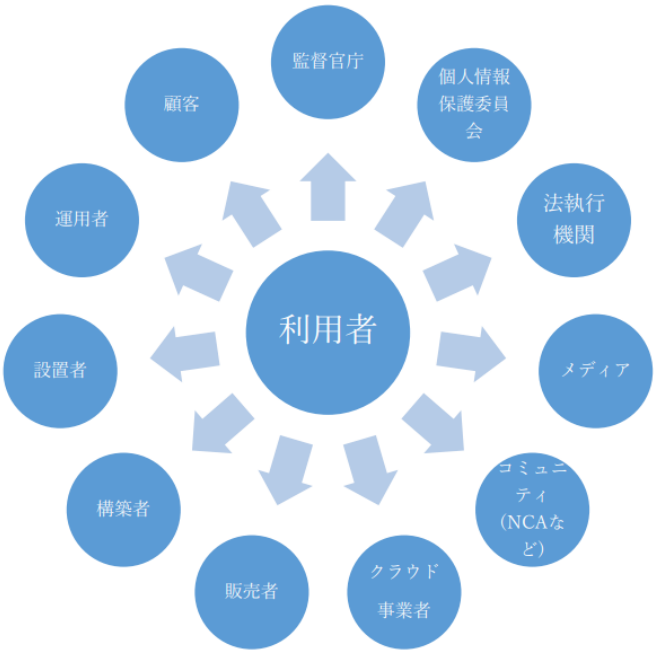
[13] https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

[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

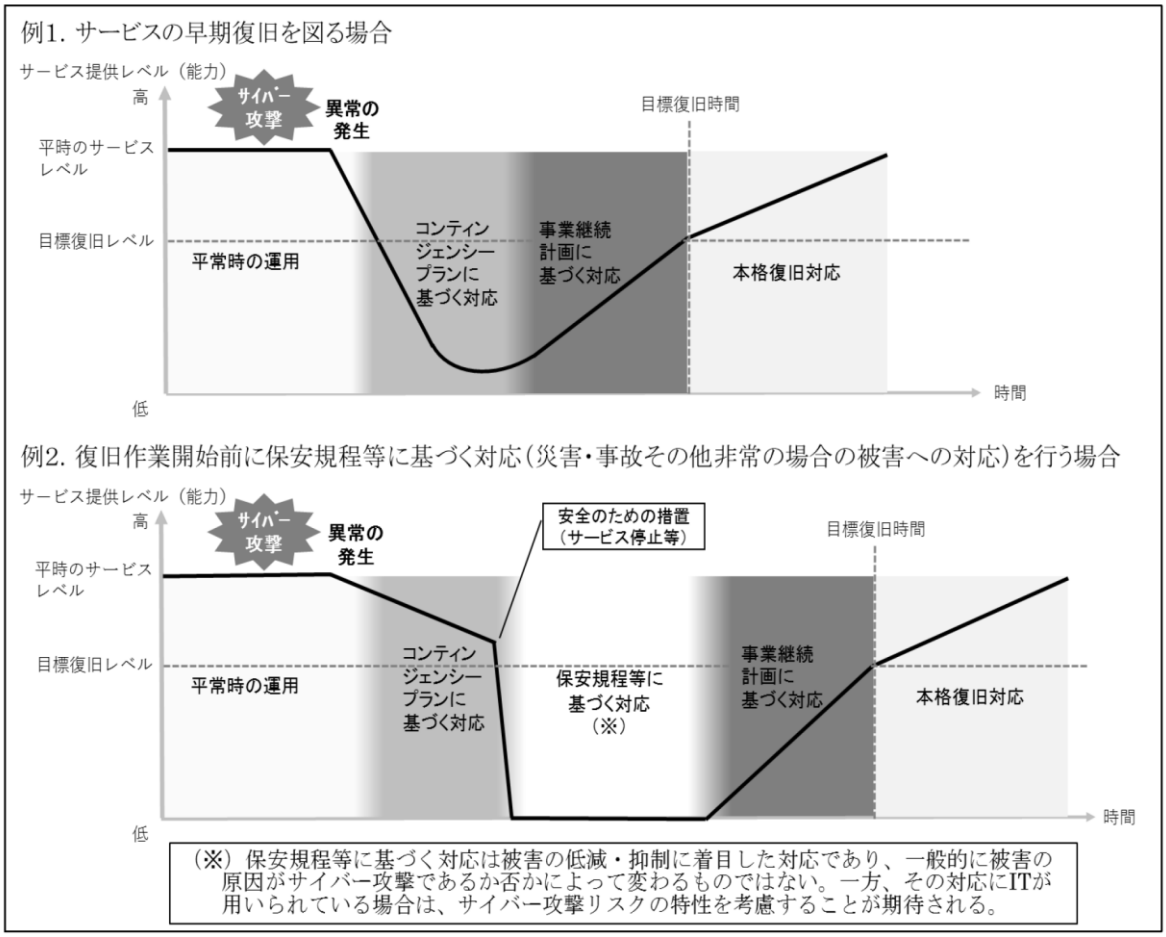
- ✓ 関係当局、供給者、顧客等、内部及び外部の利害関係者との調整
- ✓ 組織内外へのインシデント報告や証拠収集等の手順
- ✓ インシデント管理活動のログ取得
- ✓ 証拠の取扱い
- ✓ 根本原因分析又は事後分析手順
- ✓ 教訓及びインシデント管理手順、セキュリティ管理策についての改善
- ✓ インシデント報告書の作成

・ 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

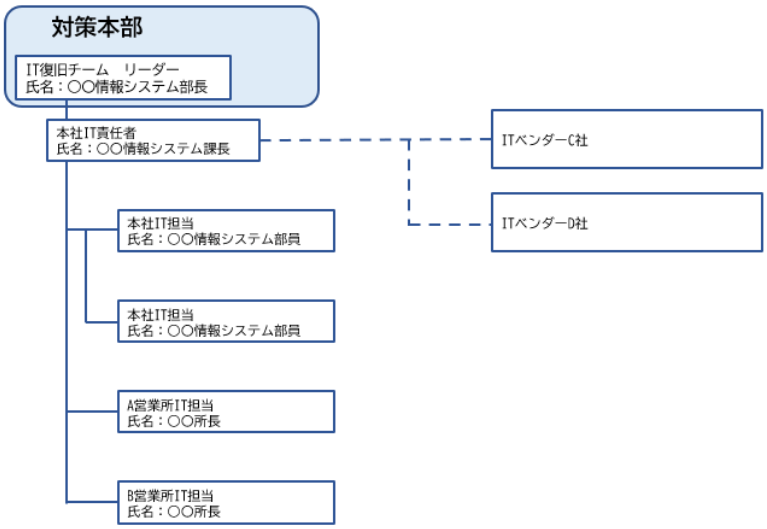
ポリシーなどに照らして可能な範囲で詳細に、報告者や関係者に連絡。

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

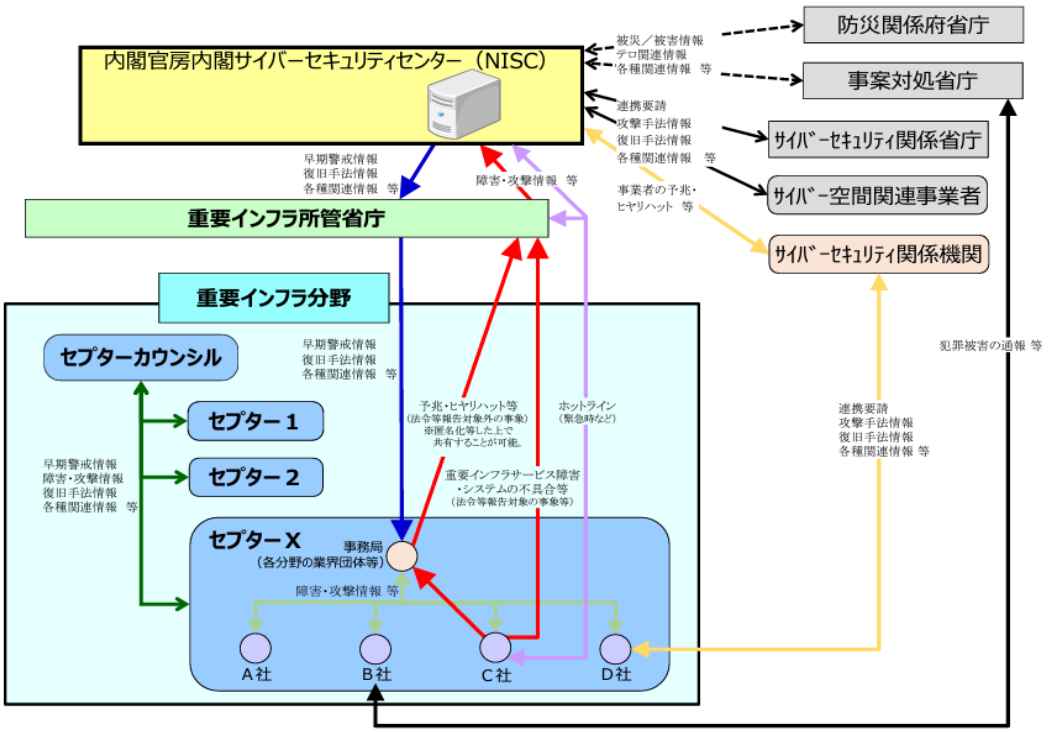
セキュリティ事案が発生した際の初動対応時の相談先となりうることから、セキュリティベンダー、セキュリティ専門機関、都道府県警察等と平時から情報交換等を行うこと。

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。

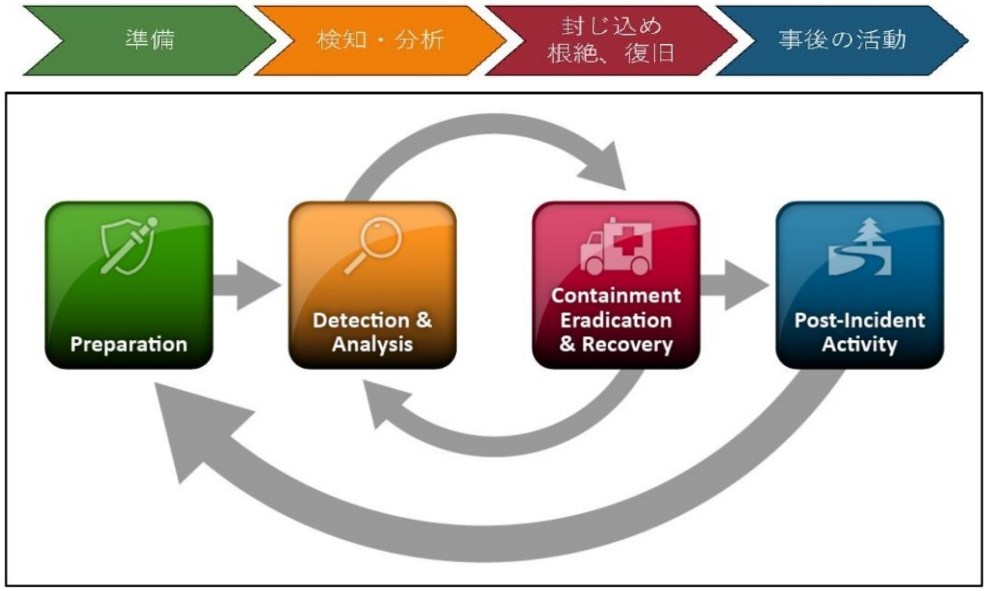


Figure 3-1. Incident Response Life Cycle

・ 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。

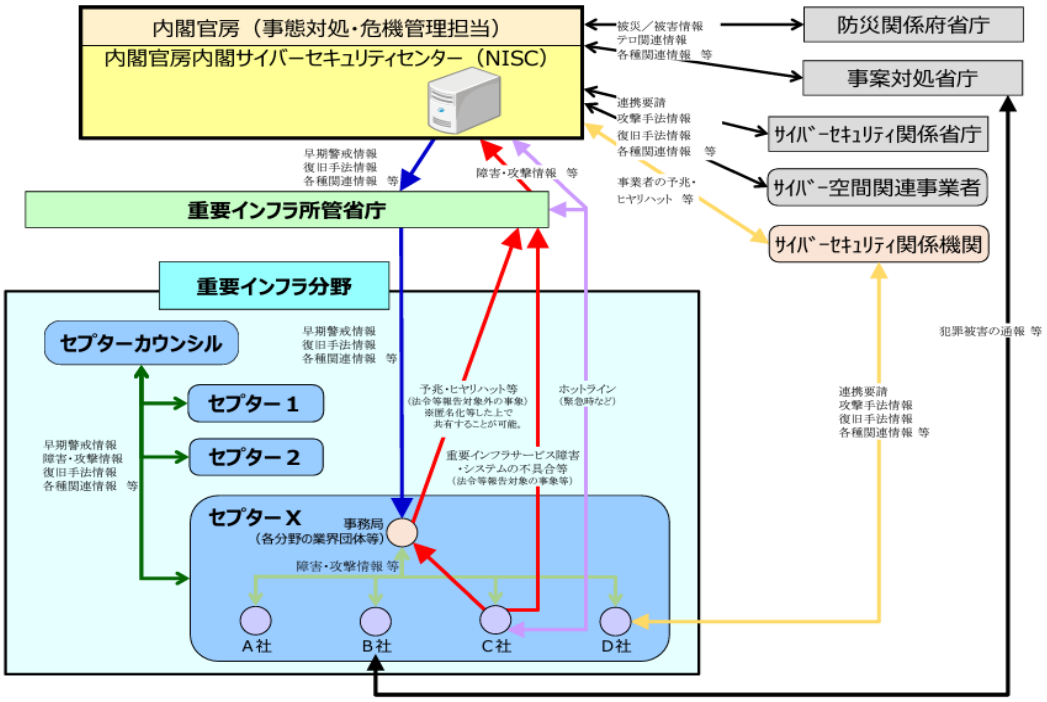
NISC「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和5年3月8日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）を参照の上、組織内外と情報共有を実施することが望ましい。

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

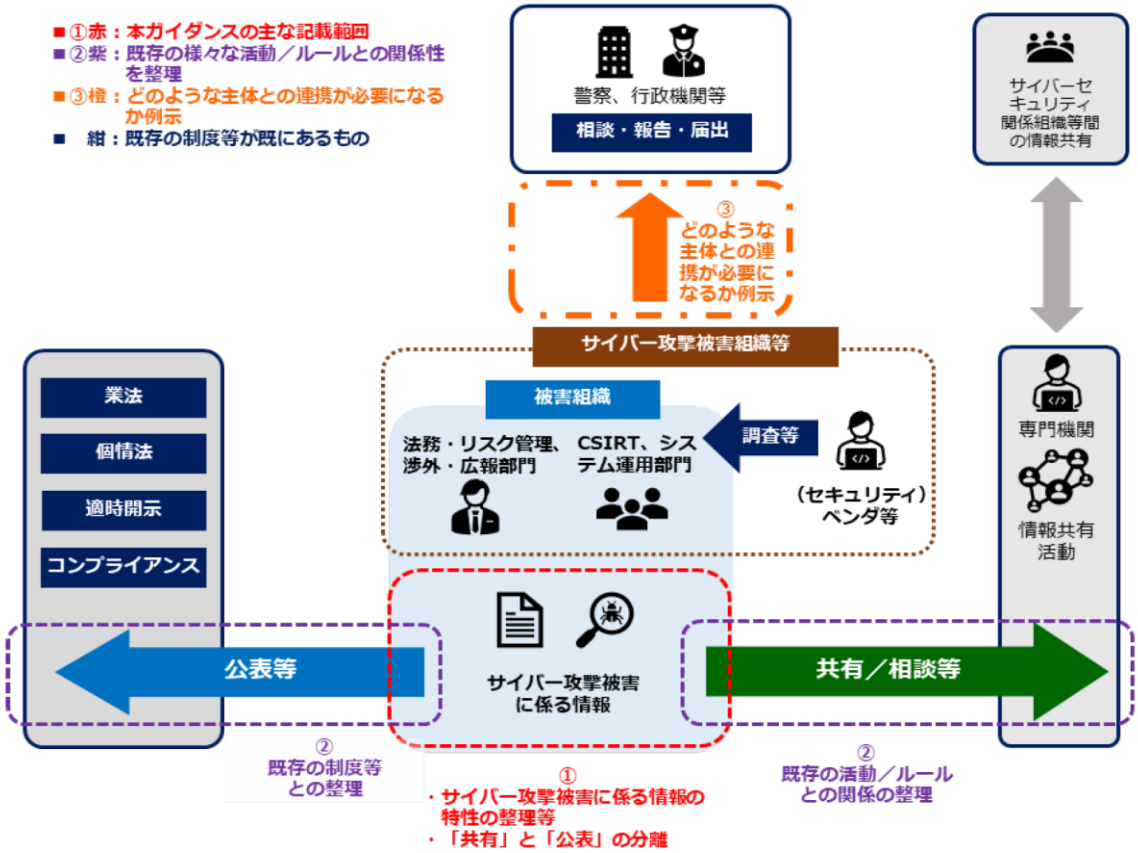
関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における[注]各関係主体の役割
○ 内閣官房 （事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房 （ＮＩＳＣ）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。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