港湾分野における
情報セキュリティ確保に係る安全ガイドライン（第2版）

～システム構築・運用者編～

令和７年３月28日

国土交通省港湾局

目次

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

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

はじめに

〔システム構築・運用者編が想定する読者〕

港湾分野の重要インフラ事業者等においては、任務保証の観点から、TOS によるターミナルオペレーション等の安全かつ持続的な提供が求められる。コンテナ荷役の提供を不確かなものとするリスクを許容水準まで低減することは、重要インフラ事業者等として果たすべき社会的責任であり、その実践は経営者層としての責務である。

本ガイドラインの「システム構築・運用者編」では、主に重要インフラ事業者等において TOS 等システムの実装・運用管理を担う担当者を対象にしており、経営者層やセキュリティ責任者の指示に基づき、TOS 等のシステムを構成する機器、ソフトウェア等の各種資源の設計、実装、運用等の実務を担う担当者（外部委託先含む）として対応すべき事項とその考え方を示している。なお、TOS 等システムの実装・運用においては、システムベンダー等に外部委託することも考えられるため、委託事業者においても本編を参照の上、重要インフラ事業者等と協働する必要がある。その際、業務や役割、責任分担のあり方については、あらかじめ両者で取り決めておくことが必要になる。

〔港湾分野における情報セキュリティ〕

港湾分野においては、令和５年７月の名古屋港における情報セキュリティ事案を受けて、「コンテナターミナルにおける情報セキュリティ対策等委員会 取りまとめ」（令和6年1月））において、緊急に実施すべき対応策が示されるとともに、同取りまとめで示された3つの制度的措置（サイバーセキュリティ基本法、港湾運送事業法、経済安全保障推進法それぞれの制度的措置）を進めている。

本ガイドラインは、サイバーセキュリティ基本法に基づき、重要インフラサービスの継続性維持に向けて、重要インフラ事業者等がサイバーセキュリティ確保に向けて、自主的に取組、対策の実施や検証にあたっての目標を定めることを目的として策定したものであり、国が定める「ガイドライン」として推奨事項を列挙しているものである。

重要インフラ事業者等におけるシステム構築・運用者においては、本編を閲読し、理解した上で、必要な措置を講じることが求められる。

〔本ガイドラインの読み方〕

本ガイドラインの「システム構築・運用者編」では、各対策項目について事業者に求める事項を、【事業者に求めること】として四角囲みで記述している。なお、それら事項は、本ガイドラインの性格上、あくまでも推奨事項である。また、【具体例】で示している具体的な対策内容については、2024 年時点の対策技術動向をもとにした内容であり、数年で陳腐化するおそれもあるため、その実装にあたっては、最新の脅威動向・対策技術動向を踏まえた内容にアップデートしていくことが重要である。

また、「経営者層編」、「セキュリティ責任者編」、「システム構築・運用者編」においては、対策内容によっては、読み手間で重複する内容があるため（【導入編 2. 3.3 第１版との関係】の表1参照）、対策の全体像の把握及び対策に関係する主体がどのような対応を実施しているのかを理解するために、関連する他編の章・節を参照することが望ましい。

1　事前準備

1.1　災害による障害の発生しにくい設備の設置及び管理

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●脅威に応じた物理的対策(例)

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

1.2　装置の管理

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●機器・装置等の物理的な保護(例)

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

●電源管理(例)

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

1.3 リモートアクセス環境導入に関する対策基準の策定

【事業者に求めること】

- システム構築・運用者は、リモートアクセス環境をテレワークに適用する場合にはリモートアクセス環境導入に関する対策基準を定めること。

〔解説〕

リモートアクセス環境を利用する際、以下の脅威が想定される。

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

これらのことを踏まえ、リモートアクセス環境導入に関する対策基準を定める必要がある。

〔具体例〕

●リモートアクセス環境をテレワークに導入する場合の対策(例)

- テレワーク勤務者が所有する無線 LAN ルータ等の機器について、ファームウェアを最新版にするようテレワーク勤務者に周知すること。
- テレワーク勤務者が無線 LAN ルータ等の機器を利用する場合は、適切なセキュリティ方式(WPA2、WPA3 等)や第三者に推測されにくいパスワードを利用するようテレワーク勤務者に周知すること。
- 組織の施設外から従業員が作業し、組織内の情報にアクセスする際に行われるテレワークにおいては、以下に例示するトピックについて方針を定め、従業員が遠隔作業している場合のセキュリティ対策を実施すること。
  - ✓ テレワークサイトにおける、他者(家族、友人等)からの情報又は資源への認可されていないアクセスの脅威
  - ✓ 公共の場所にいる他者からの情報又は資源への認可されていないアクセスの脅威
  - ✓ 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項、制限事項
  - ✓ 個人所有機器(BYOD:Bring Your Own Device)の使用
  - ✓ ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用
  - ✓ システムを遠隔で制御し初期化するためのセキュリティに配慮した仕組み(リモートワイプ)の導入
  - ✓ テレワークが終了したときの、権限及びアクセス権の失効
  - ✓ 利用開始及び利用停止時の申請手続の整備
  - ✓ 通信内容の暗号化
  - ✓ 通信を行う端末及び利用者の識別又は認証
  - ✓ 主体認証ログの取得及び管理
  - ✓ リモートアクセス中の他の通信回線との接続禁止

2　平時対策

2.1　不正アクセス等の脅威への対策

2.1.1 利用者アクセスの管理

【事業者に求めること】

- システム構築・運用者は情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、データに対する技術的な安全管理措置を講ずる。
- 外部との接続に係るVPNルータ等のネットワーク機器については、接続元 IP アドレスの指定等予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講ずる。
- システム内部のサーバ機器及びネットワーク機器については、管理者用パスワードの適正な管理等予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講ずる。

〔解説〕

情報セキュリティ責任者(CISO 等)は、重要インフラサービス障害の原因となる不正アクセス等の脅威への対策として、利用者アクセスの管理、主体認証機能及び権限管理機能についてのセキュリティ管理策を対策方針に記載する。

また、制御システム等は、一律に脆弱性対処ができない場合があるので、サイバーセキュリティ上のリスクを評価し把握した上で適切な対策をとることが望ましい。

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

システム構築・運用者は、情報セキュリティ責任者が示す対策方針を踏まえ、情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、データに対する技術的な安全管理措置を講ずることが重要である。

〔具体例〕

●外部との接続に係る不正アクセス対策

VPNルータ等のネットワーク機器については、予め許可された者のみがシステムへの接続が可能となるよう、以下の措置を執ること。

- ✓ 接続元の IP アドレスを指定することで接続元を限定、明確化する。
- ✓ 知識情報(パスワード等、利用者本人のみが知り得る情報)、所有情報(電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)、生体情報(指紋や静脈等、本人の生体的な特徴)のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの(12 文字以上、大小英文字＋数字＋記号を推奨)とする。
- ✓ 識別コードについて、安全な配布方法と運用手順を定めること。
- ✓ アカウントロック機能を実装することが望ましい。
- ✓ 不正ログイン試行を検知する機能(通常とは異なる IP アドレスからシステムへアクセスがあった際にメールで通知等)を実装することが望ましい。

※ 　は、港湾運送事業法では強制要件(全ての港)

※ ___は、港湾運送事業法では強制要件(特定の港(＊注))

＊注：特定の港とは、京浜港、名古屋港、大阪港、神戸港、博多港の5つの港。以下の事項において同様

●TOS 等ネットワーク内のサーバ機器、ネットワーク機器に係る不正アクセス対策

サーバ機器及びシステム内のネットワーク機器については、予め許可された者のみがシステムへの接続が可能となるよう、以下の措置を執ること

- ✓ 管理者の認証に当たっては、知識情報（パスワード等、利用者本人のみが知り得る情報）、所有情報（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）、生体情報（指紋や静脈等、本人の生体的な特徴）のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの（12 文字以上、大小英文字＋数字＋記号を推奨）とする。
- ✓ 識別コードについて、安全な配布方法と運用手順を定めること。

※ ＿＿は、港湾運送事業法では強制要件（特定の港）

※ ＿＿は、港湾運送事業法では強制要件として、管理者用の初期 ID 及びパスワードの変更等の適切な管理が必要。加えて、簡単に推測されない複雑なパスワードが必要。（全ての港）

●利用者アクセスの管理（例）

- 情報システムや情報等へアクセスする利用者とそのアクセス権を管理する。
  - ✓ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。
  - ✓ 利用者アクセス権を定期的にレビューする。
- ユーザアカウントに管理権限を割り当てず、管理権限も用途ごとに設定する（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 離職者のアカウント管理として、全てのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有する全てのユーザアカウントと、組織情報へのアクセスを無効にする。
- 共有アカウントを使用せざるを得ない制御システム等については、セグメントの分割や端末の制限といった対策を活用し、アクセス権を利用する利用者を管理する。

2.1.2 主体認証機能

【事業者に求めること】

- システム構築・運用者は、情報システムについて、情報の格付けに従って、識別及び主体認証を行う機能を設ける。
- 外部との接続に係るVPNルータ等のネットワーク機器については、外部ユーザに対する主体認証を実施する。
- システム内部のサーバ機器及びネットワーク機器については、管理者に対する主体認証を実施する。

〔解説〕

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

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

システム構築・運用者は、情報システムについて、情報の格付けに従って、識別及び主体認証を行う機能を設けること。この際、認可されていないアクセスのおそれを最小限に抑えるため、採用する認証技術や識別コード・主体認証情報の安全管理措置について、適切に設計することが重要である。

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

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

〔具体例〕

●外部との接続に係る主体認証機能

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

- ✓ 知識情報(パスワード等、利用者本人のみが知り得る情報)、所有情報(電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)、生体情報(指紋や静脈等、本人の生体的な特徴)のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの(12 文字以上、大小英文字+数字+記号を推奨)とする。
- ✓ 識別コードについて、安全な配布方法と運用手順を定めること。

※ ___は、港湾運送事業法では強制要件(特定の港)

●TOS 等ネットワーク内のサーバ機器、ネットワーク機器に係る主体認証機能

サーバ機器及びシステム内のネットワーク機器については、管理者の認証方式として、以下の措置

を執ること。(【2.1.1利用者アクセスの管理】参照)

- ✓ 管理者の認証に当たっては、知識情報(パスワード等、利用者本人のみが知り得る情報)、所有情報(電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)、生体情報(指紋や静脈等、本人の生体的な特徴)のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの(12 文字以上、大小英文字+数字+記号を推奨)とする。
- ✓ 識別コードについて、安全な配布方法と運用手順を定めること。

※ は、港湾運送事業法では強制要件として、管理者用の初期 ID 及びパスワードの変更等の適切な管理が必要。加えて、簡単に推測されない複雑なパスワードが必要。(全ての港)

●主体認証方式(例)

- 知識(パスワード等、利用者本人のみが知り得る情報)による認証
- 所有(電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)による認証
- 生体(指紋や静脈等、本人の生体的な特徴)による認証

●取扱者の責任(例)

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

2.1.3 権限管理機能

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●権限管理機能(例)

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

2.2　情報システム等のアクセス制御

2.2.1 アクセス制御機能

【事業者に求めること】

- システム構築・運用者は、各重要システムについて、アクセス制御を行う必要性の有無を検討し、アクセス制御を行う機能を設ける。
- 外部との接続に係るVPNルータ等のネットワーク機器については、アカウントロック機能等により、外部からのアクセスを適切に制御する。
- TOS 等システムと外部システムとが専用線により接続されている場合であっても、ファイアウォール設置等の措置を講じることが望ましい。

〔解説〕

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

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

システム構築・運用者は、情報セキュリティ責任者（CISO 等）が示す対策方針を踏まえ、全ての情報システムについて、アクセス制御を行う必要性の有無を検討して、アクセス制御を行う機能を設けることが重要である。また、取扱者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすることが望ましい。

〔具体例〕

●外部との接続に係るアクセス制御対策

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

- ✓ アカウントロック機能を実装することが望ましい。
- ✓ 不正ログイン試行を検知する機能（通常とは異なる IP アドレスからシステムへアクセスがあった際にメールで通知等）を実装することが望ましい。

※　　は、港湾運送事業法では強制要件（全ての港）

●専用線、NATで外部と接続する場合のアクセス制御対策

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

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

●情報システム等のアクセス制御の導入（例）

＜アクセス制御機能の導入＞

- 利用時間や利用時間帯によるアクセス制御
- 同一主体による複数アクセスの制限
- IP アドレスによる端末の制限
- ネットワークセグメントの分割によるアクセス制御
- 主体認証を受けたユーザのみが与えられた権限の範囲でアクセス可能となる制御
- 公開サーバなど、インターネット上の資産では、悪用可能なサービス（RDP、SSH、SMB 等）を使用しない。また、インターネットに接続された情報資産では、不要なアプリケーションやネットワークプロトコルを全て無効化する。
- 運用上明示的に必要な場合を除き、制御システムはインターネット上には配置しない。例外が存在する場合には承認、文書化し、悪用を防止する措置を具備する。悪用防止の措置として、多要素認証や VPN の活用、ロギングによる動作の監視等が挙げられる。また、OT ネットワークへの接続は、特定の機能のため明示的に許可された通信を除き、全て拒否する。IT と OT 間の必要な通信経路にはファイアウォール等中継装置を設置し、厳密に通信を監視する。中継となるファイアウォール装置の設定、脆弱性についても適切に維持管理する。
- インターネットに接続された情報システムについて、サービス不能攻撃（DoS/DDoS 攻撃）を受けるサーバ装置（IoT 機器を含む。）、端末、通信回線装置又は通信回線から監視対象を特定し、システムが扱う情報の可用性に基づいてサービス不能攻撃の発生を想定し、対応を行う。

＜アカウントロック＞

- 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する。

2.2.2 パスワード管理

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●パスワード管理(例)

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

2.3 暗号を活用した情報管理

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●暗号化機能及び電子署名の付与機能の導入（例）

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

●暗号化及び電子署名の付与に係る管理（鍵管理も含む）（例）

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

2.4 負荷分散・冗長化

【事業者に求めること】

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

〔解説〕

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

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

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

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

〔具体例〕

●バックアップシステム

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

●負荷分散・冗長化の対策(例)

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

---

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

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

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

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

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

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

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

2.5　多層防御

【事業者に求めること】

- システム構築・運用者は、重要業務を行う端末、ネットワーク、システム又はサービスには、多層防御を導入することが望ましい。

〔解説〕

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

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

サイバー攻撃の高度化により従来型の境界防御のみでは侵入を検知することが困難であるため、複数の対策を組み合わせ、一つの対策で防御できなくても次の対策で防御または検知するという考え方のもと、セキュリティ対策を検討することが重要である。

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

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

〔具体例〕

●入口対策(例)

- 不要なサービスについて機能を削除又は停止する。
- 不審なプログラムが実行されないよう設定する。
- パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

●内部対策(例)

- 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。
- 不要な管理者権限アカウントを削除する。
- 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。
- EDR(Endpoint Detection and Response)等によるソフトウェアの挙動監視により未知のマルウェア等を検知する。

2.6　資産のセキュリティ運用

2.6.1 情報システムの構成要素の運用

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●端末の運用時・運用終了時の対策(例)

＜システム構築・運用者による対策＞

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

＜端末を利用する取扱者による対策＞

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

●サーバ装置の運用時・運用終了時の対策(例)

<システム構築・運用者による対策>

- サーバ装置について、構成管理・変更管理を実施すること。また、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。
- 管理者の認証に当たっては、知識情報(パスワード等、利用者本人のみが知り得る情報)、所有情報(電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)、生体情報(指紋や静脈等、本人の生体的な特徴)のうち複数の情報を必要とする認証方式とする。特に、パスワードを使用する際は、簡単に推測されない複雑なもの(12 文字以上、大小英文字+数字+記号を推奨)とすること。その際、認証コードの安全な配布と運用手順を定めること。
- サーバ装置に保存されている情報について、情報の格付けに従って、定期的にバックアップを取得すること。また、取得した情報を記録した媒体について、安全管理措置を講ずること。
- サーバ機器のログを定期的に取得するとともに、システム外にバックアップを保存すること。
- サーバ機器に対して基幹 OS の付属品以外のセキュリティ対策ソフトを導入し、ウイルスパターンを常時最新のものにすること。
- サーバ装置のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、定期的に更新を行うとともに、不正行為及び不正利用を含むトラブル事象の発生を検知するための措置を講ずること。
- サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

●通信回線及び通信回線装置の運用時・運用終了時の対策(例)

<システム構築・運用者による対策>

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

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

<システム構築・運用者による対策>

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

2.6.2 情報システムの監視

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●情報システムの監視(例)

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

2.6.3 情報システムの更改・廃棄時の措置

【事業者に求めること】

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

〔解説〕

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

〔具体例

●情報システムの更改・廃棄時の措置(例)[6]〕

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

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

2.6.4データ管理

【事業者に求めること】

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

〔解説〕

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

事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意することが重要である。(【セキュリティ責任者編1.6クラウドサービス】参照)

2.7　サイバー攻撃等に備えた運用管理

2.7.1 マルウェアからの保護

【事業者に求めること】

- システム構築・運用者は、マルウェア感染の回避を目的とし、取扱者に対する日常的実施事項を定める。
- 外部接続するネットワーク機器、及び TOS 等ネットワーク内のサーバ機器等に係る適切なマルウェア対策を講じる。
- 外部記憶媒体(USB)を利用する際には、マルウェア感染回避のための、適切な運用ルールを定め実施する。

〔解説〕

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

なお、クラウドサービスを利用して TOS 等の機能を実現している場合においても、マルウェアからの保護や不正アクセス対策を実施するとともに、情報保管管理等のセキュリティ要件をクラウドサービスに求め、契約内容にも含めることが重要である。

〔具体例〕

●外部接続するネットワーク機器に係るマルウェア対策

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

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

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

※　　は、港湾運送事業法では強制要件(全ての港)

●TOS 等ネットワーク内のサーバ機器等に係るマルウェア対策

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

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

パターンを常時最新のものに更新する。

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

※ 　は、港湾運送事業法では強制要件(全ての港)

●外部記憶媒体(USB 等)に係るマルウェア対策

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

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

※ ___は、港湾運送事業法では強制要件(特定の港)

●マルウェア対策(例)

<システム構築・運用者による対策>

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

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

2.7.2 バックアップ

【事業者に求めること】

- システム構築・運用者は、システム障害やサイバー攻撃発生に備え、バックアップを適切に取得する。
- 取得したバックアップは、現用システムとは切り離した場所に保存する。

〔解説〕

緊急事態発生時でも、重要な情報の参照及び、情報システムを使用できることが求められる。しかし、緊急事態発生時には、通常業務に必要なデータの欠落や不整合による障害が発生するおそれがある。これらを防ぐための詳細な復帰計画をあらかじめ策定しておくことが重要である。

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

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

〔具体例〕

●バックアップ

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

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

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

※ ＿＿は、港湾運送事業法では強制要件（全ての港）

●バックアップ方式の検討（例）

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

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

●バックアップ取得管理状況の把握(例)

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

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

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

＜バックアップの保持期間・世代管理の考え方について＞

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

2.7.3 ログ取得

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●TOS 等ネットワーク内のサーバ機器、ネットワーク機器のログの取得

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

※ 　は、港湾運送事業法では強制要件(全ての港)

●ログの取得・管理の対策(例)

＜システム構築・運用者の対策＞

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

●ログとして記録することが望ましい項目(例)

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

2.7.4 運用ソフトウェアの管理

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●外部接続するネットワーク機器に係る運用ソフトウェアの管理

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

※ は、港湾運送事業法では強制要件(全ての港)

●TOS 等ネットワーク内のサーバ機器等に係る運用ソフトウェアの管理

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

●運用ソフトウェアの管理(例)

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

2.7.5 脆弱性の管理

【事業者に求めること】

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

〔解説〕

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

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

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

〔具体例〕

●脆弱性の管理(例)

＜システム運用・構築者の対策＞

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

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

2.7.6 電子メール運用時の対策

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●電子メール運用時の対策(例)

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

3　インシデント発生時及び事後対応

3.1　インシデント発生時のコンティンジェンシープランの実行

【事業者に求めること】

- システム構築・運用者は、セキュリティインシデントが発生した場合には、コンティンジェンシープランに従い、早急にその状況を把握し、被害の拡大防止、早期復旧のための対策を講ずる。

〔解説〕

セキュリティインシデントの発生及びそれによる重要インフラサービス障害が発生した場合には、早急にその状況を把握し、被害の拡大防止、早期復旧のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定められた責任者へ報告し、障害による影響や範囲をエスカレーションし、二次被害を最小限に抑えることが重要である。

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

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

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

〔具体例〕

●コンティンジェンシープラン及び BCP の実行（例）

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

●インシデント対応フロー（例）

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

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

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

●インシデント対応の流れ(例)

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

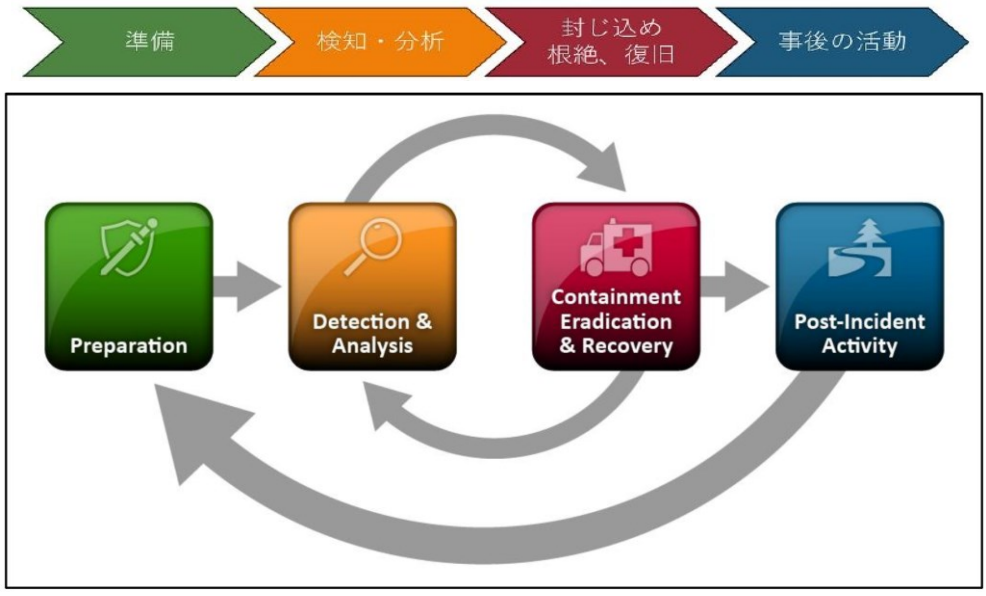

Figure 3-1. Incident Response Life Cycle

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

別紙1 システムの取得・開発・保守に係るセキュリティ管理策

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

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

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

1.1 情報システムの取得・開発・改善における要求事項の確認

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●情報システム開発時のセキュリティ要件(例)

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

1.2 情報システムのセキュリティ要件

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

1.2.1 情報システム企画・要件定義

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●情報システムのセキュリティ要件(例)

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

●望ましいセキュリティ管理策(例)

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

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

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

1.2.2 情報システムの構築

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●望ましいセキュリティ管理策(例)

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

1.3 端末、サーバ装置、複合機及び特定用途機器

1.3.1 端末

【事業者に求めること】

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

〔解説〕

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

講ずる必要がある。

〔具体例〕

●モバイル端末の管理とセキュリティ対策(例)

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

●推奨対策項目(例)

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

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

●モバイル端末に対する推奨対策項目(例)

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

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

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

1.3.2 サーバ装置

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●サーバ装置の安全運用とセキュリティ対策(例)

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

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

1.3.3 複合機及び IoT 機器を含む特定用途機器

【事業者に求めること】

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

〔解説〕

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

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

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

〔具体例〕

●複合機の対策(例)

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

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

●IoT 機器を含む特定用途機器の対策(例)

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

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

1.3.4 端末、サーバ装置、複合機及び特定用途機器の調達

【事業者に求めること】

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

〔解説〕

上記に示す端末、サーバ装置、複合機及び IoT 機器を含む特定用途機器は運用段階だけでなく、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクが懸念される。したがって、これらの機器の調達に当たっては、サプライチェーン等に関わる事業者についても、サイバーセキュリティ基本法第7条(サイバー関連事業者その他の事業者の責務)の責務があることを踏まえた対応が必要である。

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

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

望ましい。

〔具体例〕

●政府機関等の対策基準策定のためのガイドラインの記載内容（抜粋）

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

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

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

1.4 アプリケーション

1.4.1 電子メール

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●電子メールのリスク管理とセキュリティ強化（例）

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

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

1.4.2 ウェブ

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●ウェブサーバの脆弱性対策(例)

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

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

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

1.4.3 ドメインネームシステム（DNS）

【事業者に求めること】

➢ DNS 導入時は、サーバ管理などの適切な対策が必要である。

〔解説〕

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

〔具体例〕

●DNS サーバ維持と運用管理（例）

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

＜DNS 導入時の対策＞

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

＜DNS 運用時の対策＞

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

1.4.4 データベース

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●データベースのセキュリティ管理(例)

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

1.4.5 Web 会議

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●Web 会議におけるリスク管理と対策(例)

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

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

1.5 通信回線及び通信回線装置

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

1.5.1 通信回線共通対策

【事業者に求めること】

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

〔解説〕

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

〔具体例〕

●通信回線の構築時に講ずることが望ましい対策(例)

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

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

1.5.2 リモートアクセス環境導入時の対策

【事業者に求めること】

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

〔解説〕

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

VPN 回線及び公衆電話網を利用する際は、以下の対策を講ずる必要がある。

〔具体例〕

●VPN 回線利用時の対策（例）

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

・ リモートアクセス中の他の通信回線との接続禁止

●公衆電話網利用時の対策(例)

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

1.5.3 無線 LAN 環境導入時の対策

【事業者に求めること】

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

〔解説〕

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

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

〔具体例〕

●無線 LAN セキュリティ強化の対策(例)

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

1.5.4 IPv6 (Internet Protocol Version 6)通信回線

【事業者に求めること】

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

〔解説〕

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

あることから、必要な対策を講じていく必要がある。

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

〔具体例〕

●IPv6 のセキュリティ対策(例)

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

1.5.5 5G /ローカル 5G 通信回線

【事業者に求めること】

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

〔解説〕

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

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

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

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

〔具体例〕

●ローカル 5G 機器と SIM 認証のセキュリティ対策(例)

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

●参考とするガイドライン例

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

必要な対策を講ずることが望ましい。

＜参考ガイドライン例＞

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

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