# 鉄道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5版

令和6年４月18日　改定

国土交通省

# 目次

# はじめに

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある。また、重要インフラはその性質上、安全かつ持続的なサービス提供が求められていることから、その防護に当たっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を可能な限り減らすとともに、障害発生の早期検知や、障害の迅速な復旧を図ることが重要である。

国土交通省では、所管する4分野(鉄道、航空、空港、物流)における各事業分野、及び関連事業者のセキュリティ管理策の現状に配慮しながら、各事業分野におけるセキュリティ管理策の向上に資する望ましいセキュリティ管理策の水準をまとめ、サイバーセキュリティ確保に係る安全ガイドラインを策定しており、各分野の安全ガイドラインの初版策定以降、指針の改正や世の中の情勢を踏まえ、適宜本ガイドラインを改定することとしている。

昨今、新型コロナウィルス感染症の影響により、我が国の社会・経済活動は大きな打撃を受け歴史的な変革を求められており、テレワークや WEB 会議、クラウドサービス、IoT 等の ICT を活用することによる緊急事態発生時での事業継続、働き方改革への対応、事業者が行うデジタルトランスフォーメーション(DX)及び Society 5.0 への対応等、従来のサイバーセキュリティモデルでは十分賄えない新たな課題が生まれている。このような加速度的に進んでいるサイバーセキュリティを取り巻く環境変化に対応するため、関連する最新の基準、ガイドライン等に基づき、ニューノーマル時代に求められるサイバーセキュリティモデルに即した安全ガイドラインとなるよう「鉄道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 5 版」に改定したものである。

# 1 「安全ガイドライン」策定の背景

## 1.1 「安全ガイドライン」の目的と位置づけ

### 1.1.1「安全ガイドライン」の目的

重要インフラ事業者等は、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場であり、「重要インフラのサイバーセキュリティに係る行動計画(2022 年 6 月 17 日)」に記載された「任務保証(【1.1.5「安全ガイドライン」における用語の定義(9)】参照)の考え方」を踏まえ、サービスの提供に必要な情報システム(【1.1.5「安全ガイドライン」における用語の定義(5)】参照)のセキュリティを確保するなど、必要な対策に取り組むことが重要である。具体的には、サイバーセキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を実現することなどであり、特に、経営層(【1.1.6 責任者・組織等の役割(1)】参照)が積極的に関与し、サイバーセキュリティに係るリスクへの備えを経営戦略として位置付け、サイバーセキュリティに係るリスクマネジメントの実施等により、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要となっている。

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

### 1.1.2「安全ガイドライン」の形態

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

このことを踏まえ、「指針」においては、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「安全基準等」と呼び、次の①～④に分類している。

① 関係法令に基づき国が定める「強制基準」
② 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
③ 関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④ 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

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

本ガイドラインは②に対応し、国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に参考資料として活用することを想定している。

### 1.1.3「安全ガイドライン」の位置づけ

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

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

このため、「安全ガイドライン」における対策項目は、「指針」で示されている文書構成に沿って、「指針」及び以下に示す「政府機関のサイバーセキュリティ対策のための統一基準群」を始めとした国内外で用いられるベストプラクティスやスタンダード(基準)等を基に、各分野において必要と想定される事項を補足して構成する。

(1)重要インフラのサイバーセキュリティに係る安全基準等策定指針

重要インフラにおける任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、安全基準等において規定が望まれる項目を整理・記載したもの。

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

平成 18 年 2 月に制定後、現在、令和 5 年 7 月 4 日に令和 5 年度版がサイバーセキュリティ戦略本部決定されている。

(2)政府機関等のサイバーセキュリティ対策のための統一基準群

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

(3)情報セキュリティ管理基準

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

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

(4)事業継続ガイドライン

内閣府の取り組みとしての事業継続計画の普及、促進のため、中央防災会議「民間と市場の力を活かした防災力向上に関する専門委員会」の下に設置された、「企業評価・業務継続計画ワーキンググループ」において作成されたガイドライン。

平成 17 年 8 月 1 日に第一版が発行されており、現在、平成 25 年 8 月に第三版が発行されている。

(5) 個人情報の保護に関する法律についてのガイドライン(通則編)

個人情報の保護に関する法律の第七条第一項の規定に基づき定められた「個人情報の保護に関する基本方針」(平成 16 年 4 月 2 日閣議決定)を受け、事業者が個人情報の適正な取扱い確保に関して行う活動を支援すること、及び当該支援により事業者が講ずる措置が適切かつ有効に実施されることを目的として、個人情報の保護に関する法律(平成 15 年法律第 57 号)第 4 条、第 8 条及び第 60 条に基づき具体的な指針を定めたガイドライン。

(6)その他参考となるガイドライン

・ISO/IEC27000 ファミリー

情報セキュリティマネジメントシステム(ISMS)に関する国際規格であり、要求事項を規定した規格と、ISMS 実施の様々な側面に関する手引きを規定した規格から構成されている。

・IEC 62443 シリーズ

制御システムの全ての機器、装置を対象にした国際標準規格である。産業用オートメーション及び制御システム(IACS:Industrial Automation and Control System)の認証制度については、情報セキュリティマネジメントシステム(ISMS)をベースにした IACS のためのセキュリティマネージメントシステムが IEC 62443-2-1 として規格化されており、事業者の IACS が IEC 62443-2-1 に準拠していることを認証する「CSMS 認証基準(IEC62443-2-1)(JIP-CSCC100-1.0)」があり、JIPDEC(一般財団法人日本情報経済社会推進協会)が運営をしている。

・制御システムのセキュリティリスク分析ガイド

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

・サイバーセキュリティ経営ガイドライン

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

・重要インフラのサイバーセキュリティを向上させるためのフレームワーク

米国国立標準技術研究所(NIST)が、サイバーセキュリティの効果的・効率的なリスク低減を実現するために「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能から、適切なサイバーセキュリティ対策のあり方を示し、2014 年に公開している。
※国際規格や各国が定めたガイドラインではないが、さらに参考として、一般社団法人運輸総合研究所が発行しているサイバーセキュリティに関する各種手引き等もある。

(7) 内部統制システムとサイバーセキュリティとの関係

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

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

### 1.1.4「安全ガイドライン」の見直し

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

よって、国土交通省及び所管する重要インフラ分野の事業者等は、相互に協力し、各重要インフラ分野における重要インフラサービス障害(【1.1.5「安全ガイドライン」における用語の定義(2)】参照)の発生状況等を踏まえ、「安全ガイドライン」が適宜適切なものとなるよう、随時検討を行っていく。

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

### 1.1.5「安全ガイドライン」における用語の定義

本ガイドラインにおいて使用する用語の定義は、次の各項に定めるところによる。

(1)重要インフラ事業者等

サイバーセキュリティ基本法第 12 条第 2 項第 3 号に規定する重要社会基盤事業者等であり、具体的には、重要インフラ事業者及びその組織する団体並びに地方公共団体から構成される。

(2)重要インフラサービス障害

システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じることをいう。

(3)重要インフラ利用者

重要インフラ事業者等が提供する重要インフラのサービスを利用する者をいう。

(4)取扱者

重要インフラ事業者等が保有する重要インフラに関する情報システム及び情報資産を取り扱う重要インフラ事業関係者(情報資産や情報システムを直接扱う者を監督する立場にある者(経営層や幹部など)、委託先の関係者などを含む。)をいう。

(5)情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいう。サーバ装置、端末、通信回線装置、複合機、IoT 機器を含む特定用途機器(フィールド機器や監視・制御システム等の制御システム等で使われるものを含む。)、ソフトウェアが含まれる。

(6)制御システム

鉄道インフラの重要システムである列車運行管理システム等において、信号や踏切を制御するための機械や設備があり、それを制御する端末及び、列車運行管理システム等とネットワークで接続されている機械や設備、その構成要素を指す。

(7)情報資産

以下の 2 つの情報をいう。

・ 取扱者が業務上使用することを目的として重要インフラ事業者等が調達し、又は開発した情報システム若しくは 外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)

・ 重要インフラ事業者等が調達し、又は開発した情報システムの設計又は運用管理に関する情報

(8)重要システム

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

(9)任務保証

重要インフラ事業者等や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方をいう。

(10)サプライチェーン

一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活

動の川上から川下に至るまでのモノや情報の流れのこと。広義では海外拠点やグループ会社、関連団体も含められる。これらに加えてさらに、IT におけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。

(11)セプター
重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。

(12)セプターカウンシル
各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。

(13)IT-BCP 等
重要インフラサービスの提供に必要な情報システムに関する事業継続計画(関連マニュアル類を含む。)その他の事業継続計画。

(14)コンティンジェンシープラン
重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。

### 1.1.6 責任者・組織等の役割

各重要インフラ事業者等内における責任者・組織等の役割を以下のとおり定義する。
なお、該当する責任者・組織等そのものが存在しない場合、同様の役割を担っている役割・組織等に読み替えること。

(1) 経営層
経営層は、重要インフラ事業者等の社会的責任として、サイバーセキュリティを確保するよう取り組むこと。また、自らがリーダーシップを発揮し、任務保証の考え方を踏まえて対応すること。
なお、重要インフラのサイバーセキュリティに係る行動計画(2022 年 6 月 17 日)に示されたように、組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。
また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

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

（2）最高情報セキュリティ責任者（CISO）

最高情報セキュリティ責任者は事業者内における情報セキュリティ対策の推進の責任者（役員クラスが相当）であり、対策を推進する上での最終決定権及び責任をもつこと。

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

（3）情報セキュリティ委員会

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

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

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

（4）サイバーセキュリティ責任者

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

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

（5）システム管理者

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

（6）セキュリティリスクアセッサー（評価者）

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

（7）CSIRT（Computer Security Incident Response Team）

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

（8）取扱者

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

## 1.2 「安全ガイドライン」の運用について

### 1.2.1 重要インフラ事業者等の担う範囲

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

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

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

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

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

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

### 1.2.2 適用状況の評価について

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

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

（1）ISMS 適合性評価制度

重要インフラ事業者等の組織が情報を適切に管理し、機密を守るための包括的な枠組みである。

コンピュータシステムに係るセキュリティ管理策だけでなく、情報を扱う際の基本的な方針としてのセキュリティ方針や、それに基づいた具体的な対策の計画・実施・運用、及び見直しまでを含んでいる。

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

(2) プライバシーマーク制度

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

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

(3) IT セキュリティ評価及び認証制度 (JISEC)

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

(4) 情報セキュリティ監査制度

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

# 2 鉄道分野における「安全ガイドライン」の概要

## 2.1 鉄道分野における現状と課題

### 2.1.1 鉄道分野におけるセキュリティ管理策の現状

鉄道分野において、国民生活や社会経済活動に影響を及ぼし事業継続の取り組み対象となるような重要システムには「列車運行管理システム」、「電力管理システム」及び「座席予約システム」等がある。

これらの情報システムに障害が生じた場合でも、緊急の対応として人手による運用が可能であるものの、代替運用時においては作業効率が低下するため、システム利用頻度の高い時間帯などでは遅延の発生や運行等への支障の発生が予想される。

鉄道分野はその事業特性から、顧客向けのウェブサービス（座席予約等）を保有している事業者も多く、パスワードリスト攻撃による顧客情報の流出・不正操作という重要インフラサービス障害が発生する可能性がある。

鉄道分野においては、各種保安設備のDX化に伴う各種センサーの増加、安全意識の高まりによる防犯カメラの普及が行われ、その効率化のためネットワーク化が進んでいる。保安設備へのサイバー攻撃は鉄道人身事故を含む重大な被害をもたらすおそれがある。また、防犯カメラやその他情報の完全性・可用性が損なわれることそのものが、鉄道事故に直結することはまれと考えられるが、物理的な攻撃と組み合わせたテロ・犯罪の一環として行われる可能性もあり、この点もサイバーセキュリティに関する新たなリスクとして注視しておく必要がある。

### 2.1.2 鉄道分野のセキュリティ管理策における課題

鉄道分野の重要インフラ事業者等は、マルウェア感染や外部からの攻撃を防止する対策については各々実施している。しかし、先に述べたパスワードリスト攻撃や標的型攻撃、ランサムウェア攻撃等をはじめとする昨今の複雑・巧妙化するサイバー攻撃全てを防ぐことは困難である。また、外部ネットワークと内部ネットワークとの境界による防御には限界があることから、従来の境界型のセキュリティ管理策に加え、内部ネットワークにも脅威が存在しうることを前提としたゼロトラストの考え方に基づき、データや機器等の単位でのセキュリティ管理策が必要である。

また、多くの重要インフラ事業者等で、セキュリティ管理策の継続的改善の実施が不十分であるという課題認識があることから、それぞれの事業者が目標とするセキュリティ水準に向けたセキュリティ管理策の継続的改善の実施が必要である。

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

### 2.1.3「安全ガイドライン」の特徴

本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、鉄道分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめた。

## 2.2 「安全ガイドライン」の対象範囲

### 2.2.1 鉄道分野におけるセキュリティ管理策の現状

本ガイドラインにおける保護対象は、「重要インフラのサイバーセキュリティに係る行動計画（2022 年 6 月 17 日）」別紙1に掲げる「対象となる重要インフラ事業者と重要システム例」及び同別紙2に掲げる「重要インフラサービスとサービス維持レベル」等の内容を踏まえ、鉄道分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産である。

例えば、重要インフラサービス障害の発生によって列車運行の遅延、運休や列車の安全安定輸送に対する支障などの影響を及ぼす以下の重要システム及びその中で利活用される情報資産が挙げられる。

なお、例示された重要システム以外についても、事業者の責任において検討し抽出する必要がある。

① 列車運行管理システム

列車運行管理システム（PTC：Programmed Traffic Control）は、線区内の転てつ機および信号機を中央の指令所で集中制御する機能に加え、自動的に進路制御を行う機能、運転ダイヤの整理機能等を備えた統括的なシステム。従来の信号扱い所にて人が連動装置の取り扱いを行っていたものを中央に集約するとともに、機械によるダイヤ作成を行うことができ、信号扱い業務を効率化することができる。各駅に設置された駅制御装置を運転指令所にある制御装置と、主に光ファイバーによるネットワークにて接続される構成。

システムの構成要素：

・ 列車集中制御装置（CTC：Centralized Traffic Control）

運転指令所から線区内の列車を監視し、各駅の信号機や分岐器の連動装置を遠隔制御するための装置。

・ 自動進路制御装置（PRC：Programmed Route Control）

運転指令業務の効率化を図るため、ダイヤによる定常的な列車の進路制御（信号や分岐器）を自動化する装置のこと。一般には CTC と接続して使用されるもの。

② 電力管理システム

電力管理システムは、安定した電力供給、列車運行を支えるため、各変電所の変電設備及び変電所から列車や信号設備、駅舎等への電力供給系統を、中央の電力指令所から監視・制御するためのシステム。

機器運転状況のモニタリング・入切、異常が生じた場合の警報を発報する等の機能を有している。

③ 座席予約システム

特急等の座席予約を行うためのシステム。駅窓口の係員や、利用者が駅券売機又はインターネットを介して利用することができる、乗車券の発売や払戻、空席照会等の操作を即時に処理するシステム。

サーバシステムは自組織内又はデータセンターに設置するオンプレミスの場合や、クラウドサービス内に設置している場合がある。

## コラム
## 鉄道インフラにおけるサイバーセキュリティ・インシデント事例

**◆2022 年 9 月　国内地下鉄 複数の事業者**

新ロシア派ハッカー集団キルネットによる DDoS 攻撃を受けた事業者のウェブサイトが繋がりにくい状態となった。DDoS 攻撃は大量の通信を送り付け、サーバや回線をパンクさせる攻撃である。本事案では、一時的に「現在サーバが大変混みあっております」とサイト上で表示されたが、数時間後にサイトが復旧した。実際の運行には影響がなかった。

（出典：各鉄道事業者ウェブサイト、各報道機関の情報）

**◆2022 年 11 月 デンマーク DSB**

同国最大手鉄道ネットワーク DSB がソフトウェアテスト環境下でハッカーによる攻撃を受け、システムのシャットダウンを行ったため、運行状況に必要なデータに運転手がアクセスすることができなくなり、またマニュアル作業への切り替え対応が迅速に対応できなかったため、同社の安全確認手続きに従い、4 時間程度運行停止となった。

（出典：ANNUAL REPORT 2022, DSB）

**◆2021 年 12 月　カナダ　GoTransit**

GO Transit 列車は運行可能であったが、Java スクリプトの脆弱性を利用した攻撃により web サイトが不通となり、web ベースのサービスが 24 時間停止した。

（出典：Center for Strategic & International Studies）

**◆2021 年 9 月　イラン鉄道**

国営放送 IRIB が報じたところでは、イラン鉄道ネットワークにハッカーが侵入し、切符売り場、国鉄のウェブサイト、貨物のサービスが中断されたため、列車の遅延や運休が発生し、「国内の鉄道駅で前例のない混乱」が発生した。駅の電光掲示板には、最高指導者アヤトラ・アリ・ハメネイ師の事務所の番号に電話するよう鉄道利用者に呼びかける通知が映し出されていたと報じられている。

（出典：Center for Strategic & International Studies、ロイター通信）

**◆2020 年 3 月 イタリア Ferrovie dello Stato Italiane（FS）**

イタリアの国営鉄道会社 Ferrovie dello Stato Italiane（FS）は、サイバー攻撃の標的になっている恐れから、一部のチケット販売サービスを一時的に停止したと述べた。民間鉄道会社のトレニタリアと RFI のコンピュータネットワークで、クリプトロッカー感染に関連する可能性のある要素が検出された。国営鉄道会社 FS は、予防措置として、オフィスでのチケット販売と駅の自動販売機での販売を停止し、オンライン販売は通常通り機能していると述べた。鉄道の運行には影響がなかった。

（出典：ロイター通信）

**◆2017 年 10 月 スウェーデン公共交通 Trafikverket**

2017 年 10 月 11 日、スウェーデン運輸局(Trafikverket)にサービスを提供している 2 つの通信サービス・プロバイダーが DDoS 攻撃に見舞われ、列車管理システムが停止。

翌日、DDoS 攻撃は、スウェーデン運輸局(Transportyrelsen)と西スウェーデンにサービスを提供する公共交通機関(Västtrafik)を標的にした。 攻撃の影響はそれほど深刻ではなく、チケット予約を含む Web サービスに一時的に影響を及ぼすに留まった。

その結果、鉄道交通サービスを提供するため作業を手動で行う必要があり、その日の残りの列車に遅れが出た。同社はまた、電子メールシステムと Web サイトも利用できなくなり、Facebook を使用して顧客に最新の状況をアナウンスする必要性があった。

全体として、このケースは、運輸サービスがサード・パーティのサービス・プロバイダー(本件の場合は Trafikverket の通信サービス・プロバイダー)への攻撃によってどのように影響を受ける可能性があるかについて明らかにする事例となった。

(出典:英国国家サイバーセキュリティセンター)

**◆2008 年 1 月 ポーランド ウッチ市営トラム**

攻撃者は何ヶ月もかけて市内の線路を調査し、列車の方向を変えた際に最も大混乱を引き起こすのに最適な場所を特定した。古いテレビのリモコンを改造し、トラムと線路切替スイッチを作動させることができる赤外線送信機に変換した。4 台のトラムが脱線、12 人が怪我。セキュリティに疎いエンジニアによってシステムが構築されていたことが問題であり、業界で定められているセキュリティ水準はあってもそのレベルが低かった。輸送指揮統制システムは、汎用電子機器と一般的な知識を用いて構築されたものであり、セキュリティに関する知識や知識がほとんどないエンジニアによって設計されていることが多かった。後に改善策が取られた。

(出典:ENISA 等複数ソースより)

COLUMN

## コラム
## （物流分野）国内におけるサイバーセキュリティ・インシデント事例

**◆2023 年 7 月 名古屋港**

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

**＜被害＞**

物理サーバ基盤及び全仮想サーバが暗号化され、以下の影響を与えた。

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

その他、トヨタ自動車の愛知県と岐阜県にある４ つの拠点の稼働停止、アパレルメーカーにおける衣類の入荷遅延等の経済活動への影響も報道されている。

**＜感染経路＞**

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

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

**＜対応＞**

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

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

7 月6 日、14:15 頃 データと実在庫情報の整合性の確認を開始。準備が整ったターミナルより順次再開した。

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

（出典：コンテナターミナルにおける情報セキュリティ対策等検討委員会資料）

**(航空分野)大規模な情報流出の事例**

**◆2021年3月 SITA**

世界の航空業界の約90%にサービスを提供する情報通信企業である SITA 社は、2021 年 3 月 4 日、SITA Passenger Service System(SITA PSS)が管理している顧客データの一部がサイバー攻撃を受けて漏洩したことを発表した。SITA PSS は航空会社向けの旅客処理システムを運営している。

SITA は、2021 年 2 月 24 日(スイス時間)に確認されたデータセキュリティインシデントの事態が明らかになってからすぐに SITA Passenger Service System の顧客および関連組織へ連絡を取ったと説明。サイバーセキュリティの主要な外部専門家の支援を受けて、SITA のセキュリティインシデント対応チームによって引き続き調査されると説明している。

＜被害＞

ルフトハンザ、ニュージーランド航空、シンガポール航空、マレーシア国空、チェジュ航空等スターアライアンス、ワンワールド加盟航空会社が多数影響を受けており、同年 5 月にはエア・インディアは 450 万人の個人情報が流出したと発表している。このサイバーインシデントは日本の航空会社にも影響を与えている。

(出典:SITA、各種報道資料をもとに作成)

**国内におけるサプライチェーンに起因する情報流出の事例**

◆2021 年 3 月 LINE 株式会社

3 月 17 日、LINE 株式会社(現:LINE ヤフー株式会社)は、業務委託している中国の関連会社従業員が国内の個人情報データにアクセス可能な状態だったと発表した。関連会社は違反通報内容の分析ツールなどの開発業務を受託しており、2018 年 8 月から 2021 年 2 月までの期間、氏名、電話番号などのほか、通報内容にあたる「トーク」機能内や利用者が保存したメッセージ、画像等を閲覧できる状態であった。同社は業務上適切なもので、不正アクセスや情報漏洩はないと説明している。同日、対話アプリのデータ管理体制に関しても発表があった。利用者間の対話履歴や会員情報などプライバシー性の高い情報は国内サーバで管理していたが、画像や動画、LINE Pay の取引情報の一部といったデータは韓国のデータセンターで管理していた。画像や動画データは「適切なセキュリティ体制のもとで管理している」としている。今後、中国における開発拠点および外部委託先における個人情報へのアクセスコントロール等の実施、段階的なデータの国内移転、ユーザーへの説明をより一層明確化するなどプライバシーポリシーの改定やデータ・セキュリティのガバナンス体制と情報保護の強化に取り組むとしている。

＜LINE 株式会社が認識している問題点＞

・中国で個人情報にアクセスする業務を実施したこと

・トーク上の画像や動画などを韓国で保管したこと

・プライバシーポリシーで第三国へのデータ移転について明記していたものの国名の記載がなく透明性を欠いたこと

＜その後の影響＞

・LINE 株式会社は、全容把握のために外部有識者を含む第三者委員会を立ち上げたほか、総務省、個人情報保護委員会、金融庁にも報告書を提出した。

・LINE は一部自治体で住民票や給付金などの申請窓口や新型コロナウィルスワクチンの予約システムを提供するなど社会インフラとしての性格を強めている。本インシデントを受け、政府の「データ管理の適正性等に関するタスクフォース」において、「政府機関・地方公共団体等における業務での LINE 利用状況調査を踏まえた今後の LINE サービス等の利用の際の考え方(ガイドライン)がとりまとめられた。

・令和 2 年改正個人情報保護法において、外国にある第三者への個人データの提供時に、移転先の所在国、当該外国における個人情報の保護に関する制度、移転先が講ずる個人情報の保護のための措置の情報を提供すること等が追加された。

(出典:LINE、総務省、個人情報保護委員会、各種報道資料をもとに作成)

# 3　組織統治におけるサイバーセキュリティ

鉄道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、「旅客輸送サービス」及び「発券、入出場手続」等[1]の安全かつ持続的な提供が求められる。旅客輸送サービス等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、鉄道事業者として果たすべき社会的責任であり、その実践は経営層としての責務である。

この点については、「サイバーセキュリティ経営ガイドライン　Ver.3.0」(経済産業省・独立行政法人　情報処理推進機構刊)においても「サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、その観点からサイバーセキュリティリスクを把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。」とされており、経営上の重要課題として必要な人材・資金を投入するとともに、危機管理においては自らがプレイヤーになり得る経営課題であるとの認識が不可欠である。

本章では、旅客輸送サービス等の安全かつ持続的な提供にあたり、組織統治の取組において望まれる、経営層が実践すべきサイバーセキュリティ確保のための事項を示す。

## 3.1　組織方針

**【主旨・目的】**

サイバー空間からのリスクは任務保証を阻害しうるものであることを踏まえ、組織全体でサイバーセキュリティ確保に努めるため、組織方針においてその実践を明記し、宣言する。

### 3.1.1 組織方針とサイバーセキュリティ

**【対策項目】**

組織方針(経営方針、リスクマネジメント方針等)にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れる。例えば、「重要インフラサービスの安全かつ持続的な提供を実現する」「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」といった要素を盛り込み、また、あわせて維持するサービス範囲・水準を示すことが望ましい。

- **取組むべき事項**

経営層は、組織方針(経営方針・リスクマネジメント方針等)にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れる。

**【組織方針に組み入れる事項例】**

- 「重要インフラサービスの安全かつ持続的な提供を実現する」
- 「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」
- 「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」

[1] NISC「重要インフラのサイバーセキュリティに係る行動計画」別紙2　重要インフラサービスとサービス維持レベル　参照。
https://www.nisc.go.jp/policy/group/infra/siryou/index.html

- 「日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施」
- 「サイバー攻撃の結果、生産活動やサービス提供に影響が生じるリスクを考慮し、サイバーセキュリティ推進体制を構築する」
- 「ゼロトラストセキュリティの考え方を組み入れたセキュリティ管理策の実施」

**【維持するサービスの望ましい水準例】**

- 「経営方針等にサイバーセキュリティ確保に関する事項として「日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施」等を記載し、その KPI(重要業績評価指標)として「システム障害によるサービス停止からサービス復旧までの時間〇〇時間以内」等を記載する。」
- 旅客輸送サービス　許容停止時間　〇〇時間

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

### 3.1.2 サイバーセキュリティ方針

**【対策項目】.**

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。

最高情報セキュリティ責任者は、3.1.1. 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
- 経営層によるコミットメント

**【サイバーセキュリティ方針】**

- 経営層は、サイバーセキュリティの確保のため、セキュリティ対策に取り組むことをサイバーセキュリティ方針等に含め、組織の内外に対して宣言する。
- 最高情報セキュリティ責任者は、重要インフラ防護の目的、目指す方向、セキュリティ対策にて守るべき対象等を明らかにし、サイバーセキュリティへの取組姿勢をサイバーセキュリティ方針として規定すること。
- サイバーセキュリティ方針の策定・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。
- 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。

## 3.2 組織内外のコミュニケーション

**【主旨・目的】**

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

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

**【実施項目】**

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

**【組織内外のコミュニケーションの考え方】**

- 経営層は、サイバーセキュリティに関してステークホルダー[2]の信頼・安心感を醸成する観点から、平時におけるサイバーセキュリティに対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組む。
- 組織内のガバナンスや内部統制、その他のリスクマネジメントにおけるコミュニケーションの一部として、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設ける。
- セキュリティ・バイ・デザインを共通の価値として認識し、製品・サービス企画時等の内部協議プロセスの関係者にサイバーセキュリティを担当する部署を加えることが望ましい。
- 組織内外の関係者間でサイバーセキュリティに関する役割、責任分担、情報共有の体制等について意見交換を行うことが望ましい。
- グループ企業[3]において、グループ全体の組織ガバナンスを浸透するため、規程類を統一させることが望ましい。

[2]「ステークホルダー」は、株主・経営者・従業員・顧客・取引先のほか、金融機関、行政機関、各種団体など企業のあらゆる利害関係者を指す言葉であるが、ここではサイバーセキュリティに関するリスクが直接影響を及ぼす可能性のある関係者を指している。
[3] グループ企業とは、親会社、子会社、関連会社を含めた関係性のある会社全体を意味する。

COLUMN

## コラム
## リスクコミュニケーションに関する優良事例

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

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

**＜被害＞**

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

**＜感染経路＞**

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

**＜対応＞**

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

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

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

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

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

## 3.3 経営リスクとしてのサイバーセキュリティリスクの管理

**【主旨・目的】**

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

**【実施項目】**

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

経営層は、重要インフラサービスの提供に不可欠な情報システムは何か、それらがどのようにサイバー脅威にさらされる可能性があるか、どのようなセキュリティ対策をとるべきかを理解することを念頭に、サイバーセキュリティリスクについて理解を深めることが望ましい。[4]

## 3.4 責任及び権限の割当て

**【主旨・目的】**

全ての者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることでサイバーセキュリティは実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を確立することが望ましい。

### 3.4.1 サイバーセキュリティ責任者の任命

**【実施項目】**

サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てる。特に、サイバーセキュリティ責任者(CISO[5] 等)を任命すべきであり、その任命にあたっては、経営層の責任において実施する。当該責任者は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと直接コミュニケーションできる者として位置付けられるべきであり、経営層に相当する者の中から任命されることが望ましい。

- **組織・体制の確立**

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

[5] CISO (Chief Information Security Officer):最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。(NISC「重要インフラのサイバーセキュリティに係る行動計画」2022 年より)

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

CSIRT としての機能を持つ体制を整備する。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

- **責任者・組織の設置**

組織・体制を確保するにあたっては、以下【具体例】のように、責任者・組織を設置し、責任及び役割を定めることが望ましい。

また、必要に応じて外部専門家の登用や、以下の【資格例】に示すようなサイバーセキュリティに関する資格保持者の配置を検討することが望ましい。

| **【具体例】** |
| --- |
| セキュリティ管理策を推進するにあたり、以下の責任者・組織を設置する<br>・ 最高情報セキュリティ責任者<br>・ 情報セキュリティ委員会<br>・ サイバーセキュリティ責任者<br>・ システム管理者<br>・ CSIRT |
| **【資格例】** |
| ・ 情報処理安全確保支援士<br>・ 情報セキュリティマネジメント試験合格者<br>・ CISSP<br>・ CISM |

### 3.4.2 責任者・組織などの役割

**【実施項目】**

最高情報セキュリティ責任者は、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。

責任及び権限の見直しにあたっては、以下のような役割が考えられる。経営層及びサイバーセキュリティ責任者である経営層以外の幹部(CISO 等)は、以下のような業務担当者を指揮するものとする。

| 【具体例】 |
| --- |
| ・ 脅威情報等の収集及び関係主体との情報共有担当<br>・ セキュリティインシデントの管理担当(CSIRT 等)<br>・ コンティンジェンシープラン及び事業継続計画等の実行担当<br>・ サイバーセキュリティに係る取組全般に対する内部監査担当<br>・ サプライチェーン(サプライヤー、委託先等)におけるセキュリティ管理策の取組の管理担当<br>・ セキュリティ人材の職能要件の管理及び教育・研修担当<br>・ 情報システム(ネットワークを含む)の運用担当<br>・ 各資産(情報システム、ソフトウェア、情報等)の管理担当<br>・ 物理的セキュリティが要求される施設の管理担当<br>・ 制御システム等が運用される環境保有時には制御関連部門の担当 |

### 3.4.3 役割の分離

**【実施項目】**

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

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

## 3.5 資源の確保

**【主旨・目的】**

セキュリティ対策を計画に沿って進めるにあたり、情報システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクを考慮して適切に配分すること。

**【実施項目】**

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

十分な資源の確保が難しい場合には、中小企業向けのサイバーセキュリティ対策の導入・運用

の支援を目的とした、サイバーセキュリティお助け隊サービス制度[6]等の活用を検討する。

## 3.6 監査・モニタリング

**【主旨・目的】**

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。

### 3.6.1 セキュリティ対策の運用状況の把握

**【実施項目】**

サイバーセキュリティ、経営層の責任において把握する。

**【具体例】**

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

### 3.6.2 セキュリティ対策の監査

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。

**【実施項目】**

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

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。

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

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

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。

**【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サイバーセキュリティ責任者に指示する。

⇩ ⇧

**＜サイバー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。

経営層は、監査の結果等により、目標未達や進捗遅延、セキュリティ管理策の要改善点等が確認された場合は、改善指示を行う。これらを繰り返し実施し、サイバーセキュリティの取組の効果を高める。

年度情報セキュリティ監査計画には、以下の事項を含むことが望ましい。

**【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

### 3.6.2 セキュリティ対策の監査

個別の監査実施計画には、以下の事項を含むことが望ましい。

**【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

## 3.7 情報開示

**【主旨・目的】**

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。

**【実施項目】**

経営層は、平時におけるサイバーセキュリティ確保の取組に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。

重要システムの停止・低下により、列車の安全安定輸送に対する支障が発生した際等、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。

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

**【開示することが望ましいサイバーセキュリティに関する情報】**

- 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
- サイバーセキュリティ責任者の知見
- 資源の確保
- リスクの把握とリスクへの取り組み方針
- 緊急対応体制・事業継続／IT-BCP に関する取り組み内容／体制
- 重大なインシデントの発生状況及び対応状況

## 3.8 継続的改善

**【主旨・目的】**

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。

### 3.8.1 サイバーセキュリティ確保の取組の見直し

**【実施項目】**

サイバーセキュリティ責任者は、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こと。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。

見直しを実施するにあたっては、以下の点に留意する事が望ましい。

**【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。

### 3.8.2 IT に係る環境変化に伴う脅威のための対策

**【実施項目】**

・平時からの情報収集に努めるとともに、新たな脅威が顕在化した時点で速やかに検討体制が構築できる準備を行うこと。

・ISAC[7]・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

[7] 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。

# 4　リスクマネジメントの活用と危機管理

本章では「3.1 組織方針」で規定されるサイバーセキュリティ方針に従い、サイバーセキュリティに関するリスクマネジメントにおいて実施することが望まれる事項を示す。実施主体は主に CISO 及びサイバーセキュリティ責任者とする。

## 4.1　組織状況の理解

**【主旨・目的】**

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。旅客輸送サービス等継続の強靭性を確保するため、鉄道サービス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。

### 4.1.1 内部状況・外部状況の理解

次に例示する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。

**【内部状況の例】**

- 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
- 旅客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

**【外部状況の例】**

- 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[8]

[8] 鉄道分野における外部状況として以下の状況が考えられる。

・法令の改正状況

鉄道分野はその事業特性から、顧客向けのウェブサービス（座席予約等）を保有している重要インフラ事業者等も多く、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、安全なウェブサイトの構築のため、最新のウェブサイト攻撃の動向把握が望ましい。（【1.1.3「安全ガイドライン」の位置づけ（6）】参照）

### 4.1.1 内部状況・外部状況の理解

- 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
  （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

鉄道分野の関係主体(例)

| ステークホルダー | 内訳 | 役割 | 内容 |
|---|---|---|---|
| **所管省庁・局** | 鉄道局 | インシデントの通知 | 許認可・監督 |
| | 運輸局 | インシデントの通知 | 許認可・監督 |
| **沿線自治体** | 沿線都道府県 | インシデントの通知 | 地域公共交通施策の策定・実施、観光振興、防災等 |
| | 各市町村 | インシデントの通知 | 地域公共交通施策の策定・実施、観光振興、防災等 |
| **駅運営事業者** | 駅・ビル運営事業者 | 駅・ビルの運営 | 駅・ビルの運営 |
| **鉄道関連企業** | 鉄道会社 | 相互乗入・連絡運輸 | 鉄道運行 |
| | 車両整備会社 | 車両の整備・修理 | 車両の整備・修理 |
| | 燃料給油会社 | 電力駆動以外の燃料給油 | 電力駆動以外の燃料給油（軽油等） |
| | 車両販売製造会社 | 車両の製造・販売 | 車両の製造・販売 |
| | 電気設備整備会社 | 電気設備の設計・施工・修理 | 電気設備の設計・施工・修理 |
| | 軌道整備会社 | 軌道の建設・保守・整備 | 軌道の建設・保守・整備 |
| | 電気設備管理会社 | 駅EV・FD等の保守・修理業務 | 駅EV・FD等の保守・修理 |
| **鉄道物流** | 荷送人/荷受人 | 荷物の配送依頼・荷物の受取 | 荷物の配送の依頼、荷物の受け取りを行う企業、私人等 |
| | 貨物列車運行会社 | 貨物列車の運行 | 貨物列車の運行 |
| **関連企業（警備、その他）** | 保安警備会社 | 保管警備 | 民間企業 |
| | 鉄道インフラ維持管理会社 | 維持管理 | 駅ビル・鉄道インフラ維持管理 |
| | 駅テナント | 駅テナント | テナント　入居事業者 |
| | 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 |
| | ビルメンテナンス会社 | 警備・清掃 | 駅・駅ビル等の警備・清掃 |
| | サイバーセキュリティ保険会社（該当する場合） | 保険サービス提供 | サイバー事故に関する保障・各種支援 |
| | 顧問弁護士（該当する場合） | 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（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に関連するインシデント報告等 |
| **関連機関（警備、警察）** | 警察 | 鉄道・駅警備 | 鉄道・駅警備 |
| **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 |
| | 鉄道団体 | インシデントの通知 | 加盟している団体へ通知 |
| | JPCERT/CC | インシデントの通知／相談 | インシデント発生時の対処の相談、対応依頼 |
| | 情報処理推進機構（IPA） | 不正アクセス等に関する相談 | 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 |
| **重要システム** | 重要システム | 重要システムの導入ベンダー | 重要システムの導入・保守・運用 |

### 4.1.2 関係主体からの要求事項の理解

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。

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。

### 4.1.3 重要インフラサービス継続に係る特性の理解

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。

**【重要インフラサービス継続に係る特性】**

- 旅客輸送サービス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
- 旅客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
- 運行管理に関わる制御システム(運行管理システム)の特性
- 運行管理システムからの情報をもとに、利用者案内等を行う情報システム群(旅客案内や券売機、自動改札機等)の特性

### 4.1.4 現在プロファイルの特定

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。

**【現在プロファイルの特定】**

- 現在プロファイルの特定に当たっては、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。

## 4.2 リスクアセスメント

**【主旨・目的】**

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。

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

### 4.2.1 リスクアセスメントの実施

**【対策項目】**

組織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。

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、以下の手順によってセキュリティリスクアセスメントを実施する

| **【リスクアセスメントプロセス】**[9] | |
|---|---|
| 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 |

[9] 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。

| | |
|---|---|
| | 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 |

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。

**【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、旅客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。
- 旅客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[10]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、旅客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、旅客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。
- 運行管理に関わる制御システム(運行管理システム)や、運行管理システムからの情報をもとに、利用者案内等を行う情報システム群(旅客案内や券売機、自動改札機等)は、システムごとにネットワークの繋がりが疎結合している、又は独立しているなど、様々な特性があるため、それぞれの特性に応じたリスクアセスメントを実施する。

[10] 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）

### 4.2.2 制御システムのリスクアセスメント

**【実施事項】**

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。旅客輸送サービス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。

なお、運行管理システム・電力管理システムは原則、外部とは接続しないクローズドな環境で構築される。制御システムのリスクアセスメントを実施する際には、クローズド環境であることを考慮したリスク特定・分析を行う。同様に、リスク対応の実施においても、クラウドサービスやインターネット接続を伴うリスク軽減策の実施が難しいことを念頭にセキュリティ管理策を検討する。

**【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(【1.1.3「安全ガイドライン」の位置づけ(6)】参照)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

### 4.2.3 目標とする将来像の設定

**【実施事項】**

重要インフラ事業者等は、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、一例として目標プロファイルの作成が考えられる。

### 4.2.3 目標とする将来像の設定

**【目標プロファイルの作成】**

- 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。

**【目標とする将来像の設定の例】**

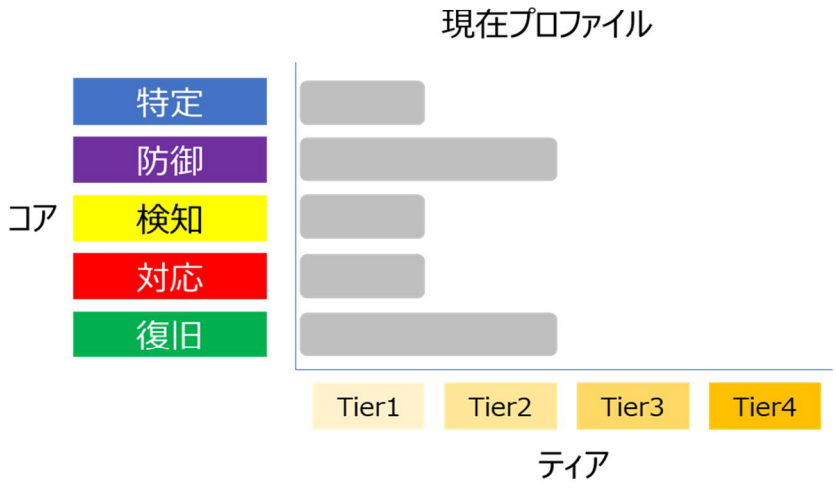
- 重大なインシデント発生時に◯◯時間以内に経営層までエスカレーションされること
- 資産管理を行い、脆弱性を把握し、適切な脆弱性管理を行うこと
- セキュリティ委員会を常設、定期開催することとし、必ず CISO が参加すること

### 4.2.3 目標とする将来像の設定

**【プロファイルの特定について】**

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）

### 4.2.3 目標とする将来像の設定

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。**<br>・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。<br>・セキュリティリスクに関して意識が不足している。<br>・情報共有のプロセスが存在しない。<br>・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。**<br>・リスクマネジメントの枠組みは経営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。<br>・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。**<br>・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。<br>・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。<br>・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。<br>・ステークホルダーと協力関係にある。<br>・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。**<br>・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。<br>・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。<br>・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。<br>・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。<br>・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

## 4.3 サイバーセキュリティリスク対応

### 4.3.1 リスク対応の決定

**【主旨・目的】**

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。

**【実施事項】**

- **ギャップ分析と優先順位付け**

**【具体例】**

- 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。

### 4.3.2 個別方針の策定

**【主旨・目的】**

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。

**【実施項目】**

- **内規の策定・見直し**

**【具体例】**

- 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。

- **個別方針の策定**

**【具体例】**

- 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。

➢ **現状のサイバーセキュリティ対処態勢の実態の例**

| **【具体例】** |
| --- |
| ・ 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。<br>・ 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。<br>・ 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。<br>・ 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の例**

| **【具体例】** |
| --- |
| ・ 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。<br>・ 情報資産を棚卸し、定期的に見直し、シャドーIT[11]を防止する。<br>・ 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。<br>・ 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。 |

➢ **違反と例外措置**

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】** |
| --- |
| **＜違反への対応＞**<br>・ 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。<br><br>**＜例外措置＞**<br>・ 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。<br>・ 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 |

[11] 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

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)
- 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

### 4.3.3リスク対応計画の策定

**【主旨・目的】**

サイバーセキュリティ責任者は、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。

**【対策項目】**

- **サイバーセキュリティの確保に係るロードマップ及び計画の作成・見直し**

  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[12]を作成し、実施する。

**【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

## 4.4 サプライチェーン・リスクマネジメント

**【主旨・目的】**

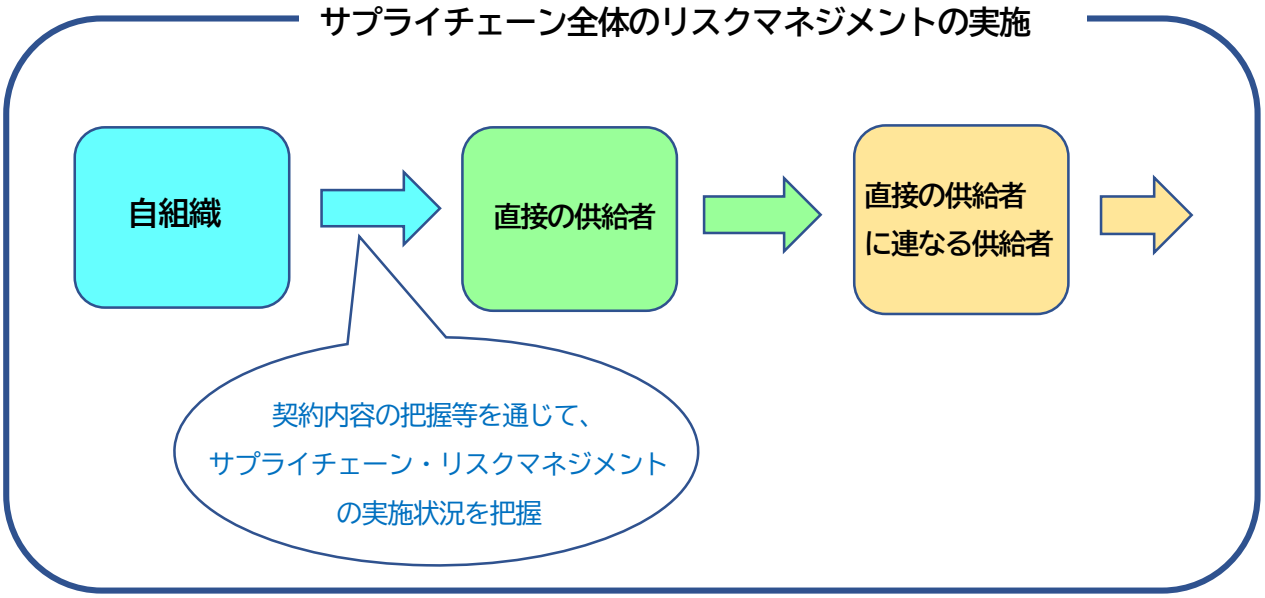
セキュリティ対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めることが重要である。なお、法制度や実施体制が十分でない、法の執行が不透明である、権力が

[12] 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

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[13]

**【対策項目】**

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。




**【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
- 委託先の管理不良による機密情報の意図しない公開
- 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。

## 4.5 事業継続計画等

**【主旨・目的】**

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、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」、事業継続を目

[13] 参照法律：経済安全保障推進法

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。

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 等との整合性運用の確保が必要である。

### 4.5.1 事業継続計画等の作成

**【対策項目】**

重要インフラサービス障害発生等により、サービス維持レベルを下回った際の行動手順として、事業継続計画等を策定し、目標とするサービス水準への早期復旧対応を行う。事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針(コンティンジェンシープラン、事業継続計画、事業復旧計画等)にサイバーセキュリティを組み入れる。

- **コンティンジェンシープランの策定**

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。

**【具体例】**

- 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」を策定すること。

- **事業継続計画(BCP)の策定**

**【具体例】**

- 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、業務継続方法、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[14]

[14] 名古屋港のサイバー攻撃被害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

✓ 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。
- 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。

### 4.5.2 重要インフラサービス障害の対応

**【対策項目】**

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。

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。

### 4.5.3 重要インフラサービス障害に対する防護・回復

**【対策項目】**

策定した IT-BCP 等又は BCP 等を発動し、規定に沿った業務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。

**【具体例】**

- 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。
- 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。

## 4.6 人材育成・意識啓発

**【主旨・目的】**

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。

**【対策項目】**

- **サイバーセキュリティに関連する教育**

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。

**【具体例】**

- 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[15]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**

「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。

以下に例示する事項を実施することが望ましい。

[15] 交通ISAC https://t-isac.or.jp/

| 【具体例】 |
| --- |
| ・ サイバーセキュリティ責任者は、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。<br>・ 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。<br>・ 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。<br>・ 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<br>・ 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。<br>・ 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層の役割等について可能な限り理解できるよう、経営層に対してセキュリティ教育を実施すること[16]。<br>・ 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**

| 【具体例】 |
| --- |
| ・ 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。<br>・ 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 |

➢ **ノウハウの蓄積**

| 【具体例】 |
| --- |
| ・ サイバーセキュリティ責任者は、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 |

[16] NISC では経営層や 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

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

## 4.7 CSIRT 等の整備

### 4.7.1 CSIRT 等の整備、関連部門との役割分担等の合意

**【主旨・目的】**

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（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。

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。

**【対策項目】**

- **CSIRT 等の整備**

最高情報セキュリティ責任者は、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。

**【具体例】**

- 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、直ちに自ら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**

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。

セキュリティ確保の取組を推進するため、次のような役割が考えられる。

**【役割の具体例】**

- 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

### 4.7.2 重要インフラサービス障害発生時の体制の整備

**【主旨・目的】**

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。

**【対策項目】**

- **障害発生時の体制の整備**

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。

**【具体例】**

- 最高情報セキュリティ責任者は、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。

## 4.8 平時の運用

### 4.8.1 セキュリティ対策の導入、運用プロセスの確立・実行

**【趣旨・目的】**

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(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)等の運用プロセスを確立することが望ましい。

#### 4.8.1.1 情報システムの運用・保守

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。

**【対策項目】**

- **平時におけるリスク対応**

**【具体例】**

- 「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。

#### 4.8.1.2 情報システムの構成要素の運用

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。

**【対策項目】**

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に関する具体的な運用方法は【5.1.1.1 資産に対する責任】を参照。

#### 4.8.1.3 情報システムの監視

**【対策項目】**

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】**

- システム管理者は、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。
- システム管理者は、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
- システム管理者は、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。

#### 4.8.1.4 情報システムの更改・廃棄時の措置

**【対策項目】**

システム管理者は、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[17]】**

- 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

### 4.8.2 情報共有

**【趣旨・目的】**

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。

**【対策項目】**

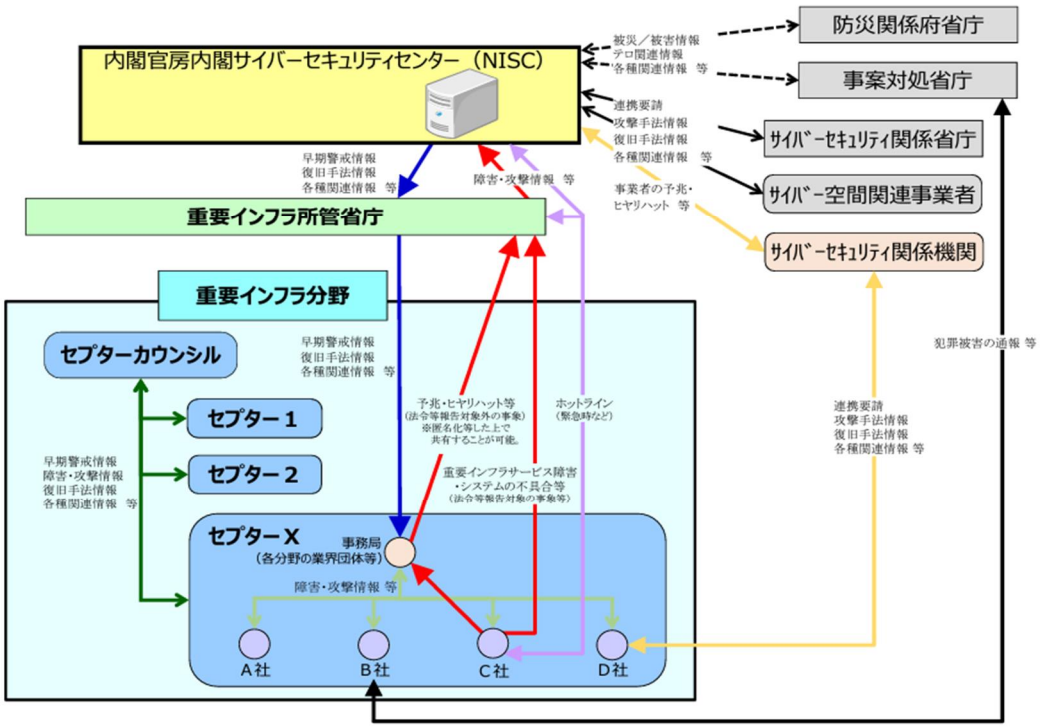
以下のような情報共有の取組については、重要インフラのサイバーセキュリティに係る行動計

[17] 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

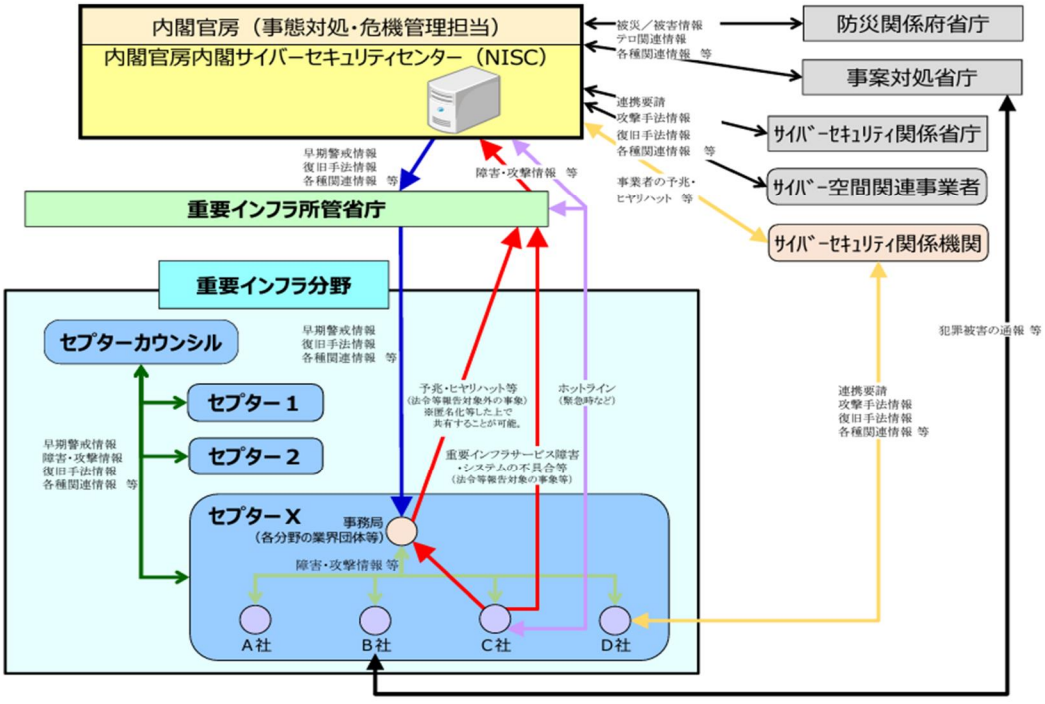
画の別紙 4－1～3 の体制に従い実施するものとする。具体的な情報共有の手引については「行動計画」に基づく手引書を参照し実施すること。

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。

**別紙４－１　情報共有体制(通常時)**




**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<br>（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<br>（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。<br>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 4-2「情報共有体制(大規模重要インフラ障害対応時)

別紙 4-3「情報共有体制における各関係主体の役割

- **関係主体からの情報提供**

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(【具体例】参照)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

| 【具体例】 |
|---|
| ・ 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。<br>・ 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。<br>・ 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。 |

➢ **国土交通省への情報連絡**

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。<br>・ 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。<br>・ 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。<br>・ 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。 |

➢ **組織内外との情報共有**

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。

情報共有を行うための関係主体は、自組織のステークホルダーを参考としながら整理する。(鉄道分野の関係主体(例)［4.1.1 内部状況・外部状況の理解］参照)

| **【具体例】** |
|---|
| ・ 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。<br>・ 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。<br>・ 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[18]、組織内外に情報提供を行うこと。<br>・ 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。 |

[18] 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

- ✓ 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
- ✓ サイバーセキュリティ責任者の知見
- ✓ 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

・ NISC「サイバーセキュリティ協議会」への相談や、警察機関等のネットワークを活用し、平時から多くの関係主体とコミュニケーションを図っておく事が望ましい。

**【重要インフラ事業者間の情報共有】**

・ 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 [4.6 人材育成・意識啓発]参照)

## 4.9 危機管理

**【主旨・目的】**

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層へエスカレーションを行うことが重要である。

### 4.9.1 サイバー攻撃の予兆

**【実施項目】**

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、システム管理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

### 4.9.2 コンティンジェンシープラン及び BCP の実行

**【実施項目】**

策定した IT-BCP 等又は BCP 等を実行し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行う。サイバーセキュリティ責任者は、サイバー攻撃等の事象が発生した際、経営層の意志決定を支援するため、経営リスクの観点から経営層へエスカレーションを行うことが重要である。

IT-BCP 等又は BCP 等を発報、実行の際には、国土交通省、警察、(個人情報漏えいが疑われる場合)個人情報保護委員会への速やかな連絡・連携を行うこと。(【4.8.2 情報共有】参照)

**【具体例】**

- サイバーセキュリティ責任者は、サイバー攻撃等の事象が発生した際、経営層の意志決定を支援するため、経営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。

### 4.9.3 本社等重要拠点の機能の確保

**【対策項目】**

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】**

- 最高情報セキュリティ責任者は、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

### 4.9.4 セキュリティ管理状況の対外説明

**【対策項目】**

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、列車の安全安定輸送に対する支障が発生した際等、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。

## 4.10 演習・訓練

**【主旨・目的】**

演習・訓練[19]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

[19] 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

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。

**【実施項目】**

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。経営層も交え、組織全体[20]での演習・訓練を実施することが望ましい。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】**

- 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[21]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。

## 4.11 モニタリング及びレビュー

**【主旨・目的】**

リスクマネジメントを通じて取組むセキュリティ管理策について、モニタリング及び監査（もしくは自己点検）を実施し、継続的な見直し・改善を行う。

### 4.11.1 モニタリング実施計画の策定と実施

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。

[20] 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。

[21] 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。

サイバーセキュリティ確保の取組により、リスクをどの程度回避、軽減が出来たかを測定・評価する。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、脆弱性診断、ペネトレーションテスト等の手段がある。

**【実施項目】**

最高情報セキュリティ責任者は、【4.3.3 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、【4.1.4 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】

- 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)
- 経営層へのエスカレーションフローの正当性
- 経営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。

### 4.11.2 監査計画の策定と実施

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。

**【実施項目】**

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。

- 監査プロセス
  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の例】 |
| --- |
| ＜準備＞<br>監査人[22]の選定を含めた体制整備等<br>＜監査方針＞<br>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<br>＜対象業務＞<br>重要インフラサービス提供に係る業務を対象とする<br>＜監査期間＞<br>＜監査報告＞<br>＜監査結果への対応＞<br>＜フォローアップ＞ |

### 4.11.3　セキュリティ対策の自己点検

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。

**【実施項目】**

最高情報セキュリティ責任者は、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。

[22]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/

### 4.11.3 セキュリティ対策の自己点検

**【セキュリティ対策の自己点検の実施例】**

＜サイバー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、サイバー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。

＜サイバー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、
サイバー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。

実施計画には、以下の項目を含む事が望ましい。

**【具体例】**

- 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。

# 5 対策項目

## 5.1 組織的対策

### 5.1.1 資産の管理

#### 5.1.1.1 資産に対する責任

**【対策の指針】**

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

**【対策項目】**

➢ **資産の管理**

**【具体例】**

- 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[23]を作成・維持管理する。
- 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。

[23] 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

➢ **端末の運用時・運用終了時**

**【具体例】**

**＜システム管理者による対策＞**

- 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。
- システム管理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、システム管理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、システム管理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、システム管理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**

**【具体例】**

**＜システム管理者による対策＞**

- 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。
- 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、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**

**【具体例】**

**<システム管理者による対策>**
- 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**

**【具体例】**

**<システム管理者による対策>**
- 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

#### 5.1.1.2 データ管理

**【対策の指針】**

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。(【5.5 クラウドサービス】参照)

### 5.1.2 供給者管理

**【対策の指針】**

事業者は「任務保証」の観点から、資材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。[24](【4.4 サプライチェーン・リスクマネジメント】参照)

**【対策項目】**

[24] 参照法律：経済安全保障推進法

➢ **サプライチェーン・リスクマネジメント**

【4.4 サプライチェーン・リスクマネジメント】に記載する対策項目に関する具体例を、以下に記載する。

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[25]。

**【具体例】**

- 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
- 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**

**【要求事項】**

[25] サプライチェーンに起因する規模の大きい情報流出も発生している【2.2.1 国内におけるサプライチェーンに起因する情報流出の事例】。別紙 1 情報の取扱い・個人情報保護も参考としながら、個人情報保護法に準拠した対応策を講じること。

- 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。

## 5.1.3 運用の管理

### 5.1.3.1 運用の手順及び責任

**【対策の指針】**

サイバーセキュリティ責任者は、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。

**【対策項目】**

- **組織的安全管理措置**

**【具体例】**

- 安全管理措置を講ずるための組織体制の整備
- 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
- データの取扱い状況を一覧できる手段の整備
- 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。

### 5.1.3.2 マルウェアからの保護

**【対策の指針】**

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。

**【対策項目】**

システム管理者は、マルウェア感染の回避を目的とした取扱者に対する以下の留意事項を含む日常的実施事項を定めることが重要である。

- **マルウェア対策**

**【具体例】**

**＜システム管理者による対策＞**

- 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(電子メール運用時の対策[5.1.3.7])
- 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じること。
- 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。
- 外部と通信がない、ソフトウェアのバージョンアップが前提でない重要システムである場合には、マルウェア対策ソフトウェア等の導入が、誤検知や誤動作により安全安心輸送を阻害する要因となる場合がある。マルウェア対策の実施の際には、重要システムに関する通信の監視や仮想パッチといった代替策を含め、慎重に検討する。

#### 5.1.3.3 バックアップ

**【対策の指針】**

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。

**【対策項目】**

システム管理者は、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】**

- バックアップの対象(対象とするシステム、データ、ソフトウェアその他)
- 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
- バックアップの頻度、世代管理の方法
- 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環境を対象)
- 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。

### 5.1.3 運用の管理

| |
|---|
| ・　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)の実施 |

## 鉄道分野の重要システムで取り扱うデータのバックアップについて

鉄道分野における重要システムである列車運行管理システム、電力管理システム、座席予約システムでは、それぞれ次のようなデータを取り扱う場合がある。各データに対し完全性、可用性を担保するため、上記 5.1.3.3 バックアップの【具体例】に示す管理策を検討し、バックアップ計画を適切に実践することが望ましい。

【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。

【定期的なバックアップが望ましいデータ項目一覧】

列車運行管理システム

- ダイヤデータ
- 進路制御情報
- 列車行先案内情報
- 操作ログ
- 処理ジャーナル

電力管理システム

- 変電所機器情報
- 故障処理情報
- 自動制御情報

座席予約システム

- 空席状況
- ダイヤデータ
- 運賃表、料金表
- 会員情報（ログイン ID、パスワード、メールアドレス、乗車履歴等）
- 予約、発売済データ
- 前受金データ（ポイント事前積立金額）

### 5.1.3.4 ログ取得

**【対策の指針】**

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、ログに関して事後の検証に必要な期間が適切に保全されていることが重要である。

**【対策項目】**

- **ログの取得・管理**

**【具体例】**

**<システム管理者の対策>**

- 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項目としては、以下の事項を含めることが望ましい。

**【ログとして記録する項目】**

- 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)<br>・　日付、時刻<br>・　成功、失敗の区別、イベントの結果<br>・　電子メールのヘッダ情報、通信内容<br>・　通信パケットの内容<br>・　操作員、監視要員及び保守要員等への通知の内容 |

➢ **取得したログの点検、分析及び報告**

システム管理者は、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。

#### 5.1.3.5　運用ソフトウェアの管理

**【対策の指針】**

システム管理者は、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。

**【対策項目】**

システム管理者は、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。)で利用するソフトウェア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】**

- 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。

#### 5.1.3.6　脆弱性の管理

**【対策の指針】**

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 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。

**【対策項目】**

システム管理者は、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】**

**＜システム管理者の対策＞**

- 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。

### 5.1.3 運用の管理

- 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

## 脆弱性管理におけるパッチ適用について

上記 5.1.3.6 脆弱性の管理【具体例】において、パッチ適用のセキュリティ管理策を示しているが、適用するパッチに不具合があるなどの理由により、システムやアプリケーションの安定稼働が損なわれる可能性がある。鉄道インフラの重要システムである列車運行管理システム及び電力管理システムは、不安定動作が人命に関わる事故につながりかねないため、パッチの適用にあたっては慎重に検討しなければならない。

下表（脆弱性管理の例）を参考に、システム、脆弱性情報、パッチ適用可否、適用時期、適用状況等を整理し、以下を考慮し、システムベンダーと相談の上対処を決定することが望ましい。

- **パッチ適用を行った場合に想定されるリスク**
- **パッチ適用を見送った場合の影響評価**
- **パッチ適用を見送った場合の代替措置の実施**

表 脆弱背管理の例

| # | システム | 脆弱性 | 深刻度(CVSS) | パッチ適用可否 | 適用時期 | 適用状況 |
|---|---|---|---|---|---|---|
| 1 | CTC | CVE-XX | 大 | 可 | 即時 | 済 |
| 2 | CTC | CVE-YY | 小 | 可 | 保守に合わせて実施 | 未適用 |
| 3 | | | | | | |

### 5.1.3.7 電子メール運用時の対策

**【対策の指針】**

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。

**【対策項目】**

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】 |
| --- |
| ・ 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。<br>・ 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。<br>・ 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。<br>・ メールに記載された URL リンクに安易にアクセスしない。<br>・ 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。 |

### 5.1.4 インシデント管理

**【対策の指針】**

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。

**【対策項目】**

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。

| 【具体例】 |
| --- |
| ・ インシデントの管理責任者を定めること。<br>・ 組織内外へのインシデント報告や証拠収集等の手順を整備すること。<br>・ インシデントへの対応を通じて得た知見を、将来のインシデントへの備えとして活用するための仕組みを確立すること。<br>・ インシデント管理責任者を定め、責任者に対しセキュリティ事象を報告できる方法を確立すること。(関連 5.2.3 エスカレーション)<br>・ 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こと。<br>・ 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計画を策定すること。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計画を策定すること。策定した対応計画については年 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。 |

インシデント対応計画には、次の活動が含まれる場合がある。

| 【インシデント対応計画に含まれる事項】 |
|---|
| ・ 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<br>・ 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<br>・ 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<br>・ 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<br>・ インシデント管理活動のログ取得<br>・ 証拠の取扱い<br>・ 根本原因分析又は事後分析手順<br>・ 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<br>・ インシデント報告書の作成 |

## 5.2 人的対策

### 5.2.1 従業員の管理

**【対策の指針】**

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。

**【対策項目】**

サイバーセキュリティ責任者は、取り扱う情報の漏えい、滅失又はき損の防止その他の情報の安全管理のため、人的な安全管理措置を講ずること。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。

- **記録及び報告**

  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。

  ・(例)制限区域への入退室の情報(事後に追跡できる手段を含む)

記録の作成に当たっては次の事項を考慮する。

**【具体例】**

| |
|---|
| ・　記録の作成及び維持管理の費用及び労力<br>・　閲覧方法、検索の容易性及び保存媒体<br>・　保有期間<br><br>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。

| **【具体例】** |
|---|
| ・　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<br>・　報告の費用、頻度及び適時性<br>・　報告の方法<br>・　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**

| **【具体例】** |
|---|
| ・　サイバーセキュリティ責任者は、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<br>・　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<br>・　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**

| **【具体例】** |
|---|
| ・　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。 |

- **経営層の訓練及び従業員の管理**

| **【具体例】** |
|---|
| ・　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。<br>・　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。<br>・　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。 |

### 5.2.2 リモートアクセス環境

**【対策の指針】**

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。

**【対策項目】**

システム管理者は、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、以下の事項を含む対策を講ずることが望ましい。

**【具体例】**

- 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
  - ✓ 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 |

### 5.2.3 エスカレーション

**【対策の指針】**

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。

**【対策項目】**

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。

## 5.3 物理的対策

**【対策の指針】**

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。

鉄道インフラにおいては、各駅にも制御システム等が設置されていることがあるため、不特定多数の者による物理的な不正侵入への対策を行う必要がある。

### 5.3.1 セキュリティ確保が求められる領域

**【対策項目】**

- **情報システム施設に係る職員の入退出管理**

サイバーセキュリティ責任者は、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」)を保護することが望ましい。

**【具体例】**

- 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。<br>・ 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退できるようにする 。 |

➢ **訪問者及び受渡業者の管理**

サイバーセキュリティ責任者は、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】** |
|---|
| ・ 許可されていない者の入室手続きを定めること<br>・ 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。<br>・ 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、システム管理者の承認を求めること<br>・ 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 |

### 5.3.2 災害による障害の発生しにくい設備の設置及び管理

**【対策項目】**

- **脅威に応じた物理的対策**

システム管理者は、情報システムについては、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】**

- 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

### 5.3.3 装置の管理

**【対策項目】**

- **機器・装置等の物理的な保護**

社内の情報機器を安全に利用するためには、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】**

- 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。<br>・ 鉄道インフラは広範囲にわたって、各駅や線路沿いにも機器が設置されている特性がある。各機器の不正な操作や物理的に破壊されるリスクも想定し、敷地、施設への物理的侵入のリスクを考慮したリスク低減策を実施する。 |

➢ **電源管理**

| **【具体例】** |
|---|
| ・ 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。<br>・ 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。<br>・ 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。<br>・ 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。 |

## 5.4 技術的対策

### 5.4.1 不正アクセス等の脅威への対策

**【対策の指針】**

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。

#### 5.4.1.1 利用者アクセスの管理

**【対策項目】**

サイバーセキュリティ責任者は、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ことが重要である。

| **【具体例】** |
|---|
| ・ 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。<br>✓ 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。<br>✓ 利用者アクセス権を定期的にレビューする。<br>・ ユーザー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）。<br>・ 離職者（異動者含む）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ーアカウントと、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。(【5.4.2 情報システム等のアクセス制御】参照)

#### 5.4.1.2 主体認証機能

**【対策項目】**

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。

- **主体認証機能の導入**

システム管理者は、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。

**【主体認証方式の一例】**

- 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**

サイバーセキュリティ責任者は、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、以下の対策を規定することが望ましい。

**【具体例】**

**<取扱者の責任に関する具体例>**

- 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、システム管理者に届け出ること
- 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、直ちにシステム管理者にその旨を報告すること

#### 5.4.1.3 権限管理機能

**【対策項目】**

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】**

- 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。
- システム管理者は、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

### 5.4.2 情報システム等のアクセス制御

**【対策の指針】**

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。

**【対策項目】**

システム管理者は、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】**

**＜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 攻撃、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（DoS 攻撃、DDoS 攻撃）の発生を想定し、対応を行う。

**＜アカウントロック＞**

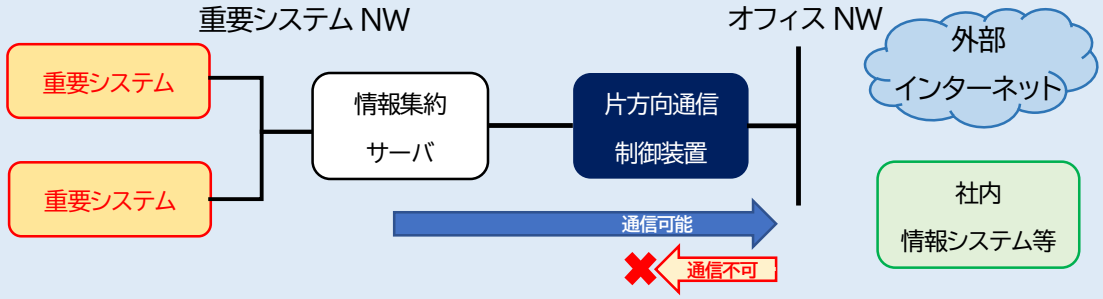
- 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する。

コラム COLUMN

## 重要システムとのネットワーク境界について

鉄道インフラの重要システムである列車運行管理システムは、外部と通信をしないクローズドな環境で運用されることが一般的である。利用者向けアプリへのリアルタイム情報通知(列車走行位置、遅延、種別等)といった顧客サービスの品質向上や、オフィスエリアからの稼働状況のモニタリング等の理由により、列車運行管理システムの一部を外部ネットワークと接続する必要がある場合には、外部から重要システム側のネットワークへの侵入を防ぐための措置を講じる。

一部の鉄道事業者においては、片方向通信制御等を活用し、列車運行管理システムが稼働するネットワークに対して、一切送信ができない環境を構築している。




片方向通信制御装置等による、重要システムへのアクセス制御イメージ

### 5.4.2.1 パスワード管理

**【対策項目】**

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。

鉄道分野では、顧客向けのインターネットサービス(座席予約等)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】**

- 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
- システム管理者は、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。
- システム管理者は、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。
- システム管理者は、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。

## 5.4.3 暗号を活用した情報管理

**【対策の指針】**

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。

**【対策項目】**

- **暗号化機能及び電子署名の付与機能の導入**

**【具体例】**

| |
|---|
| ・ システム管理者は、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。<br>・ 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。）**

| **【具体例】** |
|---|
| ・ 暗号の利用方針や暗号鍵の管理方針を策定する。システム管理者は、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。<br>・ 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。<br>・ 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<br>・ 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<br>・ 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<br>・ 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 |

### 5.4.4 通信のセキュリティ

**【対策の指針】**

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。

**【対策項目】**

サイバーセキュリティ責任者は、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】**

- 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。
- システム管理者は、サービス不能攻撃（DoS 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。

### 5.4.5 負荷分散・冗長化

**【対策の指針】**

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。

**【対策項目】**

- **負荷分散・冗長化**

システム管理者は、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。

- **サービス不能(DoS)攻撃対策**

システム管理者は、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】 |
| --- |
| ・ パケットフィルタリング[26] |
| ・ 3-way handshake[27] 時のタイムアウトの短縮 |
| ・ Syn Flood、UDP Flood 等の各種 DoS/DDoS 攻撃[28]への防御 |
| ・ WAF(Web Application Firewall)[29]の導入 |
| ・ CDN(Contents Delivery Network)[30]サービスの使用 |

### 5.4.6 多層防御

**【対策の指針】**

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

---

[26] 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

[27] 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

[28] 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

[29] 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

[30] 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 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。

型攻撃に備える必要がある。

**【対策項目】**

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。

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。

- **入口対策**

システム管理者は、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。

**【具体例】**

- 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**

システム管理者は、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】**

- 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。

## 5.5 クラウドサービス

**【対策の指針】**

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。

**【対策項目】**

- **クラウドを利用したシステム運用**

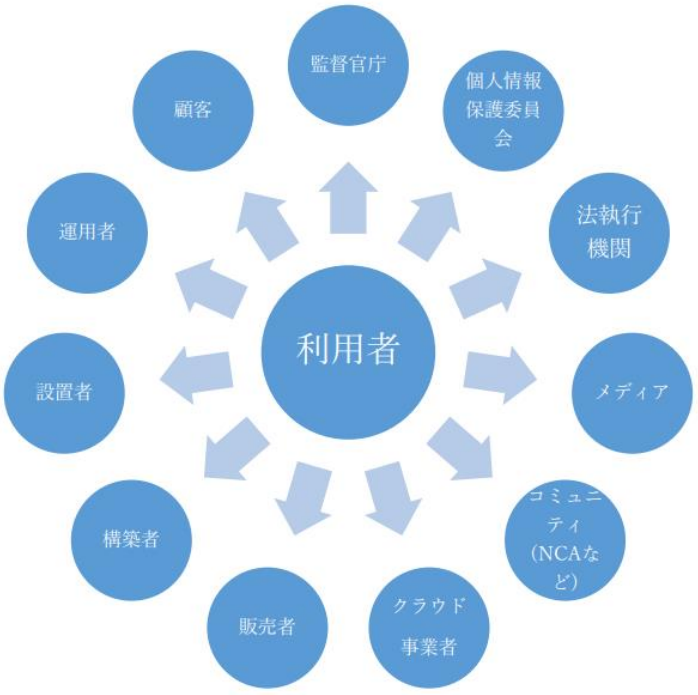
  クラウドサービスでは、クラウド事業者が提供する動作環境を活用していることから、利用者が制御できない環境や領域が存在する。 そのため、クラウド事業者の作業によってインシデントが発生する場合もあり、利用者はクラウド事業者から Web サイトへの公開等により提供される情報の把握や変更管理などを適切に行うことが望ましい。クラウドサービス活用にあたり、以下の注意点に留意することが望ましい。

**【具体例】**

- 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

## クラウド利用におけるインシデント発生時のステークホルダー[31]

インシデント発生後は、4.1.1 鉄道分野の関係主体で示したステークホルダーに加えて、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。




クラウド利用におけるインシデント発生時のステークホルダー例

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

31 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

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、以下クラウドサービス利用における設定不備の対策【具体例】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

- **データ管理**

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。

**【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。
- 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
- ✓ ウィルス対策の実施
- ✓ 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**

**【具体例】**

- 事業部門等が、サイバーセキュリティ責任者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。

また、以下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。

**【参考とするガイドライン・評価制度例】**

**＜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)[32]
- 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

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

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)[33]
- 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)[34]
- 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)[35]

**＜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)[36]
- The Federal Risk and Authorization Management Program (FedRAMP)[37]

## 5.6 委託先管理

**【対策の指針】**

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。

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。

**【外部委託の例】**
- 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

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

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

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

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

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

### 5.6.1 業務委託(共通事項)

**【対策項目】**

- **事業者内におけるサイバーセキュリティ確保の仕組みの整備**

  サイバーセキュリティ責任者は、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。

- **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**

  システム管理者は、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、「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】**

- 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)

### 5.6.2 情報システムに関する業務委託

情報システム、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。

5.6.2 情報システムに関する業務委託

**【対策項目】**

- **外部委託先の選定における手続の遵守**

  システム管理者は、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。

- **外部委託の実施における手続の遵守**

システム管理者は、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。

**【具体例】**

**＜システム管理者による対策＞**

- 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、運用・保守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
- 情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策
- 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の提供

**＜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

- **外部委託終了時の手続の遵守**

システム管理者は、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。

- **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**

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】** |
| --- |
| ・ システム管理者は、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。 |

## 外部委託におけるセキュリティ管理策

列車運行管理システムや電力管理システムの保守・メンテナンス業務を外部委託している場合がある。メンテナンスの際に、保守作業員が使用する PC や USB メモリ等に起因するセキュリティインシデントを防止するため、自組織のセキュリティポリシーに則り業務を遂行するよう、委託契約の際に、契約条項に必要なセキュリティ管理策を盛り込み、運用対処することが望ましい。

### 5.6.3 委託先に係る人的安全管理措置

**【対策項目】**

サイバーセキュリティ責任者は、取扱者に対する、業務上秘密と指定された情報の NDA(機密保持契約)の締結や教育・訓練等を行うことが望ましい。

**【具体例】**

- 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。
- 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。

# 6　参考文献

本ガイドライン 3 章～5 章及び別紙で提示した各対策項目の参考文献を以下のとおり示す。また、対策等を講じる上でその他参考とすべき情報も以下に示す。

| 鉄道分野における「安全ガイドライン」 目次 | 引用元 |
|---|---|
| 3 組織統治におけるサイバーセキュリティ | 【策定指針(令和5年)】: 3 |
| 3.1 組織方針 | |
| 3.1.1 組織方針とサイバーセキュリティ | 【策定指針】: 3.1.1. |
| 3.1.2 サイバーセキュリティ方針 | 【策定指針】: 3.1.2.<br>【企業経営のためのサイバーセキュリティの考え方】<br>【サイバーセキュリティ経営ガイドライン Ver.2.0】<br>【IoT セキュリティガイドライン ver.1.0(平成28年度)】: 要点1<br>【JIS Q 27002:2014】: 5.1.1、5.1.2 |
| 3.2 組織内外のコミュニケーション | 【策定指針】: 3.2.<br>【企業経営のためのサイバーセキュリティの考え方】<br>【サイバーセキュリティ経営ガイドライン Ver.2.0】<br>【IoTセキュリティガイドライン ver.1.0】: 要点1<br>【事業継続ガイドライン(令和5年3月)】(以下、【事業継続】): 4.2.2.2 |
| 3.3 経営リスクとしての サイバーセキュリティリスクの管理 | 【策定指針】: 3.3. |
| 3.4 責任及び権限の割当て | 【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)】(以下、【政府統一基準】): 2.1.1<br>【情報セキュリティ管理基準(平成28年改正版)】: 8.1 |
| 3.4.1 サイバーセキュリティ責任者の任命 | 【策定指針】: 3.4.、4.7.<br>【政府統一基準】: 2.1.1<br>【情報セキュリティ管理基準】: 8.1 |
| 3.4.2 責任者・組織などの役割 | 【政府統一基準】: 2.1.2<br>【情報セキュリティ管理基準】: 4.4.1.2<br>【JIS Q 27002:2014】: 5.1.1、5.1.2、17.1.1 ～ 17.1.3、17.2.1<br>【JIS Q 22301:2013】<br>【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】<br>【IT-BCP 策定モデル】<br>【CSIRTマテリアル】 |
| 3.4.3 役割の分離 | 【政府統一基準】: 2.1.1 |
| 3.5 資源の確保 | 【策定指針】: 3.5.<br>【情報セキュリティ管理基準】: 4.5.1.1、4.5.1.2 |
| 3.6 監査・モニタリング | 【企業経営のためのサイバーセキュリティの考え方】<br>【サイバーセキュリティ経営ガイドライン Ver.2.0】<br>【IoTセキュリティガイドライン ver.1.0】: 要点1<br>【情報セキュリティ管理基準】: 4.5.3.1、4.6.3.1 ～ 4.6.3.3、4.7.1.1 ～ 4.7.1.7<br>【JIS Q 27014:2015】:5.3.2 ～ 5.3.6.6 |
| 3.6.1 セキュリティ対策の運用状況の把握 | 【策定指針】: 3.6.<br>【企業経営のためのサイバーセキュリティの考え方】<br>【サイバーセキュリティ経営ガイドライン Ver.2.0】<br>【IoTセキュリティガイドライン ver.1.0】: 要点1<br>【情報セキュリティ管理基準】: 4.5.3.1、4.6.3.1 ～ 4.6.3.3、4.7.1.1 ～ 4.7.1.7<br>【JIS Q 27014:2015】: 5.3.2 ～ 5.3.6.6 |
| 3.6.2 セキュリティ対策の監査 | 【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(以下、手引書)】: 9.2.<br>【政府統一基準】: 2.3.2<br>【情報セキュリティ管理基準】: 4.7.1.1 ～ 4.7.1.7<br>【ISO/IEC 27014:2013】: 5.3.5 |
| 3.7 情報開示 | 【策定指針】: 3.7.<br>【企業経営のためのサイバーセキュリティの考え方】<br>【サイバーセキュリティ経営ガイドライン Ver.2.0】<br>【IoTセキュリティガイドライン ver.1.0】: 要点1<br>【事業継続】: 4.2.2.2 |
| 3.8 継続的改善 | 【政府統一基準】: 2.4.1、2.4.1(1) |
| 3.8.1 サイバーセキュリティ確保の取組の見直し | 【策定指針】: 3.8.<br>【手引書】: 9.3.<br>【政府統一基準】: 2.4.1、2.4.1(1) |
| 3.8.2 ITに係る環境変化に伴う脅威のための対策 | 【テレワークセキュリティガイドライン(第5版)】: 第5章12<br>【Web 会議サービスを使用する際のセキュリティ上の注意事項(2020)】: 3.5 |
| 4 リスクマネジメントの活用と危機管理 | |
| 4.1 組織状況の理解 | 【策定指針】: 4.1.<br>【手引書】: 4. |
| 4.1.1 内部状況・外部状況の理解 | 【手引書】: 4.1.1.、4.1.2. |
| 4.1.2 関係主体からの要求事項の理解 | 【情報セキュリティ管理基準】: 4.4.2.1、4.4.3.1<br>【JIS Q 27002:2014】: 18.1.1 |
| 4.1.3 重要インフラサービス継続に係る特性の理解 | 【手引書】: 4.1.3. |
| 4.1.4 現在プロファイルの特定 | 【手引書】: 4.2. |

| | | | | |
|---|---|---|---|---|
| | 4.2 リスクアセスメント | | | 【策定指針】: 4.2.<br>【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】<br>【制御システムのセキュリティリスク分析ガイド】<br>【CSMS認証基準 Ver.2.0】: 4.2、4.3<br>【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1<br>【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7<br>【テレワークセキュリティガイドライン】: 第2章 2. (1) |
| | | 4.2.1 リスクアセスメントの実施 | | 【策定指針】: 4.2.<br>【手引書】: 5.1.<br>【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】<br>【制御システムのセキュリティリスク分析ガイド】<br>【CSMS認証基準 Ver.2.0】: 4.2、4.3<br>【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1<br>【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7<br>【テレワークセキュリティガイドライン】: 第2章 2. (1) |
| | | 4.2.2 制御システムのリスクアセスメント | | 【策定指針】: 4.2.<br>【手引書】: 5.2. |
| | | 4.2.3 目標とする将来像の設定 | | 【手引書】: 4.2.、6.1. |
| | 4.3 サイバーセキュリティリスク対応 | | | |
| | | 4.3.1 リスク対応の決定 | | 【策定指針】: 4.3.1.<br>【手引書】: 6.2. |
| | | 4.3.2 個別方針の策定 | | 【策定指針】: 4.3.2.<br>【手引書】: 6.3.<br>【政府統一基準】: 2.2.2<br>【JIS Q 27002:2014】: 5.1.1、5.1.2<br>【テレワークセキュリティガイドライン】: 第2章 2. (1)<br>【情報セキュリティ管理基準】: 7.2.3 |
| | | 4.3.3 リスク対応計画の策定 | | 【策定指針】: 4.3.3.<br>【手引書】: 6.3.<br>【情報セキュリティ管理基準】: 4.4.8.4、4.4.8.5 |
| | 4.4 サプライチェーン・リスクマネジメント | | | 【策定指針】: 4.4.<br>【手引書】: 6.4. |
| | 4.5 事業継続計画等 | | | 【手引書】: 7.<br>【JIS Q 22301:2013】<br>【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1<br>【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】<br>【IT-BCP 策定モデル】<br>【CSIRTマテリアル】 |
| | | 4.5.1 事業継続計画等の作成 | | 【策定指針】: 4.5.<br>【手引書】: 7.1<br>【事業継続】: 4.2.2.2、5.1 |
| | | 4.5.2 重要インフラサービス障害の対応 | | 【政府統一基準】: 2.2.4、2.2.4(2)、2.2.4(3)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.6、16.1.7<br>【情報セキュリティ管理基準】:16.1 |
| | | 4.5.3 重要インフラサービス障害に対する防護・回復 | | 【策定指針】: 4.9.<br>【手引書】: 8.4.<br>【JIS Q 22301:2013】<br>【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1<br>【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】<br>【IT-BCP 策定モデル】<br>【CSIRTマテリアル】 |
| | 4.6 人材育成・意識啓発 | | | 【策定指針】: 4.6., 5.2.1.<br>【手引書】 8.1., 11.2.1.<br>【政府統一基準】: 2.2.3<br>【情報セキュリティ管理基準】: 4.5.2.3、4.5.2.4、4.5.2.6 ～ 4.5.2.8<br>【テレワークセキュリティガイドライン】: 第2章 2. (1) |
| | 4.7 CSIRT等の整備 | | | |
| | | 4.7.1 CSIRT等の整備、関連部門との役割分担等の合意 | | 【策定指針】: 4.7.<br>【手引書】: 8.2. |
| | | 4.7.2 重要インフラサービス障害発生時の体制の整備 | | 【政府統一基準】: 2.2.4、2.2.4(1)(c)<br>【JIS Q 27002:2014】:16.1.1、16.1.2、16.1.6、16.1.7 |
| | 4.8 平時の運用 | | | |
| | | 4.8.1 セキュリティ対策の導入、運用プロセスの確立・実行 | | 【対策指針】: 4.8.1. |
| | | | 4.8.1.1 情報システムの運用・保守 | 【手引書】: 8.3.<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】 |
| | | | 4.8.1.2 情報システムの構成要素の運用 | 【政府統一基準】: 7.1.1(2)、7.1.1(3)、7.3.1(1)、7.3.1(2)、7.3.1(3)、8.1.1(3)<br>【テレワークセキュリティガイドライン】: 第2章2.(3), 第5章3<br>【ICT サイバーセキュリティ総合対策 2022】: 1(1)ウ<br>【IoT セキュリティガイドラインVer 1.0】: 2.5 |
| | | | 4.8.1.3 情報システムの監視 | 【政府統一基準】: 5.2.3(1)(a)、5.2.4、5.2.5<br>【情報セキュリティ管理基準】: 4.6.2.2、4.6.2.3<br>【JIS Q 19011:2012】 |
| | | | 4.8.1.4 情報システムの更改・廃棄時の措置 | 【政府統一基準】: 5.2.3(1)(a)、5.2.4、5.2.5<br>【情報セキュリティ管理基準】: 4.6.2.2、4.6.2.3<br>【JIS Q 19011:2012】<br>【廃棄するパソコンやメディアからの情報漏洩】 |

| | |
|---|---|
| 4.8.2 情報共有 | 【策定指針】: 3.7.、4.8.2.<br>【手引書】: 3.<br>【政府統一基準】: 2.2.3<br>【情報セキュリティ管理基準】: 4.5.2.3、4.5.2.4、4.5.2.6 ～ 4.5.2.8<br>【重要インフラのサイバーセキュリティに係る行動計画(令和4年)】(以下行動計画):<br>別紙4-1～4－3<br>【サイバー攻撃被害に係る情報共有・公表ガイダンス検討会の開催について】 |
| 4.9 危機管理 | 【手引書】: 8.4. |
| 4.9.1 サイバー攻撃の予兆 | 【策定指針】: 4.9. |
| 4.9.2 コンティンジェンシープラン及びBCPの実行 | 【手引書】: 8.4.<br>【JIS Q 22301:2013】<br>【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1<br>【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】<br>【IT-BCP 策定モデル】<br>【CSIRTマテリアル】 |
| 4.9.3 本社等重要拠点の機能の確保 | 【事業継続】: 4.2.2、4.2.2.1 |
| 4.9.4 セキュリティ対策状況の対外説明 | 【JIS Q 22301:2013】<br>【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1<br>【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】<br>【IT-BCP 策定モデル】<br>【CSIRTマテリアル】 |
| 4.10 演習・訓練 | 【策定指針】: 4.10.<br>【手引書】: 8.5.<br>【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】<br>【制御システムのセキュリティリスク分析ガイド】<br>【CSMS認証基準 Ver.2.0】: 4.2、4.3<br>【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1<br>【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7 |
| 4.11 モニタリング及びレビュー | |
| 4.11.1 モニタリング実施計画の策定と実施 | 【手引書】: 9.1.<br>【情報セキュリティ監査基準 実施ガイドライン Ver1.0】<br>【NIST CSF】 |
| 4.11.2 監査計画の策定と実施 | 【情報セキュリティ監査基準 実施ガイドライン Ver1.0】 |
| 4.11.3 セキュリティ対策の自己点検 | 【政府統一基準】: 2.3.1、2.3.1(1) |
| 5 対策項目 | |
| 5.1 組織的対策 | |
| 5.1.1 資産の管理 | |
| 5.1.1.1 資産に対する責任 | 【策定指針】: 5.1.1.1.<br>【手引書】: 11.1.1.<br>【政府統一基準】: 6.1.1(2)、6.1.1(3)、6.4.1(1)、6.4.1(3)、6.4.2(3)、8.1.1(3)<br>【テレワークセキュリティガイドライン】: 第2章2.(3)、第5章3<br>【ICT サイバーセキュリティ総合対策 2022】: 1(1)ウ<br>【IoT セキュリティガイドラインVer 1.0】: 2.5 |
| 5.1.1.2 データ管理 | 【策定指針】: 5.1.1.3. |
| 5.1.2 供給者管理 | 【策定指針】: 4.4.、5.1.2.<br>【手引書】: 6.4.<br>【政府統一基準】: 6.2.1. |
| 5.1.3 運用の管理 | |
| 5.1.3.1 運用の手順及び責任 | 【策定指針】: 5.1.3.1.<br>【手引書】: 11.1.3.1.<br>【個人情報ガイドライン(通則編)(令和4年)】: 3-3-2<br>【JIS Q 22301:2013】: 8.5<br>【JIS Q 27002:2014】: 17.1.3 |
| 5.1.3.2 マルウェアからの保護 | 【策定指針】: 5.5.1.<br>【手引書】: 11.1.3.2.<br>【政府統一基準】:7.2.1(1)、7.2.2、7.2.2(1)、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12 |
| 5.1.3.3 バックアップ | 【策定指針】: 5.1.3.3.<br>【手引書】: 11.1.3.3.<br>【統一基準ガイドライン】: 3.1.1(8)(a)解説<br>【事業継続】: 4.2.3、5.1.2<br>【テレワークセキュリティガイドライン】: 第2章 2.(1)<br>【IoT セキュリティガイドライン Ver 1.0】: 1.1.2 |
| 5.1.3.4 ログ取得 | 【策定指針】: 5.1.3.4.<br>【手引書】: 11.1.3.4.<br>【政府統一基準】: 7.1.4、7.1.4(1) |
| 5.1.3.5 運用ソフトウェアの管理 | 【策定指針】: 5.1.3.5.<br>【手引書】: 11.1.3.5. |
| 5.1.3.6 脆弱性の管理 | 【策定指針】: 5.1.3.6.<br>【手引書】: 11.4.3.<br>【政府統一基準】: 7.2.1、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12 |

| | | | | |
|---|---|---|---|---|
| | | | 5.1.3.7 電子メール運用時の対策 | 統一基準: 7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12<br>【誤送信に関する総務省の注意喚起】<br>【IPAの情報セキュリティ10大脅威】 |
| | | 5.1.4 インシデント管理 | | 【策定指針】: 5.1.5.<br>【手引書】: 11.1.5. |
| | 5.2 人的対策 | | | |
| | | 5.2.1 従業員の管理 | | 【策定指針】: 5.2.1.<br>【手引書】: 10.2.、11.2.1.<br>【個人情報ガイドライン(通則編)】: 3-3-2 |
| | | 5.2.2 リモートアクセス環境 | | 【手引書】: 11.2.3.<br>【政府統一基準】: 6.4.1(2)<br>【テレワークセキュリティガイドライン】: 第1章1、第2章2(1)(2)<br>【Web 会議サービスを使用する際のセキュリティ上の注意事項】: 3.1、4.3(1)<br>【テレワークを行う際のセキュリティ上の注意事項】: 2.(3) |
| | | 5.2.3 エスカレーション | | 【策定指針】: 5.2.4.<br>【手引書】: 11.2.4. |
| | 5.3 物理的対策 | | | 【政府統一基準】: 3.2.1、3.2.1(1)、3.2.1(2)、3.2.1(3)、6.1.1、 6.2.1<br>【JIS Q 27002:2014】: 11.1.1 ～ 11.1.6、11.2.1、11.2.3、11.2.5<br>【IoTセキュリティガイドライン ver.1.0】: 要点2 |
| | | 5.3.1 セキュリティ確保が求められる領域 | | 【手引書】: 11.3.<br>【政府統一基準】: 3.2.1、3.2.1(1)、3.2.1(2)、3.2.1(3)、6.1.1、6.2.1<br>【JIS Q 27002:2014】: 11.1.1 ～ 11.1.6、11.2.1、11.2.3、11.2.5<br>【IoTセキュリティガイドライン ver.1.0】: 要点2 |
| | | 5.3.2 災害による障害の発生しにくい設備の設置及び管理 | | 【手引書】: 11.3.<br>【政府統一基準】: 3.2.1、3.2.1(1)、3.2.1(2)、3.2.1(3)、6.1.1、6.2.1<br>【JIS Q 27002:2014】: 11.1.1 ～ 11.1.6、11.2.1、11.2.3、11.2.5<br>【IoTセキュリティガイドライン ver.1.0】: 要点2 |
| | | 5.3.3 装置の管理 | | 【策定指針】: 5.3.3.<br>【手引書】: 11.3.1.、11.3.2. |
| | 5.4 技術的対策 | | | |
| | | 5.4.1 不正アクセス等の脅威への対策 | | 【政府統一基準】: 7.1.1、7.1.2、7.1.3<br>【JIS Q 27002:2014】: 9.2.1 ～ 9.2.6、9.4.1 ～ 9.4.3 |
| | | | 5.4.1.1利用者アクセスの管理 | 【策定指針】: 5.4.1.<br>【手引書】: 11.4.1. |
| | | | 5.4.1.2主体認証機能 | 【政府統一基準】: 7.1.1、8.1.1(6) |
| | | | 5.4.1.3権限管理機能 | 【政府統一基準】: 7.1.3 |
| | | 5.4.2 情報システム等のアクセス制御 | | 【手引書】: 11.4.2.、11.4.2.1.<br>【政府統一基準】: 7.1.1、7.1.2、7.1.3<br>【JIS Q 27002:2014】: 9.2.1 ～ 9.2.6、9.4.1 ～ 9.4.3 |
| | | | 5.4.2.1パスワード管理 | 【手引書】: 11.4.2.2.、11.4.2.3.<br>【政府統一基準】: 7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12 |
| | | 5.4.3 暗号を活用した情報管理 | | 【策定指針】: 5.4.3.<br>【手引書】: 11.4.4.2.<br>【政府統一基準】: 7.1.5、7.1.5(1)、7.1.5(2)、8.1.1(7)<br>【JIS Q 27002:2014】: 10.1.1、10.1.2、18.1.5<br>「輸出貿易管理令別表第1第9項(7) 暗号装置又はその部分品」 |
| | | 5.4.4 通信のセキュリティ | | 【策定指針】: 5.4.4.<br>【手引書】: 11.1.3.6.、11.4.4.2.<br>【政府統一基準】: 3.1.1(6)、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12 |
| | | 5.4.5 負荷分散・冗長化 | | 【政府統一基準】: 7.2.3(1)、6.2.1(1) |
| | | 5.4.6 多層防御 | | 【策定指針】: 5.4.5.<br>【手引書】: 11.4.5.<br>【政府統一基準】: 7.2.4(1)<br>【テレワークセキュリティガイドライン】: 第5章 6. |
| | 5.5 クラウドサービス | | | 【策定指針】: 5.1.1.3.、5.5.2.<br>【政府統一基準】: 4.2.1、4.2.2、4.2.3、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e)<br>【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)】:<br>1、3.2、3.3、6、11.5、12.4<br>【中小企業のためのクラウドサービス安全利用の手引き】: 第2章 3.(3)②～③、第5章7.<br>【ICT サイバーセキュリティ総合対策 2022】: 1(1)<br>【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5<br>【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】<br>【インシデントハンドリングマニュアル】<br>【テレワークセキュリティガイドライン】: 第5章6、第6章12 |

# 6 参考文献

| | | | |
|---|---|---|---|
| | 5.6 委託先管理 | | 【政府統一基準】: 4.1.1、4.1.1(2)<br>【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1<br>【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】: 3.1, 3.2<br>【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 】: 12.5 |
| | | 5.6.1 業務委託(共通事項) | 【政府統一基準】: 4.1.1、4.1.1(1)、4.1.1(2)(a)<br>【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1<br>【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】: 3.1、3.2<br>【個人情報ガイドライン(通則編)】: 3-3-4 |
| | | 5.6.2 情報システムに関する業務委託 | 【政府統一基準】: 4.1.1、4.1.1(2)<br>【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1<br>【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】: 3.1, 3.2<br>【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】: 12.5 |
| | | 5.6.3 委託先に係る人的安全管理措置 | 【策定指針】: 5.2.2.<br>【手引書】: 11.2.2.<br>【個人情報ガイドライン(通則編)】: 3-3-2<br>【JIS Q 22301:2013】: 8.5<br>【JIS Q 27002:2014】: 17.1.3 |

| その他参照とすべき情報 | | |
|---|---|---|
| ランサムウェアに関する情報提供サイト | | |
| | 内閣サイバーセキュリティセンター(NISC) ランサムウェア特設ページ STOP! RANSOMWARE | https://www.nisc.go.jp/tokusetsu/stopransomware/index.html |
| | 警察庁(サイバー警察局) ランサムウェア被害防止対策 | https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html |
| | 独立行政法人 情報処理推進機構(IPA)セキュリティセンター ランサムウェア対策特設ページ | https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html |
| | 一般社団法人 JPCDRTコーディネーションセンター(JPCET/CC) ランサムウェア対策特設サイト | https://www.jpcert.or.jp/magazine/security/nomore-ransom.html |
| | 一般財団法人 日本サイバー犯罪対策センター(JC3) ランサムウェア対策について | https://www.jc3.or.jp/threats/topics/article-375.html |

| 別紙1 情報の取扱い・個人情報保護 |
|---|
| 【策定指針】: 5.1.1.2.、5.1.1.3.、5.2.2.、5.3.1.、5.3.3.、5.4.1.、5.4.2.、5.4.4.<br><br>【手引書】: 11.1.2.、11.1.3.1.、11.1.3.6.、11.2.2.、11.3.、11.3.1.、11.3.2.、11.4.1.、11.4.2.、11.4.4.1.、11.4.4.2.<br><br>【政府統一基準】: 3.1.1、3.1.1(a)、3.1.1(4)、3.1.1(5)、3.1.1(6)、3.1.1(7)、3.1.1(8)、4.1.1、4.1.1(1)、4.1.1(2)、4.1.1(2)(a)、6.1.3<br>【個人情報ガイドライン(通則編)】:3-3-1、3-3-2、3-3-3、3-3-4<br>【データ消去技術 ガイドブック第 2.3 版】: p.11～<br>【Web 会議サービスを使用する際のセキュリティ上の注意事項】: 3.4<br>【JIS Q 22301:2013】: 8.5<br>【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1、8.1.1 ～ 8.1.4、8.2.1 ～ 8.2.3、17.1.3<br>【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】:3.1、3.2<br>【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】:12.5 |

| 別紙2 システムの取得・開発・保守に係るセキュリティ管理策 |
|---|
| 【策定指針】: 5.1.4.、5.4.5.<br><br>【手引書】: 11.1.4.、11.2.3.、11.4.5.<br><br>【政府統一基準】:<br>5.2.1、5.2.2、5.2.3、6.1.1、6.2.1、6.2.2、6.2.3、6.3.1(1)、6.3.1(2)、6.2.4、6.2.5、6.4.1、6.4.3(1)、6.4.4、6.6.1(1)、6.6.1(2)、7.1.4、7.2.1<br>【JIS Q 27002:2014】: 12.1.1、12.1.2、12.1.4、12.2.1、12.3.1、12.4.1 ～ 12.4.4、12.5.1、12.6.1、13.1.1 ～ 13.1.3、14.1.1 ～ 14.1.3、14.2.1 ～ 14.2.9、14.3.1<br>【高度サイバー攻撃への対処におけるログの活用と分析方法】<br>【IoTセキュリティガイドライン ver.1.0】: 2.3、2.4、2.5、要点2、要点8 ～ 16、要点17、18、21<br>【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】:4.1、4.2<br>【IT製品の調達におけるセキュリティ要件リスト】<br>【IT製品の調達におけるセキュリティ要件リスト活用ガイドブック】<br>【情報システムに係る政府調達におけるセキュリティ要件策定マニュアル】<br>【Web 会議サービスを使用する際のセキュリティ上の注意事項】: 3、3.1、4、4. 3(1)、5<br>【テレワークを行う際のセキュリティ上の注意事項】: 2. (3)<br>【テレワークセキュリティガイドライン】: 第1章1、第2章2(1)(2)、第5章2、3、5、6、7、9、11<br>【IoT・5G セキュリティ総合対策2020】: Ⅰ(2)②、Ⅲ(2)① |

# 7　専門用語集

本ガイドラインにおける専門用語を以下に掲載する。

## 7.1　多要素認証機能

多要素認証とは、以下の認証方式を複数組み合わせた認証方式のことである。

- 対象者の知識を利用したもの（ID/パスワード、暗証番号、事前に登録した質問事項への回答など）
- 対象者の持ち物を利用したもの（セキュリティトークン、ICカードなど）
- 対象者の身体の特徴を利用したもの（指紋認証、静脈認証など）

## 7.2 ウェブアプリケーションの脆弱性

本章は、一般的なセキュリティ用語の解説であるため、解説中の「利用者」については特定の重要インフラに限らない、一般的な情報システムの利用者を指す。

（1）SQL インジェクション脆弱性

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

（2）OS コマンドインジェクション脆弱性

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

（3）ディレクトリトラバーサル脆弱性

ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する

対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

(4) セッション管理の脆弱性

ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS(SSL)を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器(CSPRNG)で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

(5) アクセス制御欠如と認可処理欠如の脆弱性

ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりすまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

(6) クロスサイトスクリプティング脆弱性

ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる。

- HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
- URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
- SCRIPT 要素の内容を動的に生成しないようにする。

・ スタイルシートを任意のサイトから取り込める仕様を排除する。
・ 全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

(7) クロスサイトリクエストフォージェリ脆弱性

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに「アクセス制御欠如と認可処理欠如の脆弱性」の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害(具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害)が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

(8) クリックジャッキング脆弱性

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した(透明色で表示して利用者の目に見えないように設定された)フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

(9) メールヘッダインジェクション脆弱性

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、

電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法(又は設定ファイルから読み込む実装方法)を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

(10) HTTP ヘッダインジェクション脆弱性

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

(11) eval インジェクション脆弱性

ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

(12) レースコンディション脆弱性

ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

(13) 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

ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合

がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

## 7.3 その他

(1) アプリケーション・コンテンツ

アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

(2) ドメインネームシステム(DNS)

インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールに使われるドメイン名と、IP アドレスとの対応づけ(正引き、逆引き)を管理するために使用されるものをいう。DNS では、端末等のクライアント(DNS クライアント)からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。

(3) データベース

データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものをいう。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び取扱者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

(4) IPv6(Internet Protocol Version 6) 通信回線

従来の IPv4 にかわるものとして設計された、次世代のインターネットプロトコルのことをいう。従来よりも IP アドレスを多く作成することにより、より多くのユーザやデバイスがインターネット上で通信できるようになった。

サーバ装置、端末及び通信回線装置等に、IPv6 技術を利用する通信(以下「IPv6 通信」)の機能が標準で備わっているものが多く出荷されているが、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性がある。これらは、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、不正アクセスを検知する対策等を講じていく必要がある。

(5) HSE

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。

(6) MDM

Mobile Device Management の略称。スマートフォン等のセキュリティ設定を統合的に管理するためのツール。

(7) VDI

Virtual Desktop Infrastructure の略称。サーバ上に仮想の PC を複数台用意し、サーバに接続した利用者からはあたかも個別に PC が用意されているような使い勝手で利用できるようにする環境のこと。

(8) VPN

Virtual Private Network の略称。主にインターネット上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。

(9) ゼロトラストセキュリティ

ゼロトラストセキュリティとは、外部ネットワーク(インターネット)と、内部ネットワーク(LAN)との境界による防御(境界型セキュリティ)には限界があり、内部ネットワーク内にも脅威が存在しうるという考えのもと、データや機器等の単位でのセキュリティ強化をうたった考え方を指す。

(10)ランサムウェア

感染した端末上のデータを勝手に暗号化してしまうマルウェア。攻撃者はその端末の利用者に対し暗号化を解除する見返りに金銭等を要求して利益を得ること。

(11)リモートデスクトップ

自らの手元にある機器から、ネットワークを経由して他の端末を操作するための仕組みのこと。

(12)ローカルブレイクアウト

オフィスネットワークやデータセンター等の拠点を介することなく、端末から直接インターネットへアクセスするネットワーク構成のこと。

(13)オンプレミス

従来型のシステム構築手法で、自組織の施設内(事務所内や自組織で保有するデータセンター内等)にシステムを設置する方式のこと。

(14)クラウドサービス

ネットワークに接続されたコンピュータ資源(計算能力、記録装置、情報システム等)を、ネットワーク(インターネット)を介して必要なときに必要な分だけ利用できるようなサービスを指す。クラウドサービス事業者が利用者に提供する資源の範囲(レベル)によって、SaaS・PaaS・IaaS とい

う分類がある。

(15)IaaS(Infrastructure as a Service)

クラウドサービスモデルの一つ。利用者に CPU、ストレージ、メモリ等のコンピュータリソースが提供される。利用者はそのリソース上に OS 等を構築することができる。

(16)PaaS(Platform as a Service)

クラウドサービスモデルの一つ。IaaS に加えて、OS、基本機能、開発環境等もサービスとして提供される。利用者はそれらを組み合わせて情報システムを構築することができる。

(17)SaaS(Software as a Service)

クラウドサービスモデルの一つ。PaaS に加えて、利用者に特定のアプリケーション(メールサービスやファイルサービス、グループウェア等)の機能がサービスとして提供されるもの。

(18)5G

4G など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 時代の基盤技術として、様々な産業分野での利活用が期待されている。

(19)ローカル 5G

地域の企業や自治体等の様々な主体が自らの建物や敷地内でスポット的に柔軟に構築し利用することのできる 5G のこと。

(20)テレワーク

テレワークの形態として「在宅勤務」、「サテライトオフィス勤務」、「モバイル勤務」があげられる。テレワークにおいて情報資産を守るためには、「ルール」・「人」・「技術」のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることが重要である。

# 別紙1. 情報の取扱い・個人情報保護

## 1 情報の取り扱いついての規定化

**【主旨・目的】**

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。

**【実施項目】**

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】**

- 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

**【実施項目】**

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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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**
  - 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**
  - 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**

・ 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**

・ 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**

・ 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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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**

・ 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**

・ 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

**【実施項目】**

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。

システム管理者は、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**

・ システム管理者は、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

・ 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
- システム管理者は、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。
- 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。
- 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。

※「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**
- 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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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**
  - 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、サイバーセキュリティ責任者の許可を得ること

- **情報の運搬・送信の選択**
  - 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**
  - 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、サイバーセキュリティ責任者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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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**

・ 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、サイバーセキュリティ責任者の許可を得ること
・ 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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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**

・ 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**

・ 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

**【実施項目】**

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**

サイバーセキュリティ責任者は、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**

サイバーセキュリティ責任者は、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**

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

**【実施項目】**

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。

- **データ内容の正確性の確保**

サイバーセキュリティ責任者は、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。

- **ライフサイクルに基づいた個人情報の管理対策**

サイバーセキュリティ責任者は、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。

**【取得・入力時における個人情報の管理策】**

- **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】**

➢ **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】**

➢ **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】**

- **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の具体例】**

- **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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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。

- **組織的安全管理措置**

**【具体例】**

サイバーセキュリティ責任者は、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**

**【具体例】**

サイバーセキュリティ責任者は、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**

**【具体例】**

サイバーセキュリティ責任者は、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**

| **【具体例】** |
| --- |
| サイバーセキュリティ責任者は、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<br>✓ 入退館(室)管理の実施<br>✓ 盗難等の防止<br>✓ 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**

サイバーセキュリティ責任者は、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。

| **【具体例】** |
| --- |
| ・ 個人データの安全管理に関する事項<br>✓ 個人データの漏えい等の防止、盗用の禁止に関する事項<br>✓ 委託契約範囲外の加工、利用の禁止<br>✓ 委託契約範囲外の複写、複製の禁止<br>✓ 委託期間<br>✓ 委託終了後の個人データの返還・消去・破棄に関する事項<br>・ 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<br>・ 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<br>・ 委託契約の内容、期間が遵守されていることの確認<br>・ 委託契約の内容、期間が遵守されなかった場合の措置<br>・ 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<br>・ 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**

システム管理者は、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

**【実施項目】**

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。

サイバーセキュリティ責任者は、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】**

- 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、サイバーセキュリティ責任者の許可を得ること
- 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

**【実施項目】**

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】**

- サイバーセキュリティ責任者は、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

**【実施項目】**

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。

➢ **安全管理措置**

サイバーセキュリティ責任者は、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。

➢ **取扱者の監督**

サイバーセキュリティ責任者は、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<br>・　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<br>・　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<br>・　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**

サイバーセキュリティ責任者は、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。

| 【具体例】 |
| --- |
| ・ 雇用契約時における情報の守秘や非開示の契約の締結<br>・ 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

**【実施項目】**

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**

最高情報セキュリティ責任者は、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**

最高情報セキュリティ責任者は、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**

最高情報セキュリティ責任者は、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**

最高情報セキュリティ責任者は、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。 |

# 別紙2. システムの取得・開発・保守に係るセキュリティ管理策

## 2 システムの取得・開発・保守

**【主旨・目的】**

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ー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。

### 2.1 情報システムの取得・開発・改善における要求事項の確認

**【対策項目】**

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。

## 2.2 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。

### 2.2.1 情報システム企画・要件定義

**【対策項目】**

システム管理者は、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】**

- システム管理者は、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。
- システム管理者は、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。

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。

| 望ましいセキュリティ管理策 |
| --- |
| ・ システム管理者は、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<br>・ システム管理者は、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<br>・ システム管理者は、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。<br>・ システム管理者は、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<br>・ システム管理者は、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<br>・ システム管理者は、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 |

### 2.2.2 情報システムの構築

**【対策項目】**

システム管理者は、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。

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。

| 情報システムの構築時に望ましいセキュリティ管理策 |
| --- |
| ・ 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<br>・ 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<br>・ 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<br>・ 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。 |

## 2.3 端末、サーバ装置、複合機及び特定用途機器

### 2.3.1 端末

**【対策項目】**

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】**

- システム管理者は、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。
- システム管理者は、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。
- システム管理者は、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。
- システム管理者は、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。
- システム管理者は、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。

また、システム管理者は、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。

| 【推奨対策項目】 |
| --- |
| ・ 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。<br>・ 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。<br>・ 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。<br>・ 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。<br>・ 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。<br>・ 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。<br>・ 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。 |

さらに、モバイル端末に対して上記の対策に加え、システム管理者は、以下【具体例】を例とする対策を講じることが望ましい。

| 【具体例】 |
| --- |
| ・ 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、業務用のユーザーアカウントを別途作成する。<br>・ 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。<br>・ 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<br>・ 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。<br>・ 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。<br>・ 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。<br>・ 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。 |

### 2.3.2 サーバ装置

**【対策項目】**

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、システム管理者は、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。

### 2.3.3 複合機及び IoT 機器を含む特定用途機器

**【対策項目】**

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**

システム管理者は、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。システム管理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**

システム管理者は、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。

### 2.3.4 端末、サーバ装置、複合機及び特定用途機器の調達

**【対策項目】**

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[38]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。

[38] 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

- 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。

## 2.4 アプリケーション

### 2.4.1 電子メール

**【対策項目】**

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】**

- システム管理者は、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

### 2.4.2 ウェブ

**【対策項目】**

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】**

- システム管理者は、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。
- システム管理者は、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

  各脆弱性の解説については、「7.2 ウェブアプリケーションの脆弱性」を参照の

こと
- システム管理者は、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
- システム管理者は、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

### 2.4.3 ドメインネームシステム(DNS)

**【対策項目】**

ドメインネームシステム(DNS)(7.3(2)参照)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】**

- システム管理者は、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

### 2.4.4 データベース

**【対策項目】**

データベース(7.3(3)参照)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。システム管理者は、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】**

- 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

### 2.4.5 Web 会議

**【対策項目】**

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】**

- システム管理者は、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
- 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（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（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。

## 2.5 通信回線及び通信回線装置

**【主旨・目的】**

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。

### 2.5.1 通信回線共通対策

**【対策項目】**

システム管理者は、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。

＜通信回線の構築時に講ずることが望ましい対策＞

- 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<br>・ 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<br>・ 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<br>・ 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<br>・ 通信回線装置を要管理対策区域に設置すること<br>・ 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<br>・ 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<br>・ 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 |

### 2.5.2 リモートアクセス環境導入時の対策

**【対策項目】**

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。

| **【VPN 回線利用時の対策】** |
|---|
| ・ 利用開始及び利用停止時の申請手続の整備<br>・ 通信内容の暗号化<br>・ 通信を行う端末の識別又は認証<br>・ リモートアクセス環境を利用する者の認証<br>・ 主体認証ログの取得及び管理<br>・ 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<br>・ アクセス可能な情報システムの制限<br>・ 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】 |
| --- |
| ・ 利用開始及び利用停止時の申請手続の整備<br>・ 通信を行う者又は発信者番号による識別及び主体認証<br>・ 主体認証ログの取得及び管理<br>・ 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<br>・ リモートアクセス中に他の通信回線との接続の禁止 |

### 2.5.3 無線 LAN 環境導入時の対策

【対策項目】

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。

システム管理者は、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】 |
| --- |
| ・ SSID の隠ぺい<br>・ 無線 LAN 通信の暗号化<br>・ MAC アドレスフィルタリングによる端末の識別<br>・ 802.1X による無線 LAN へのアクセス主体の認証<br>・ 無線 LAN 回線利用申請手続の整備<br>・ 無線 LAN 機器の管理手順の整備<br>・ 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 |

### 2.5.4 IPv6（Internet Protocol Version 6）通信回線

【対策項目】

インターネットの規格である IPv6（7.3(4)参照）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。

システム管理者は、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 通信を行う情報システムに係る対策<br>・ 意図しない IPv6 通信の抑止・監視 |

### 2.5.5 5G /ローカル 5G 通信回線

**【対策項目】**

移動通信システムの規格である 5G(7.3(18)参照)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(7.3(19)参照)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。

システム管理者は、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】**

- 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。

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。

**【参考とするガイドライン例】**

<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