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
（案）

年　月　日

サイバーセキュリティ戦略本部

目次

1. 目的及び位置付け 1
1.1. 重要インフラにおけるサイバーセキュリティの確保の重要性 1
1.2. 「安全基準等」とは何か 1
1.3. 安全基準等策定指針の位置付け 1
2. 総則 3
2.1. 策定目的 3
2.2. 対象範囲 3
2.3. 関係主体の役割 3
3. 組織統治におけるサイバーセキュリティ 4
3.1. 組織方針 5
3.2. 組織内外のコミュニケーション 5
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 5
3.4. 責任及び権限の割当て 6
3.5. 資源の確保 7
3.6. 監査・モニタリング 7
3.7. 情報開示 7
3.8. 継続的改善 8
4. リスクマネジメントの活用と危機管理 9
4.1. 組織状況の理解 9
4.2. リスクアセスメント 9
4.3. サイバーセキュリティリスク対応 10
4.4. サプライチェーン・リスクマネジメント 10
4.5. 事業継続計画等 11
4.6. 人材育成・意識啓発 11
4.7. CSIRT 等の整備 12
4.8. 平時の運用 12
4.9. 危機管理 12
4.10. 演習・訓練 12
5. 対策項目 14
5.1. 組織的対策 14
5.2. 人的対策 16
5.3. 物理的対策 17
5.4. 技術的対策 17
5.5. 動向を踏まえた対策 18

1. 目的及び位置付け

1.1. 重要インフラにおけるサイバーセキュリティの確保の重要性

我が国の国民生活及び経済社会は、重要インフラサービスの安全かつ継続的な提供に支えられている。安全で安心な社会の実現には、任務保証の考え方を踏まえ、重要インフラのサイバーセキュリティを確保し、強靭性を高めることが不可欠である。

サイバーセキュリティ体制が不十分・不適切なことにより損害が生じた場合、体制の決定に関与した経営層[1]は、任務懈怠に基づく損害賠償責任を問われうる。

経営層から担当者層まで、それぞれが役割と責任を果たし、リスクマネジメントによる事前対応と、障害の拡大防止・早期復旧の両面からサイバーセキュリティの確保に取り組むことが重要である。

1.2. 「安全基準等」とは何か

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。本文書（以下「安全基準等策定指針」という。）においては、サイバーセキュリティの確保に関して、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」と呼ぶ。

安全基準等は、重要インフラ分野ごとにその特性に応じて策定され、次の①～④に分類される。

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。

セキュリティ対策の項目及び水準が安全基準等に明示され、重要インフラサービスに携わる全ての関係者に理解されていることが望まれる。

1.3. 安全基準等策定指針の位置付け

安全基準等策定指針は、「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 日サイバーセキュリティ戦略本部決定）（以下「行動計画」という。）に基づき、安全基準等の策定・改定を支援するために策定される。

安全基準等策定指針には、各重要インフラ分野に共通して求められるサイバーセキ

[1] 組織の代表者として統括責任を負う者（CEO、理事長、首長等）、組織の業務を執行する者、及び、もしあれば、取締役会・理事会等。

ュリティの確保に向けた取組を整理・記載する。これらの取組は原則として安全基準等に規定されることを期待しているが、組織状況に応じて採否が検討されうる取組は推奨事項として「～することが望ましい」「～することが望まれる」という表現にしている。

各取組をどの安全基準等に定めるかについては、関係法令の規定及び安全基準等の構成等を踏まえ、重要インフラ分野又は重要インフラ事業者等ごとに検討されることを想定している。

安全基準等が一層高度かつ網羅的になるよう、関連する各種規格、国内外のベストプラクティス等も適宜参照することが望ましい。

なお、安全基準等策定指針において使用する用語は、行動計画において使用する用語の例による。

2. 総則

次に掲げる項目を安全基準等に規定することが望まれる。

2.1. 策定目的

安全基準等の策定目的として、「重要インフラの強靭性を確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、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[2]ためには、安全基準等の内容に照らしたサイバーセキュリティの確保に取り組むことが必要である」旨を記載する。

2.2. 対象範囲

行動計画「別紙１　対象となる重要インフラ事業者等と重要システム例」に記載された「対象となる重要システム例」や、「別紙２　重要インフラサービスとサービス維持レベル」に記載された「重要インフラサービス（手続を含む）」、「重要インフラサービス障害の例」、「サービス維持レベル」等の内容を踏まえて、安全基準等の規定項目が対象とする範囲を記載する。

2.3. 関係主体の役割

重要インフラ所管省庁、重要インフラ事業者、サプライチェーンに関わる事業者等の関係主体について、網羅的かつ具体的に記載し、それぞれのセキュリティ対策に関する役割を明記する。重要インフラ事業者等の役割については、経営層の取組についても記載する。

[2] 行動計画「Ⅰ総論 1. 重要インフラ防護の目的」参照。

3. 組織統治におけるサイバーセキュリティ

重要インフラのサイバーセキュリティの確保には、任務保証の観点から取り組むべきである。任務保証とは、サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者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」である。

重要インフラサービスの安全かつ持続的な提供を不確かなものとするリスクを許容水準まで低減することは、重要インフラ事業者等として果たすべき社会的責任であり、その実践は経営層としての責務である。重要インフラサービスの安全かつ持続的な提供にあたり、サイバーセキュリティの確保が不可欠であることを念頭に、既存の組織統治[3]の取組（組織方針、体制構築、監査、情報開示等）においてサイバーセキュリティも扱うべく、次に掲げる項目を安全基準等に規定することが望まれる[4]。

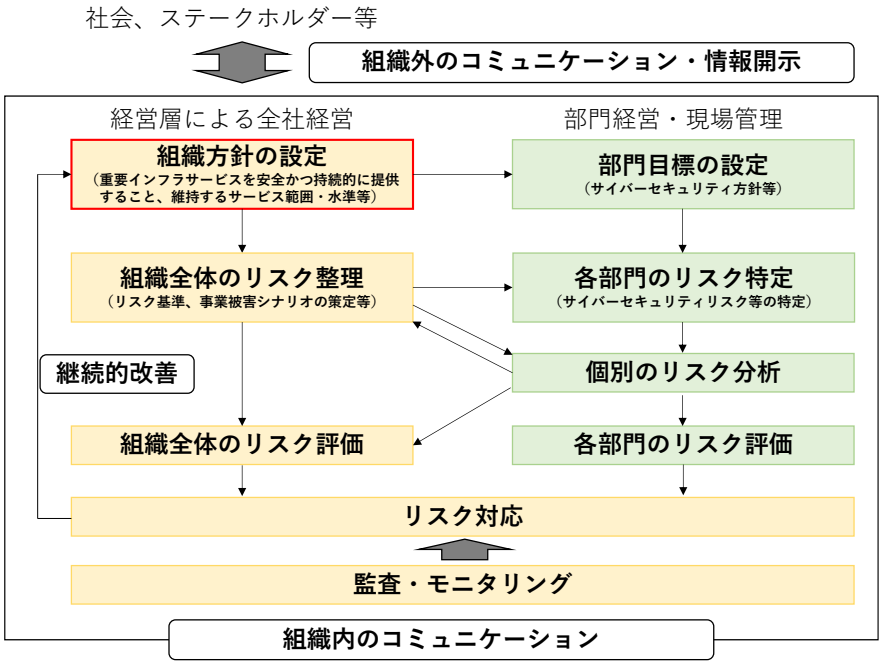

図　組織統治とサイバーセキュリティのイメージ

[3] 安全基準等策定指針では、組織統治とは、「組織の活動やその経営者・理事等の行動を規律する仕組み」及び「組織の不正を防止し、組織の財務の健全性および組織の競争力・持続可能性を高めるための仕組み」を意味する。なお、コーポレートガバナンス・コード（2021 年 6 月 11 日株式会社東京証券取引所）におけるコーポレートガバナンスの定義「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み」や、会社法（平成 17 年法律第 86 号）の求める内部統制システム「会社が営む事業の規模、特性等に応じたリスク管理体制」の構築も念頭に置かれるべきである。

[4] 経済産業省「サイバーセキュリティ経営ガイドライン」、内閣サイバーセキュリティセンター（以下「NISC」という。）「サイバーセキュリティ関係法令 Q&A ハンドブック」が参考になる。

3.1. 組織方針

3.1.1. 組織方針とサイバーセキュリティ

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。

3.1.2. サイバーセキュリティ方針

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

3.2. 組織内外のコミュニケーション

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。

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

組織全体[5]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。すなわち、組織方針を踏まえ、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、

[5] 経営層、CISO、戦略マネジメント層、担当者層といった縦の階層のほか、情報システム部門、事業部門、広報部門といった横方向にも留意。

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[6]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可能な限り理解するよう努めることが望ましい。

3.4. 責任及び権限の割当て

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[7]。特に、サイバーセキュリティに関する責任者（CISO 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[8]。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。

---

[6] 在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全てを含むサプライチェーン全体を俯瞰し、総合的にサイバーセキュリティを確保すべきである。

[7] 適切な管理体制の構築を前提としつつ、サイバーセキュリティに関する専門的な事項については、外部委託、業界団体との連携等により補完してもよい。

[8] 会社法第 362 条第 4 項の柱書及び同項第 3 号は、取締役会を設置する株式会社について「取締役会は、支配人その他の重要な使用人の選任及び解任の決定を取締役に委任することができない」旨を定めている。取締役会設置会社には、①監査役（会）を設置する会社、②監査等委員会設置会社、③指名委員会等設置会社の３つがある。

以上の①から③のいずれであっても、CISO 等の任命は、通常は「重要な使用人の選任」に該当する。該当する場合には、①監査役（会）設置会社は、CISO 等の任命は取締役会で決定しなければならない。また、②監査等委員会設置会社は、原則として CISO 等の任命は取締役会で決定しなければならないが（同法第 399 条の 13 第 4 項第 3 号）、例外として、取締役の過半数が社外取締役の場合（同条第 5 項柱書本文）、又は、定款の定め（同条第 6 項）がある場合には、CISO 等の任命を担当取締役に委任することができる。そして、③指名委員会等設置会社においては、取締役会の決議で、CISO 等の任命を含む業務執行の決定を執行役に委任することができる（同法第 416 条第 4 項柱書本文）。言い換えると、③では、そのような執行役への委任を行わない場合に限り、CISO 等の任命は取締役会で決定することになる。

他方、取締役会を設置しない株式会社について、同法第 348 条第 3 項の柱書及び同項第 3 号は、「取締役は、支配人の選任及び解任の決定を各取締役に委任することができない」旨を定めている。CISO 等は通常「支配人」には該当しないものの、取締役会を設置する会社とのバランスを考えると、取締役会を設置しない会社においても、CISO 等を任命する際には取締役の過半数の賛成を得ることが必要であると考えるべきである（同条第 2 項を参照）。

また、サイバーセキュリティに関する内部統制システムの構築において、「必要な内部組織及び権限」等について取締役会で決定されるべき事項としている。（NISC「サイバーセキュリティ関係法令 Q&A ハンドブック」〔2020 年 3 月 2 日〕）

3.5. 資源の確保

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、組織の価値を維持・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[9]であるとの考え方[10]のもとで配分する。

3.6. 監査・モニタリング

情報セキュリティ監査、システム監査等の監査[11]（難しい場合には少なくとも自己点検）を経営層の責任において実施する。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。

3.7. 情報開示

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、可能な範囲でサイバーセキュリティに関する取組を開示[12]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に関する責任者の知見
- 資源の確保
- リスクの把握と対応計画策定
- 緊急対応体制・復旧体制
- インシデントの発生状況

---

[9] 投資の概念については、会計、経営等様々な領域で定義が異なる。ここでは、直接の利益（リターン）を期待するものではないが、将来的なリスクを抑制し、リスクと利益の総和においてプラスの結果をもたらすための手段という意味で用いている。

[10] 一般に、セキュリティ対策への投資による直接的な収益を算出することは困難であり、サイバーセキュリティに関しては考え方の転換が必要。

[11] 内部監査を担当する部局は、組織トップの下に設けられることが多いが、その場合でも、事案の性質に応じて、報告先は組織トップとする場合と監査役等とする場合とを使い分けることとすべきである（デュアルレポートライン。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 6 月 28 日〕72 頁以下）。

[12] サイバーセキュリティに関する組織の情報を開示することは、組織の社会への説明責任を果たすとともに、組織運営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。

3.8. 継続的改善

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。

4. リスクマネジメントの活用と危機管理

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サイバーセキュリティの確保に取り組むことが重要である。

自組織の特性やリスクを特定した上で、①自組織の現在のセキュリティ対策の実施状況等に係る自己評価、②本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施を繰り返せるよう、次に掲げる項目を安全基準等に規定することが望まれる。

4.1. 組織状況の理解

重要インフラサービスに関する外部環境（政治、経済、社会等）及び内部環境（組織体制、戦略、能力等）の状況について、近い将来の状況も含めて整理する。また、関係法令、契約等に規定された義務、供給者・委託先が提示する制限事項等、関係者からの要求事項を整理する。任務保証の観点から次のような組織の特性を理解することが望ましい。

- 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

さらに、サイバーセキュリティに関する部門においては、組織状況を理解した上で、現段階におけるセキュリティ対策の実施状況等の実態を把握する。

4.2. リスクアセスメント

情報システム、ソフトウェア、情報等の資産を特定する。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。
- 制御システム[13]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[14]ことを念頭に、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[15]。

---

[13] 社会インフラや工場・プラントの監視・制御や生産・加工ラインにおいて、他の機器やシステムを管理・制御するために用いられている機器群。

[14] 一般に、重要インフラの制御システムは、独自仕様の機器や通信プロトコルで構成され、また、外部と接続のない閉域環境で運用される。

[15] IPA「制御システムのセキュリティリスク分析ガイド第 2 版～セキュリティ対策におけるリスクアセスメントの実施と活用～」に記載されている具体的な作業手順等が参考になる。

・ 情報システムの運用中も、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する。
・ 本来あるべき状況や要件を検討し、目標とする将来像を決定する。

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

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、マチュリティ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。

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

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。また、必要に応じて委託先に対しても伝達する。

4.3.3. リスク対応計画の策定

サイバーセキュリティに関するリスク対応計画を策定する。計画には次を記載することが望ましい。

・ 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

対応すべき代表的なサプライチェーン[16]に係る脅威は次のとおり。

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

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

[16] サプライチェーンとは、一般に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するものであり、安全基準等策定指針においては、外部組織が関与する製品（機器・ソフトウェア）又はサービス（クラウドサービス、保守管理役務等）を自組織で調達・利用するプロセスとする。

ュリティ対策の状況の把握を行う。

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。

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。さらに、リスクに応じて直接の供給者に連なる供給者への関与の程度を決定しつつ、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。また、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望ましい。

4.5. 事業継続計画等

サイバーインシデントが事業継続に及ぼす影響を踏まえ、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[17]、事業復旧計画[18]等）にサイバーセキュリティを組み入れる。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、情報システムに係る記載を詳細化した対応方針（IT-BCP 等）[19]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。

4.6. 人材育成・意識啓発

「サイバーセキュリティは全員参加（Cybersecurity by All）」との考え方のもと、全ての従業員がサイバーセキュリティの内規等への理解を深め、また、部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、人材育成・意識啓発を行う。

- セキュリティ対策業務に従事する人材を確保するため、キャリアパスの設計や外部人材活用の検討をすることが望ましい。
- セキュリティ対策業務に従事する人材に対し、「情報処理安全確保支援士」等の資格取得、演習・訓練への参加等を推進することが望ましい。
- セキュリティ対策が不十分であった場合に生じる影響例を示す等の方法によりセキュリティ対策の重要性について啓発をすることが望ましい。

---

[17] 大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、又は中断しても可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画。（内閣府「事業継続ガイドライン」〔令和３年４月〕３頁）

[18] 平時のサービス水準までの完全復旧対応の方針。

[19] サイバーセキュリティ基本法におけるサイバーセキュリティの定義には、情報システムの安全性及び信頼性の確保のために必要な措置も含まれる。

4.7. CSIRT 等の整備

CSIRT[20]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。

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

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[21]等の運用プロセスを確立することが望ましい。

4.8.2. 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）も踏まえ、組織内外と情報共有を実施する。

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。

- ISAC 等の分野専門性の高い情報共有活動に参加し、情報収集することが望ましい。
- 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が望ましい。
- 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、組織内外に情報提供を行うことが望ましい。

4.9. 危機管理

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。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。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。

4.10. 演習・訓練

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

[20] Computer Security Incident Response Team の略(シーサート)。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。

[21] 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のこと。

行う。経営層も交え、組織全体での演習・訓練[22]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、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。

[22] 例えば、NISC が主催する「分野横断的演習」。

5. 対策項目

「4.3.1.リスク対応の決定」において、安全基準等への盛り込みが望ましいセキュリティ対策を示す。

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

- 情報システム、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（利用が許される範囲）等を明確化した資産目録を作成・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。
- ネットワーク構成図、データの流れ図等を作成する。
- 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。

5.1.1.2. 情報分類と取扱い

- 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。

5.1.1.3. データ管理

- 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。

5.1.2. 供給者管理

- 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。
- 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。
- 供給者が提供するサービスの変更に対する管理を行う。
- 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。

5.1.3. 運用の管理

5.1.3.1. 運用の手順及び責任

- 情報システム等の運用に関連する手順書を整備する。
- 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。
- 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。
- 運用環境と開発・試験環境を分離する。

5.1.3.2. マルウェアからの保護

- マルウェアを検出及び予防する仕組みを整備し、マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。対策として、例えば、マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトの利用、システム負荷を抑えつつ未知の脅威に対応できることを特徴とするゼロトラスト型エンドポイントセキュリティのマルウェア無効化機能を導入する。

5.1.3.3. バックアップ

- 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する。

5.1.3.4. ログ取得

- 情報システムのイベントログや運用担当者の作業ログを記録・管理する。
- 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。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。

5.1.3.5. 運用ソフトウェアの管理

- 情報システム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。
- 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。サポート対象バージョンへの更新が困難な場合には、補完的な措置を講じる。

5.1.3.6. 脆弱性の管理

- 脆弱性情報を収集し、運用中の情報システムに対する影響の有無を確認する。
- 定期的な脆弱性スキャンを実施する。
- 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。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。

5.1.4. システムの取得・開発・保守

- 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。

5.1.5. インシデント管理

- インシデントの管理責任者を定める。
- 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。
- インシデントへの対応を通じて得た知識を、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。

5.2. 人的対策

5.2.1. 従業員の管理

- 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。

5.2.2. 委託先管理

- 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[23]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。

5.2.3. テレワーク・遠隔制御

- テレワーク・遠隔制御に関するサイバーセキュリティ確保のための対策を実施する。

5.2.4. エスカレーション

- 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。

[23] 自組織の従業員の管理に関する事項と同等の内容が考えられる。

5.3. 物理的対策

5.3.1. セキュリティ確保が求められる領域

・ セキュリティ確保が求められる領域を管理する。
  ＊ 物理的なセキュリティ境界を設定する。
  ＊ 入退管理の仕組みを構築する。
  ＊ 持ち込まれる物品の確認・制限を実施する。

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

・ 災害による障害が発生しにくい設備配置とする等の災害対策を実施する。

5.3.3. 装置の管理

・ 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。
・ 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る事前承認の仕組みを整備する。

5.4. 技術的対策

5.4.1. 利用者アクセスの管理

・ 情報システムや情報等へアクセスする利用者とそのアクセス権を管理する。
  ＊ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。
  ＊ 利用者アクセス権を定期的にレビューする。

5.4.2. 情報システム等のアクセス制御

・ 最小権限及び職務の分離の原則を踏まえて、情報やシステムの重要度に応じて、情報システムや情報へのアクセスを制限する。
  ＊ ログイン失敗回数を制限する。
  ＊ 良質なパスワードを利用する。
  ＊ 多要素認証を活用する。

5.4.3. 暗号を活用した情報管理

・ 暗号の利用方針や暗号鍵の管理方針を策定する。

5.4.4. 通信のセキュリティ

・ 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。

5.4.5. 多層防御

・ 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。

5.5. 動向を踏まえた対策

5.5.1. ランサムウェア対策

・ 速やかなパッチ適用等による脆弱性対策を講じる。
・ 海外拠点、サプライチェーンを含めて資産管理をする。
・ 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。
・ 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。
・ 役割等に基づいてネットワークを分割する。
・ 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。
・ ベンダーなどの関係者と協力関係を構築する。
・ 攻撃を受けた際は所管省庁や警察に連絡し、逐次時系列で状況を保存する。
・ ランサムウェア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。

5.5.2. クラウドサービス利用時の対策

・ 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[24]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。
・ 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。

24 利用者とクラウドサービス提供者が、責任分界点を定めるだけではなく、運用責任を共有し合っているという考え方。