重要インフラのサイバーセキュリティに係る
安全基準等策定ガイドライン

令和８年９月 11 日

内閣官房 国家サイバー統括室

目次

1　基本的な考え方

1.1　目的及び位置付け

「重要インフラ[1]のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）第３部では、重要インフラ所管省庁や各重要インフラ分野の業界団体等（以下「所管省庁等」という。）が策定する安全基準等[2]において、重要インフラ事業者等[3]が分野・事業者横断的に講ずべき対策として規定されるべき事項を記載している。そして、「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ガイドライン」（以下「安全基準等策定ガイドライン」という。）では、所管省庁等が安全基準等を策定するに当たって参照するための詳細事項を記載する。

重要インフラ事業者等が分野・事業者横断的に講ずべき対策を、安全基準等において明示することにより、重要インフラ事業者等のほかサプライチェーン[4]に関わる事業者等、重要インフラサービス[5]に携わる全ての関係者において理解の共有が進み、必要な対応が行われることを目指す。

統一基準第３部に定める各対策をどのような形で安全基準等に盛り込むかについては、関係法令の規定及び安全基準等の構成等を踏まえ、重要インフラ分野ごとに検討されることを想定する。

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。

---

[1] 国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの。

[2] 重要インフラにおける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。具体的には次の４分類が想定される。

① 関係法令に基づき政府機関が定める「強制基準」

② 関係法令に準じて政府機関が定める「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

[3] 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。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。

[4] 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。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。

[5] 重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。

なお、各分野におけるリスクベース[6]の取組については、統一基準第３部に定める対策の水準に止めることなく、更なる水準の向上を図ることが望ましい。

1.2 記載の観点及び構成

重要インフラは、被害を受ければ、国民生活や社会経済、ひいては国家安全保障に甚大な影響を及ぼすおそれがあり、重要インフラ事業者等は、自らの社会的責務を果たすためにも、サイバーセキュリティの確保に大きな責任を負う。

サイバー脅威の深刻化が進む中、あらゆるサイバー攻撃から完全に防御することは困難であるところ、事前対応によるサイバー攻撃の防御・抑止のみならず、障害等が発生した際の影響を許容範囲内に抑制するレジリエンス[7]の確保が必要となっている。

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[8]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、レジリエンスを高めることが不可欠である。

サイバーセキュリティ対策は、企業の存続の鍵となり得る重要な経営課題である。経営層[9]は、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不十分なことに起因して組織や第三者に損害が生じた場合、善管注意義務違反や任務懈怠（けたい）に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う。

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、自組織のリスクを幅広く踏まえて、リスクマネジメント等による事前対応と、障害等が発生した際の被害の

---

[6] 統一基準において「リスクベース」とは、「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といったリスクであって、分野の特性・実情等を踏まえて特定、評価したものをベースとする考え方」と定義する。

[7] インシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のこと。

[8] 任務保証とは、サイバーセキュリティ戦略（令和７年 12 月 23 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。

[9] 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。

拡大防止・早期復旧といった危機管理の両面から、重要インフラのサイバーセキュリティ確保に取り組むことが重要である。

以上の観点から、統一基準第３部では、「組織統治[10]」、「識別」、「防御」、「検知」、「対応及び復旧」等のそれぞれにおいて必要となる対策事項を記載している。

1.3 対象範囲

重要インフラを標的とするサイバー脅威のリスクが顕在化する中、これまでの考え方にとらわれることなく、サイバー脅威の動向等を踏まえた対策が必要となっている。例えば、従来、事業者によっては閉域網という理由でサイバー攻撃を想定していなかった基盤・制御システムも、システム更改による環境変化や攻撃手法の変化によって、リスクは高まっている。閉域網だから安全とは限らないとの認識の下、基盤・制御システムのセキュリティ対策を徹底することが重要である。このように、「閉域網だから安全」、「専用 OS だから安全」、「独自技術仕様だから安全」といった過信により、サイバー攻撃の被害に遭う危険性が高まることを改めて認識する必要がある。

重要インフラのレジリエンスを確保し、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観点から、安全基準等における対象範囲の設定に当たっては、各分野において、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[11]や、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスク[12]などを踏まえ、リスクベースの考

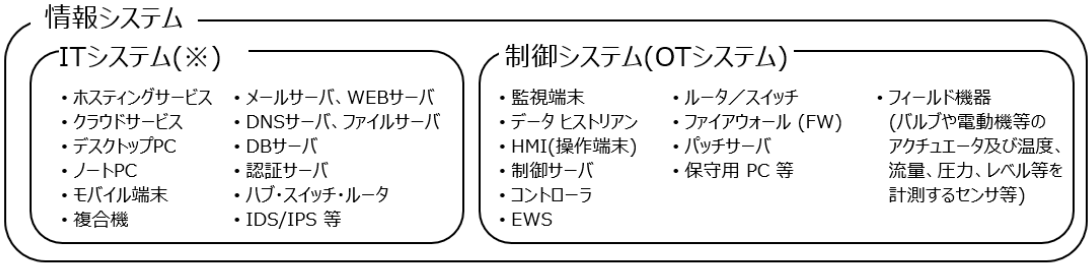
[10] 統一基準では、組織統治とは、「組織の活動やその経営者・理事等の行動を規律する仕組み」及び「組織の不正を防止し、組織の財務の健全性及び組織の競争力・持続可能性を高めるための仕組み」を意味する。なお、コーポレートガバナンス・コード（2021 年６月 11 日株式会社東京証券取引所）におけるコーポレートガバナンスの定義「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み」や、会社法（平成 17 年法律第 86 号）の求める内部統制システム「会社が営む事業の規模、特性等に応じたリスク管理体制」の構築も念頭に置かれるべきである。

[11] 事務処理等を行う IT を用いたシステム、フィールド機器や監視・制御システム等の制御系のシステム等を含むシステム全般。

[12] 例えば、①不正機能等の埋め込み、②サービスの供給途絶、③外部サービスにおける情報の不適切な取扱い、④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等が想定される。

え方に基づく適切な範囲を設定する。その際、「重要システム[13]」のみならず、例えば、重要システムが属するネットワークに影響が及び得るサイバー攻撃が発生した場合の重要システムへの影響等も考慮する必要がある。

なお、安全基準等策定ガイドラインにおける「情報システム」の概念及び具体例は下記図表１「情報システムの概念図及び具体例」のとおりであり、この情報システムには「制御システム[14]」も含まれるところ、次章「２　組織統治」以降に記載の各対策事項は、原則として制御システムにも適用されることを想定している。



図表１　情報システムの概念図及び具体例

安全基準等策定ガイドラインでは、必ずしも制御システムには適用されない、あるいは適用が容易ではない場合が想定される次の対策事項においては、「［IT システムのみ］」と記載している[15]。

・　ペネトレーションテストの実施［3.6②-3］
・　メールインフラの保護［4.3.2①-5］
・　高度なマルウェア対策機能等の導入[4.4.4①-2］

1.4 関係主体の役割

[13] 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。
[14] 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。
[15] ［IT システムのみ］と記載した対策事項を制御システムについて実施するかどうかについては、実施の効果と実施に際するリスクを考慮し、分野ごと（あるいは運用上は事業者等ごと）に、分野の特性等を踏まえつつ個別に判断することが期待される。

安全基準等においては、重要インフラ所管省庁、重要インフラ事業者等、サプライチェーンに関わる事業者等の主要な関係主体について、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とともに、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ことが望ましい。

1.5 安全基準等策定ガイドラインの構成

次章「２　組織統治」以降では、統一基準第３部に定める対策事項ごとに、より具体的に「講ずべき対策事項」及び「講ずることが望ましい対策事項」を記載しているところ、それら記載内容は次のとおりである。

「統一基準における規定」

統一基準第３部における規定を引用。

「講ずべき対策事項」

統一基準第３部における規定に基づき、重要インフラ事業者等が分野・事業者横断的に講ずべき対策事項を「講ずべき対策事項」として記載するとともに、「解説」として、対策事項の実施に際しての考え方や補足説明等を記載する。これにより、所管省庁等が、安全基準等策定ガイドラインを参照しつつ、分野の特性・実情等を踏まえて安全基準等を策定し、分野・事業者横断的なセキュリティ対策の水準の底上げ等を図ることを目的とする。なお、「解説」はあくまでも参照のための補足であり、これによって対策事項に係る対応方法を詳細に定め、一律の対応を求めるものではない。

「講ずることが望ましい対策事項」

分野・事業者によっては直ちに実施することが困難である場合が想定されるが、可能な範囲で講ずることが望ましい対策事項を「講ずることが望ましい対策事項」として記載する。これにより、各分野におけるリスクベースの取組の更なる水準の向上等を図ることを目的とする。本対策事項は、所管省庁等が、各分野において重要インフラ事業者等の対策状況等を踏まえ判断の上、安全基準等に規定することが望ましい。

例えば、以下の対策が該当する。

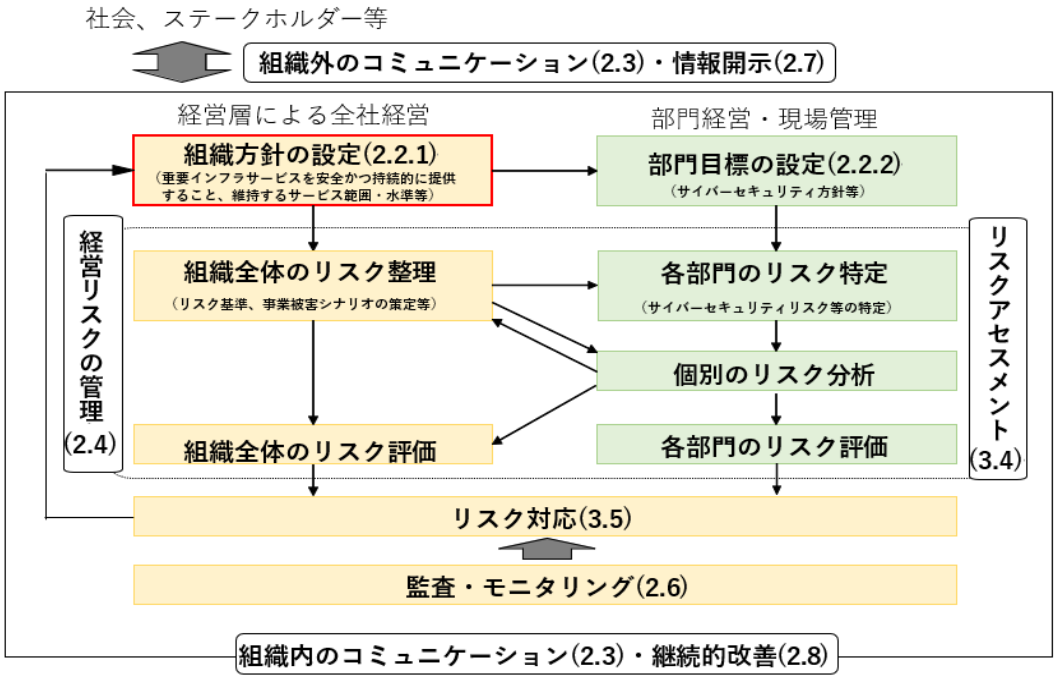
- 機微な情報を取り扱っている、標的にされやすい等の理由から特にセキュリティリスクの高いサービス・事業者・分野等において必要になると考えられる対策
- コスト・人材・専門知識等の観点から、必ずしも全ての事業者にとっては導入が容易ではないと考えられる対策
- 制御システムに関する対策等、特に分野によりとるべき具体的な対策が異なり得ると考えられる対策
- 技術・脅威の動向等を踏まえた先進的な対策

1.6 安全基準等策定ガイドラインの改定

統一基準は、その内容や水準を適切に維持するため、原則として３年に１度、見直しを行うこととされている。安全基準等策定ガイドラインについても、これを踏まえ適切な頻度において、技術や脅威等、重要インフラを取り巻く環境変化に応じて適宜内容の見直しを行う。

2　組織統治

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、任務保証の観点から、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当たり、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[16]。



図表２　組織統治とサイバーセキュリティのイメージ

[16] 経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」、国家サイバー統括室「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」〔令和５年９月〕が参考になる。

2.1 組織状況の理解

統一基準における規定

① 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。

講ずべき対策事項

①-1 任務保証の観点から次のような自組織の特性を把握・整理する。

- 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

①-2 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。

（解説）

- 「外部環境」については、例えば次のものが想定される。
  - 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
  - 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、サイバー攻撃への悪用可能性のある技術（高性能 AI[17]等）、それらの報道等による社会からのセキュリティ認識の広まり
  - 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等のサービス
  - 自組織・他組織においてセキュリティインシデントが発生した場合の相互依存性

[17] AI の定義について、総務省・経済産業省「AI 事業者ガイドライン（第 1.2 版）」では、「広義の人工知能の外延を厳密に定義することは困難である。本ガイドラインにおける AI は『AI システム･･･』自体又は機械学習をするソフトウェア若しくはプログラムを含む抽象的な概念とする。」としている。

・　「内部環境」については、例えば次のものが想定される。
  - 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
  - 重要インフラサービスに係る情報システム・制御システム・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の状況
  - 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
  - 役職員のセキュリティリテラシー

講ずることが望ましい対策事項

なし

統一基準における規定

② 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。

講ずべき対策事項

②-1 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。

（解説）

・ 関係法令については、例えば、以下が想定される。その他を含む詳細については、国家サイバー統括室「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」〔令和５年９月〕も参照することが考えられる。

- 各重要インフラ分野の事業法、安全基準等
- 重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法。令和７年法律第 42 号）
- 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法。令和４年法律第 43 号）
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 私的独占の禁止及び公正取引の確保に関する法律（独占禁止法。昭和 22 年法律第 54 号）
- 製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法。昭和 31 年法律第 120 号）

講ずることが望ましい対策事項

なし

統一基準における規定

③　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。

講ずべき対策事項

③-1　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。

（解説）

- セキュリティ対策の実施状況等の実態把握では、組織的なモニタリングプロセスによる実態把握も想定される（2.6「監査・モニタリング」参照）。
- 統一基準第２部 2.2「把握・分析」に定める「全ての分野・事業者を対象とした質問調査」に基づく重要インフラ・サイバーセキュリティ・セルフアセスメント（CI-CSA）では、重要インフラ事業者等が自身の回答を通じて自己評価を行い、自組織のセキュリティ対策の実施状況を客観的に把握すること（成熟度モデル[18]）を主要な目的の１つとしている。各重要インフラ事業者等において成熟度モデルを活用することにより、現段階におけるセキュリティ対策の実施状況と、求められるセキュリティ要件との差異を分析、改善すべき対策の優先順位を明確化し、継続的なセキュリティ水準の向上を図ることが期待される。
- 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、他の例として、NIST サイバーセキュリティフレームワーク（CSF）におけるプロファイルの活用や、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）の活用も考えられる。

講ずることが望ましい対策事項

なし

[18] 組織において現在取り組んでいる対策や手法等の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仕組み。

2.2 組織方針

2.2.1 組織方針とサイバーセキュリティ

統一基準における規定

① 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。

講ずべき対策事項

①-1 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。

（解説）

- 重要インフラのサイバーセキュリティ確保に関して、組織方針に組み入れるべき事項としては、例えば、次のものが想定される。
  - 重要インフラサービスの安全かつ持続的な提供の実現
  - サイバー脅威はサービス提供を阻害するリスクの一つ（例：電力供給が止まる、送金サービスが停止するなど）
  - リスクマネジメントの対象にサイバーセキュリティに関する事項を含める
  - 維持すべきサービス範囲・水準

講ずることが望ましい対策事項

なし

2.2.2 サイバーセキュリティ方針

統一基準における規定

① 組織方針を踏まえ、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及び法規制等への対応、経営層によるコミットメントが記載されたサイバーセキュリティ方針を策定する。

講ずべき対策事項

①-1 組織方針を踏まえ、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及び法規制等への対応、経営層によるコミットメントが記載されたサイバーセキュリティ方針を策定する。

（解説） ・ サイバーセキュリティ方針は、経営層の責任において策定する。 ・ 細目等ではなく基本方針について記載することが想定される[19]。

講ずることが望ましい対策事項

なし

[19]「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」17 頁

2.3 組織内外のコミュニケーション

統一基準における規定

① 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。

講ずべき対策事項

①-1 リスクマネジメントにおけるコミュニケーションの一環として、経営層と担当者層との間で定期的な対話の機会を設け、サイバーセキュリティリスク、インシデント等の情報を取り扱う。

（解説）

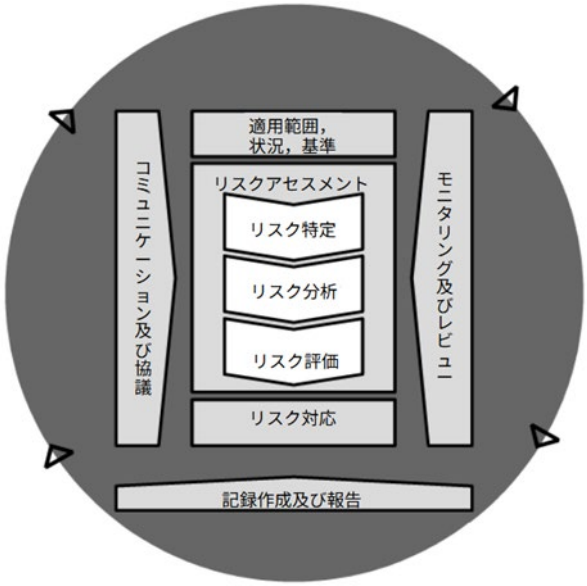
- 「経営層と担当者層との間で定期的な対話の機会」に関して、例えば、組織横断的な事項の審議のため、サイバーセキュリティを推進するセキュリティ対策推進体制及び各部局（部門）の代表者から構成される委員会を設置することが考えられる。また、委員会の配下に実務を担当する下位委員会を設置し、実務レベルの詳細な事項を調整することで、委員会の運営を効率化することも考えられる。
- 「サイバーセキュリティリスク、インシデント等の情報」については、例えば、次のものが想定される。
  - サイバーセキュリティに関する環境変化
  - 自組織及び参考となる他組織のインシデントの発生状況・得られた教訓
  - セキュリティ対策の実施状況・有効性評価等

①-2 リスクマネジメントの一環として、サイバーセキュリティに関するリスクが影響を及ぼす可能性のある組織内外のステークホルダーを把握し、コミュニケーション及び協議のための体制を構築する。

（解説）

- 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おいては、リスクアセスメントにおいて分析したリスクについてステークホルダーと共有や議論を行うほか、例えば、リスクマネジメントの各ステップの活動を行うために必要な分析に使用する最新の情報・手法や、リスク特定・評価に必要なステークホルダーに関する情報の共有を行うことが考えられる。

・ 重要インフラサービスの安全かつ持続的な提供の観点から、コミュニケーション及び協議のための体制を構築すべきステークホルダーとしては、例えば、政府機関、サプライチェーンに関わる事業者、当該分野や（影響が及び得る）他分野の業界団体・重要インフラ事業者等の関係主体（1.4「関係主体の役割」参照）が考えられる。
・ 3.3「情報共有」もあわせて参照。
・ リスクマネジメントのプロセスについては、JIS Q 31000:2019 を参照。



図表３　リスクマネジメントのプロセス

［出典］JIS Q 31000:2019

講ずることが望ましい対策事項

①-3 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。

①-4 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。

2.4 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

統一基準における規定

① 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。

講ずべき対策事項

①-1 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。

（解説）

- 経営層、CISO[20]等を含む、ガバナンスが適切に展開できる体制を整備する。また、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ガバナンスを展開できる体制とすることに留意する。
- 組織内の体制整備に関して、例えば、組織横断的な事項の審議のため、サイバーセキュリティを推進するセキュリティ対策推進体制及び各部局（部門）の代表者から構成される委員会を設置することが考えられる。また、委員会の配下に実務を担当する下位委員会を設置し、実務レベルの詳細な事項を調整することで、委員会の運営を効率化することも考えられる。（再掲（2.3①-1 参照））
- 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形で整理を行うに当たっては、例えば、事業被害ベースのリスク分析[21]に基づき、回避したい事業被害（例：広域でのサービス供給停止）を洗い出すとともに、当該事業被害を引き起こすと想定される攻撃を特定することが考えられる。

[20] Chief Information Security Officer の略。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。

[21] 回避したい事業被害を明確化し、事業被害を引き起こすと想定される攻撃について、事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析手法。

・ 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よう、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のみならず、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する体制を整備する。

①-2 経営層の意思決定を補助するため、サイバーセキュリティに関する責任者（CISO等）は、サイバーセキュリティリスク及びそれによる事業運営への影響について報告する。

（解説）

・ 報告に当たっては、例えば、次の事項を考慮する。
  - 報告の頻度、適時性
  - 報告の方法
  - 情報と組織の目的及び意思決定との関連

①-3 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等について整理することを念頭に、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理解する。

講ずることが望ましい対策事項

なし

統一基準における規定

②　サイバーセキュリティリスクに係るリスクファイナンスを検討する。

講ずべき対策事項

②-1 サイバーセキュリティリスクに係るリスクファイナンスを検討する。

（解説）

- 近時のランサムウェア攻撃事案でも示されているように、サイバー攻撃により極めて大きな財務的インパクトが発生し得る。そのため、リスクファイナンスは、企業が事業体として存続するために必要な資源を手当てするといったレジリエンスの観点から重要である。
- リスクファイナンスの手段としては、例えば、サイバー保険によるリスク共有・移転等が考えられる。
- 「検討」については、実効性確保の観点から、検討結果を経営層に報告し、承認を得ることが考えられる（他の対策事項記載の「検討」においても同様であり、本対策事項に限らない。）。
- なお、インシデント対応における費用負担及びサイバー保険については、「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」・Q65 を参照。

講ずることが望ましい対策事項

なし

2.5 役割・責任・権限

2.5.1 責任及び権限の割当て

統一基準における規定

① 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職員を決定するとともに責任及び権限を割り当てる。

講ずべき対策事項

①-1 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職員を決定するとともに責任及び権限を割り当てる。

（解説）

- 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、外部委託や、業界団体との連携等による補完も考えられる。
- 責任及び権限の割当てに当たっては、「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き[22]」を参照。
- サイバーセキュリティを担当する部署及び職員は、自らが主体となって業務を実施することに加え、事業部門（制御システムを含む各事業部で活用するシステムを管理する部門等を含む）や管理部門（例：総務、法務、内部監査、人事）が主体となって行う実務を、一定の専門的な知見を用いて支援することも考えられる。

【「サイバーセキュリティ人材フレームワーク」について】

- 役割・責任・権限の検討にあたっては、国家サイバー統括室「サイバーセキュリティ人材フレームワーク」及び「同活用の手引き」が参考になる。フレームワークに沿って、自組織のサイバーセキュリティ体制や配置されている人材を可視化することで、現状の体制及び人材の配置と理想的な姿との乖離を把握できるようになる。その乖離の解消に向けて、採用、配置、教育・訓練を継続的に進めることで、自組織として目指すサイバーセキュリティ体制の実現につなげることが可能となる。

[22] https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

講ずることが望ましい対策事項

①-2 業務部門、リスク管理部門、内部監査部門のサイバーセキュリティに関する責任分担を明確化する。

①-3 制御システムに関するセキュリティ責任者を設置し、IT 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。

統一基準における規定

② サイバーセキュリティに関する責任者（CISO 等）を任命し、その任命に当たっては、経営層の責任において実施する。

講ずべき対策事項

②-1 サイバーセキュリティに関する責任者（CISO 等）を任命し、その任命に当たっては、経営層の責任において実施する。その際、CISO 等は CIO 等と兼務ではなく、専任者として任命することを検討する。

（解説）

- CISO 等の任命に関して、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。CISO 等の任命は、通常は「重要な使用人の選任」に該当するところ、その場合には、監査役（会）を設置する会社や監査等委員会設置会社は、原則として[23]CISO 等の任命を取締役会で決定しなければならない（同法第 399 条の 13 第４項第３号）。また、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[24]（同法第 416 条第４項柱書本文）。
- 他方、取締役会を設置しない株式会社においても、取締役会を設置する会社とのバランスを考えると、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られる[25][26]（同法第 348 条第２項）。

[23] 監査等委員会設置会社は、例外として、取締役の過半数が社外取締役の場合（同法第 399 条の 13 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。

[24] 言い換えると、指名委員会等設置会社では、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。

[25] 前提として、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」旨を定めており、CISO 等は通常「支配人」には該当しない。

[26] また、「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」19 頁では、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。

・ 牽制も含めたCISO等の機能の実効性の確保の観点から、CISO等をCIO等と兼務ではなく、専任者として任命することが考えられるところ、組織の規模等も考慮の上、検討する。

講ずることが望ましい対策事項

②-2 CISO等は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、通常時から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るべく、経営層に相当する者の中から任命する。

②-3 経営層は、CISO等が必要な権限を有していることを確認するため、定期的なレビューを実施する。

（解説）

・ CISO等の必要な権限としては、例えば、経済産業省「サイバーセキュリティ経営ガイドラインVer.3.0」における「サイバーセキュリティ経営の重要10項目」に関する権限等が考えられる。

・ 経営層の責任においてレビューを実施し、その結果を把握することが求められるところ、その上で、レビューの形式・方法等については、内部・外部のいずれにより実施するかも含め、自組織に有効と考えられる形式・方法等を選択し、実施することが考えられる。

2.5.2 資源の確保

統一基準における規定

① 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、組織の社会的責務を果たすため、また、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も必要不可欠な投資[27]であるとの考え方のもとで配分する。

講ずべき対策事項

①-1 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、組織の社会的責務を果たすため、また、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も必要不可欠な投資であるとの考え方のもとで配分する。

（解説）

- サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資 （将来の事業活動・成長に必須な費用）と位置付けることが重要である。特に重要インフラサービスの機能停止が経済社会にもたらす影響の大きさを踏まえる必要がある。
- 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。適切な予算確保ができていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダーへの委託が困難となるおそれがある。
- サイバーセキュリティ対策のための資源（予算、人材等）確保の検討に当たっては、経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」及び「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き」を参照。

[27] 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。

講ずることが望ましい対策事項

①-2 経営層は、組織が設定したリスク許容度と対応策に応じた資源の配分となっているかを確認するため、定期的なレビューを実施する。

（解説）

・ レビューに係る体制については、内部・外部も含め、自組織に有効と考えられる体制を選択し、実施することが考えられる。

2.5.3 CSIRT 等の整備

統一基準における規定

① CSIRT[28]としての機能を持つ体制を整備する。

講ずべき対策事項

①-1 サイバー攻撃リスクの特性を考慮した事業継続計画等[29]の実行に必要な組織体制の一つとして、CSIRT としての機能を持つ体制（以下「CSIRT 等」という。）を重要インフラ事業者等の内部に整備する。

（解説）

- CSIRT 等について、組織として常設する場合又はインシデント発生時のみ設置する場合があり得る。

  また、CSIRT 等は、実効性を確保する観点から、重要インフラ事業者等の内部に整備すべきところ、自組織内の CSIRT 等を窓口として、外部（例えばグループ会社に設置された CSIRT 等）にインシデント対応の支援を要請するといった体制もあり得る。

  これらについては、トップマネジメントの一環として、自組織に有効と考えられる体制を選択し、整備することが考えられる。
- CSIRT 等は、規程・社則・技術的ガイドラインの策定、リスクアセスメント実施等の通常時のセキュリティマネジメントに係る業務を推進する役割のほか、セキュリティ確保の観点から、例えば、次の役割を担うことも考えられる。
  - 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[30]及び事業継続計画[31]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

[28] 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。

[29] 「事業継続計画等」については、6.1「事業継続計画等」参照。

[30] 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。

[31] 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）

- 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

・ CSIRT 等に係る体制の整理及び見直しについては、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）「CSIRT マテリアル[32]」を参照。

・ 企業内の情報システムを対象とする CSIRT に限らず、顧客向けに提供される製品・サービスを対象としてインシデント対応を行う組織（xSIRT: Security Incident Response Team）については、国家サイバー統括室「xSIRT 構築の事例」[33]を参照。

①-2 CSIRT 等は、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する。

（解説）

・ 関連部門としては、例えば、インシデントの当事者となる部門、広報部門、調達部門、法務部門、総務部門等が考えられる。

①-3 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の専門知識を持つ組織との連携体制を整備する。

（解説）

・ 例えば、サイバー空間関連事業者[34]及びサイバーセキュリティ関係機関[35]との連携が想定される。

[32] https://www.jpcert.or.jp/csirt_material/

[33] https://security-portal.cyber.go.jp/dx/xsirt.html

[34] 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のうち、重要インフラサービス提供に必要な情報システムに関係するサプライチェーン等に関わる、機器納入、システムの設計・構築・運用・保守等を行うシステムベンダー、ウィルス対策ソフトウェア等のセキュリティ対策を提供するセキュリティベンダー等、ハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー及びクラウドサービス等の外部サービスを提供する事業者

[35] 国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）及び一般財団法人日本サイバー犯罪対策センター（JC3）。

①-4 インシデント等について、組織外から CSIRT 等に通知する手段（例：メールアドレス、WEB フォーム等）を確立する。

（解説）

・ いわゆるインデント・脆弱性・情報セキュリティ報告窓口等、顧客等を含めて幅広く CSIRT に通知する手段を確立することを想定している。

講ずることが望ましい対策事項

①-5 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関連部門の専門知識が要求される可能性を踏まえ、CSIRT 等が制御システム関連部門と連携できる体制を整備する。

2.5.4 役職員の管理

統一基準における規定

① 役職員（特に重要システムの構築・運用に携わる職員）について、情報やシステムの重要度に応じて、配置・管理する。

講ずべき対策事項

①-1 役職員（特に重要システムの構築・運用に携わる職員）について、情報やシステムの重要度に応じて、配置・管理する。

①-2 全ての役職員を対象とする守秘義務のルールを定める。

（解説）

- 守秘義務のルールは、職務の内容、取り扱う情報やシステムの重要度等に応じて、個別に定めることも考えられる。
- 守秘義務のルールについては、経済産業省「秘密情報の保護ハンドブック ～企業価値向上に向けて～[36]」を参照。

講ずることが望ましい対策事項

①-3 人事プロセス（例：採用審査、入社・退社手続、人事異動）において、サイバーセキュリティリスク管理を考慮する。

（解説）

- 人事プロセスにおけるリスク管理の例としては、サイバーセキュリティ担当者等採用時の力量の確認、雇用契約における守秘義務の明記、人事異動後のセキュリティ教育等が考えられる。

①-4 採用、教育、人材定着等に関する決定において、サイバーセキュリティに係る知見の保有を考慮する。

[36] 例えば、参考資料２「各種契約書等の参考例」が記載されている。
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

2.6 監査・モニタリング

統一基準における規定

① 情報セキュリティ監査、システム監査等の監査（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。

講ずべき対策事項

①-1 情報セキュリティ監査、システム監査等の監査（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。

（解説）

- 監査については、内部監査・外部監査のいずれの形式もあり得るところ、トップマネジメントの一環として、自組織に有効と考えられる監査形式を選択し、実施することが考えられる。
- セキュリティ対策の実効性を担保するためには、独立性及び専門的能力を有する者による監査を実施することが重要であるが、監査に係る要員や工数等が確保できない等、監査が難しい場合には、少なくとも事業部門又は管理部門による自己点検を行う。自己点検のみを実施する場合には、例えばCISO等に対して自己点検結果を報告することを定めるなど、自己点検の実効性を確保するための仕組みを検討する必要がある。
- 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）。
- 監査実施計画の策定における考え方や計画に含めるべき内容等については、経済産業省「情報セキュリティ監査基準 実施基準ガイドラインVer2.0[37]」を参照。
- 監査業務を外部事業者に請け負わせる場合について、経済産業省が定める「情報セキュリティサービス基準[38]」及び当該基準を満たすと認められた企業を記載し

[37] https://www.meti.go.jp/policy/netsecurity/is-kansa/IS_Audit_Annex12.pdf

[38] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

た「情報セキュリティサービス基準適合サービスリスト[39]」（うちセキュリティ監査サービスに係る部分）を参照。

講ずることが望ましい対策事項

①-2 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、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。

①-3 サイバーセキュリティ要件の遵守状況についてツール等を用いて継続的に評価する。

（解説）

- 例えば、端末やサーバ等における脆弱性の対応状況、構成の規定遵守状況、承認状況（未承認機器の有無）、ユーザーの管理状況（未承認ユーザーの有無）について、ツール等を用いて継続的にモニタリングし、評価することが考えられる。

[39] https://www.ipa.go.jp/security/service_list.html

統一基準における規定

② 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）を定期的にモニタリングする。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モニタリングする。

講ずべき対策事項

②-1 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）を定期的にモニタリングする。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モニタリングする。

（解説） ・ セキュリティ対策の導入・運用に伴うリスクの状況変化としては、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）の発生頻度の変化や、当該事象の結果の影響度の変化等を想定している。

講ずることが望ましい対策事項

なし

2.7 情報開示

統一基準における規定

① 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する。

講ずべき対策事項

①-1 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する。

（解説）

- サイバーセキュリティに関する取組を開示（公表）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される。
- 例えば、次の情報を開示することが考えられる。ただし、これらについて一律の公表を求める趣旨ではなく、攻撃者の攻撃を助長する可能性等を考慮の上、情報開示の対象・内容や開示タイミングを適切に決定することが想定される。
  - 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（例：スキル・マトリックスにおける取締役のスキル等）
  - 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
- インシデントの発生状況等、サイバー攻撃被害に係る情報開示については、6.2.3「インシデントの報告とコミュニケーション」も参照。
- サイバー攻撃被害に係る情報の共有・公表の具体的な方法や留意点等について、経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」、「サイバー攻

撃被害に係る情報の共有・公表ガイダンス[40]」（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）、「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」・Q6 を参照。

講ずることが望ましい対策事項

なし

[40] https://www.cyber.go.jp/council/cs/kyogikai/guidancekentoukai.html

2.8 継続的改善

統一基準における規定

① 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。

講ずべき対策事項

①-1 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。

講ずることが望ましい対策事項

なし

統一基準における規定

② 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、リスク対応計画を含む各種計画等の継続的改善を行う。

講ずべき対策事項

②-1 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、リスク対応計画を含む各種計画等の継続的改善を行う。

（解説）

- 継続的改善の対象文書として、以下が想定される。
  - ・サイバーセキュリティ方針[2.2.2.①-1]
  - ・リスク対応計画[3.5.3.①-1]
  - ・事業継続計画等[6.1.①-1]
  - ・以下に例示する個別方針等
    - 情報分類と取扱いの手順[3.1.2.②-1]
    - 情報システムへのパッチ適用等に関する作業方針[3.6.③-1]
    - データの管理方針[4.3.1.①-1]
    - 情報システム等の運用に関連する手順書[4.4.1.①-1]
    - テレワーク・遠隔制御に関する対策方針[4.6.2.①-1]

講ずることが望ましい対策事項

②-2 サイバーセキュリティ方針、各種計画等の改善の要否の判断を、少なくとも１年に１回行う。

2.9 サプライチェーン・リスクマネジメント

統一基準における規定

① 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・委託先のセキュリティ対策の状況の把握を行う。

講ずべき対策事項

①-1 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・委託先のセキュリティ対策の状況の把握を行う。

（解説）

【サプライチェーン・リスクマネジメント全般について】

- クラウドサービスの利用等を含め、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た上で、必要なサイバーセキュリティを確保することが重要である。
- サプライチェーンに係る脅威として主に想定されるものは次のとおり。また、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については、これらの脅威の観点も踏まえて把握することが考えられる。
  - 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
  - 不正機能等の埋め込み
- サプライチェーンに係る供給者・委託先等の管理（サードパーティリスク管理）においては、供給者・委託先等が遵守すべきサイバーセキュリティ要件を明確化の上、重要度に応じ、契約やSLA（サービスレベルアグリーメント）等（以下「契約書等」という。）に明記することが重要である。
- サプライチェーン・リスク対応の詳細については、国家サイバー統括室「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[41]」を参照。また、対応が進んでいるとされる米国・EU・英国の金

[41]本手引書におけるサプライチェーン・リスクの範囲は、「発注者の意図しない変更を攻撃者が情報システムや機器等に加えることにより、機密情報を窃取するなどの情報セキュリティ上のサプライチェーン・リスク」に限定されている点に留意（同書３頁）。
https://www.cyber.go.jp/pdf/policy/general/risktaiour7.pdf

融機関における管理手法を調査した「金融機関のサードパーティ・サイバーセキュリティリスク管理強化に関する調査[42]」の報告書も参考になる。

【供給者・委託先のセキュリティ対策の状況の把握について】

- 供給者・委託先のセキュリティ対策の状況の把握に際し、第三者による評価検証結果（例えば、ISMS 適合性評価制度や、経済産業省・国家サイバー統括室「サプライチェーン強化に向けたセキュリティ対策評価制度[43]」（以下「SCS 評価制度」という。））を活用し、把握の負担を軽減することが考えられる。

【SCS 評価制度について】

- SCS 評価制度は、サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化することで、委託元企業・委託先企業双方の負担を軽減しつつ、サプライチェーン全体のセキュリティ水準の底上げを図る仕組み。「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」に基づき検討が進められており、2026 年度末頃に制度開始が予定されている。

①-2 供給者・委託先を管理するための台帳等を整備し、維持する。

（解説）

- 台帳等に記載する供給者・委託先については、外部サービスも含め様々な対象が想定されるところ、台帳等の維持の負担軽減の観点からも、重要度に応じて記載する供給者・委託先、あるいは管理項目を設定することが考えられる。

講ずることが望ましい対策事項

①-3 供給者・委託先に対し、サプライチェーン企業のリスクマネジメント実施状況について、リスクや関与の程度に応じて把握するように求めることで、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。

[42] https://www.fsa.go.jp/common/about/research/20260403/20260403.html

[43] https://www.meti.go.jp/policy/netsecurity/scs.html

統一基準における規定

② 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（供給者や委託先の選定・管理・対策の助言等）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。

講ずべき対策事項

②-1 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（供給者や委託先の選定・管理・対策の助言等）を行う。海外拠点については、現地の法令、文化等も踏まえた対応を行う。

（解説）

- サプライチェーン・リスクへの対応としては、例えば次のものが想定される。

【サービスの供給途絶に係る脅威に対するリスク対応】

- 部品の供給役務の継続提供の担保又は代替手段の検討
- 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するリスク対応】

- 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

【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に係る脅威に対するリスク対応】

- 第三者による評価検証結果（SCS 評価制度、ISMS 適合性評価制度等）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

【不正機能等の埋め込みに対するリスク対応】

（2.9.③-4 を参照）

- 発注者となる組織においては、独占禁止法及び取適法を考慮したパートナーシップ体制を構築する[44]。
- 「対策の助言」については、大手企業から、サプライチェーンに参加する中小企業に対し、対策の要請とあわせて、具体的な対策内容等について助言・支援を行

[44] 経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」
https://www.meti.go.jp/policy/netsecurity/partnership2.html

うといったケースが想定される。助言・支援に当たっては、政府機関が提供する中小企業等への支援施策（サイバーセキュリティお助け隊[45]等）を活用することが考えられる。

・ 海外拠点について踏まえることが想定される「文化等」としては、例えば、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のカントリーリスクに関連するものが想定される。

②-2 供給者・委託先の選定に当たっては、遵守すべきサイバーセキュリティ要件を明確化するとともに、重要度に応じて、契約書等に明記する。

（解説）

・ 契約書等に明記する項目として、例えば、以下の項目が考えられる。

- 供給者・委託先との役割分担・責任分界（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含む。）
- 監査権限
- 再委託手続
- 実施すべきセキュリティ対策（供給者・委託先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含む。）
- 供給者・委託先の役職員が遵守すべきルール
- インシデント又はサービス障害発生時の対応及び報告（通知・報告する事象の種類、通知方法、事象発生から通知までの時間等を含む。）
- 脆弱性診断等の実施及び報告
- 深刻な脆弱性が判明した場合の対応及び報告
- サイバーセキュリティに係る演習・訓練の実施（共同演習・訓練への参加を含む。）
- データの所在・保管・保持・移転・廃棄に関する取決め

[45] 中小企業を対象に、サイバーセキュリティに関する「見守り」「駆付け」「保険」をまとめて提供するサービス
https://www.ipa.go.jp/security/otasuketai-pr/

- 契約終了の条件及び契約終了時の取決め
- 外部評価等の実施（第三者保証報告書の提出、第三者認証の取得を含む。）

・ 委託先会社等の外部組織と適切なコミュニケーションを取りながらサイバーインシデント報告を行うために、通常時に結ぶことが望ましい契約内容については、IPA「情報システム・モデル取引・契約書（第２版）[46]」も参照。

②-3 供給者・委託先の契約の履行状況等について、定期的に、又はリスクに応じて適宜確認し、必要な改善を求める。

②-4 システム開発等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等の方針の遵守状況を委託先に対して定期的に、又はリスクに応じて適宜確認する。

（解説）

・ サイバーセキュリティに配慮した開発方針の遵守状況や、セキュアな開発・保守のプロセス整備等を委託先に対して確認するに当たっては、「サイバーインフラ事業者に求められる役割等に関するガイドライン」を参照。

・ 本ガイドラインは、サイバーセキュリティ基本法第７条第１項及び第２項を踏まえ、情報システム等の供給者としてソフトウェア[47]の設計・開発・供給・運用を行う事業者を「サイバーインフラ事業者」と称し、その役割等について整理・解説するとともに、供給者及びユーザーにおいてサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示すものである。

・ 4.4.3「システムの取得・開発・保守」もあわせて参照。

講ずることが望ましい対策事項

②-5 供給者・委託先の選定に当たっては、デューデリジェンス（第三者保証報告書や第三者認証といった外部評価の活用によるものも含む。）を行う。

[46] https://www.ipa.go.jp/digital/model/model20201222.html

[47] 「サイバーインフラ事業者に求められる役割等に関するガイドライン」における「ソフトウェア」には、製品として顧客に提供されるソフトウェアのほか、クラウドサービス等のソフトウェアサービス、IT/OT/IoT 機器等のハードウェア製品として提供される組み込みソフトウェア・ファームウェア、システム・サービスの構成要素として提供されるソフトウェアも含まれる。

（解説）

- デューデリジェンスでは、例えば、供給者・委託先に関する以下の事項について評価することが考えられる。
  - 供給者・委託先との取引がもたらす潜在的なサイバーセキュリティリスクや脆弱性の評価
  - 自組織が求めるサイバーセキュリティ（契約等で求める事項）の充足状況
  - 過去のインシデントの発生状況、当該インシデントへの対応、復旧、再発防止策の状況等
  - サイバーセキュリティリスク管理体制
  - 事業継続計画等（6.1「事業継続計画等」参照）

②-6 供給者・委託先の重要度を踏まえて優先順位付けの判断基準を定め、適用する。

（解説）

- 供給者・委託先の優先順位付けの判断基準は、例えば、供給者・委託先が処理又は保有するデータの重要性、自組織のシステムへのアクセス権限の程度、供給者・委託先が提供する製品・サービスの重要性等を考慮して設定することが考えられる。

②-7 供給者・委託先との契約書等の見直しが必要な場合が想定されることを踏まえ、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。

②-8 サプライチェーン企業に対する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。

②-9 基幹インフラ事業者[48]でもある重要インフラ事業者等は、上記②-1 から②-8 までの対策事項等の実施に当たっては、経済安全保障推進法に基づくリスク管理措置との整合性に留意する。

（解説）

[48] 経済安全保障推進法に基づく特定社会基盤事業者

・ リスク管理措置については、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（令和５年４月 28 日閣議決定）[49]」、内閣府政策統括官（経済安全保障担当）「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説[50]」を参照。

[49] https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin2.pdf

[50] https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_kaisetsu.pdf

統一基準における規定

③　製品（情報システムを構成する機器等を含む。）・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。

講ずべき対策事項

③-1　製品（情報システムを構成する機器等を含む。）・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選定基準の整備や要求事項の整理を行う。

（解説）

- 製品・サービスの調達・利用に際しては、その製品・サービスのセキュリティ水準を容易に把握し、事業者等における個々のセキュリティ対策の実装確認を簡略化する観点から、以下の認定制度を参照の上、調達・利用にかかる選定基準の整備を行うことが望ましい。
  - IoT 製品：セキュリティ要件適合評価及びラベリング制度（JC-STAR）[51]
  - クラウドサービス：政府情報システムのためのセキュリティ評価制度（ISMAP、ISMAP-LIU）
  - IT 製品：独立行政法人情報処理推進機構（IPA）「IT セキュリティ評価及び認証制度（JISEC）」[52]
- 他方で、上記制度が活用できない場合や補足的な要求事項の整理に際しては、製品・サービスの特性を考慮の上、以下のガイドライン等を参照することが考えられる。
  - 安全なソフトウェア開発の慣行に基づく開発：サイバーインフラ事業者に求められる役割等に関するガイドライン[53]
  - IT 製品の調達におけるセキュリティ要件リスト[54]
  - 情報システム：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[55]

[51] https://www.ipa.go.jp/security/jc-star/index.html
[52] https://www.ipa.go.jp/security/jisec/index.html
[53] https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html
[54] https://www.ipa.go.jp/security/it-product/index.html
[55] https://www.cyber.go.jp/policy/group/general/sbd_sakutei.html

- SBOM：経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」[56]

・ クラウドサービスの調達・利用については、4.3「データのセキュリティ対策」、4.7「クラウドサービス利用時の対策」も参照。

③-2 調達・利用する製品・サービスの変更等について把握及び管理を行う。

③-3 調達・利用する製品・サービスに関連して脆弱性を把握した場合やインシデントが発生した場合、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。

講ずることが望ましい対策事項

③-4 不正機能等の埋め込みに係る脅威に対応するための対策を実施する。

（解説）

・ 不正機能等の埋め込みに係る脅威に対応するための対策としては、経済安全保障推進法に基づくリスク管理措置の内容[57]を参照。

・ ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合には、SBOM の作成及び提供を調達先に求めること、調達先が安全なソフトウェア開発の慣行に基づく開発を実施していることを確認することや、JC-STAR のラベルを取得した製品群から選定すること等が考えられる。

[56] https://www.meti.go.jp/files/900016245.pdf

[57] https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf

3　識別

3.1　資産の管理

3.1.1　資産に対する責任

統一基準における規定

①　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。

講ずべき対策事項

①-1 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。

（解説）

- 制御システムについても作成する。
- ファームウェア[58]についても留意する。例えば、制御システムや、重要な機器（ネットワーク機器等）について、ファームウェアのバージョンを把握することが考えられる。
- 資産目録のフォーマットは用途等に応じて任意であるところ、例えばリスクアセスメントに活用することを意図する場合、資産の持つ機能、接続先ネットワーク、OS の種類・バージョン、使用するプロトコルを示すこと等が考えられる[59]。
- 基幹インフラ事業者でもある重要インフラ事業者等は、サイバー対処能力強化法第４条に基づく特定重要電子計算機の届出義務との整合性に留意。
  特に制御システムについて、サイバー対処能力強化法第４条に基づく特定重要電子計算機の届出の内容を活用することも考えられる。
- 外部（インターネット）からアクセス可能な資産の情報を調査し、それらに存在する脆弱性を継続的に評価する取組である Attack Surface Management（ASM）については、経済産業省「ASM（Attack Surface Management）導入ガイダンス～

[58] 安全基準等策定ガイドラインでは、「ファームウェア」とは、ソフトウェアの一種であり、ハードウェアの機能を制御するためのプログラムを意味している。

[59] 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」65 頁
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～[60]」を参照。

また、複数業界・複数規模の中小企業を対象に、ASM 診断等を実施し、業種別の傾向等を分析した IPA「ASM 診断および事例集作成業務実施報告書」、中小企業のシステムにおいて脆弱性が悪用された場合の被害を想定し、診断結果に基づく実際の対応状況を踏まえて、攻撃シナリオ及び実施すべき対策をまとめた IPA「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」も参考になる[61]。

・ SBOM については、経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」を参照。

講ずることが望ましい対策事項

①-2 情報システム、ソフトウェア、情報等の資産の優先順位付けの判断基準を定め、適用する。

（解説）

・ 資産の優先順位付けの判断基準は、対象となる資産の機密性、完全性、可用性が損なわれた場合の被害の大きさを踏まえて設定する。

例えば、資産の可用性を損なった際のシステム停止等の規模や期間、漏えい等により機密性を損なった場合の経済的損失の程度、情報の改ざん又はシステムの停止等が発生した場合に生じ得る人的・環境被害の程度等を考慮して作成することが考えられる。

①-3 レジリエンス向上の観点から、重要な資産については、その他の資産よりも高い頻度で資産目録の更新を行う。

[60] https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

[61] https://www.ipa.go.jp/security/reports/sme/asm-jirei.html

統一基準における規定

② 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。

③ ネットワーク構成図、データの流れ図等を作成・維持管理する。

④ 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。

講ずべき対策事項

②-1 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。

③-1 ネットワーク構成図、データの流れ図等を作成・維持管理する。

（解説）

- ネットワーク構成図、データの流れ図等の作成については、IPA「制御システムのセキュリティリスク分析ガイド 第２版」の「３．リスク分析のための事前準備（１）～分析対象の明確化～」を参照。
- 制御システムについても作成する。

④-1 未承認の資産がネットワークに接続・運用されないための仕組みを導入し、対処する。

（解説）

- ハードウェア・ソフトウェアの導入前に承認を必要とする仕組みを整備する。
- 個人所有端末や未承認のクラウドサービスの利用（シャドーIT 等）に留意する。

講ずることが望ましい対策事項

④-2 技術的に可能な範囲で、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関係する資産目録との整合を維持する。

3.1.2 情報分類と取扱い

統一基準における規定

① 機密性、完全性、可用性の観点から、情報を格付けし、情報媒体へのラベル付け等により管理する。

講ずべき対策事項

①-1 機密性、完全性、可用性の観点から、情報を格付けし、情報媒体へのラベル付け等により管理する。

①-2 情報及びその他の関連資産を適切に保護するため、情報分類と取扱いの手順（以下「取扱い手順」という。）を整備する。

①-3 情報の格付けや情報媒体の管理等について、取扱い手順に記載する。

（解説）

- 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（電子・磁気・書面を問わない。）へのラベル付けを行う。
- 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個別方針と整合させる。
- 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。ラベル付けには物理的、電子的手段等があり、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。なお、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、取扱い手順を定める。
- 情報の格付け及びライフサイクルに応じた管理方法については、経済産業省「秘密情報の保護ハンドブック ～企業価値向上に向けて～」を参照。

講ずることが望ましい対策事項

なし

統一基準における規定

② 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。

講ずべき対策事項

②-1 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。

②-2 取扱い手順に、情報のライフサイクル（媒体の廃棄、データの安全な消去、外部委託先によるデータの取得・返却・破棄に至るまでの過程を含む）を踏まえた必要な取扱制限（例：複製禁止、持出禁止、配布禁止、媒体の廃棄等）を含める。

講ずることが望ましい対策事項

なし

3.2 脅威情報及び脆弱性情報の収集・分析

統一基準における規定

① 脅威情報及び脆弱性情報を収集する。収集した脅威情報及び脆弱性情報を踏まえ、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。

講ずべき対策事項

①-1 職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（例：メールアドレス、WEB フォーム等の報告先の整備・周知）

①-2 脅威情報及び脆弱性情報を収集し、意思決定等に活用できるよう整理する。

（解説） ・ 脆弱性情報については、製品ベンダーからの情報提供のほか、国家サイバー統括室、JPCERT/CC、IPA からの注意喚起や脆弱性情報提供サイト等からの通知を参照することが考えられる。

①-3 収集した脅威情報及び脆弱性情報を踏まえ、リスクアセスメント及びリスク対応要否の判断を行う。

講ずることが望ましい対策事項

①-4 自組織の業務に即して、業界 ISAC 等の専門性の高い情報共有活動や、業界横断的な団体、国際的な団体等に参加し、脅威情報及び脆弱性情報等を収集する。

①-5 技術・脅威の動向や業界・組織を取り巻く環境の変化等に留意して情報収集を行う。

3.3 情報共有

統一基準における規定

①	サイバー攻撃の被害の未然防止や、影響の極小化のため、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、セプター[62]や ISAC、協議会[63]等を活用し、組織内外と情報共有を実施する。

講ずべき対策事項

①-1 サイバー攻撃の被害の未然防止や、影響の極小化、厳しいサイバー安全保障環境への柔軟かつ適切な対応のため、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、自組織内での情報共有とともに、セプターや ISAC、協議会等を活用し、政府機関や各分野の業界団体等の組織外との情報共有を実施する。

講ずることが望ましい対策事項

①-2 情報共有を行う連絡先等、連絡体制に係る情報を定期的に更新する。

（解説）

- 所管省庁等のほかに情報共有を行うことが考えられる連絡先として、警察では、被疑者の検挙に加えて、捜査で判明した犯罪の手口等を関係機関に情報提供してさらなる被害を防止するなどの取組を行っているので、サイバー事案が生じた際には警察への通報・相談を積極的に行うことが望ましい[64]。

[62] 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）。

[63] サイバー対処能力強化法第 45 条に基づく協議会

[64] サイバー攻撃被害に係る情報の共有・公表ガイダンス 83 頁

①-3 官民双方向でのコミュニケーションの強化を含め、厳しい安全保障環境に柔軟かつ適切に対応していくため、サイバー脅威の分析に必要な情報を政府機関に共有する。

（解説）

- サイバー脅威の分析に必要な情報とは、例えば、以下のような情報をいう。
  - IoC[65]（侵害の痕跡）[66]
  - 攻撃の手口・侵入経路[67]
  - システム構成がわかる図
  - 攻撃の時系列
  - インシデントに関係するフォレンジック結果報告書

[65] Indicators of Compromise の略。

[66] 攻撃元の IP アドレス・ポート、攻撃先（被害システム）の IP アドレス・ポート、関連する URL・ドメイン、マルウェアのハッシュ値やマルウェア本体等

[67] 想定される攻撃手法、悪用された脆弱性情報、攻撃対象の機器・ソフトウェアの名称・バージョン等、攻撃対象のシステム等が取扱う情報や有する機能、攻撃対象のアカウント（ID）・アカウント利用者の属性等

3.4 リスクアセスメント

統一基準における規定

① 各事業者等の実情に応じたリスク対応を戦略的に講ずるため、情報システム、ソフトウェア、情報等の資産を特定し、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（リスクの特定・分析・評価）を実施する。

講ずべき対策事項

①-1 各事業者等の実情に応じたリスク対応を戦略的に講ずるため、情報システム、ソフトウェア、情報等の資産を特定し、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（リスクの特定・分析・評価）を実施する。

（解説）

- リスク分析に当たっては、任務保証の考え方を踏まえ、重要インフラサービス障害等が社会に与える影響を念頭に分析する。
- 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、例えば、次のような手順に沿ってリスクアセスメントを実施する。

A. 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重要システム等の経営資源を特定する。その際、対象範囲の考え方は 1.3「対象範囲」を、資産の特定は 3.1.1「資産に対する責任」を参照。

B. リスク特定

情報システム等の経営資源に対する「セキュリティリスク」を特定する。

C. リスク分析

「事象の結果によるサービス・業務への影響度合い」や「事象の発生頻度（発生可能性、起こりやすさ）」等を評価軸として策定されるリスク基準[68]を活用して、特定されたリスクの大きさを確認する。

D. 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。

[68] リスク基準の設定イメージについて、国家サイバー統括室「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」18 頁を参照。

- 資産ベース[69]に加え、事業被害ベース[70]の脅威を想定したリスクアセスメントも実施することが有効。
- リスクアセスメントは、情報システムの運用中も含め、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継続的に実施する。
- リスクアセスメントの具体的なプロセスについては、国家サイバー統括室「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」、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」を参照。
- サイバーセキュリティに係るリスクマネジメントの全体像及び具体的なリスクアセスメントの手法等については、以下を参照。
  - ISO/IEC27001 情報セキュリティ，サイバーセキュリティ及びプライバシー 保護－情報セキュリティマネジメントシステム－要求事項
  - ISO/IEC27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ
  - National Institute of Standards and Technology（NIST、米国国立標準技術研究所）Special Publication 800-30 revision1[71]
- サイバーセキュリティに係るリスク以外を含むリスクマネジメントの全体像及び具体的なリスクアセスメントの手法等については、以下を参照。
  - JIS Q 31000:2019 リスクマネジメント－指針
  - JIS Q 31010:2022 リスクマネジメント－リスクアセスメント技法（IEC31010:2019,Risk management-Risk assessment techniques）

講ずることが望ましい対策事項

①-2 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リスクについてのシナリオを作成し、リスク分析を実施する。

①-3 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。

[69] 資産ベースのリスク分析は、保護すべき制御システムを構成する資産群を明確化し、各資産に対するシステム構成上及び運用管理上に想定される脅威について、各資産の重要度と、その脅威の発生可能性と受容可能性（脆弱性）の相乗値によって、資産のリスクを評価するリスク分析手法。

[70] 事業被害ベースのリスク分析は、回避したい事業被害を明確化し、事業被害を引き起こすと想定される攻撃について、事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析手法。

[71] https://www.ipa.go.jp/security/reports/oversea/nist/about.html

（解説）

- 制御システムを構成する装置・機器は、汎用 OS や TCP/IP 等の標準的な通信プロトコルの採用が進んでおり、独自仕様の機器や通信プロトコルで構成されていないものがあることを念頭に確認する必要がある。
- 制御システムが外部ネットワークに接続していない場合でも、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。
- 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。パッチ適用等[72]、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おそれがある場合には、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ことを想定しつつ、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。
- 制御システムのリスクアセスメントの詳細については、IPA「制御システムのセキュリティリスク分析ガイド 第２版[73]」に記載されている具体的な作業手順等や、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」を参照。

①-4 セキュリティリスクに加えて、HSE[74]等の観点からのリスクも特定し、分析・評価を行う。

（解説）

- 重要インフラサービスの安全かつ持続的な提供のためには、HSE 等の観点からのリスクも特定し、分析・評価を行うことも求められる。
  HSE 等の観点として、例えば、重要インフラサービスの提供を担う職員等の労働安全・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、重要インフラサービスの提供に伴う環境負荷の低減等が考えられる。

[72] バージョンアップも含む。

[73] なお、「制御システムのセキュリティリスク分析ガイド 第２版」では、フィールド機器と、制御機器からフィールド機器へ接続されているセンサバスについては、サイバーセキュリティの観点のリスク分析対象から除外している。これらを対策事項の範囲に含めるかどうかについては、フィールド機器・センサバスについてのリスク等を考慮し、分野ごと（あるいは運用上は事業者等ごと）に、分野の特性等を踏まえつつ個別に判断することが期待される。

[74] 健康（Health）、安全（Safety）及び環境（Environment）を指す。例えば、「制御システムのセキュリティリスク分析ガイド 第２版」では、「制御システムは、製造ラインや供給ライン、社会インフラ、更にはそれを取り巻く環境等にも大きく関わっている。従って、事業被害を考察する場合には、情報システムでの典型的な観点である、CIA（C：機密性、I：完全性、A：可用性）という指標だけではなく、HSE（H:健康、S：安全性、E:環境への影響）という観点を考慮に入れることが必要となる。」とされている（同ガイド 99 頁）。

①-5 リスクアセスメントの結果、リスク対応の対象としなかったリスクについても、所管部署等の管理状況（セキュリティ管理策の導入有無等）について適時確認できる仕組みを整備する等により、可能な範囲でリスク管理を実施する。

3.5 サイバーセキュリティリスク対応

3.5.1 リスク対応の決定

統一基準における規定

① 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、成熟度モデルも活用しつつ、自組織における評価基準等をもって優先順位付けする。

講ずべき対策事項

①-1 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、成熟度モデルも活用しつつ、自組織における評価基準等をもって優先順位付けする。

（解説）

- セキュリティ対策の目的は、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ことにある。重要インフラ事業者等は、リスクアセスメントの結果や、自組織の状況、関係主体等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。

【成熟度モデルの活用について】

- 成熟度モデルを活用し、目標とする将来像を決定するに当たっては、重要インフラ・サイバーセキュリティ・セルフアセスメント（CI-CSA）等の活用が想定される（2.1.③-1 参照）。

講ずることが望ましい対策事項

なし

3.5.2 個別方針の策定

統一基準における規定

①	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等の関係者に対しても伝達する。

講ずべき対策事項

①-1 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等の関係者に対しても伝達する。

講ずることが望ましい対策事項

①-2 制御システムを対象とした個別方針を策定し、重要な運用機能、制御システム固有のセキュリティ上の懸念事項、代替管理策の優先順位を識別する。

3.5.3 リスク対応計画の策定等

統一基準における規定

① 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。

講ずべき対策事項

①-1 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。

（解説）

- リスク対応計画には、例えば、次の事項を記載することが想定される。
  - 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
- 個々の取組の実施に当たって詳細計画が必要となる場合は、リスク対応計画に則して、それぞれの取組の責任者がその権限の下に詳細計画を策定することも考えられる。
- リスク対応計画の策定に当たっての考え方や主眼点等については、国家サイバー統括室「対策推進計画策定マニュアル[75]」 を参照。

講ずることが望ましい対策事項

①-2 リスク対応計画の達成状況等を、経営層に対して定期的に報告する。

[75] https://www.cyber.go.jp/pdf/policy/general/sakutei-manual.pdf

統一基準における規定

② 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。

講ずべき対策事項

②-1 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。

（解説） ・ リスク対応計画に基づき決定したセキュリティ対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。

講ずることが望ましい対策事項

なし

3.6 脆弱性の管理

統一基準における規定

① 収集した脆弱性情報を踏まえ、運用中の情報システムに対する影響の有無を確認する。

講ずべき対策事項

①-1 収集した脆弱性情報を踏まえ、運用中の情報システムに対する影響の有無を確認する。

（解説）

- 脆弱性の管理のプロセスとしては、①情報の絞り込み（脆弱性情報の中から自組織に関連する情報を抽出）、②脆弱性の危険度（深刻度）を確認（脆弱性の特性や攻撃状況を確認）、③自組織への影響を分析し、自組織のリスクを考慮した対策を実施することが考えられる。
  具体的な脆弱性関連情報の収集先や分析手法等については、IPA「脆弱性対策の効果的な進め方（実践編）第２版 ～脆弱性情報の早期把握、収集、活用のスヽメ～[76]」も参照。
- 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、関連する脆弱性を特定し、組織の資産とあわせて整理する。
- 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。
- 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」、「更新等に伴うリスクを文書化する」、「ロールバックの手順を定める」等、適切な対策を実施する。

①-2 外部から調達した情報システムの場合には、保守契約等に基づき、供給者に対して脆弱性の報告、取扱い、開示等を要求する。

[76] https://www.ipa.go.jp/security/reports/technicalwatch/20150331.html

講ずることが望ましい対策事項

なし

統一基準における規定

② 定期的な脆弱性診断を実施する。脆弱性診断が困難な場合には、リスクに応じた措置を講じる。

講ずべき対策事項

②-1 リスクアセスメントの結果等を踏まえ、脆弱性診断の対象を選定し、定期的な脆弱性診断を実施する。

（解説）

- 脆弱性診断の対象は、システムを構成するネットワーク機器、端末、サーバ、サービスアプリケーション等（クラウドサービス上に構築されるものも含む。）が想定される。3.4 で行うリスクアセスメントの結果等を踏まえ、例えば、以下の条件も考慮してスキャン箇所を選定することが考えられる[77]。
  - 外部との界面に位置しているネットワーク装置等（ファイアウォール等）
  - 重要な処理が可能な操作端末
  - 保守要員等、外部の要員が操作する可能性のある端末
  - 重要度の高い資産（サーバ類等）で、リスク値を十分に下げられてない資産
- 脆弱性診断を外部事業者に請け負わせる場合は、「情報セキュリティサービス基準」及び「情報セキュリティサービス基準適合サービスリスト」（うち脆弱性診断サービス、ペネトレーションテストサービスに係る部分）を参照。

②-2 システム運用上の制約等により脆弱性診断が困難な場合には、リスクに応じた措置を講じる。

（解説）

- リスクに応じた措置としては、例えば次のものが想定される。
  - 脆弱性悪用の対象となる機能を無効化する。
  - ベンダーが推奨する回避策を実施する。
  - 対象となる情報機器を、重要システム等を構成するネットワークから分離する。
  - 対象となる情報機器と重要システム等を構成するネットワークとの通信を監視

[77] 制御システムのセキュリティリスク分析ガイド第２版 302 頁

し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェア（仮想パッチの適用も含む。）を導入する。

講ずることが望ましい対策事項

②-3 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、ペネトレーションテストを実施する。[IT システムのみ]

統一基準における規定

③　攻撃者にAIが悪用されることにより、脆弱性の発見から悪用まで短時間で行われ、また、多数の脆弱性対応が必要となることも踏まえた上で、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。迅速なパッチ適用が困難な場合には、可能なパッチ適用頻度の設定や脆弱性リスクの高い機器の更改等、リスクに応じた措置を講じる。

講ずべき対策事項

③-1　攻撃者にAIが悪用されることにより、脆弱性の発見から悪用まで短時間で行われ、また、多数の脆弱性対応が必要となることも踏まえた上で、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。迅速なパッチ適用が困難な場合には、可能なパッチ適用頻度の設定や脆弱性リスクの高い機器の更改等、リスクに応じた措置を講じる。

（解説）

- 生成AIを始めとするAI技術等の悪用による攻撃側の能力の飛躍的な向上により、脆弱性の発見と当該脆弱性を突いた攻撃手法の確立が容易かつ極めて短時間で可能になる恐れがある。こうした脅威の高まりを十分に認識し、攻撃被害のリスクを把握・分析した上で、適切な措置を講じることが重要である。
- パッチ適用等に関する手順を整備する。
- 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）について、重要な資産から優先的にパッチ適用等により緩和する。
- 公開された脆弱性についての影響度と緊急度を判断するためには、脆弱性の深刻度を示すCVSS[78]の値や当該脆弱性を悪用した攻撃の段階（例えば、脆弱性を用いた攻撃手法が出回っている、既に脆弱性を用いた攻撃が確認されている[79]など）などを考慮して検討することが考えられる。
  CVSSについては、IPA「共通脆弱性評価システム CVSS v3 概説[80]」を参照。

[78] Common Vulnerability Scoring Systemの略。
[79] CISAが公開している実際に悪用が確認された脆弱性を掲載したカタログであるKEV（Known Exploited Vulnerabilities）を参考にすることも考えられる。KEVについては、以下を参照。
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[80] https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

・ なお、脆弱性への対処に関する判断については、SSVC[81]と呼ばれる脆弱性の管理手法を用いて検討することも考えられる。
SSVC については、Cybersecurity and Infrastructure Security Agency（CISA）「Stakeholder-Specific Vulnerability Categorization[82]」を参照。
・ 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迅速なパッチ適用等又はパッチ適用等自体が困難な場合には、リスクに応じて、例えば、可能なパッチ適用頻度の設定や、3.6②-2 の脆弱性悪用のリスクを低減する対策等を採用・文書化し実施する。
また、パッチ適用等自体が困難な場合には、パッチ適用等を実施しない旨及びそのリスクについて経営層から承認を得ることや、脆弱性リスクの高い機器の更改も検討する。
・ 制御システムを構成する装置・機器においても、汎用 OS や TCP/IP 等の標準的な通信プロトコルの採用が進んでいるため、外部ネットワークからのサイバー攻撃を受けるリスクを十分評価した上、特定されたリスクに応じて、パッチ適用等（リスクに応じた措置の実施を含む。）を含むセキュリティ対策を行う。
・ パッチ適用等が不可能又はパッチ適用等によって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、ネットワークの物理的又は論理的分離、USB メモリ等の外部電磁的記録媒体からの感染防止対策、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。
・ 参考として、CISA が以下の文書にて、高性能 AI の影響等を踏まえ、パッチ適用等において優先するシステムを選定する基準を示している。
- CISA「BOD 26-04: Prioritizing Security Updates Based on Risk[83]」

講ずることが望ましい対策事項

③-2 収集した脆弱性情報について、脆弱性対応に係る計画や対応履歴の作成等により、対応実績を管理する。

（解説）
・ 対応実績管理の対象としては、収集した脆弱性情報のうち、情報システムへのパッチ適用等に関する作業方針（3.6.③-1 参照）に基づきパッチ適用等が適当と

[81] Stakeholder-Specific Vulnerability Categorization
[82] https://www.cisa.gov/resources-tools/resources/stakeholder-specific-vulnerability-categorization-ssvc
[83] https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

判断されたものを想定しており、パッチ適用等が困難と判断したものは含まない。

③-3 攻撃者にAIが悪用されることにより、脆弱性の発見から悪用まで短時間で行われ、また、多数の脆弱性対応が必要となることも踏まえた上で、必要に応じて情報システムへのパッチ適用に関する作業方針を見直し、実行可能な運用体制を構築・維持する。

4　防御

4.1　アカウント管理・認証・アクセス制御

4.1.1　アカウント管理

統一基準における規定

①　最小権限及び職務の分離の原則を踏まえて、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。

講ずべき対策事項

①-1 ユーザーアカウント・管理者アカウント及びそれらに割り当てられるアクセス権の登録・変更・削除の正式なプロセス（申請ルート、承認者、作業者等）を定める。

①-2 ユーザーアカウント・管理者アカウントに割り当てられるアクセス権を定期的にレビューする。

（解説） ・　例えば、人事異動等に伴うアクセス権の変更が適切に実施されているかといった点に留意する。

①-3 管理者アカウントについて、必要最低限の権限と利用に制限し、管理する。

（解説） ・　管理者アカウントの制限・管理に当たり、例えば、以下の点にも留意することが考えられる。 － 可能な限り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（例：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） － 多要素認証 － アカウントの時間制限の設定

①-4 離職等によりアカウントが不要になった場合、離職者等が保有する全てのアカウントと、組織情報へのアクセスを無効にする。

（解説）

- アカウントと、組織情報へのアクセスを無効にするに当たっては、関連するクレデンシャル（電子証明書、アクセストークン、認証情報等）も失効させる。また、全ての物理的なトークン、バッジ、キーカード等を失効させ、返却させる。
- 無効化の対応期限については、例えば、アカウントが不要になった日の当日中を目安とすることが考えられる。
- 無効化にはアカウントの停止も含まれるところ、例えば事後的にアカウントの調査を行うため、当該アカウントを停止して無効化しつつ、データは保持しておくことも想定される。

講ずることが望ましい対策事項

①-5 利用者アクセスを定期的に見直し、一定期間（例：30 日間）非アクティブな状態が続いているアカウントを無効化する。

4.1.2 認証・アクセス制御

統一基準における規定

① 情報やシステムの重要度に応じて、良質なパスワードの利用や多要素認証の活用等により、情報システムや情報へのアクセスを制限する。

講ずべき対策事項

＜アカウントロック関連＞

①-1 ログインの成否を記録し、複数回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やセキュリティ担当者への通知を行う。該当機能がない場合は、代替セキュリティ管理策を実施する。

（解説）

・ 過度に厳しい制限は、正当な利用者がログインできずに適切な業務遂行に悪影響を及ぼし得るリスクを伴うため、ログイン試行回数制限の設定については、セキュリティ水準の向上と業務運営に対する影響等のバランスについて慎重に考える必要がある。

そのような観点から、例えば、以下を本対策事項の対象とすることが考えられる。

- 情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定されるサーバ（例：ファイルサーバ、Active Directory（AD）サーバ）にログインする場合
- 重要システムにインターネット経由でログインする場合

＜パスワード管理関連＞

①-2 パスワードの用途ごとに最小パスワード長を設定する。

（解説）

・ パスワードの用途には、例えば、「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」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、パスワード長を設定する。

・ 安全に関わる緊急対応を必要とする表示器等の端末を対策の対象から除くことも考えられる。

①-3 パスワードは容易に推測することができないものとする。また、自組織のサービスや資産及び外部のアカウントやサービス等において、同一のパスワードを使い回さないようにする。

（解説）

・ パスワードは、複数サービスでの使い回しや、人にとって覚えやすい脆弱なものが使用されるリスクが高いため、少なくとも重要な認証プロセスにおいては多要素認証を必須とする。

①-4 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パスワードを変更する方針とする。ハードコード（ハードコーディング）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。

＜多要素認証関連＞

①-5 重要システムにインターネット経由でログインする場合、多要素認証を使用する。

（解説）

・ 多要素認証がサポートされていない場合、インターネット経由のアクセスを廃止し、追加のセグメンテーション手順を導入する等のリスク軽減措置を導入することが考えられる。
・ 認証機能がサポートされていない場合、又はパフォーマンス・安全性・信頼性への影響により組織が認証を推奨できないと判断した場合、当該制御システムに対して同等のセキュリティ機能または保護レベルを確保するため、補償的な対策を選択することが考えられる。
・ ローカルアクセスについては、セキュリティ確保が求められる領域への物理的アクセスに対して制御を行う等、リスク軽減措置がある場合に、ID とパスワードのみを要求し、多要素認証までは要求しないことも考えられる。

①-6 多要素認証の使用に当たっては、以下のいずれかの要素から２種類以上を選択し、利用する。

・知識情報（例：ID・パスワード）

・所有情報（例：ワンタイムパスワード又は電子証明書）

・生体情報（例：指紋、顔、虹彩又は静脈）

（解説）

- ワンタイムパスワードには、利用者のメールアドレスや電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。ただし、これらの一部の２段階認証と呼ばれる方式は、フィッシング攻撃等により突破されてしまう可能性がある点に留意（フィッシング耐性のある多要素認証技術については、①-10 参照）。
- 直ちに多要素認証を導入することが困難な場合、暫定的なリスク軽減措置として、特定の IP アドレス以外からのアクセスを制限することも考えられる。
- 本人確認手法の選定方法等については、デジタル庁「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン[84]」を参照。

講ずることが望ましい対策事項

＜パスワード管理関連＞

①-7 利用者による十分な長さのパスワードの維持等のため、パスフレーズ、パスワード管理ツール、シングルサインオンを活用する。

①-8 最小パスワード長の適用が技術的に不可能な場合、補完的な措置を適用・記録するとともに、該当資産への全ログイン試行を記録する。十分な強度を持つパスワードをサポートできない資産は、優先的に更新又は交換の対象とする。

[84] https://www.digital.go.jp/resources/standard_guidelines/

＜多要素認証関連＞

①-9 以下の場合、多要素認証を使用する。

- 重要な情報[85]を取り扱うクラウドサービスにおいて、ユーザー及び管理者がサービスにアクセスする場合
- ユーザー及び管理者がインターネット経由で重要な情報を取り扱うシステムにアクセスする場合
- ユーザー認証にパスワードを利用し、かつ、アカウントロックの制限がされていない場合[86]
- 管理者がファイアウォール等の重要なネットワーク機器にアクセスする場合
- 取得・保管を求められているログを保存する媒体及びシステムにインターネット経由でアクセスする場合

①-10フィッシング耐性のある多要素認証技術（例：FIDO 認証等）が利用可能な場合は利用する。利用できない場合には、モバイルアプリベースのソフトトークン（利用可能な場合は番号照合によるプッシュ通知）を利用する。

（解説）

- ID・パスワードやワンタイムパスワードは、技術的手法やフィッシング詐欺等により窃取され、悪用されるリスクがある。そのため、公開鍵暗号方式を用いた、より強度の高い認証方式を適用することが望ましい。
  フィッシング耐性のある多要素認証技術として、例えば、FIDO 認証[87]や、公開鍵暗号基盤（PKI）ベースの認証[88]等が考えられる。これらは、フィッシングサイトへの認証情報等の送信を避けることができるため、フィッシング対策に有効とされる。
  他方で、モバイルアプリベースのソフトトークンを利用する場合は、不正な認証

[85] 「重要な情報」とは、例えば、重要インフラサービスを提供するために必要な情報や、漏洩等した場合に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情報等が想定される。

[86] 本対策事項は、多要素認証の使用が望ましい場合を列挙したものであり、アカウントロックを実施している場合に多要素認証が不要という趣旨を含むものではなく、リスクに応じて両者の併用も想定される。

[87] 端末等のデバイス側で生体情報等を用いた認証を行った上で、デバイスに保管された秘密鍵を用いた公開鍵暗号方式によりサーバ側で端末認証を行う仕組み。なお、「パスキー」は、最新仕様である FIDO2 の適用仕様の一つである。

[88] 例えば、クライアント証明書による認証等が該当する。

要求に対して誤って許可をしてしまう多要素認証疲労攻撃のリスクを考慮し、番号照合によるプッシュ通知を利用する。

- 「マルチデバイス対応 FIDO 認証資格情報（マルチデバイス FIDO クレデンシャル）[89]」と呼ばれる仕組み等、プラットフォーマーのアカウントが侵害された場合、当該サービスのアカウントも侵害されてしまう方式があるため、アカウント管理・端末管理の徹底が重要である。

[89] デバイスの紛失等が生じた場合であっても、秘密鍵を OS 等のプラットフォームの機能を介して複数のデバイス間で同期することによって認証を可能とする仕組み。

4.1.3 セキュリティ確保が求められる領域

統一基準における規定

① 物理的なセキュリティ境界の設定、入退管理の仕組みの構築等により、セキュリティ確保が求められる領域を管理する。

講ずべき対策事項

①-1 セキュリティ確保が求められる領域（機密性の高い区域及びコンピュータ室、データ保管室等。以下「管理領域」という。）の範囲を定める。

①-2 管理領域における物理的なセキュリティ境界を設定する。

（解説） ・ 管理領域の建物の屋根、壁、天井及び床を強固な構造物とし、要員が不在の場合には、外部に接する全ての扉を施錠する。

①-3 管理領域における入退管理の仕組みを構築する。

（解説） ・ 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の仕組みを構築する。

①-4 管理領域に持ち込まれる物品の確認・制限を実施する。

（解説） ・ 悪意ある活動を防止する観点から、管理領域への認可されていない物品の持ち込みを制限する。

講ずることが望ましい対策事項

①-5 悪意ある活動を防止する観点から、複数の作業要員を確保できる場合、管理領域での単独作業を制限する。

4.1.4 装置の管理

統一基準における規定

① 傍受や損傷の可能性を考慮して通信・電源ケーブル等の装置を管理する。

講ずべき対策事項

①-1 重要システム及び重要システムを構成する機器等を、認可されていないアクセスの機会を低減するため、管理領域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。

①-2 重要システムが稼働する施設について、雷対策及び定期的な計画停電のスケジュールの管理を行う。

①-3 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に加え、点検・終端箇所の施錠可能な部屋又は箱内への設置を実施する。

講ずることが望ましい対策事項

①-4 重要システムに係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、ケーブルの各端への始点及び終点を示すラベル付けを行う等、管理する。

（解説）

- 攻撃者からも識別されるリスクを踏まえ、入退管理等の管理領域に関する対策（4.1.3「セキュリティ確保が求められる領域」参照）が実施されていることが前提となる点に留意。

①-5 重要システムへ供給する電源系統を複数にする、あるいは無停電電源装置等を使用するなど、可用性を考慮した対策を実施する。

統一基準における規定

② 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る仕組みを整備する。

講ずべき対策事項

②-1 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る仕組みを整備する。

（解説）

・ 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る仕組みにおいては、例えば以下を考慮することが考えられる。

- 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。
- 取り外し可能な記録媒体の使用時のルール（使用制限、暗号化、マルウェアスキャン等）を定める。
- 取り外し可能な記録媒体を持ち出す場合、責任者の認可を要求し持ち出し管理を行う。

講ずることが望ましい対策事項

②-2 モバイル機器等の通信機能がある記録媒体について、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。

②-3 不正な機器の接続を防止するため、物理ポートの除去、無効化、その他の方法による保護を確立する、又は例外措置としてアクセスを許可する手順を確立する。

4.2 意識向上とトレーニング

4.2.1 人材育成・意識啓発

統一基準における規定

① 「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、全ての役職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、CISO 等を含む人材育成・意識啓発を行う。

講ずべき対策事項

①-1 全ての職員を対象としたトレーニングを年１回以上実施する。トレーニングにおいては、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、OS やソフトウェアのアップデート等の基本的な概念を網羅する。

（解説）

- 重要インフラ事業者等の職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、職員に対し、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）。特に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の育成においては、政府機関の人材育成プログラム、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」等の資格取得等も期待される。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。
- 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などの方法により、セキュリティ対策の重要性について啓発する。

①-2 新入職員に対し、サイバーセキュリティ研修を実施する。

①-3 経営層がサイバーセキュリティリスクについて理解できるようにするための学習機会を確保する。

講ずることが望ましい対策事項

①-4 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の活用を検討する。

（解説）

・ 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、セキュリティ対策業務に従事する人材のキャリアパス等をあらかじめ検討しておくことが重要である。必要に応じて外部人材を活用することも有効であり、例えば「情報処理安全確保支援士」等の一定の専門性及び倫理性を有する資格者を外部専門家として活用し、助言・支援等を受ける体制を構築することが考えられる。

①-5 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。

①-6 組織内で追加のサイバーセキュリティ研修を必要とする専門職（例：物理的セキュリティ及びサイバーセキュリティ担当者、システム管理者、財務担当者、上級管理職、業務上重要なデータへのアクセス権限を持つ者）を特定し、外部人材を含む専門職に就く者全員に対し、役割に応じたサイバーセキュリティのトレーニングを提供する。

①-7 制御システムの運用・維持・保全の担当者に対し、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提供する。

（解説）

・ 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、IPA 産業サイバーセキュリ

ティセンター（ICSCoE）[90]による短期プログラム[91]や、中核人材育成プログラム[92]を活用することが考えられる。

[90] 参考：OT と IT の知見を結集させた世界最高レベルのサイバーセキュリティ対策の中核拠点（https://www.ipa.go.jp/icscoe/index.html）

[91] https://www.ipa.go.jp/jinzai/ics/short-pgm/index.html

[92] テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ１年程度（７月～翌年６月）のトレーニング（https://www.ipa.go.jp/jinzai/ics/core_human_resource/index.html）

4.2.2 演習・訓練

統一基準における規定

①	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。

講ずべき対策事項

①-1 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。

（解説）

- 演習・訓練には、国家サイバー統括室が主催する「全分野一斉演習」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への参加が想定される。
- 改善の方法としては、例えば、演習・訓練により抽出した課題を踏まえ、インシデント対応計画を見直すことが想定される。

講ずることが望ましい対策事項

①-2 経営層も交え、組織全体での演習・訓練を実施する。

①-3 他事業者等との合同演習・訓練、他事業者等のインシデント対応事例の研究等を実施する。

（解説）

- 合同の演習・訓練には、「全分野一斉演習」の他、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次の演習等がある。
  - （国研）情報通信研究機構（NICT） 実践的サイバー防御演習（CYDER）[93]
  - 金融庁 金融業界横断的なサイバーセキュリティ演習（Delta Wall）
  - IPA 産業サイバーセキュリティセンター（ICSCoE） 短期プログラム[94]

[93] https://cyder.nict.go.jp/

[94] https://www.ipa.go.jp/jinzai/ics/short-pgm/index.html

4.3 データのセキュリティ対策

4.3.1 データ管理

統一基準における規定

① 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。

講ずべき対策事項

①-1 システムのリスクアセスメントを実施し、データの管理方針を策定する。

（解説）

- データの管理方針には、例えば、次の事項を含めることが考えられる。
  - データの管理
  - データの保存
  - 適切な暗号化方式の採用
  - 暗号鍵と電子証明書について、そのライフサイクルを通じた管理及び保護
  - 暗号の危殆化時の対応
- 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る仕組み等については 4.1.4.②、暗号については 4.3.2.①もそれぞれ参照。

①-2 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。

講ずることが望ましい対策事項

なし

統一基準における規定

② 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。

講ずべき対策事項

②-1 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。

（解説）

- 日本国内で利用できるクラウドサービスを提供しているデータセンターは、必ずしも日本国内にあるわけではなく、データセンター内のデータ取扱いについて、国内法以外の法令及び規制が適用される場合がある。データセンターが設置されている国が、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のリスクの高い国である場合、データセンター内のデータが法執行機関の命令により強制的に開示されることが考えられる。情報の開示が懸念される場合は、重要インフラ事業者等の管理する暗号鍵で暗号化するなどの措置の検討や、クラウドサービス提供者へデータ保護の措置等についての確認を行うようにすることが考えられる。特にマルチクラウド等を活用してシステムを運用する場合には、各クラウドサービスにおいてデータ保護の措置を検討する。

講ずることが望ましい対策事項

なし

4.3.2 暗号を活用した情報管理

統一基準における規定

① 暗号の利用方針や暗号鍵の管理方針（危殆化時の対応を含む。）を策定する。

講ずべき対策事項

①-1 暗号の利用方針や暗号鍵の管理方針（危殆化時の対応を含む。）を策定する。

（解説）

- 暗号化（鍵交換、ハッシュ化、署名等を含む。）に際して用いる暗号技術（アルゴリズム）や鍵長の選択、鍵の管理手順等については、以下を参照。

  ＜CRYPTREC 暗号リスト等＞[95]

  - 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」
  - 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」

  ＜CRYPTREC 暗号運用ガイドライン＞[96]

  - 「TLS 暗号設定ガイドライン」
  - 「暗号鍵管理システム設計指針（基本編）」
  - 「暗号鍵設定ガイダンス」
  - 「暗号鍵管理ガイダンス Part 1」
  - 「暗号鍵管理ガイダンス Part 2」
- 非推奨や脆弱な暗号化が行われている資産を特定し、適切な暗号に更新する計画を立てて実施する。

①-2 機微なデータ（認証情報、秘密鍵、API キー、アクセストークン、証明書秘密鍵等）は、その性質に応じた適切な保護措置を講じ、許可された者又は機能のみがアクセスできるようにする。

（解説）

[95] https://www.cryptrec.go.jp/list.html

[96] https://www.cryptrec.go.jp/op_guidelines.html

・ 適切な保護措置としては、対象となるデータの性質に応じて、例えば、データの暗号化、パスワードのハッシュ化（暗号化）、アクセス権限の制限、アクセス記録の取得、不要となった機微なデータの削除等を行うことが考えられる。
・ 特に認証情報を保存する場合は、平文で保存しないことを原則とし、パスワードについては、ソルト（パスワードに付加するランダムな値）を用いたハッシュ化等により保護することが望ましい。
・ 機微なデータは、ソースコード、設定ファイル、ログ、チケット、メール等に不用意に保存又は記録されないよう留意する。

①-3 端末、外部電磁的記録媒体等を外部に持ち出す場合、記録媒体全体の暗号化やファイル単位の暗号化等によりデータを保護する。

①-4 外部との通信については、転送中のデータを適切に保護する。

（解説）
・ 外部との通信については、インターネット経由の通信のほか、閉域網であってもタッピング等による情報窃取リスクを勘案して検討を行い、対象となる通信の性質に応じて、暗号化、通信相手の認証等の必要な対策を講じる。
・ 暗号技術の取扱いについては、輸出・技術提供規制等に関する国内外の法令及び規制の対象となる場合があることに留意する。
・ 暗号の使用により、暗号化、認証に必要な追加の時間と演算リソースを要することで、通信等の遅延が引き起こされる可能性がある。特に制御システム等においては、暗号技術を導入する前に、生じ得る遅延が許容可能かどうかを判断することが望ましい。また、暗号技術が導入できない場合には、代替対策の導入も併せて検討してリスク軽減を図ることが望ましい。

①-5 電子メールのセキュリティ向上のため、メールゲートウェイでのマルウェア対策等とともにDMARC等による対策として、事業者等が利用するメールインフラにおいて、以下の対策を実施する。[ITシステムのみ]
・STARTTLSを有効化する。
・DMARCによる送信側の対策を行う。DMARCによる送信側の対策を行うため、

SPF、DKIM のいずれか又は両方による対策を行う。

・DMARC による受信側の対策を行う。DMARC による受信側の対策を行うため、SPF、DKIM の両方による対策を行う。

・DMARC ポリシーには、“p=quarantine”又は“p=reject”を設定する。やむをえず、”p=none”を設定する場合も設定期間が可能な限り短くなるようにする。

（解説）

・ 対策の詳細については、政府機関等の対策基準策定のためのガイドライン（令和７年度版）6.2.2 電子メール【基本対策事項】6.2.2(1)-3 関連の（解説）を参照。

講ずることが望ましい対策事項

①-6 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、リモートアクセスや外部との通信について、運用への影響を考慮の上、暗号化を行う。

4.3.3 バックアップ

統一基準における規定

① 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する。その際、サイバー攻撃によるバックアップデータ削除等のリスクがあることを考慮し、バックアップデータをバックアップ元のシステムと異なるセグメントやオフラインで保管する等の対応を検討する。

講ずべき対策事項

①-1 重要システムについて、少なくとも年１回以上の定期的なバックアップを実施する。年１回以上のバックアップが難しい場合にも、適切な取得間隔を設定する。

（解説）

- バックアップの取得対象として、システムで取り扱うファイルやデータベースのデータ等に加え、OS の各種設定情報、システムのスクリプトや設定パラメータ等が考えられるところ、取得間隔や取得方法の設定に当たっては、対象データの特性（例：更新頻度等）を考慮することが考えられる。
- 重要システムに係る運用上の制約等により、定期検査時等にしかバックアップが取得できないなど、年１回以上のバックアップが難しい場合にも、サイバー攻撃によるバックアップデータ削除等により回復できないリスク等を考慮し、現状の取得間隔の短縮等、サイバー脅威を踏まえた、より適切な取得間隔を設定する。

①-2 バックアップデータについて、バックアップ元のシステムと異なるセグメントやオフラインで保管する等、切り離して保管し、データの重要度に応じて保存方法、保存期間、世代管理の方法を定める。

（解説）

- 攻撃を受けた情報システムや情報が格納されている場所からバックアップ保管場所にアクセスができる場合、情報システムや情報と同時にバックアップも破壊されてしまう可能性があるため、情報システムや情報が格納されている場所から物理的又は論理的に隔離された場所にバックアップを保管することが重要である。

・ 物理的な隔離として、例えば、バックアップ保管媒体等（例：外付けハードディスク、磁気テープ、クラウドストレージ）をネットワークから完全に切り離して保管する場合が挙げられる。
・ 論理的な隔離として、情報システムや情報が格納されている場所とバックアップ保管場所の間の通信経路において、アクセス制御による通信経路の分離を行っている場合が挙げられる。アクセス制御による通信経路の分離としては、通信が必要な単位でセグメントを分割し、他のセグメントとの間に次世代ファイアウォール等を設置することや仮想ネットワーク技術を活用する等により、セグメント間の通信を必要最小限とするアクセス制御を行うことが考えられる。
論理的な隔離の場合は、バックアップ保管場所でもインシデントが発生するリスクがある点に留意。
・ その他のバックアップの保存方法等としては、データの重要度に応じて、例えば、イミュータブルバックアップを利用することや、バックアップを複数取得した上で異なる媒体や環境で保存することも考えられる。

①-3 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、定期的にバックアップを実施する。定期的なバックアップが難しい場合には、適切な取得間隔を設定する。

講ずることが望ましい対策事項

①-4 リアルタイムでバックアップが可能な重要システムについては、可能な限りリアルタイムでバックアップを実施する。

（解説）
・ リアルタイムでのバックアップについて、オンライン接続を伴う場合は、バックアップ保管場所でもインシデントが発生するリスクがある点に留意。

統一基準における規定

② 取得したシステムイメージやデータ等に対するバックアップリカバリー検査の実施を検討する。

講ずべき対策事項

②-1 取得したシステムイメージやデータ等に対するバックアップリカバリー検査等の実施を検討する。

（解説）

- 運用不備等によりバックアップから復元できない可能性があることを踏まえ、バックアップリカバリーに係る手順を整備するとともに、バックアップリカバリー検査等（復旧テストを含む。）を実施し、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が重要である。
- システムリソース等の関係で実機でのリカバリー検査が困難な場合は、バックアップリカバリーに係る手順の確認を定期的に実施することも考えられる。

講ずることが望ましい対策事項

②-2 取得したシステムイメージやデータ等に対し、定期的なバックアップリカバリー検査等を実施する。

4.4 システムのセキュリティ対策

4.4.1 運用の手順及び責任

統一基準における規定

① 情報システム等の運用に関連する手順書を整備する。
② 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。
③ 情報システム等の更新に関する事前承認手続を定める。
④ 運用環境と開発・試験環境を分離する。

講ずべき対策事項

①-1 情報システム等の運用に関連する手順書を整備する。

（解説）

・ 手順書には、例えば以下の事項について記載することが考えられる。

- ログ管理運用
- 情報システムの容量管理
- EoL（End of Life）・EoS（End of Support）・パッチ管理
- 暗号鍵・電子証明書の更新
- セキュリティ監視
- バックアップ・リストア運用
- インシデント対応

②-1 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。

③-1 情報システム等の更新に関する事前承認手続を定め、不正な変更を防止するための構成制限を適用する。

③-2 構成変更管理プロセスを整備し、承認されていない変更を禁止する。提案された変更は、本番環境外でテスト及び文書化するなどし、実装前に潜在的なセキュリティ影響を分析する。

④-1 運用環境と開発・試験環境を分離する。

（解説）

・ 運用環境と開発・試験環境の分離について、ネットワークの物理的又は論理的な分離・アクセス制御のほか、例えば以下の対策が考えられる。

- 本番用ファイルと開発・試験用ファイルの分離
- 本番用データベースへのアクセス防止
- 本番用アカウントと開発・試験用アカウントの分離

講ずることが望ましい対策事項

なし

4.4.2 ハードウェア・ソフトウェアの管理

統一基準における規定

① 情報システムで利用するハードウェア・ソフトウェアの個々の設定について把握・理解し、安全性の確保に努める。

講ずべき対策事項

①-1 情報システムで利用するハードウェア・ソフトウェアの個々の設定について把握・理解し、安全性の確保に努める。

①-2 情報システムで利用するハードウェア・ソフトウェアについて、セキュリティを保って管理するための手順を策定する。

（解説）

- 手順の策定に当たっては、4.4.1「運用の手順及び責任」も参照。
- ハードウェア・ソフトウェアのセキュリティを保った設定について、例えば以下がある[97]。
  - 全ての機器においてマクロや類似の埋め込みコードが無効化され、コードやアプリケーションの自動実行が防止される。
  - 特定の状況でマクロを有効にする必要がある場合、承認された利用者により特定の資産でマクロを有効化するよう要求できるポリシーを定める。
  - USB や光学ドライブ等からの意図しないコード実行を防ぐため、自動実行を無効化する。
  - 情報システムの運用に必要な特定の機能、プロトコル、サービスのみを許可することで、機能制限を実施する。
- セキュリティ管理において把握することが有用なハードウェアの設定として、例えば、管理ポートの接続先、操作インタフェース／USB ポートの有無、無線機能の有無のほか、IP アドレスや MAC アドレス等が考えられる。詳細については、IPA「制御システムのセキュリティリスク分析ガイド 第２版」の「3.1.3. 資産の洗い出し」を参照。

[97] これらの設定により、マルウェア等のセキュリティ脅威を一定程度低減することができる（4.4.4 マルウェアからの保護）。

①-3 ハードウェア・ソフトウェアの更新は、定めた手順に基づき適切に実施する。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。

講ずることが望ましい対策事項

①-4 制御システムを構成するハードウェア・ソフトウェア（ファームウェアを含む。）の真正性を検証可能とするシリアル番号、チェックサム、電子証明書/署名、その他の識別情報を文書化・維持管理する。

①-5 認可されたバージョンを明記した承認済みハードウェア・ソフトウェア（ファームウェアを含む。）の一覧[98]を作成・維持管理する。

①-6 ソフトウェアについて、多要素認証や最小権限によるアクセス制御等、適切な設定についてのベースラインを定め、ソフトウェアがこれを満たしているか監視する。

[98]「ホワイトリスト」と同義（3.1.1④-2 参照）。

統一基準における規定

② 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とともに、サポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行を検討する。

講ずべき対策事項

②-1 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。

②-2 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とともに、サポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行を検討する。

（解説）

- 安全に関する要求事項を優先する等の理由により、サポート対象バージョンへの更新が困難な場合には、補完的な措置として、例えば、3.6②-2 の脆弱性悪用のリスクを低減する対策を実施する。
- 採用するセキュリティ管理策は文書化し、リスクに応じて適切に承認を得る。

講ずることが望ましい対策事項

②-3 サポート対象バージョンへの更新が困難な場合には、サポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行計画を策定及び実施する。

4.4.3 システムの取得・開発・保守

統一基準における規定

① 情報システムの取得・開発・保守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。

講ずべき対策事項

①-1 情報システムの取得・開発・保守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。

（解説）

- 重要インフラサービスの提供に係る情報システムを新たに取得・開発する際や、既存の情報システムを保守する際には、「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サイバーセキュリティについての要求も含める（必要に応じて、HSE 等の観点からの要求も含めて検討を行う。）。
- 情報システムのセキュリティ要件を定める考え方については、以下を参照。
  - 国家サイバー統括室「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[99]」
  - デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン[100]」

講ずることが望ましい対策事項

①-2 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。

[99] https://www.cyber.go.jp/policy/group/general/sbd_sakutei.html

[100] https://www.digital.go.jp/resources/standard_guidelines/

統一基準における規定

② 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など、情報システムの取得・開発・保守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。

講ずべき対策事項

②-1 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。

講ずることが望ましい対策事項

②-2 情報システムの重要度に応じて、上記②-1 に加え、情報システムの取得・開発・保守時にサイバーセキュリティを確保するための手順、環境等を整備し、必要な対応を行う。

（解説）

・ 例えば、以下についての手順、環境等の整備が考えられる。
- 定期的な脆弱性診断
- セキュアコーディングに係る基準
- データの機密性、アクセス管理、イベントログ取得等のセキュリティ要求事項
- セキュリティ技術・アーキテクチャに係る設計標準
- システムへの脆弱性の混入及び作込みを未然に防止し、早期に検知するツール（ソースコード解析ツール等）の活用

4.4.4 マルウェアからの保護

統一基準における規定

① 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。

講ずべき対策事項

①-1 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、許可されたユーザーが特定の状況下で実行できることを承認する仕組みを構築する。

（解説）

- 4.4.2.①-2「情報システムで利用するハードウェア・ソフトウェアについて、セキュリティを保って管理するための手順を策定する。」もあわせて参照。

①-2 マルウェアの検知率向上が期待されるマルウェア検知ソフトの利用や、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マルウェア対策機能等を導入する。[IT システムのみ]

（解説）

- マルウェアの検知率向上が期待されるマルウェア検知ソフトの利用として、例えば、複数の検知方式を組み合わせたり、マルチエンジン型のマルウェア検知ソフトを利用することが考えられる。
- マルウェア検知ソフトの利用が不可能、又は利用により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、ネットワークの物理的又は論理的分離、USB メモリ等の外部電磁的記録媒体からの感染防止対策、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。

講ずることが望ましい対策事項

①-3 被害が発生した際の攻撃の拡散に備えた対策として、ネットワークのセグメンテーション（重要インフラの分離）を行う。

①-4 被害が発生した際の攻撃の拡散に備えた対策として、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）、NDR(ネットワーク全体の包括的な監視と脅威検知)等を導入・運用する。

（解説）

- Living Off The Land 戦術（システム内寄生戦術）のような高度なサイバー攻撃は、既存のセキュリティ対策を回避するものが少なくない。そこで、IPS/プロキシサーバ、EDR、NDR 等製品を検知精度の向上等に活用するだけでなく、事象発生後の対応及び復旧に係る活動にも活用できるよう、通常時から継続的な監視やインシデント対応等にかかわる体制整備を行うことが重要である。

①-5 制御システムを構成する機器においてマルウェア検知ソフト等を利用する場合、互換性チェック、変更管理、パフォーマンス影響測定等を含む手順を整備し、マルウェア検知ソフト等の更新時に適用する。

①-6 ソフトウェアの実行をあらかじめ許可されたものに制限する、又は禁止及び未承認ソフトウェアの実行を拒否する。

①-7 ソフトウェア等の実行後も継続的にプロセス等を監視し、不正な行為を検知した場合は必要に応じて遮断等の対応を行う。

4.5 ログ取得

統一基準における規定

① 情報システムのイベントログや運用担当者の作業ログ等、セキュリティの確保に必要なログを記録・管理する。

講ずべき対策事項

①-1 情報システムのイベントログや運用担当者の作業ログ等、セキュリティの確保に必要なログを記録・管理する。ログの保存期間については、分析の必要性も踏まえ、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。

（解説）

- セキュリティの確保に必要なログとして、例えば、以下が考えられる。
  - システム及びネットワーク機器（ファイアウォール、ルーター、VPN 装置）等のアクセス・認証ログや通信ログ
  - セキュリティ対策システムのイベントログ、通信ログ
- ログは、検知及びインシデント対応、サイバー脅威の分析で使用する観点から取得する。
  重要インフラサービス障害に繋がる可能性のある事象を検知するため（5「検知」参照）、IoC（侵害の痕跡）、アノマリ（異常値）にも留意する。
- ログの分析及びインシデント対応に支障が生じないように、ログを出力する機器やシステム等について、時刻を適切に同期する。
- 重要システムのセキュリティ確保に必要なログの保存期間については、例えば、１年間以上を目安とすることが考えられる。
- 機器等における必要なログの取得・分析に当たっては、以下を参照。
  - デジタル庁「政府情報システムにおける脅威の検知・対応のためのログ取得・分析導入ガイドブック [101]」
  - JPCERT/CC「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 [102]」
  - 総務省「サイバー攻撃（標的型攻撃）対策防御モデルの解説 [103]」

[101] https://www.digital.go.jp/resources/standard_guidelines
[102] https://www.jpcert.or.jp/research/apt-loganalysis.html
[103] https://www.soumu.go.jp/main_content/000495298.pdf

- 内閣サイバーセキュリティセンター「豪州主導の国際文書『イベントログと脅威検知のためのベストプラクティス』への共同署名について[104]」

①-2 ログ機能が非搭載の制御システムについては、制御システムと他の資産との間のセキュリティ確保に必要な通信ログを記録・管理する。

（解説）

・ 制御ネットワーク（フィールド側）のコントローラ等の接続機器とフィールドに存在する機器においては、ログ機能が非搭載、あるいは可用性確保等の観点からログ機能の利用が難しい場合が想定される。
その場合、代替手段として、ネットワーク機器（ファイアウォール、プロキシサーバ、ネットワークスイッチ等）の通信ログ等、制御システムと他の資産との間のセキュリティ確保に必要な通信ログを記録・管理する。また、SCADA[105]等の監視・制御を行うシステムのログを記録・管理することも有用と考えられる。

講ずることが望ましい対策事項

①-3 収集したログをツールや中央システム（統合ログ管理システム、SIEM[106]等）で一元的に保存し、許可された管理者のみがアクセスできるようにする。

[104] https://www.cyber.go.jp/pdf/press/press_ASD_LOTL_Guidance.pdf

[105] Supervisory Control and Data Acquisition の略。制御とデータ収集を行うシステムの総称。

[106] SIEM（Security Information and Event Management）とは、ファイアウォールや IDS／IPS、プロキシなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことにより、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とする。

統一基準における規定

②　ログが改ざん、消去されないよう管理する。

講ずべき対策事項

②-1 ログが改ざん、消去されないよう、情報システムの重要度に応じて定期的に、保存したログの点検及び分析を行う。

②-2 設定可能な場合は、イベントログ等の重要なログソースが無効化された場合にセキュリティ担当者に通知するよう設定する。

講ずることが望ましい対策事項

②-3 ログが改ざん、消去されないよう保全する。

（解説）

・ ログの改ざん、消去を防止するための保全方法として、以下の例が考えられる。

- 収集したログをツールや中央システム（統合ログ管理システム、SIEM 等）やイミュータブルストレージ等で一元的に保存し、許可された管理者のみがアクセスできるようにする。
- ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保存する。
- ログを書き換え不能な外部電磁的記録媒体（DVD-R 等）に書き出して保存する。

4.6 インフラストラクチャ（ネットワーク等）の対策

4.6.1 通信のセキュリティ

統一基準における規定

① レジリエンスの観点から、ネットワークをセグメントに分割、セグメント間の通信を必要最小限となるようアクセス制御を行う。

講ずべき対策事項

①-1 ネットワークのセグメンテーションやファイアウォールの利用等により、インターネットに接続される資産を可能な限り最小限とする。

①-2 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配置しない。例外が存在する場合には文書化・承認し、悪用を防止する措置を具備する。

（解説）

- 悪用防止の措置として、例えば、多要素認証の活用、ロギングによる動作の監視が考えられる。

①-3 インターネットに接続された資産について、不要なポート、プロトコル、サービス等を全て無効化する。

（解説）

- 無効化の際、例えば、RDP[107]、SSH[108]、SMB[109]等が悪用される可能性がある点にも留意する。

①-4 情報系のネットワーク（クラウドベースのものを含む。）と制御システムを構成するネットワークを物理的又は論理的に分離し、必要な通信のみを許可する。

（解説）

[107] Remote Desktop Protocol の略。
[108] Secure Shell の略。
[109] Server Message Block の略。

- 昨今、リモート運用・保守やクラウドサービス等の利用を通じて十分に把握・管理されていない外部とのネットワーク接続がなされ、それらが悪用されることにより、結果として不正アクセス等の被害を受けるリスクは高まっている。
- 重要システムに係るネットワークを他のネットワークから物理的又は論理的に分離して閉域網として運用することは、従来よりセキュリティ管理上重要な対策とされるが、閉域網であるがゆえに外部から侵入されるリスクはないと考え、境界を構成するネットワーク機器を含む内部システムのセキュリティ対策（例：認証・認可、脆弱性対策、マルウェア対策）を疎かにするのは、危険とも言える。
- 境界を構成するネットワーク機器等に対する対策事項については、以下を参照。
  - CISA「Enhanced Visibility and Hardening Guidance for Communications Infrastructure[110]」
  - CISA「BOD 26-02: Mitigating Risk From End-of-Support Edge Devices[111]」

①-5 重要システムに係るネットワークと他ネットワークとの接続点には、ファイアウォール等中継装置を設置し、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。

講ずることが望ましい対策事項

①-6 重要システムに係るネットワーク内において、利用目的等に応じてネットワークを分割する。

①-7 ネットワークセグメントを細分化し、マルウェアの水平移動（ラテラルムーブメント）を阻止することなどにより、サイバー攻撃の被害拡大防止を図る。

①-8 データダイオード等の通信方向を一方向のみに制御する方法により、制御システムへのアクセスを制限する。

[110] https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

[111] https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices

統一基準における規定

② 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等によってネットワークのセキュリティを確保する。

講ずべき対策事項

②-1 専用線や暗号技術の活用によってネットワークのセキュリティを確保する。

（解説）

- ネットワークを介して情報を取り扱う場合には、通信経路における情報の盗聴、改ざん等のリスクを踏まえ、取り扱う情報の重要度やネットワークの構成等に応じ、専用線や閉域網の利用、VPN 等による通信経路の保護、通信内容の暗号化、通信相手の認証等を実施する。
- 暗号技術の活用は、特にインターネットその他の組織外のネットワークを経由して接続する場合に重要である。また、専用線や閉域網を利用する場合であっても、接続機器の管理不備、通信回線からの情報窃取（タッピング）等のリスクがあり、それのみをもって必要なセキュリティが確保されるとは限らないことに留意する。
- 暗号技術の導入に当たっては、取り扱う情報の重要度、通信の特性、処理性能、遅延が業務に及ぼす影響等を踏まえて、活用の範囲並びに適切な暗号方式及び実装方法を選定する。

講ずることが望ましい対策事項

②-2 インターネットに接続された情報システムについて、サーバ装置（IoT 機器含む。）、端末、通信回線装置又は通信回線から重要度に応じて、サービス不能攻撃（DoS 攻撃、DDoS 攻撃）対策を実施する対象を特定し、当該対策を実施する。

（解説）

- 具体的なサービス不能攻撃対策の方法を検討するに当たっては、内閣サイバーセキュリティセンター「DDoS 攻撃への対策について（注意喚起）[112]」を参照。

[112] https://www.cyber.go.jp/pdf/news/press/20250204_ddos.pdf

統一基準における規定

③　重要な情報を通信手段により転送するに当たり、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。

講ずべき対策事項

③-1 重要な情報を通信手段により転送するに当たり、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。

（解説）

・ 重要な情報を、電子メール、電子データ交換、インスタントメッセージ等の通信手段により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の合意を図る。

講ずることが望ましい対策事項

なし

4.6.2 テレワーク・遠隔制御

統一基準における規定

① 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。

講ずべき対策事項

①-1 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方針を定め、それらに基づいて対策を実施する。

（解説）

・ 対策方針には、例えば、以下について記載することが考えられる。

- テレワーク・遠隔制御サイトにおける、他者（家族、友人等）からの認可されていないアクセスリスクへの対策
- 公共の場所にいる他者からの認可されていないアクセスリスクへの対策
- 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
- 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・遠隔制御が終了したときの、権限及びアクセス権の失効

・ 業務上の必要性がある場合にのみリモートアクセスを許可する。その際、リモートアクセスの申請及び許可に関する手順を策定し、組織内に周知徹底する。なお、重要システムへリモートアクセスする場合には多要素認証を導入する（4.1.2「認証・アクセス制御」①-5 参照）。

・ テレワークの導入に当たっては、セキュリティ対策についての考え方や対策例を示した総務省「テレワークセキュリティガイドライン（第５版）[113]」を参照するとともに、テレワーク実施前及び実施後に確認するチェックリストとして総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第３版）[114]」を参照。

[113] https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

[114] https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

講ずることが望ましい対策事項

なし

4.6.3 災害による障害の発生を踏まえた対策

統一基準における規定

① 災害による障害が発生しにくいよう設備を管理する等の災害対策を実施する。

講ずべき対策事項

①-1 火災、洪水、地震等の自然災害が重要インフラサービスの継続的提供に与える影響について、リスクアセスメントを実施し、リスクアセスメントの結果を踏まえて必要な対策を実施する。

（解説） ・ 4.1.4.①「装置の管理」もあわせて参照。

講ずることが望ましい対策事項

①-2 災害による障害が発生しにくいよう設備を管理・配置する。

①-3 システムを運用するサービスプロバイダーに対する要件に、環境的脅威からの保護と適切な運用インフラの整備を含める。

4.7 クラウドサービス利用時の対策

統一基準における規定

① 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。

講ずべき対策事項

①-1 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。

（解説）

・ セキュリティ確保の観点から、例えば以下のクラウドサービスの仕様について確認することが考えられる。

- 主体認証情報（パスワード等）の管理機能
- クラウドサービス上に保管された情報や当該サービスの機能に対するアクセス制御機能
- クラウドサービス内及び通信経路全般における暗号化
- クラウドサービスのリソース（ネットワーク、仮想マシン等）設定を変更するユーティリティプログラムを使用する場合の機能
- クラウドサービス内及び通信経路全般における暗号化に係る鍵管理に係る機能及び手順
- バックアップ機能
- クラウドサービスの利用に係るログの取得及び管理に関する機能
- シングルサインオンや外部認証連携に関する機能

・ クラウドサービスを利用する際に参照可能な評価制度等として、例えば以下がある。

- 政府情報システムのためのセキュリティ評価制度（ISMAP、ISMAP-LIU）
- ISMS クラウドセキュリティ認証
- クラウドセキュリティ・マーク（CS マーク）

・ セキュリティ確保のためにクラウドサービス利用者自らが行うべきこと、クラウドサービス提供者に対して求めるべきことについては、以下を参照。

- デジタル庁「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針[115]」

[115] https://www.digital.go.jp/resources/standard_guidelines/

- 総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）[116]」
- 総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン[117]」
- 総務省「クラウドの設定ミス対策ガイドブック[118]」
- 経済産業省「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）[119]」
- 経済産業省「クラウドセキュリティガイドライン活用ガイドブック（2013 年度版）[120]」
- 公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書[121]」

講ずることが望ましい対策事項

なし

[116] https://www.soumu.go.jp/main_content/000771515.pdf
[117] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00149.html
[118] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00209.html
[119] https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf
[120] https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf
[121] https://www.fisc.or.jp/document/fintech/file/190_0.pdf

統一基準における規定

② 責任共有モデル[122]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。

講ずべき対策事項

②-1 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。

（解説）

・ 下記図表４は責任共有モデルの例であるが、あくまでも例であり、各クラウド事業者やサービスによって、具体的な責任範囲や内容が異なる場合がある。

図表４　責任共有モデルの例[123]

[122] 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。

[123] IaaS：Infrastructure as a Service の略。利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上に OS や任意機能（セキュリティ機能を含む。）を構築することが可能である。
PaaS：Platform as a Service の略。IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。

- どのようなクラウドサービスでも、組織としての活用の目的や指針、設定や接続する端末の安全性の確保、さらには管理する（又は生み出される）データ等の取扱いは、おおむね利用者側の責任である。また、クラウドサービスの活用に当たっては多数のステークホルダーが存在し、一般的に利用者側に責任がある領域も外部へ委託している場合や外部からの支援を受けている場合がある。そのため、責任共有モデルは構築者や設置者等のステークホルダー（4.7⑤-1 参照）を踏まえた上で理解する必要がある。

講ずることが望ましい対策事項

なし

SaaS：Software as a Service の略。利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。

統一基準における規定

③　情報公開等の設定にミスがないか確認する。

講ずべき対策事項

③-1 提供されるクラウドサービスの特性等を考慮し、情報公開等の設定にミスがないか確認する。

（解説）

・　情報公開等の設定ミスについて、クラウドサービスの提供者・利用者双方が設定ミスを起こさないための対策について記載された総務省「クラウドの設定ミス対策ガイドブック」[124]では、以下の事例が紹介されている。

- 自社の業務で扱う機密情報をファイルに保存し、当該ファイルが公開設定であったことが外部からの指摘で発覚した事例
- 自社のシステムをクラウドに移行する際に、ストレージの設定が「公開」になっていたため、長期間機密情報が公開されていた事例

・　インフラやプラットフォームを提供する IaaS・PaaS の設定項目には、以下がある。

- ID とアクセス管理
- ロギングとモニタリング
- オブジェクトストレージ
- 仮想マシン（VM, VPS）
- ネットワークセキュリティ等の集中管理
- 鍵管理
- （PaaS が提供する）アプリケーションの設定
- データベースの設定
- コンテナの設定

・　業務アプリケーションを提供する SaaS の設定項目には、以下がある。

- 組織の設定
- ユーザーの設定
- セキュリティとアクセスの設定（パスワードやログインポリシーの設定）
- オブジェクトの設定

[124] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00209.html

- アプリケーションの設定
- プロセスの自動化の設定

講ずることが望ましい対策事項

なし

統一基準における規定

④　サービス仕様が変わる際には影響を確認する。

講ずべき対策事項

④-1 クラウドサービスの仕様が変わる際には、サービス運用者又はクラウドサービス提供者から情報提供を得つつ、影響を確認する。

（解説）

- クラウドサービス利用者は、サービス運用者又はクラウドサービス提供者から情報提供を得つつ、サービスの更新予定・内容などについて協議する。サービスを更新する場合は、 更新理由や更新による変更点、機能追加等がある場合は、追加機能、利用時の注意点や設定方法の確認を利用者と運用者又は提供者で行う。
- 利用者は、サービス運用者等からサービス更新時の影響に関する説明を受け、その影響を踏まえた上で、組織への影響を考え、更新や設定を行うかを検討する必要がある。
- なお、協議した内容や資料については議事録を残し、少なくともサービスを利用している間は保管し続けることが重要である。

講ずることが望ましい対策事項

なし

統一基準における規定

⑤　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。

講ずべき対策事項

⑤-1　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。

（解説）

【ステークホルダーについて】

- クラウドサービスに係るシステム上のステークホルダーには、例えば以下が挙げられる。
  - クラウドサービス提供者：クラウドサービスを提供している組織
  - 販売者：クラウドサービスやシステムを販売する組織
  - 利用者：クラウドサービスやシステムを利用する組織
  - 構築者：クラウドサービスを活用してシステムを構築する組織（利用者の子会社やシステムインテグレータなど）
  - 設置者：クラウド構築者を支援して、実作業や設置を行う組織（システムインテグレータやその委託企業など）
  - 運用者：構築されたシステムの運用を支援する組織（システムインテグレータやその委託企業など）
  - 顧客：利用者がクラウドサービスを利用してシステムを構築し、何らかのサービス等を提供する対象者
- 上記のステークホルダーについてはあくまでも例示であり、サービスによっては全てのステークホルダーが存在しない場合もある（利用者とクラウドサービス提供者のみなど）。例えば、受託開発の場合、受託開発に加えてライセンスを利用する場合、利用規約に同意して利用する場合等、ステークホルダーの構成は様々である。

【情報共有体制・インシデント対応体制について】

- 利用するクラウドサービスにおいてインシデントの発生を検知した場合に備え、連絡体制を事前に定めておく必要がある。その際は、クラウドサービス提供者からの通知を複数の職員等が受け取れるようにする等、確実かつ効率的な連絡体制を構築し、インシデントの早期検知につなげることが重要である。
- また、連絡先には、クラウドサービス提供者や当該クラウドサービスの運用者等の連絡先も含むように運用規程等に含めることが考えられる。

講ずることが望ましい対策事項

なし

統一基準における規定

⑥　クラウドサービスの利用終了時における、クラウドサービス上のデータの取扱い（論理的な廃棄）について確認する。

講ずべき対策事項

⑥-1　クラウドサービスの利用終了時における、クラウドサービス上のデータの取扱い（論理的な廃棄）について確認する。

（解説）

・　確認方法としては、暗号化消去に用いた鍵については、バックアップを含めて抹消することや、クラウドサービス提供者に、契約時に同意した情報の廃棄手順の実施報告書を要求し確認することなどが考えられる。また、対象はバックアップ等により複製された物にも及ぶ点に注意が必要である。

講ずることが望ましい対策事項

なし

5　検知

5.1　監視・分析体制の整備

統一基準における規定

①　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）を早期検知するための体制を整備する。

講ずべき対策事項

①-1　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）を早期検知するための体制を整備する。

（解説）

- 早期検知のための体制整備に当たっては、外部委託を行うことも想定される。
- 重要インフラサービス障害に繋がる可能性のある事象を早期検知するためには、IoC（侵害の痕跡）、アノマリ（異常値）に留意しつつ、セキュリティ確保に必要なログを取得していることが前提となる（4.5「ログ取得」参照）。
- 上記のセキュリティ確保に必要なログの監視・分析を含め、5.2「継続的監視」・5.3「事象の分析」を行うための体制を整備する。
- CSIRT 等の連携にも留意する。

①-2　早期検知するための体制整備を外部委託により行う場合、委託先で実施している対策の具体的な内容を把握するとともに、対策の講じられていない領域が判明した際に必要な措置をとる。

（解説）

- 早期検知するための体制整備を外部委託により行う、あるいは委託先で実施している対策の具体的な内容を把握するに当たっては、セキュリティ運用サービスを選定する際のポイント等を解説した日本セキュリティオペレーション事業者協議会（ISOG-J）「マネージドセキュリティサービス（MSS）選定ガイドライン Ver.2.0[125]」を参考にすることも考えられる。

[125] https://isog-j.org/output/2020/MSS-Guideline_v200.html

・　必要な措置の例としては、当該委託先へ未実施事項のフィードバックを行うことに加え、今後の対策実施に向けた協議を実施することが考えられる。

講ずることが望ましい対策事項

なし

5.2 継続的監視

統一基準における規定

① 重要インフラサービス障害に繋がる可能性のある事象を検知するために、継続的な監視を実施する。

講ずべき対策事項

①-1 重要インフラサービス障害に繋がる可能性のある事象を検知するために、継続的な監視を実施する。

（解説）

- 例えば、以下について継続的な監視を実施することが想定される。
  - ネットワーク及びネットワークサービス（例：情報系ネットワークと制御システムのネットワークとの境界を構成するファイアウォール）
  - 物理的な環境（例：管理領域（機密性の高い区域及びコンピュータ室、データ保管室等））
  - システム上における人員の活動と技術の使用状況（例：重要な情報を取り扱うシステムに対するアクセス、重要システムに対するユーザー又は管理者の操作）
- 制御システム等に対して継続的な監視を行うためにセキュリティ製品等を新たに導入する場合、制御システムを構成する機器へ展開する前に、まずはテスト環境で実装した上、テストを実施する必要がある。その際、懸念事項としては、機器上のホストベースエージェントによるパフォーマンスへの影響、機器に対するアクティブスキャンによる影響、ネットワークインフラの処理能力等が挙げられる。
- 外部事業者の選定については、事業者における一定の技術要件及び品質管理要件を確保する観点から、「情報セキュリティサービス基準」及び「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監視・運用サービスに係る部分）を参照。

講ずることが望ましい対策事項

①-2 SIEM 等のツールを活用し、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繋がる可能性のある事象を早期検知する。

5.3 事象の分析

統一基準における規定

① インシデントとして扱う事象の範囲をあらかじめ定め、重要インフラサービス障害に繋がる可能性のある事象がインシデントに該当するかどうかを分析する。

講ずべき対策事項

①-1 重要インフラサービス障害に繋がる可能性のある事象がインシデントに該当するかどうかを分析するため、あらかじめ、インシデントとして扱う事象の範囲及びインシデントのレベル（影響範囲・重要度を含む）を定める。

講ずることが望ましい対策事項

①-2 分析を迅速に行うため、SIEM 等のツールを活用し、重要インフラサービス障害に繋がる可能性のある事象の分析を可能な限り自動化する。

①-3 制御システムにおいて、侵入を示唆する行動や事象に対するアラート等が、実際には正常な動作である場合があることを踏まえ、制御システム特有の事象や異常を考慮して分析を行う。

6　対応及び復旧

6.1　事業継続計画等

統一基準における規定

① 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、事業復旧計画[126]、IT-BCP[127]、インシデント対応計画等。以下あわせて「事業継続計画等」という。）にサイバーセキュリティを組み入れる。その際、3.6.2「インシデントへの対応及び復旧」に定める事項を含める。

講ずべき対策事項

①-1 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、事業継続計画等にサイバーセキュリティを組み入れる。その際、統一基準 3.6.2「インシデントへの対応及び復旧」に定める事項（インシデント管理等）についても言及する。

（解説）

- 重要インフラサービス障害の発生又はそのおそれがあることを認識した際に、経営層や職員等がまず実施すべき対応を明確にし、迅速に行動することが求められる。そこで、初動対応（緊急時対応）の方針、手順、態勢等を定めることが必要である（例：コンティンジェンシープラン）。
- 重要インフラサービス障害発生時において、サービスを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を目的とし、復旧に向けた目標水準、優先順位、その他の方針、手順、態勢等を定めることが必要である（例：事業継続計画）。
- 統一基準 3.6.2「インシデントへの対応及び復旧」に定める事項を事業継続計画等のうちいずれの文書に含めるかについては、既存の文書体系や体制等に応じて、分野ごと、あるいは重要インフラ事業者等ごとに判断することが想定される。

[126] 通常時のサービス水準までの完全復旧対応の方針。

[127] 情報システムに係る記載を詳細化した対応方針。この点、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。なお、IT-BCP は、事業継続計画等に該当する文書の例示の一つであり、事業継続計画等には、OT-BCP を含む制御システムに関する対応方針も含まれる。

・ インシデント対応計画には、例えば、次の活動が含まれる。
  - 何がセキュリティインシデントに相当するか、基準に従ったセキュリティ事象の評価
  - 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
  - インシデントの種類に従った対応、危機管理の発動及び事業継続計画の発動の可能性、インシデントからの復旧、内部及び外部の利害関係者への伝達を含む、セキュリティインシデントの終結までの管理
  - 関係当局、供給者及び顧客等の内部及び外部の利害関係者との調整
  - インシデント管理活動のログ取得
  - 証拠の取扱い
  - 根本原因分析又は事後分析手順
  - 教訓及びインシデント管理手順、セキュリティ管理策についての改善
  - インシデント報告書の作成
・ 事業復旧計画等を策定するに当たり、安全基準等策定ガイドライン末尾の「【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することも考えられる。
・ 事業継続計画等の検討の詳細については、以下を参照。
  - 国家サイバー統括室「政府機関等における情報システム運用継続計画ガイドライン（第3版）」[128]
  - 内閣府・「防災情報のページ」記載の事業者向けのガイドライン等のうち「事業継続ガイドライン[129]」
  - JPCERT/CC「インシデントハンドリングマニュアル[130]」
・ 参考として、米国CISAによる重要インフラのレジリエンス強化のためのガイダンス[131]において、外部ネットワークとの接続を能動的に遮断し通信が制限された状態でも重要なサービスの提供を継続する運用の確保（隔離）や、隔離状態のまま侵害された重要なシステムを迅速に復旧させるための計画や手順の策定、訓練等（復旧）の重要性が示されている。

[128] https://www.cyber.go.jp/policy/group/general/itbcp-guideline.html
[129] https://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk.html
[130] https://www.jpcert.or.jp/csirt_material/operation_phase.html
[131] https://www.cisa.gov/topics/industrial-control-systems/ci-fortify

講ずることが望ましい対策事項

①-2 目標復旧水準から通常時のサービス水準まで完全復旧させることを目的とした計画を策定する（例：事業復旧計画）。

①-3 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インシデント対応計画を策定する。

①-4 制御システムを対象としたインシデント対応計画を策定し、安全対策及び封じ込めに関する制御システム固有の事項を考慮する。

統一基準における規定

②　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。

講ずべき対策事項

②-1 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。

（解説）

- サプライチェーンに係る脅威としては、例えば、供給者・委託先が保有する機密情報の漏えい、ソフトウェア開発元や MSP（マネージドサービスプロバイダー）等を踏み台とした不正アクセス等が考えられる。
- サプライチェーンに係る脅威への対応としては、例えば、インシデントが発生した際の供給者・委託先との間の報告・連絡・相談が考えられる（必要な対応について、2.9「サプライチェーン・リスクマネジメント」②-2・③-3 も参照。）。

講ずることが望ましい対策事項

なし

6.2 インシデントへの対応及び復旧

6.2.1 インシデント管理

統一基準における規定

① インシデントの管理責任者を定める。

講ずべき対策事項

①-1 インシデントの管理責任者を定める。

（解説）

- インシデントの管理責任者として、例えば、2.5.1.②により設置するCISO等や、重要システムの管理に責任を有する経営層が考えられる。

講ずることが望ましい対策事項

なし

統一基準における規定

② 証拠収集等の手順を整備する。

③ 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。

④ 重要インフラサービス障害に繋がる可能性のある事象が検知された場合における、関係部署等との情報共有、トリアージ[132]等の運用プロセスを確立する。

講ずべき対策事項

②-1 証拠収集等の手順を整備する。

（解説）

・ 整備すべき手順として、例えば、インシデント管理活動のログ取得、証拠の取扱い、インシデント対応に必要な連絡先（エスカレーションの報告先等）等が考えられる。

③-1 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。

（解説）

・ インシデントの速やかな報告実施を支援するため、6.1.①で策定する事業継続計画等において各役職員に対してインシデント対応に必要な役割（例：発見した事象の報告等）を割り当てるとともに、4.2.2 で実施する演習・訓練を通じて実施の成熟度を継続的に向上させることが考えられる。

④-1 重要インフラサービス障害に繋がる可能性のある事象が検知された場合における、関係部署等との情報共有、トリアージ等の運用プロセスを確立する。

講ずることが望ましい対策事項

なし

[132] 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。

統一基準における規定

⑤　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。

講ずべき対策事項

⑤-1　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。

（解説）

- 例えば、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、将来の対応活動や対策に活かすべく、事業継続計画等の継続的な改善プロセスに取り入れることが想定される。
- 情報システムへのセキュリティ機能の実装等、計画的に実施する必要がある再発防止策については、リスク対応計画（3.5.3 参照）に反映させるなどして、適切に実施させるよう取組を推進することが求められる。

講ずることが望ましい対策事項

なし

6.2.2 インシデント分析

統一基準における規定

① トリアージの結果、対応が必要と判断したインシデントについて、事象の詳細を分析する。

講ずべき対策事項

①-1 事象のトリアージや詳細分析を実施するための手順や方針を策定する。

①-2 トリアージを実施し、その結果、対応が必要と判断したインシデントについて、事象の詳細を分析する。

（解説）

- 適切な管理体制の構築を前提としつつ、インシデント分析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することも想定される。
- 調査方針においては、情報システム等へのフォレンジック調査についても検討する。
- 外部事業者の選定については、「情報セキュリティサービス基準」及び「情報セキュリティサービス基準適合サービスリスト」（うちデジタルフォレンジックサービスに係る部分）を参照。
- 参考として、IPA の「サイバーレスキュー隊（J-CRAT）[133]」は、標的型サイバー攻撃（APT 攻撃）の被害の発生が予見され、その対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織や、標的型サイバー攻撃の連鎖の元（ルート）となっていると推測される組織等に対して、初動対応の支援を行っている。

講ずることが望ましい対策事項

①-3 インシデントについて、攻撃の手口や原因・経路、システムへの影響、現在発生している業務影響及び今後発生し得る業務影響等について分析する。

①-4 調査中に実施された操作を記録し、記録の完全性と出所を保持する。

[133] https://www.ipa.go.jp/security/j-crat/about.html

①-5 インシデントの他の潜在的な標的を調査し、IoC（攻撃者によるシステムへのアクセスの維持・潜伏に関する証拠を含む。）を探索するとともに、検知、封じ込め、根絶及び再発防止に活用できるよう整理する。

①-6 攻撃対象システムにおいてツールを自動的に実行し、IoC（攻撃者によるシステムへのアクセスの維持・潜伏に関する証拠を含む。）を探索する。

6.2.3 インシデントの報告とコミュニケーション

統一基準における規定

① インシデントについて、関係法令等に基づく報告、組織内外との情報共有、供給者及び顧客等の関係者との調整を行う。

講ずべき対策事項

①-1 インシデントについて、関係法令等に基づく報告を行う。

（解説）

- 情報開示については 2.7「情報開示」、自組織外への情報共有、サイバー脅威の分析に必要な情報の共有については 3.3「情報共有」、サイバー攻撃被害に係る情報の公表の詳細については「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）をそれぞれ参照。
- 「関係法令等」については、「重要インフラのサイバーセキュリティに係る行動計画」の「別紙２　重要インフラサービスとサービス維持レベル」を参照。
- 基幹インフラ事業者でもある重要インフラ事業者等は、サイバー対処能力強化法第５条に基づく特定侵害事象等の報告義務に留意。

①-2 インシデントについて、事業継続計画等に基づき、組織内外との情報共有を行う。

①-3 顧客保護、二次被害防止、顧客や自組織等のセキュリティ上のリスク等を考慮の上、顧客への連絡が適切な場合には、顧客に対してインシデントに関する連絡を行う。

（解説）

- 顧客への連絡手段については、個別通知又は公表があり得るところ、関係法令、顧客保護等の観点を考慮の上、適切な手段を選択する。
- 顧客へ連絡する内容については、例えば、以下の事項が考えられる。
  - 影響範囲

- 注意事項
- 対応方法

講ずることが望ましい対策事項

なし

6.2.4 インシデント軽減

統一基準における規定

① インシデントの封じ込め（通信の遮断やシステム停止等、サイバー攻撃による被害拡大を防止するための対応）を行う。

講ずべき対策事項

①-1 インシデントの封じ込めの実施を判断する際の判断権限者を明確にする。

（解説）

- 封じ込めにおいては、必要に応じて情報システムの全部又は一部を一時的に停止するなど、業務継続に影響を及ぼす判断を下すこともあり得るため、あらかじめ判断権限者を明確にしておく必要がある。

①-2 インシデントの封じ込め（通信の遮断やシステム停止等、サイバー攻撃による被害拡大を防止するための対応）を行う。

講ずることが望ましい対策事項

①-3 封じ込めの実施を判断する際の検討要素として、停止する時間帯や期間、停止するサービスの範囲に応じた業務影響、業務の代替手段や通信経路、封じ込めと証拠保全のいずれを優先すべきか等を整理する。

統一基準における規定

② インシデントの根絶（マルウェアの駆除、パッチの適用等による脆弱性の修正等、サイバー攻撃による被害が発生した原因を除去するための対応）を行う。

講ずべき対策事項

②-1 インシデントの根絶（マルウェアの駆除、パッチの適用等による脆弱性の修正等、サイバー攻撃による被害が発生した原因を除去するための対応）を行う。

講ずることが望ましい対策事項

②-2 インシデントの根絶を行う際、インシデント分析結果等を踏まえ、セキュリティを高めるための対策（ネットワークの監視レベルの引上げ、ファイアウォールやセキュリティ装置の設置及びアクセス制御の適切な実施等）を検討する。

6.2.5 復旧

統一基準における規定

① インシデントからの復旧（被害を受けた機器の初期化、システム再構築等）を行う。

講ずべき対策事項

①-1 インシデントからの復旧（被害を受けた機器の初期化、システム再構築等）を行う。

①-2 復旧を完了し業務再開を判断する際の判断権限者を明確にする。

（解説）

- 復旧においては、早期復旧が求められる一方で、被害を受けた原因を特定しないまま復旧を行うことにより、再度同様の攻撃を受け、被害が発生することが想定されるなど、業務継続に影響を及ぼす判断を下すこともあり得るため、あらかじめ判断権限者を明確にしておく必要がある。

①-3 バックアップからの復旧の際には、対象のバックアップデータ及びその他の資産の完全性（例えば、攻撃の手法に応じて、既にバックアップデータ等が改ざんされている可能性や、マルウェア等に感染している可能性等）に留意する。

講ずることが望ましい対策事項

①-4 復旧を完了し業務再開を判断する際の判断要素を整理する。業務再開の判断要素には、原因への対応がなされたことの確認を含める。

（解説）

- 重大なサイバーインシデントを受けた後に隔離された組織に再びアクセスし、再度接続を図る際の技術的なプロセスについては、G7 サイバー・エキスパート・グループ「再接続枠組みのベストプラクティス[134]」及び技術的付属文書[135]を参照。

[134] https://www.fsa.go.jp/inter/etc/20250623/20250623.html

[135] https://www.fsa.go.jp/inter/etc/20260804/reconnection.html

①-5 被害を受けたシステムと他システムを再接続する前に、システムの正常な稼働や接続がなされていることを確認する。

①-6 重要な業務が適切な手順で復旧され、通常どおりの業務が稼働していることをシステム責任者と共に確認するなど、復旧が適切に行われたことを確認する。

6.3 危機管理

統一基準における規定

① 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。

講ずべき対策事項

①-1 サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施する。

（解説）

- サイバー攻撃等の予兆としては、例えば、IoC（侵害の痕跡）、アノマリ（異常値）のほか、対処可能性を確認すべき脅威情報が想定される。
- サイバー攻撃等の予兆を認識した場合に実施できる対策の見直しとして、予兆として検出された IoC（例：不審なファイルのハッシュ値、通常とは異なる IP アドレス）に基づく IDS/IPS のシグネチャ更新、特定の IP アドレスからの通信の遮断等が考えられる。

講ずることが望ましい対策事項

なし

統一基準における規定

② 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から復旧までの対応を実施する。

講ずべき対策事項

②-1 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から復旧までの対応を実施する。

講ずることが望ましい対策事項

なし

統一基準における規定

③　サイバーセキュリティを担当する部署は、初動から復旧までの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。

講ずべき対策事項

③-1 サイバーセキュリティを担当する部署は、初動から復旧までの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。

（解説）

- サイバーセキュリティを担当する部署、あるいはサイバーセキュリティに関する責任者は、サイバー攻撃等の事象が発生した際、経営層の意思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必要がある。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、初動から復旧まで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。
- 1.2「記載の観点及び構成」に記載のとおり、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、自組織のリスクを幅広く踏まえて、リスクマネジメント等による事前対応と、障害等が発生した際の被害の拡大防止・早期復旧といった危機管理の両面から、重要インフラのサイバーセキュリティ確保に取り組むことが重要である。それも踏まえ、経営層は、初動から復旧までの対応に関して適切な意思決定を行うための前提となる、サイバーセキュリティに関する知識等を得ておく必要がある。

講ずることが望ましい対策事項

なし

7　技術・脅威の動向等を踏まえた対策

統一基準における規定

①　リスクベースの観点から、AI 等の悪用による攻撃の高速化・大規模化などの技術・脅威の動向等を踏まえ、対策を講ずる。

（解説）

- 前章までにおいて記載した対策事項のほか、リスクベースの観点から、技術・脅威の動向等を踏まえ、対策を講ずることが求められる。
- 例えば、生成 AI を始め AI 技術の進展による恩恵の一方で、AI を活用した攻撃の自動化や AI に対する攻撃等、新たなサイバーセキュリティ上のリスクが生じている。量子計算機技術の進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・ 危殆化が懸念されるなど、多岐にわたる課題への対応が必要な状況となっている。
- また、今日のサイバー攻撃では、例えば、ランサムウェアの開発・運営を行う者が、身代金の一部を見返りとして攻撃の実行者にランサムウェア等を提供する形態（RaaS：Ransomware as a Service）が確認される等、攻撃者の裾野の広がりも見られる。
- こうした重要インフラのサイバーセキュリティに大きな影響を及ぼし得る技術・脅威の動向等を踏まえ、特に対応が必要と考えられる対策事項を「技術・脅威の動向等を踏まえた対策」として記載する。
- なお、サイバーセキュリティに大きな影響を及ぼし得る新たな技術・脅威は、予測できない形で発生する可能性があることから、安全基準等策定ガイドラインに示したもの以外についても、動向等を注視の上、必要な対応を柔軟に実施することが望ましい。

技術・脅威の動向等を踏まえた対策

①-1　ランサムウェア対策を講ずる。

講ずべき対策事項

①-1-1　ランサムウェア攻撃のリスクを考慮し、脆弱性の管理、アカウント管理・認証・アクセス制御、バックアップ、ログ取得、ネットワークの分割、継続的監視についての対策を実施する。

（解説）

- ランサムウェア攻撃のリスクとしては、例えば、次が考えられる。
  -VPN 機器やリモートデスクトップ用の機器を悪用した外部からの侵入が主要な侵入経路となっているところ、VPN 機器等の脆弱性・認証情報を悪用されるリスク
  -同一ネットワーク内のバックアップデータを探索されて削除されるリスク
- 具体的な対策内容について、脆弱性の管理については 3.6、アカウント管理・認証・アクセス制御については 4.1.1・4.1.2、バックアップについては 4.3.3、ログ取得については 4.5、ネットワークの分割については 4.6.1.①、継続的監視については 5.2 をそれぞれ参照。
  なお、これらの対策事項を含め、本項記載の各対策事項は、あくまでもランサムウェア対応に係る基本的な対策事項である点に留意。対処能力向上に向けた更なる管理体制の高度化のためには、本項及び前章までの「講ずることが望ましい対策事項」や、各事業者等のリスクアセスメント結果等も踏まえ、施策を具体化することが期待される。
- 関係機関におけるランサムウェアに対する取組については、国家サイバー統括室「ストップ！ ランサムウェア ランサムウェア特設ページ STOP! RANSOMWARE について[136]」を参照。

[136] https://www.cyber.go.jp/tokusetsu/stopransomware/index.html

・ ランサムウェア攻撃対策のための設定については、一般社団法人ソフトウェア協会、大阪急性期・総合医療センター、日本マイクロソフト株式会社「Cyber A2/AD ランサムウェア防御チェックシート[137]」を参照。

①-1-2 ベンダー等の関係者と協力関係を構築する。

（解説）

・ 協力関係の構築においては、例えば、脆弱性情報の共有体制の整備、インシデント発生時の対応手順の確認等を実施することが想定される（関連する対応について、2.9「サプライチェーン・リスクマネジメント」②-2・③-3 も参照。）。

①-1-3 ランサムウェア攻撃を助長しないようにするためにも、金銭の支払は厳に慎む。

講ずることが望ましい対策事項

①-1-4 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。

（解説）

・ インシデント報告様式について、「サイバー攻撃による被害発生時のインシデント報告様式の統一について[138]」を参照。

①-1-5 国内拠点で利用される情報システムとネットワーク接続するものを中心に、海外拠点を含めて資産管理をする。

①-1-6 必要に応じて、サプライチェーンを含めて資産管理をする。

[137] 当該チェックシートは、ランサムウェア攻撃を失敗させるための設定を取りまとめたもので、医療機関のみならず、一般の中小・中堅・大企業にも十分適用が可能なものとされている。
https://www.softwareisac.jp/a2ad/cybera2ad/

[138] https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

技術・脅威の動向等を踏まえた対策

①-2　AI システム・サービス利用時の対策を講ずる。

講ずべき対策事項

①-2-1　例えば不正操作によって AI の振る舞いに意図せぬ変更又は停止が生じることのないよう、AI の機密性・完全性・可用性を維持し、その時点での技術水準に照らして合理的な対策を実施する。

（解説）

- AI の機密性・完全性・可用性の維持に際しては、AI の推論対象データに微細な情報を混入させることで、関係者の意図しない判断が行われる可能性等、AI の脆弱性を完全に排除することはできないことを考慮する必要がある。
  また、重要インフラサービスの安全かつ継続的な提供の観点から、関連する情報や情報システムの重要度に応じて、人間の判断を介在させる程度についても検討する。
- AI を自組織内のデータと連携させるなど、AI を情報システムに接続して利用する場合は、AI の正常な稼働に必要な情報システム間の接続を適切に行う。
- 外部サービス利用の観点から、2.9「サプライチェーン・リスクマネジメント」、4.3「データのセキュリティ対策」、4.6.1「通信のセキュリティ」、4.7「クラウドサービス利用時の対策」も参照することが考えられる。
- AI 開発・提供・利用にあたって必要な取組についての基本的な考え方等については、総務省・経済産業省「AI 事業者ガイドライン（第 1.2 版）[139]」を参照。
- AI に不正な出力を行わせたり、AI を搭載するシステムの停止を生じさせたりするといった AI への脅威に対する、AI 開発者及び AI 提供者における技術的対策については、総務省「AI のセキュリティ確保のための技術的対策に係るガイドライン[140]」を参照。

[139] https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

[140] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00282.html

・ 制御システムにおけるセキュアなAI活用については、CISA「Principles for the Secure Integration of Artificial Intelligence in Operational Technology[141]」を参照。

講ずることが望ましい対策事項

なし

[141] https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology

技術・脅威の動向等を踏まえた対策

①-3　高性能 AI の悪用リスクに備えた対策を講ずる。

講ずべき対策事項

①-3-1　高性能 AI を悪用した攻撃の高速化・大規模化などのリスクを考慮し、資産管理、リスクアセスメント、脆弱性の管理、アカウント管理・認証・アクセス制御、バックアップの確保、監視・分析、事業継続計画の策定、インシデントへの対応及び復旧、組織の壁を越えたサプライチェーン・リスクへの対応等を行う。

（解説）

- 高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、そうした悪用リスクを前提として、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要である。
- 高性能 AI によるサイバーセキュリティに対する影響・対策等については、短期的及び中長期的に、例えば以下が想定される。

  【短期的な影響・対策】

  - 短期間で多くの脆弱性の発見や修正プログラム（パッチ）の提供が想定されるところ、パッチ適用等の緊急性や重要性と、パッチ適用等によりシステムが停止するリスクとのバランスについて改めて確認した上、適切な優先順位付けと速やかなパッチ適用等を行うとともに、必要に応じてパッチ適用等に関する作業方針を見直し、実行可能な運用体制を構築・維持する（3.6③参照）。
  - その上で、制御システム等へのパッチ適用等が困難な場合は、ネットワーク分離、また、例えば仮想パッチの適用や他ネットワーク接続点の監視等といったリスク低減策の実施等、厳格な管理が求められる。
  - 経営層は、各種対策を徹底してもサイバー攻撃の完全な防御は困難であることを前提に、サイバー攻撃により情報システムが停止する場合や、サービス／情報システムを能動的に停止せざるを得ない場合を想定しつつ[142]、事業継続計画等を策定し、サイバーインシデントへの対応及び復旧のための方針を明確にしてお

[142] 金融庁・日本銀行「『フロンティア AI による脅威変化を踏まえた金融機関等の短期的な対応』に係る要請について」参照
https://www.fsa.go.jp/news/r7/sonota/20260522-5/20260522.html

く必要がある。

【中長期的な影響・対策】

- 高性能 AI 活用の社会への浸透が想定される。高性能 AI を活用したサイバーセキュリティ対策の強化（例：脅威検知・インシデント対応・脆弱性発見等）を含め、基本的な対策の更なる徹底が推奨される。
- パッチ適用等が困難なシステムについては、例えば、中長期的なリプレイス（迅速な脆弱性対応が可能なクラウド環境への移行等も含む。）を視野に入れた対策を検討することも考えられる。

・ 具体的な対策内容について、資産管理については 3.1、リスクアセスメントについては 3.4、脆弱性の管理については 3.6、アカウント管理・認証・アクセス制御については 4.1.1・4.1.2、バックアップの確保については 4.3.3、監視・分析については 5、事業継続計画の策定を含むインシデントへの対応及び復旧について 6、組織の壁を越えたサプライチェーン・リスクへの対応については 2.9 をそれぞれ参照。

講ずることが望ましい対策事項

なし

技術・脅威の動向等を踏まえた対策

①-4　PQC[143]への移行に関する対策を講ずる。

講ずべき対策事項

①-4-1　PQC への移行について、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野における検討方針や具体的な進め方等の動向を把握・整理する。

（解説）

- 量子計算機技術については、その進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・危殆化が懸念されている。このような中で、米国や EU 等の諸外国においては PQC への移行についての方針をそれぞれ公表しており、その多くが 2035 年までを期限として進めている。
- そうした中、我が国では、政府機関等における PQC への移行について、原則として 2035 年までに行うことを目指すとしている。PQC への移行は、政府機関等に限らず、重要インフラ事業者等においても考慮しなければならない課題であるところ、重要インフラ事業者等についても原則として 2035 年を目標としつつ、より早期に移行を行うことも含め、情報システムごとに適切に検討を行うことが考えられる。
- 他方で、PQC への移行の具体的な進め方（ステップ）については、現在、政府機関等や各業界分野において検討が進められているところ、それら動向を確認しながら対応していくことが考えられる。

  現時点での政府機関等や業界における検討状況については、以下を参照。

  - 政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）[144]」
  - CRYPTREC 「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト）[145]」
  - CRYPTREC「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版

[143] 量子計算機及び従来型の電子計算機の双方に対して安全性が確保される暗号

[144] https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf

[145] https://www.cryptrec.go.jp/list.html

[146]」

- 金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書[147]」

講ずることが望ましい対策事項

①-4-2　PQC への移行に向けた準備対応として、自らの資産を網羅的に把握、それぞれの資産の重要性を評価し、どのような暗号が用いられているかをリスト化したクリプト・インベントリを作成するとともに、優先順位に応じた移行の進め方を検討する。

（解説）

・ 重要インフラ事業者等における PQC 移行の基本的な考え方については、金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書」を参照。そのポイントの一部を以下に記載する。

- 金融機関はまず、自らの情報資産を網羅的に把握した上で、それぞれの情報資産の重要性を評価し、どのような暗号が用いられているかをリスト化したインベントリ（台帳・目録）を作成すること
- その際、自らが運用するシステムだけではなく、サードパーティに運用を委託している重要システムの情報資産と暗号に関するインベントリも作成すること
- インベントリの作成作業にはかなりの労力を要するので、早い段階から IT ベンダーの協力を得ること

[146] https://www.cryptrec.go.jp/tech_guidelines.html
[147] https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

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

次頁以降に示す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は、重要インフラ事業者等が主にコンティンジェンシープラン（以下、「CP」という。）及び事業継続計画（以下、「BCP」という。）を策定・改定する際に考慮されることを期待するものである。

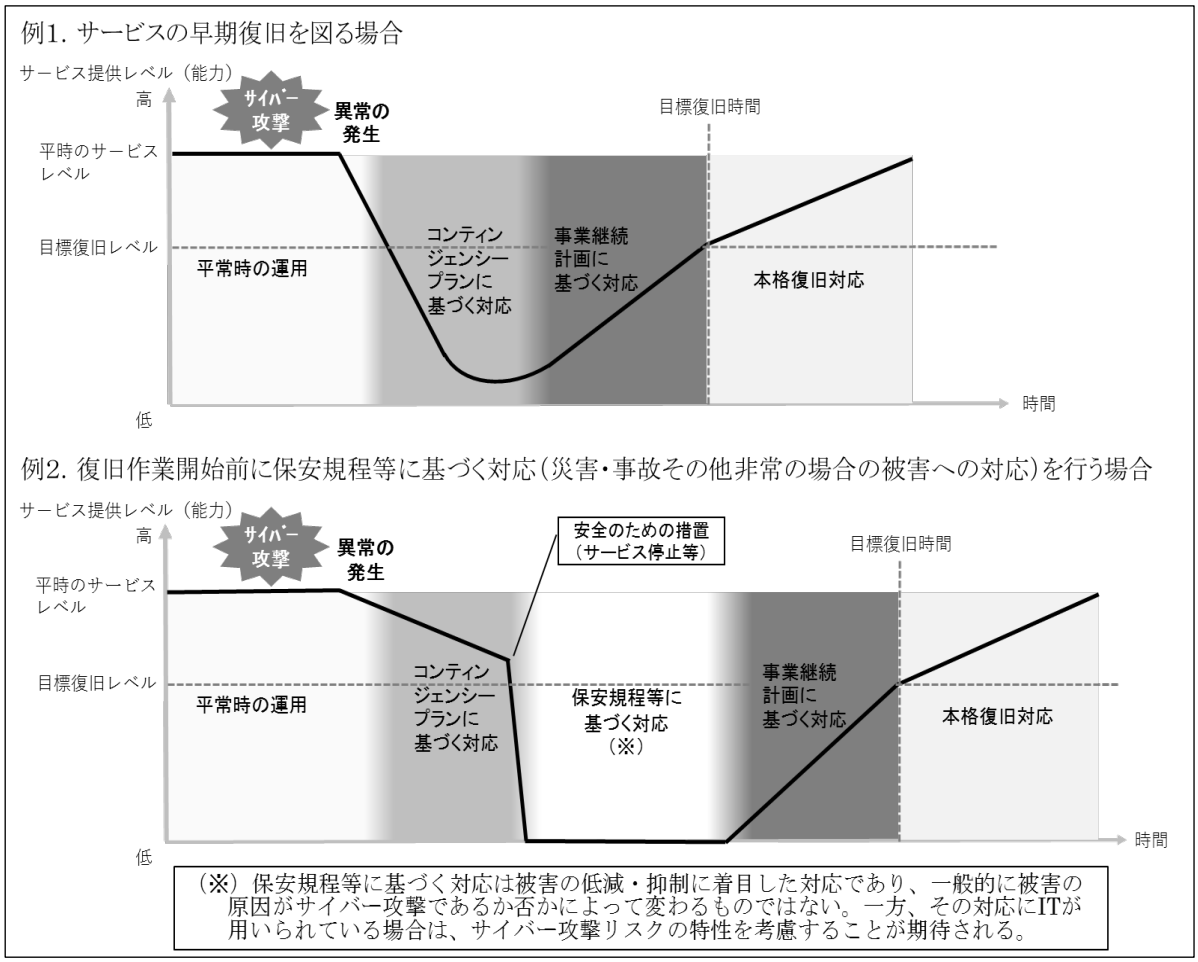
CP 及び BCP の名称や記載の範囲、発動のタイミング等は分野や事業者等によって異なる場合があるため、次頁以降の特性等を考慮して策定・改定すべき対象ドキュメント（以下、適用対象）は各事業者等の状況に応じて検討される必要がある。

適用対象の検討の参考として、図１にサイバー攻撃の発生から復旧までのフローの例を示す。図１に示す例（例１及び例２）はいずれもサイバー攻撃により異常が発生し、サービスレベルが時間とともに低下した後、CP や BCP に基づく対応を経てサービスレベルを復旧させる一連のプロセスを表したものである。

例１では、サービスの早期復旧を図るため早いタイミングで BCP に基づく対応を開始している。一方例２では、安全のための措置として意図的にサービスを停止し、保安管理規定等に伴う対応を実施した後に BCP に基づく対応を開始している。いずれの例においても CP 及び BCP は、次頁以降の特性等を考慮すべき適用対象となる。例２の保安規程等に基づく対応は被害の低減・抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応に IT が用いられている場合は、次頁以降の特性等を考慮することが期待される。

図１　サイバー攻撃の発生から復旧までのフローの例

（下記以外にも様々なフローが存在する。）



なお、以降に記載するサイバー攻撃リスクの特性は各々相互に関連しており、ある特性に対する考慮事項は他の特性に対しても有効なものもある。よって、CP 及び BCP の策定・改定においては、特定の特性に対する考慮事項だけではなく、他の特性に対する考慮事項も踏まえて、対応及び対策を検討することが必要である。

サイバー攻撃リスクの特性①

攻撃者の存在と多様な攻撃目的

サイバー攻撃は、自然災害等とは異なり、目的を持った攻撃者によって引き起こされる。その攻撃目的は、金銭・情報の窃取、主義・主張の表明、システム破壊によるサービスの停止等多様化している。組織的に計画されて行われる攻撃から内部犯行による攻撃まで、多様な攻撃者・攻撃目的に応じた様々な手法による攻撃が考えられるが、事前に攻撃者や攻撃目的を知ることは困難なケースが多い。

対応及び対策の考慮事項

【ポイント】
サイバー攻撃リスクの認識と被害発生に至るシナリオの作成

【CP 及び BCP の策定・改定における考慮事項】

- 自組織の重要インフラサービスの障害に繋がる可能性のあるサイバー攻撃の脅威（マルウェア等を用いた標的型攻撃、DDoS 攻撃等）とその影響を特定し、特に事業への影響が大きい脅威について、被害発生に至るシナリオの作成とそのシナリオへの対応を検討する。
  - ▶ 被害発生に至るシナリオの例
    マルウェアに感染した機器（端末、USB メモリ等）を保守要員が持ち込むことにより、マルウェアが組織内の情報システムに感染し、さらにネットワークを介して最終的な攻撃目標である重要システムに侵入し、システムの改ざんや破壊、機密情報の漏えい等を引き起こす。結果として、サービスや事業の継続に深刻な影響を受ける。
- 攻撃予告、情報漏えいの疑い、攻撃の予兆（不審な通信やログの増加等）が検知された場合等のサイバー攻撃の発生のおそれがある状況においても、攻撃や障害の発生に備えた警戒態勢への移行や対策状況の緊急点検等の対応が必要になる可能性があることを考慮する。
  - ▶ サイバー攻撃の発生のおそれがある状況の例
    インターネットを通じて重要インフラサービスを提供しているシステムに対する DDoS 攻撃を示唆して金銭や特定の事業活動の停止等を要求される。

サイバー攻撃リスクの特性②

攻撃手口の高度化

サイバー攻撃の手口は絶えず考え出され高度化している。新たな脆弱性を狙った攻撃のように現行技術をベースとした対策だけでは回避困難な攻撃や、事業者側が想定していない新しい手口で行われる攻撃等が考えられる。

また、新しい手口で攻撃が行われた場合、その影響の度合や範囲を正確に把握できない可能性がある。

対応及び対策の考慮事項

【ポイント】
攻撃手口に関する日々の情報収集並びに CP 及び BCP の適時見直し

【CP 及び BCP の策定・改定における考慮事項】

- 攻撃手口等に関して、国家サイバー統括室、IPA 等の関係主体が提供する情報を日々収集し、新たな攻撃手口に対しては現状の CP 及び BCP で対応可能か確認し、必要に応じて見直しを図る。
- 新たな攻撃手口の情報を入手した場合は、自組織の対策の状況とその有効性及び被害の有無を早急に確認するとともに、自組織への攻撃到達に備え、一定期間、監視機能・体制を強化する。
- サイバー攻撃手口の高度化に追随するため、サイバーセキュリティに関する十分な知識と判断能力を持った人材を、CP 及び BCP の策定・改定や対応時の体制に加える。必要に応じて外部の専門組織を活用する。
- 影響範囲等が正確に把握できていない状況でも、重要インフラサービスの提供において最低限要求されるサービスレベルを維持するため、必要な調査項目や調査の優先順位を CP 及び BCP 策定時に検討しておく。

（CP 及び BCP の発動に備えた通常時の対策）

- 新たな攻撃手口をサイバー攻撃リスクとして認識した場合、計画発動時の対応に関与する可能性のある要員に対して、当該リスクの管理方針や、見直しを行った CP 及び BCP の浸透を図る。

サイバー攻撃リスクの特性③

急速な被害拡大に繋がる攻撃が行われる可能性

サイバー攻撃の被害は、攻撃を受けた箇所を起点にネットワークを介して急速に拡大する可能性がある。特定の端末に感染したマルウェアが同一組織内のネットワーク上にある別の端末に自身を複製することで被害が広がるケースや、外部委託先で発生したサイバー攻撃の被害が自社システムにまで広がるケース、自社システムが不正に操作され他社への攻撃に利用されることで自らが加害者の立場になってしまうケース等も考えられる。

対応及び対策の考慮事項

【ポイント】
サービス中断に繋がる手段も視野に入れた被害拡大への対応

【CP 及び BCP の策定・改定における考慮事項】

- サイバー攻撃の被害の拡大を防止するため、通信の遮断や重要システムの停止等を行うことも視野に入れる。ネットワークやシステムの構成を把握し、遮断・停止を行うポイントについて検討しておく。
- 遮断・停止を行う場合、重要インフラサービスの継続に大きな影響を与える可能性があるため、実施の判断を行う責任者を明確にしておく。また、的確な判断を行うため、停止可能なタイミングや期間、停止した場合の影響範囲、代替手段の有無等を計画策定時に整理しておく。
- 調査に必要な情報には遮断・停止後に取得できなくなるものもあるため、遮断・停止前に時間の許す限り情報を収集する。収集すべき情報の例として、遮断・停止により失われるメモリ情報、プロセス情報や、遮断・停止中は取得できないログ等があり、環境に合わせて取得方法や手順を検討しておく。
- サイバー攻撃の被害が相互に及ぶ可能性のある外部委託先との対応状況の共有や、重要インフラサービスの利用者等への対応状況の公表を検討しておく。サイバー攻撃の場合に公表を検討すべき特徴的な情報として、対応や調査で判明した攻撃手口、被害原因（ソフトウェアの脆弱性、設定の不備等）、攻撃への対処状況（被害拡大防止のための暫定対処、被害原因に対する根本対処）、顧客等への二次被害の発生状況や今後発生する可能性の有無等がある。

（CP 及び BCP の発動に備えた通常時の対策）

攻撃の拡散に備えた対策の導入を必要に応じて検討する。対策の例として、セグメンテーション（重要システムの隔離）、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）等がある。

サイバー攻撃リスクの特性④

執拗な攻撃が行われる可能性

サイバー攻撃は、その目的が達成されるまで執拗に行われる可能性がある。システム復旧の際、被害に遭う以前の状態に漫然と戻した場合にまた同じ攻撃が行われ被害を受けるケースや、システム復旧対応中に再度攻撃が行われるケース、攻撃への対処後にそれを回避する方法で再度攻撃が行われるケースも考えられる。

また、インターネットに接続していないクローズド環境や、汎用性の低いシステムで構成される環境であっても、システム構成やシステム仕様等に関する情報を様々な手段で時間をかけて収集した上で攻撃が行われるケースも考えられる。

対応及び対策の考慮事項

【ポイント】

サイバー攻撃の再発の可能性及び環境の特殊性の考慮

【CP 及び BCP の策定・改定における考慮事項】

- 重要インフラサービス復旧前に被害原因（ソフトウェアの脆弱性、設定の不備等）の分析、特定、対処（パッチ適用、マルウェア駆除、システム再構築等）を行う。非常用システムを使用してサービスを復旧する場合も、同様の手口による攻撃への対処を非常用システムに行った上で稼動させる。
- 復旧中に再度サイバー攻撃を受けた場合に備え、サイバー攻撃への対処を行うチームと重要インフラサービスの復旧を行うチームの体制を分けるとともに、役割分担や連携方法を検討しておく。
- ログ等の調査の結果、サイバー攻撃が執拗に行われていた痕跡（長期間に渡る繰り返しの攻撃の試行、対策後の攻撃の再発等）が見られた場合、重要インフラサービスの復旧後においても、一定期間、監視機能・体制を強化する。
- 被害の発生原因が十分に特定できていない状況で、システム復旧せざるを得ない場合には、攻撃者が仕掛けたプログラム等が残存する可能性を想定し、被害を受けたシステムに加え、周辺のシステムに対する監視機能・体制を強化する。
- 汎用性の低いシステムが存在する環境での対応においては、当該環境のシステムに対して取り得る対応の制約（システム動作への影響の懸念によりパッチの適用不可等）、対応に使用できる機器やネットワークの制約（特殊な通信仕様により調査機器の接続や通信の解析が困難等）、対応に関与できる人員の制約（特殊なシステム仕様を理解した人員が必要等）を考慮する。

（CP 及び BCP の発動に備えた通常時の対策）

- クローズドな環境や汎用性の低いシステムにおいてもサイバー攻撃による被害が発生し得ることを認識した上で、監視等の必要な対策を検討する。

サイバー攻撃リスクの特性⑤

同時多発的な攻撃が行われる可能性

サイバー攻撃では物理的な距離に関係なく、広範囲にわたるターゲットを同時に攻撃することが可能である。自組織の複数の拠点に同時に攻撃が行われるケースや、自組織のシステムと供給者のシステムに同時に攻撃が行われるケース、メインシステムと非常用システムに同時に攻撃が行われるケース等が考えられる。

対応及び対策の考慮事項

【ポイント】
関係主体等との連携を前提とした同時多発攻撃への対応

【CP 及び BCP の策定・改定における考慮事項】

- 複数のインシデントが同時に発生した場合には、業務影響、リスク許容度、対応に必要な資源等を踏まえて、対応の要否・優先順位を判断する必要があるため、計画策定時に判断基準を明確にする。
- 重要インフラサービスの提供に係る供給者や外部委託先がサイバー攻撃を受けた場合に備え、供給者や外部委託先の CP 及び BCP の整備状況や対応時の自組織との連携内容等について確認する。
- 複数の重要インフラ事業者等に同様のサイバー攻撃が行われる可能性を考慮し、各分野の業界団体、セプター、サイバーセキュリティ関係機関等を通じて、自組織が受けたサイバー攻撃の手口、攻撃元、特徴的な痕跡等、他組織での被害防止に資する情報を積極的に共有し、更なる被害の発生の防止に分野全体で努める。

（CP 及び BCP の発動に備えた通常時の対策）

- メインシステムと非常用システムが同時に使用不能になる可能性を低減する対策を検討する。対策の例として、業務上必要な通信（メインシステムと非常用システムの間のデータコピーやバックアップ等）以外の遮断や、メインシステムと非常用システムのネットワークの分離等がある。
- システムによる重要インフラサービスの維持が困難になるケースを想定し、手動での機能制御、要員による代替業務、代替サービスの提供等の代替手段を用意する。
- 組織内外の関係者への情報共有手段について、サイバー攻撃の影響によりメール等の通常時の情報共有手段が使用できなくなることを考慮し、複数の情報共有手段をあらかじめ用意する。

サイバー攻撃リスクの特性⑥

検知が困難な攻撃が行われる可能性

サイバー攻撃に対して十分な検知策を講じていない場合、攻撃を認識できず長期間にわたり攻撃を受け続ける可能性がある。不正行為の検知に繋がるログを削除して回避しようとするケースや、実態とは異なる数値を表示して正常に動作しているように見せかけ不正行為を行うケース等も存在し、検知が遅れるほど被害が拡大する可能性が高くなる。また、攻撃を検知した以後も、攻撃者及び攻撃目的を特定するのは困難なケースが多い。

対応及び対策の考慮事項

【ポイント】
影響調査に係る情報等の開示手続きの明確化

【CP 及び BCP の策定・改定における考慮事項】

- システムベンダー等の保守業者による影響範囲の特定が困難な攻撃に対しては、外部のセキュリティベンダー、インシデント対応組織等に調査協力を依頼する場合も想定されるが、その際、ログや侵害された機器等の開示が必要になる場合もあるため、必要な手続き（開示の責任者や判断基準、開示可能な組織、機密を含む情報を安全に伝達するための提供手段等）、開示する情報（ログ項目や形式等）とその制限（機密情報や個人情報等の開示不可な情報の種類等）を明確にしておく。

（CP 及び BCP の発動に備えた通常時の対策）

- 攻撃による異常の痕跡を調査するため、重要システムの構成を把握するとともに、当該システムの通常時の動作や出力ログの内容について把握しておく。また、ログを改ざん、削除等から保護するための対策を行う。
- 長期間に渡り発覚しなかった攻撃を過去に遡って調査するため、通常時に取得している各種ログを一定期間保存する。保存期間はサイバーセキュリティ関係機関やセキュリティベンダーが推奨しているログの保存期間等を考慮し検討する。また、サイバーセキュリティ関係機関等が公開している情報を参照し、調査のために通常時から取得が推奨されるログの取得状況を確認するとともに、必要に応じて取得を検討する。

サイバー攻撃リスクの特性⑦

誤った判断や対処を誘発する攻撃が行われる可能性

サイバー攻撃によって、誤った判断や対処が誘発される可能性がある。例として、監視や制御等に使用する管理システムに実態と異なるアラートや数値を表示して判断を誤らせるケースや、障害対応時のシステム操作が意図しない動作を引き起こすようにシステムを不正変更（数値を上げる操作で数値が下がる、システム停止の操作でシステムが停止しない等）するケース等が考えられる。

対応及び対策の考慮事項

【ポイント】
異なる種類の監視情報の併用による正確な事態把握

【CP 及び BCP の策定・改定における考慮事項】

- サイバー攻撃の影響範囲が特定できていない段階では、管理システムに対しても攻撃の影響が及んでいる可能性を考慮し、改ざんの痕跡や監視情報間の不整合等がないか確認を行う。
- 管理システムが改ざんされている疑いがある場合は、重要インフラサービスの提供状況の目視確認や手動での物理的な制御操作等、他の信頼できる手段を用いて監視や制御等を行うなど、複数の対応手順を検討しておく。

（CP 及び BCP の発動に備えた通常時の対策）

- システムに対する不正な変更の有無を確認するための体制・仕組みを検討する。確認すべき箇所の例として、ハードウェア構成（接続機器等）、ソフトウェア構成、ファイル構成、システム設定等がある。
- 重要インフラサービスの監視機能へのサイバー攻撃による、実態と異なる監視情報の表示等に備え、監視手段を複数用意する。