重要インフラのサイバーセキュリティ対策のための統一基準

（案）

令和８年●月●日

サイバーセキュリティ戦略本部

目次

第1部 総則

1.1 統一基準の目的等

（1）統一基準の目的

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。）は、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の施行に伴う関係法律の整備等に関する法律（令和7年法律第43号）において改正されたサイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）第25条第1項第3号[2]に基づき、重要インフラ事業者等[3]におけるサイバーセキュリティの確保に関し国の行政機関（以下「政府機関」という。）が実施する施策について統一的な基準を定めることにより、重要インフラ事業者等が分野・事業者横断的に講ずべきサイバーセキュリティ対策の実施の促進等を図り、重要インフラのサイバーセキュリティ強化のため政府機関としてより積極的な役割を果たし、もって深刻化の進むサイバー脅威に対する重要インフラの一層の防護を図ることを目的とする。

（2）統一基準による重要インフラのサイバーセキュリティ強化

国民生活及び経済活動の基盤である重要インフラにおいては、そのサービスの安全かつ持続的な提供のため、官民が連携して重点的に防護していく必要があることから、官民の共通の重要インフラのサイバーセキュリティに係る行動計画（以下「行動計画」という。）を策定し、これまでも取組を行ってきているところである。

他方で、各重要インフラ分野における政府機関の施策や重要インフラ事業者等の取組の評価と改善につながるような具体的かつ統一的な基準はなく、サイバーセキュリティ確保の取組やその水準は、分野・事業者によってばらつきが見られる。

国家を背景とした攻撃キャンペーンの発生等、深刻化するサイバー脅威に対し、重要インフラ事業者等におけるサイバーセキュリティの一層の確保を図るためには、上記のような従来行ってきた事業者の自主的な取組の

---

[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] 基本法第25条第1項第3号　重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュリティの確保の状況の調査を含む。）及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること。

[3] 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。

促進をより効果的に図るなど、政府機関としてより積極的な関与をしていく必要がある。

そのため、統一基準を作成し、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に係る政府機関の施策について、国家サイバー統括室及び重要インフラ所管省庁が連携協力して取組を進め、各分野の特性・実情や、各分野の業法その他の法制度の施行状況等も勘案しつつ、効果的な施策の実施が図られるよう努めることにより、分野・事業者横断的なセキュリティ対策の水準の底上げとともに、各分野におけるリスクベース[4]の取組の更なる水準の向上を図る。

（3）統一基準と行動計画との関係

行動計画は、関係主体として政府機関、重要インフラ事業者等、セプター[5]事務局、サイバーセキュリティ関係機関[6]、サイバー空間関連事業者[7]等を対象に、それぞれの責務や取組、目指すべき将来像を具体的に提示し、明確にすることによって、各関係主体における自主的かつ積極的な取組の促進を図るものである。

他方、統一基準は、政府機関を対象としており、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促進するための政府機関の施策について、PDCA サイクルを実施し、重要インフラにおけるサイバーセキュリティ強化の実効性を確保するためのスキームである。

PDCA サイクルの実施により重要インフラのサイバーセキュリティ強化の実効性を確保する統一基準と、関係主体の責務・取組や目指すべき将来像を提示し、自主的かつ積極的な取組を促進する行動計画は、両者が相まって重要インフラのサイバーセキュリティの一層の確保・向上を図る相補的な関係と位置づけられる[8]。

---

[4] 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。

[5] 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）。

[6] 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）。

[7] 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。

[8] 例えば、重要インフラ所管省庁が、第２部で定める「取り組むべき施策」を実施するに当たり、他の関係主体との連携取組や全体として目指すべき将来像等、その背景となる考え方については、行動計画を参照することを想定する。

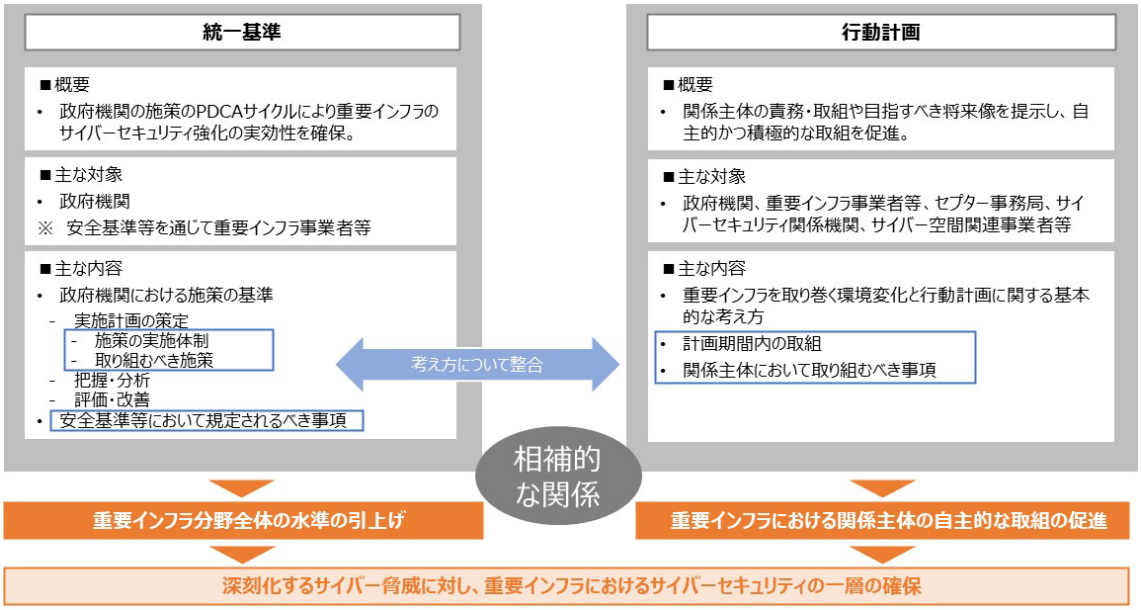

図１　統一基準と行動計画の関係

（４）統一基準と他法令との関係

政府機関は、統一基準に基づき、重要インフラのサイバーセキュリティ強化を図るに当たっては、他法令との整合性に留意する。

1.2　統一基準の適用範囲

重要インフラ防護の範囲 [9]として対象となる分野は、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」、「港湾」及び「郵便」の 16 分野とする。統一基準では、これら分野を適用対象分野とする。

[9] 重要インフラ事業者等と基幹インフラ事業者は、法律の趣旨の下に対象範囲（分野・事業者）が定められており、それらの間には差異があり得る。そうした中、基幹インフラ事業者は、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（令和７年法律第 42 号。以下「サイバー対処能力強化法」という。）に基づきインシデント報告等が求められるなど、サイバーセキュリティ確保の重要性が増大していることから、基幹インフラの対象範囲については、原則として、重要インフラ防護の範囲に含める。これにより、統一基準に基づき、基幹インフラ事業者を対象とした制度における届出やインシデント報告等に当たって前提となるサイバーセキュリティ対策を含め、分野・事業者横断的に講ずべき基本的な対策の徹底を図り、関係事業者においてより効果的な取組がなされるようにする。

1.3　統一基準に基づく施策の改善

統一基準では次のとおり、「実施計画の策定」や「把握・分析」、「評価・改善」といった PDCA サイクルのプロセスを通じて、政府機関における施策の実施及び改善を図り、重要インフラ事業者等におけるサイバーセキュリティ対策の取組の向上につなげることにより、重要インフラにおけるサイバーセキュリティ強化の実効性を確保する（詳細は第２部に記載）。

- 実施計画の策定：国家サイバー統括室及び重要インフラ所管省庁は、統一基準に定める政府機関の施策の基準に基づき、施策の実施計画を策定し、施策の実施を進める。
- 把握・分析：国家サイバー統括室及び重要インフラ所管省庁は、重要インフラ事業者等における取組の実施状況について調査し、その結果等を踏まえ、把握・分析を行う。
- 評価・改善：サイバーセキュリティ戦略本部（以下「戦略本部」という。）は、統一基準に基づく施策の評価を行い、国家サイバー統括室及び重要インフラ所管省庁は、当該評価結果を踏まえ実施計画を更新し、施策の改善を進める。

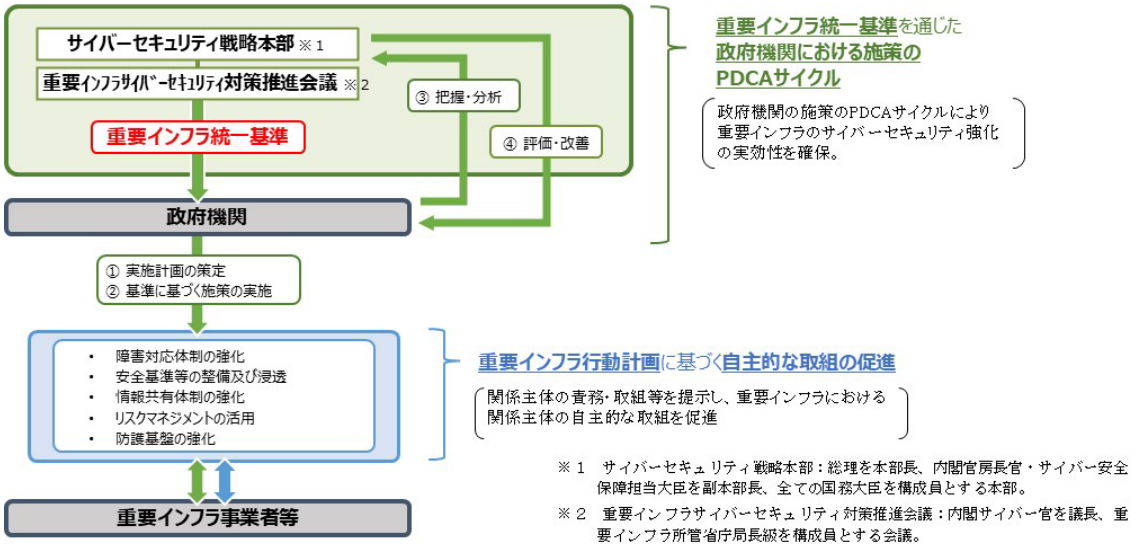

図２　統一基準における PDCA サイクル

1.4　統一基準の構成等

統一基準は、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に係る政府機関の施策についての統一的な基準を定めるものであるところ、第２部では、政府機関における施策の実施体制や取り組むべき施策等についての考え方を記載する。

また、第３部では、重要インフラ所管省庁や各分野の業界団体等（以下「所管省庁等」という。）が策定する安全基準等[10]において、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として規定されるべき事項を記載する。

なお、第３部に関しては、国家サイバー統括室が別途策定する「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。）において、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。

1.5　統一基準の改定

統一基準の内容や水準を適切に維持するため、技術や脅威等、重要インフラを取り巻く環境変化を踏まえ、定期的な点検及び改定が必要と考えられることから、原則として３年に１度、統一基準の見直しを行う。

---

[10] 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

第2部 政府機関における施策の基準

2.1 実施計画の策定

国家サイバー統括室及び重要インフラ所管省庁は、年に１回を目途に、各分野における特性・実情や、業法その他の法制度の施行状況等も勘案しつつ、重要インフラのサイバーセキュリティ強化のため効果的な施策の実施が図られるよう実施計画を策定（更新を含む。）し、戦略本部に報告する。

重要インフラ所管省庁は、各分野における実施計画を策定し、また、国家サイバー統括室は、分野横断的な実施計画を策定する。実施計画には、2.1.1 に定める施策の実施体制や、2.1.2 に定める取り組むべき施策についての具体的な計画内容を記載する。

また、実施計画の更新に当たっては、各分野における重要インフラ事業者等の取組の実施状況等についての把握・分析（2.2）や戦略本部による評価結果（2.3）等を踏まえ、現行の施策取組の見直しや新たに必要となる施策の追加等の改善を行う。

2.1.1 施策の実施体制

（１）政府機関における連携体制

統一基準により、政府を挙げた取組を推進し、重要インフラの一層の防護を図るため、重要インフラサイバーセキュリティ対策推進会議等を通じた関係省庁間の連携を強化する。これにより、国家サイバー統括室及び重要インフラ所管省庁が連携協力し、各分野及び分野横断的な取組を進め、政府が一丸となって重要インフラのサイバーセキュリティの確保・向上を図る。

また、関係省庁間の連携に加え、各省庁内においても、サイバーセキュリティ政策担当部局や各分野担当部局をはじめ、関係部局間における連携の強化により、効果的な施策の実施が図られるよう努めるとともに、他法令・政策との整合性にも留意する。

（２）官民の連携体制

サイバー脅威に対する重要インフラの防護に当たっては、政府機関と重要インフラ事業者等との信頼関係に基づく、緊密な連携が必要である。また、そうした関係の基に、官民が相互に積極的な関与を行い、分野の特性・実情等を踏まえたリスクベースの考え方に基づく、より効果的な取組を行っていく必要がある。このため、各分野において、政府機関や業界団体、重要インフラ事業者等の関係主体間における連携体制及びそれぞれの役割を明確

にする。

また、統一基準においてPDCAサイクルを推進し、重要インフラのサイバーセキュリティ水準の継続的な向上を図るためには、PDCAサイクルの対象となる各分野における重要インフラ事業者等を特定することが必要と考えられることから、重要インフラ所管省庁は、実施計画において対象となる重要インフラ事業者等を特定（更新を含む。）する。

2.1.2 取り組むべき施策

重要インフラ事業者等における分野・事業者横断的に講ずべき対策の推進を図るため、国家サイバー統括室及び重要インフラ所管省庁は次に定める施策を実施する。

（１）障害対応体制の強化

重要インフラ防護の適切な実施のためには、重要インフラ事業者等における、組織統治[11]の一部としての障害対応体制の整備による、経営層[12]をはじめとする組織全体としての取組等の推進や、組織の壁を越えたサプライチェーン全体でのセキュリティの向上等を推進する必要があるところ、次の施策を実施する。

（主な施策）

- 重要インフラ事業者等における組織統治の一部としての障害対応体制整備の促進
- 重要インフラ事業者等におけるサプライチェーン・リスク[13]を踏まえた対応等の促進
- 官民一体となった障害対応体制の強化
- 情報共有、演習、人材育成等を通じた事業者間や分野間での障害対応体制の強化
- その他各分野の特性や事情を踏まえた施策等

（２）安全基準等の整備及び浸透

安全基準等の整備及び浸透により、重要インフラ事業者等が、重要インフ

---

11 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。

12 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。

13 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。

ラを取り巻く環境の変化や脅威の多様化を踏まえ、自組織の抱えるリスクを把握し、自組織に最適な防護対策を実施できる状況を実現する必要があるところ、次の施策を実施する。

（主な施策）

・ 安全基準等の策定及び継続的改善（その際、安全基準等には第３部に定める対策事項を含めることとする。）
・ 各分野におけるリスクベース・アプローチによる必要な対策事項や重要インフラ事業者等の取組状況についての把握・分析と安全基準等への反映
・ 安全基準等の浸透に向けた取組（対策を実装するための環境整備、小・中規模／地域事業者等への支援等）の推進
・ 業界団体等が安全基準等の策定主体である場合は、上記取組について業界団体等との連携
・ その他各分野の特性や事情を踏まえた施策等

（３）情報共有体制の強化

サイバーセキュリティ動向が日々変化する中、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、自身のセキュリティ対策の推進とあわせて、官民・分野横断的な情報共有が必要であるところ、次の施策を実施する。

（主な施策）

・ 通常時及び大規模重要インフラサービス障害[14]対応時における情報共有体制の運用等
・ 重要インフラ事業者等との緊密な情報共有体制の維持・強化
・ サイバー攻撃による被害拡大の防止に向けた重要インフラ事業者等からの情報の集約、整理・分析及び共有等のための官民双方向でのコミュニケーションの強化
・ 情報共有体制の強化に資する関係主体（セプター、セプター事務局、セプターカウンシル[15]、ISAC 等）との連携や活動支援
・ その他各分野の特性や事情を踏まえた施策等

（４）リスクマネジメントの活用

重要インフラ防護の目的である重要インフラサービス[16]の継続的提供を

---

[14] 官邸対策室等が官邸危機管理センターに設置されるなどの政府として集中的な対応が必要となる規模の重要インフラサービス障害。

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

[16] 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

可能とするためには、その阻害要因となるリスクを明確にし、許容できる範囲に抑えるリスクマネジメントの活用が必要であるところ、次の施策を実施する。

（主な施策）

・ 重要インフラ事業者等におけるリスクマネジメントの取組の推進
・ その他各分野の特性や事情を踏まえた施策等

（５）防護基盤の強化

重要インフラを取り巻く社会環境・技術環境やサイバーセキュリティ動向の変化に対応しつつ、重要インフラ防護を可能としていくためには、重要インフラ事業者等における障害対応体制の有効性検証や人材育成等を推進し、サイバーセキュリティ水準の底上げを図ることが必要であるところ、次の施策を実施する。

（主な施策）

・ 演習・訓練の取組の促進（演習・訓練の実施・協力、重要インフラ事業者等の参加支援等）
・ 産学官の連携、演習や教育等を通じたサイバーセキュリティ人材（CISO等を含む。）育成の取組促進及び支援等
・ 各国政府等との情報共有等、協力・連携の強化
・ その他各分野の特性や事情を踏まえた施策等

2.2 把握・分析

国家サイバー統括室は、年に１回を目途に、各分野における重要インフラ事業者等による取組の実施状況等を把握するため、重要インフラ所管省庁と連携し、次の調査を行う[17]。また、重要インフラ所管省庁においても必要に応じて、各分野の重要インフラ事業者等に対する類似の調査を行う。

・ 全ての分野・事業者を対象とした質問調査
・ 一部の分野・事業者を対象とした実地調査
・ その他調査（国内外における関連制度との比較等）

これら調査結果を踏まえ、重要インフラ所管省庁は各分野における重要

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。

[17] 基本法第 25 条（戦略本部の所掌事務等）及び第 33 条（資料の提出その他の協力）の規定に基づく調査。当該調査は、同法第 31 条（事務の委託）の規定に基づき独立行政法人情報処理推進機構に委託することができる。

インフラ事業者等の取組の実施状況や、安全基準等と現状との差分等について把握・分析を行う。その際、必要に応じて、セプター事務局や重要インフラ事業者等と調査結果等を共有しつつ、各分野における特性・実情等の観点から分析の深掘りを行う。

また、国家サイバー統括室は、重要インフラ所管省庁による各分野の把握・分析の結果を取りまとめるとともに、それらを踏まえつつ、分野横断的な把握・分析を行う。

2.3 評価・改善

重要インフラ所管省庁は、分野ごとに、把握・分析の結果を踏まえつつ、当該分野における施策の実施状況についての評価案を作成する。

国家サイバー統括室は、重要インフラ所管省庁が作成する、各分野における施策の実施状況についての評価案を取りまとめるとともに、分野横断的な評価案を作成する。その上で、2.2 で作成した調査結果及び把握・分析結果とあわせて、戦略本部に報告する。

戦略本部は、同報告内容をもとに、統一基準に基づく施策の実施状況等の評価を行う。評価は、組織体制や所要の予算措置の検討を含む、施策の改善・見直しについて行う。評価に当たっては、サイバー空間上のリスク・脅威動向や重要インフラを取り巻く社会環境・技術環境の変化等を踏まえるとともに、分野横断的なセキュリティ対策の底上げの観点及び、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を図る観点の両方から実施する。

国家サイバー統括室及び重要インフラ所管省庁は、戦略本部による評価結果を踏まえて、実施計画を更新し戦略本部に報告する。国家サイバー統括室及び重要インフラ所管省庁は、更新後の実施計画に基づき、連携協力して、より効果的・効率的な施策の実施が図られるよう努める。

第3部 安全基準等において規定されるべき事項

3.1 基本的な考え方

（１）目的及び位置付け

第３部では、所管省庁等が策定する安全基準等において、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として規定されるべき事項を記載する。

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に関わる事業者等、重要インフラサービス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。

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、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。

なお、各分野におけるリスクベースの取組については、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。

（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[18]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[19]の

---

[18] 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。

[19] 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。

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、3.2 以降では、「組織統治」、「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する。

（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、「閉域網だから安全」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。

安全基準等における対象範囲の設定に当たっては、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、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[20]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・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定する。

（4）関係主体の役割

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、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。

---

[20] 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。

3.2 組織統治

3.2.1 組織状況の理解

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。
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。
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。

3.2.2 組織方針

3.2.2.1 組織方針とサイバーセキュリティ

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。

3.2.2.2 サイバーセキュリティ方針

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。

3.2.3 組織内外のコミュニケーション

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。

3.2.4 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

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。
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。

3.2.5 役割・責任・権限

3.2.5.1 責任及び権限の割当て

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。
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。

3.2.5.2 資源の確保

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[21]であるとの考え方のもとで配分する。

3.2.5.3 CSIRT 等の整備

① CSIRT[22]としての機能を持つ体制を整備する。

3.2.5.4 役職員の管理

① 役職員（特に重要システム[23]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。

3.2.6 監査・モニタリング

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。
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。

---

[21] 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。
[22] 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。
[23] 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。

3.2.7 情報開示

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。

3.2.8 継続的改善

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。
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。

3.2.9 サプライチェーン・リスクマネジメント

① 自組織の重要システムや機能とサプライチェーン[24]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。
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。
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。

3.3 識別

3.3.1 資産の管理

3.3.1.1 資産に対する責任

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。
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

[24] 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。

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。

3.3.1.2 情報分類と取扱い

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（紙、電子）へのラベル付け等により管理する。
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。

3.3.2 脅威情報及び脆弱性情報の収集・分析

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。

3.3.3 情報共有

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、セプターやISAC、協議会[25]等を活用し、組織内外と情報共有を実施する。

3.3.4 リスクアセスメント

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。

[25] サイバー対処能力強化法第45条に基づく協議会

3.3.5 サイバーセキュリティリスク対応

3.3.5.1 リスク対応の決定

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[26]等も活用しつつ、自組織における評価基準等をもって優先順位付けする。

3.3.5.2 個別方針の策定

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。

3.3.5.3 リスク対応計画の策定等

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。
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。

3.3.6 脆弱性の管理

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。
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。
③ 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。

3.4 防御

3.4.1 アカウント管理・認証・アクセス制御

3.4.1.1 アカウント管理

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

[26] 組織において現在取り組んでいる対策や手法等に能力レベルを評価し、目標や改善のための優先順位を設定するための仕組み。

スする利用者とそのアクセス権を管理する。

3.4.1.2 認証・アクセス制御

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。

3.4.1.3 セキュリティ確保が求められる領域

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。

3.4.1.4 装置の管理

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。
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。

3.4.2 意識向上とトレーニング

3.4.2.1 人材育成・意識啓発

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。

3.4.2.2 演習・訓練

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。

3.4.3 データのセキュリティ対策

3.4.3.1 データ管理

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。
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。

3.4.3.2 暗号を活用した情報管理

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。

3.4.3.3 バックアップ

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。
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。

3.4.4 システムのセキュリティ対策

3.4.4.1 運用の手順及び責任

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。

3.4.4.2 ハードウェア・ソフトウェアの管理

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。
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。

3.4.4.3 システムの取得・開発・保守

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。
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。

3.4.4.4 マルウェアからの保護

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。

3.4.5 ログ取得

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。
② ログが改ざん、消去されないよう管理する。

3.4.6 インフラストラクチャ（ネットワーク等）の対策

3.4.6.1 通信のセキュリティ

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。
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。
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。

3.4.6.2 テレワーク・遠隔制御

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。

3.4.6.3 災害による障害の発生を踏まえた対策

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。

3.4.7 クラウドサービス利用時の対策

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。
② 責任共有モデル[27]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。
③ 情報公開等の設定にミスがないか確認する。
④ サービス仕様が変わる際には影響を確認する。
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。
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

[27] 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。

扱い（論理的な廃棄）について確認する。

3.5 検知

3.5.1 監視・分析体制の整備

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監視・分析体制を整備する。

3.5.2 継続的監視

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。

3.5.3 事象の分析

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。

3.6 対応及び復旧

3.6.1 事業継続計画等

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[28]、事業復旧計画[29]、IT-BCP[30]、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。
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。

3.6.2 インシデントへの対応及び復旧

3.6.2.1 インシデント管理
① インシデントの管理責任者を定める。
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[31]等の運用プロセスを確立する。
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。

3.6.2.2 インシデント分析
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。

3.6.2.3 インシデントの報告とコミュニケーション
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。

3.6.2.4 インシデント軽減
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。
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

---

[28] 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）
[29] 平時のサービス水準までの完全復旧対応の方針。
[30] 情報システムに係る記載を詳細化した対応方針。この点、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。
[31] 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。

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。

3.6.2.5 復旧

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。

3.6.3 危機管理

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。
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。
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。

3.7 技術・脅威の動向等を踏まえた対策

① 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。

附 則

この決定は、令和８年 10 月１日から施行する。