内閣サイバーセキュリティセンター
重要インフラ
関係規程集

令和７年 １ 月

内閣官房　内閣サイバーセキュリティセンター

制度・監督ユニット

目次

１　重要インフラ施策等関係

２　戦略

３　根拠法令等

１　重要インフラ施策等関係

重要インフラのサイバーセキュリティに係る行動計画

２０２２年６月１７日

サイバーセキュリティ戦略本部

２０２４年３月８日

サイバーセキュリティ戦略本部改定

この行動計画は、サイバーセキュリティ基本法(平成 26 年法律第 104 号)第 12 条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第 14 条(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促進)及び第 26 条第 1 項第 5 号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定するものである。

目次

Ⅰ. 総論

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、特に情報通信、電力、金融等、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる。このため政府では、重要インフラ防護に係る基本的な枠組みとして、重要インフラにおけるサイバーセキュリティに関して重要インフラ事業者等の自主的な取組の促進その他の必要な施策の実施に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画(以下「行動計画」という。)を策定し、これを推進してきたところである。

重要インフラを取り巻く脅威は年々高度化・巧妙化しており、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。かかる状況を踏まえ、「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「本行動計画」という。)では、「重要インフラの情報セキュリティ対策に係る第4次行動計画」(以下「第4次行動計画」という。)を基本としつつ、重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図る。

1. 重要インフラ防護の目的

重要インフラにおいて、任務保証[1]の考え方を踏まえ、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等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済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ことを重要インフラ防護の目的とする。

[1]サイバーセキュリティ戦略(令和3年9月28日閣議決定)において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」

2. 理想とする将来像

本行動計画に基づく取組によって実現が期待される将来像を示す。

（責務の明確化）

○重要インフラ防護の目的、各関係主体の責務、実施事項等が明確化され、各関係主体に共通理解として浸透している。

（組織統治）

○環境変化に対して、重要インフラ防護の目的を組織単位で常に確実に達成できるよう、組織内の責任と権限を明確にし、適切な資源配分が行われ、PDCAサイクルを的確に回せるための組織統治が十全に機能している。

（重要インフラ事業者等における自組織に最適な防護対策の確保）

○組織及び提供する重要インフラサービスの特性に基づき、経営層がリスクを明確にし、組織内に周知している。

○重要インフラサービスの継続的な提供に関する要求事項が明確であり、そのための基準、マニュアル等が制定、維持され、関係者が遵守している状況が評価可能な状況にある。

（脅威への包括的な取組）

○重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応に係る取組が促進されている。

（コミュニケーション）

○自組織内及び各関係主体間それぞれにおいて、重要インフラサービス障害の予防的対策を強化するためのコミュニケーションが日常的に行われている。また、重要インフラサービス障害が発生した場合には、充実したコミュニケーションを通して冷静に対処できるようになっており、更にその経験を確実に将来の対策に活かすための継続的な改善がなされている。

（社会との共存共栄）

○各関係主体の自主的かつ積極的な取組がサイバーセキュリティ文化の醸成に寄与するとともに、社会の持続的な発展を支えている。

○重要インフラサービスの継続的提供がなされるとともに、各関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている。

（定期的な評価・見直し）

○各関係主体の取組が定期的に評価されるとともに、必要に応じて行動計画が適切に見直されている。

3. サイバーセキュリティ基本法との整合性について

3.1 サイバーセキュリティ基本法における行動計画の位置付け

行動計画は、サイバーセキュリティ基本法(平成26年法律第104号)第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、同法第14条(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促進)及び第26条第1項第5号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定される。

3.2 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

サイバーセキュリティとは、サイバーセキュリティ基本法第2条に規定する、電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう。

3.3 サイバーセキュリティ基本法における関係主体の責務

重要インフラ防護に関係する主体に対するサイバーセキュリティ基本法における責務は以下のとおり規定されている。

(1) 国

国は、サイバーセキュリティ基本法第4条の規定に基づき、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。

(2) 重要インフラ事業者等

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

重要インフラ事業者は、サイバーセキュリティ基本法第3条第1項に規定する重要社会基盤事業者であり、同法第6条の規定に基づき、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努める責務を有する。

地方公共団体は、サイバーセキュリティ基本法第5条の規定に基づき、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

(3) サプライチェーン等に関わる事業者

重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者は、サイバーセキュリティ基本法第7条に規定するサイバー関連事業者その他の事業者に当たる。サイバー関連事業者その他の事業者は、サイバーセキュリティ基本法第7条の規定

に基づき、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努める責務を有する。

4. 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群と補強・改善の方向性等を表に示す。

表 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群	第4次行動計画の施策群との対応	第4次行動計画からの主な補強・改善の方向性
1. 障害対応体制の強化	「4. リスクマネジメント及び対処態勢の整備」の一部と「5. 防護基盤の強化」の一部を統合した上で整理	○ 重要インフラ防護を適切に行うためには、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の取組の必要性が高まってきていることを踏まえ、組織統治の一部としての障害対応体制の強化を推進 ○ サイバーセキュリティを取り巻く環境が大きく変化することを背景としたサプライチェーン・リスク等の新たな脅威への先取りした対応の推進 ○ 重要インフラ事業者等の自組織のリスクに応じた最適な防護対策の推進 ○ 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討 ○ 事前対応のリスクマネジメントと障害発生時の危機管理の一体的な対応の推進
2. 安全基準等の整備及び浸透	「1. 安全基準等の整備及び浸透」を基本的に踏襲	○ 障害対応体制の強化及びリスクマネジメントに資する安全基準等を整備することを明確化 ○ 重要インフラ事業者等の取組の継続的な改善を図ることができる調査手法の検討
3. 情報共有体制の強化	「2. 情報共有体制の強化」を「3. 障害対応体制の強化」の一部と統合した上で整理	○ 重要インフラ事業者等の自主的な取組の活性化を前提とした共助の推進 ○ ISAC 連携等による分野間・官民連携の枠組みの整備の検討 ○ ナショナルサートの枠組みの強化の検討との整合性保持
4. リスクマネジメントの活用	「4. リスクマネジメント及び対処態勢の整備」の一部を整理	○ 組織の特性を踏まえた経営層による組織のリスクの明確化 ○ 自組織に適した防護対策の実現を支援するため、既存の手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンスの整備の方向性の明示 ○ 2020 年東京オリンピック・パラリンピック競技大会開催に向けて官民が連携して行ってきた取組の活用を検討
5. 防護基盤の強化	「5. 防護基盤の強化」の一部を「3. 障害対応体制の強化」の一部と統合した上で整理	○ 障害対応体制の有効性検証としての分野横断的演習の推進 ○ 警察による重要インフラ事業者等との協力等の必要な取組の支援 ○ デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施

II. 本行動計画の要点（エグゼクティブサマリー）

本行動計画を推進するに当たっての、①「重要インフラ防護」の目的、②関係主体の責務、③基本的な考え方、④障害対応体制の強化に向けた取組を以下に示す。

① 「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、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等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靱性を確保し、国民生活や社会経済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こと。

② 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。
- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

③ 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

④ 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を経営の重要事項としてサイバーセキュリティを取り込む。
- サイバーセキュリティの確保には、サイバーセキュリティ基本法第 2 条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

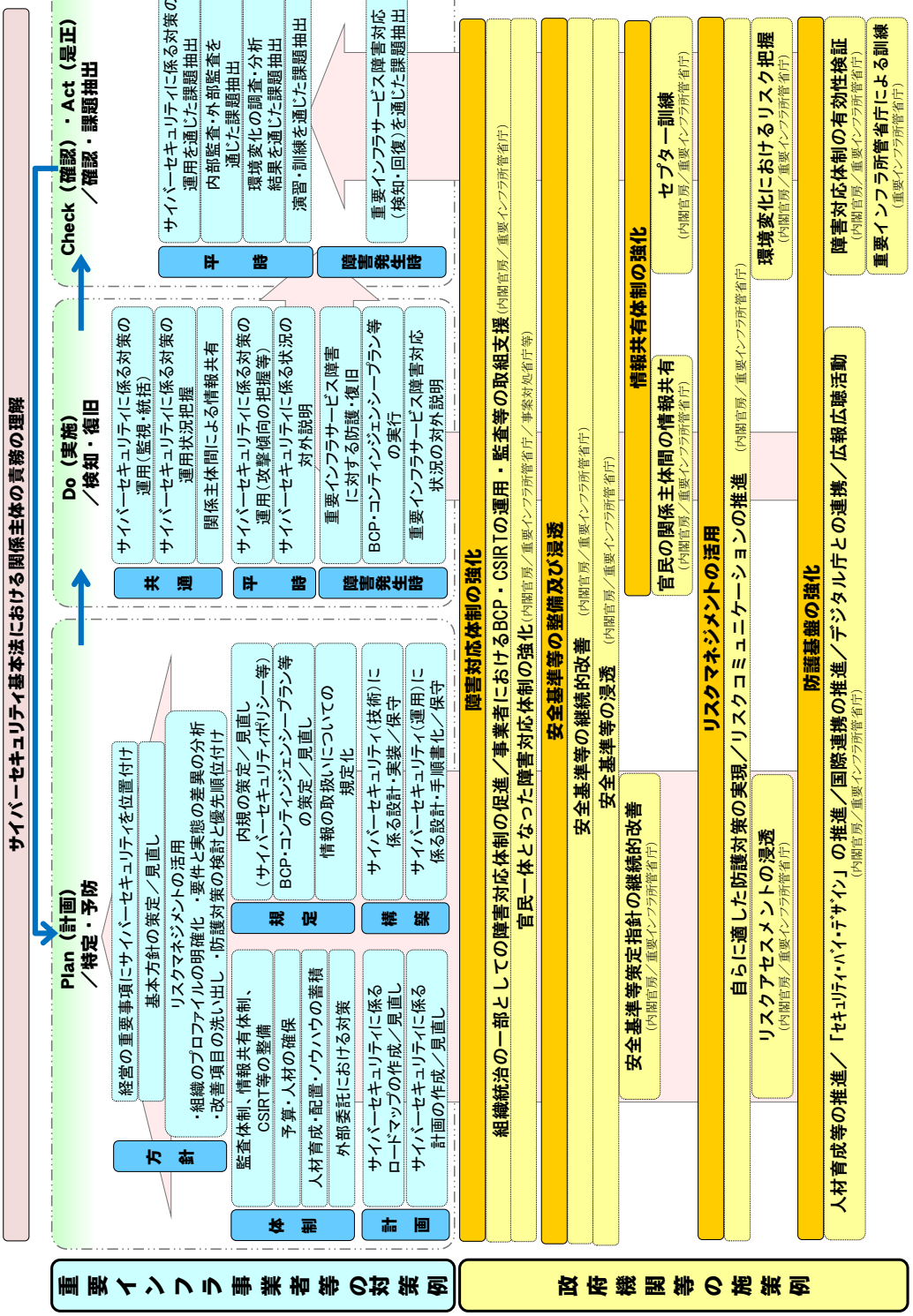


図１「重要インフラ事業者等の対策例」と「政府機関等の施策例」

III. 重要インフラを取り巻く環境変化と行動計画に関する基本的な考え方

重要インフラサービス障害の原因の多くは管理不良となっており、外部からの攻撃のみならず、システム調達、設計及び運用についても、より適切に管理する必要がある。また、経済社会活動の相互依存関係の深化が進みリスクが高度化・複雑化しており、サプライチェーン全体を俯瞰することが重要になっていることから、重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者の位置付けを明確化する。また、組織統治の一部にサイバーセキュリティを組み入れ、障害対応体制を抜本的に強化するとともに、自組織に適した防護対策を実現する。障害対応体制の強化に当たっては、①経営層からシステム担当者までの各階層の視点を有機的に組み合わせること、②リスクマネジメントによる事前対応及び危機管理の両面から取り組むことを促進する。

1. 重要インフラを取り巻くサイバーセキュリティの環境変化

2017年度に決定した第4次行動計画以降、サイバーセキュリティを取り巻く環境は大きく変化してきた。特に、2020年代を迎えた最初の１年に、世界はコロナ禍の影響による不連続な変化に直面し、結果として人々のデジタル技術の活用は加速した。さらに、2020年代は、サイバー空間と実空間が高度に融合したSociety5.0の実現へと大きく前進する「Digital Decade」となり得ると考えられる。一方で、国家間での競争の顕在化を含む国際社会の変化の加速化・複雑化、情報通信技術の進歩や複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず変容かつ増大している。このような中で、2021年には、2020年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）の開催や、デジタル社会の形成に向けた司令塔たるデジタル庁の設置があった。

こうした環境変化等を背景に、2021年9月28日、新たなサイバーセキュリティ戦略が閣議決定された。この中で、東京大会開催に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組を、我が国におけるサイバーセキュリティの向上に活用していくこととされた。また、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針において、サイバーセキュリティについても基本的な方針を示し、その実装を推進することとされた。さらに、我が国を取り巻く安全保障環境が厳しさを増している中、サイバー攻撃からの防御、サイバー攻撃の抑止、サイバー空間の状況把握に係る能力向上のため、政府全体としてのシームレスな対応を抜本的に強化していくこととされた。

重要インフラに着目すると、一部分野において、環境変化に起因するサービス障害が既に発生し始めている。重要インフラサービス障害のリスクは、サイバー攻撃だけではなく、自然災害、人的要因等の多岐にわたり、特に、適切な組織管理がなされれば防げたサービス障害が目立ち始めている。さらに、システム間の連鎖が進み、サービス障害による影響が大規模化する傾向にある。

2. 重要インフラ防護の範囲

重要インフラ事業者等が、各種法令等に基づき重要インフラサービスを提供する際、自らが重要インフラ防護の当事者であるという認識を持ち、重要インフラ防護に取り組む必要がある。このため、重要インフラ所管省庁は、各重要インフラ分野における重要インフラ事業者等を明確化し、自らが重要インフラ事業者等であることを認識できるようにする。また、内閣官房及び重要インフラ所管省庁は、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しを行う。

対象となる重要インフラ分野と重要システム例については、第4次行動計画に引き続き、別紙１に示し、重要インフラ分野は、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の15分野とする。重要インフラサービスとサービス維持レベルについては、第4次行動計画に引き続き、別紙2に示す。

さらに、公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保のために、重要インフラに関与するあらゆる組織が、経済社会活動の相互依存関係の深化が進みリスクが高度化・複雑化していることを認識しつつ、サプライチェーン全体を俯瞰し責任ある行動をとることが期待される。このため、重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者についても、サイバーセキュリティ基本法第７条(サイバー関連事業者その他の事業者の責務)の責務が認識され、責任ある行動がとられるよう取り組む。

3. 組織統治の一部としてのサイバーセキュリティ

従来、サイバーセキュリティに係る取組はシステム担当者だけで対応されることが多かった。しかし、DXの進展によりデジタル技術の活用が加速しつつある中で、組織全体を俯瞰した上でのリスクの明確化、対応策の検討等、経営層でなければ対応できないものも多くなってきている。例えば、近年の重要インフラサービス障害の主な原因は、自然災害、管理不良であり、特にその多くは管理不良によって発生している。管理を適切にすれば防げた類似障害が繰り返し発生していることを低減させるため、組織全体での取組が必要となっている。そのため、組織統治にサイバーセキュリティを組み入れるための取組を推進する。

4. 自組織に適した防護対策の実現

リスクが高度化・複雑化しているため、求められるサイバーセキュリティの水準や取組は分野や事業者によって異なりつつある。さらに、DXの進展により、重要インフラを取り巻く環境やリスクは今後も大きく変化していくと考えられる。したがって、サイバーセキュリティの実効性を高めるためには、画一的な安全基準等を参照するだけでは十

分でなく、自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを経て、適した防護対策を実施することが一層重要となる。

そのため、発生したサービス障害へ事後的に対応するのみならず、将来に向けて変容していく当該重要インフラサービスの性質と社会との関係を組織ごとに適切に把握した上で、自然災害、管理不良、サイバー攻撃等による重要インフラサービス障害へのリスクを明確化し対応できるようにするための取組を促進する。その際、当該重要インフラサービスを提供するために必要なサプライチェーン等及び海外拠点を含めるものとする。

Ⅳ. 計画期間内の取組

1. 障害対応体制の強化

昨今の重要インフラを取り巻くサイバーセキュリティの状況では、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織一丸となった対応が求められるようになってきた。重要インフラ事業者等は、組織統治の中にサイバーセキュリティを組み入れ、当該組織の特性に応じた適切な予防措置及び被害発生時の措置を構築、維持することを含め、障害対応体制の強化を推進していく必要がある。

本行動計画では、サイバーセキュリティ関係法令を明確にし、政府及び重要インフラ事業者等における障害対応体制の強化に関する取組を推進する。

1.1 組織統治の一部としての障害対応体制

昨今の重要インフラサービス提供の支障事案の原因は、自然災害、管理不良、サイバー攻撃等であり、多くは、適切な組織管理がなされれば防げたものが多いことから、組織全体の体制管理を適切に行う必要がある。

重要インフラ事業者等においては、組織の各階層において適切な責任と権限を明確にし、組織一丸となって重要インフラ防護を行う必要があるが、経営層のコミットメントによる組織運営上のリスクのひとつとして、重要インフラ防護の観点を含める必要がある。

内閣官房は、本行動計画において、障害対応体制の強化に資する組織統治の在り方について、安全基準等策定指針において、規定化をする。

重要インフラ事業者等は、本行動計画及び策定された安全基準等策定指針を踏まえ、自組織の障害対応体制の改善に努めるものとする。

(1) 組織統治に必要な観点

組織統治の一部として障害対応体制を強化するためには、「サイバーセキュリティ関係法令Q&Aハンドブック Ver1.0(令和2年3月2日 内閣官房内閣サイバーセキュリティセンター)」における４つの観点[2]が必要となる。

① 内部統制システムとサイバーセキュリティとの関係

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

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各組織が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情

[2] 具体的には Q3 から Q6

を勘案の上、各組織において決定されるべきである。また、組織の意思決定機関は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定することでもよい。

② サイバーセキュリティと取締役等の責任

組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

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

③ サイバーセキュリティ体制の適切性を担保するための監査等

組織内のサイバーセキュリティ体制が適切であることを担保するための方策としては、内部監査、情報セキュリティ監査、システム監査等の各種監査、内部通報、情報開示、CSIRTの設置といった方策が考えられる。

④ サイバーセキュリティと情報開示

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

そこで、組織としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

(2) 経営層、CISOをはじめとする重要インフラ防護体制の役割の責任

DXの進展に伴い、ITが情報系という役割から事業基盤へと変貌を遂げたことで、IT障害は事業に直接的な影響を与えるようになった。これまで、ITに関するリスクはシステムの問題として個別に捉えられてきたが、主要な事業に関するリスクのひとつとして再定義が求められる。つまり、経営層はIT障害が事業に与える影響を把握することが不可欠であり、想定される障害を受容可能なリスクとして管理することが求められる。

こういった現状を踏まえると、経営層、CISO、戦略マネジメント層、システム担当者等の組織全体及びサプライチェーン等に関わる事業者における役割と責任を明確にした上で、サイバーセキュリティの専門的・技術的な問題点と、経営層が抱えている事業運

営の問題点を融合させることが必要である。しかしながら、経営層がサイバーセキュリティの専門的な知見を必ずしも有するとは限らない。経営層が、経営的な立場からITリスクに取り組むCISO等を経営層の一員として、事業運営の一端を担わせることが重要になる。

1.2 障害対応体制の強化に向けた取組

DXの推進においては、製品・サービスにセキュリティを取り込んでいくことが、企業の競争力強化に貢献し、企業活動の維持・発展の基盤となる。そのため、内閣官房は、企業における製品・サービスの関係者が「セキュリティ・バイ・デザイン」を共通の価値として認識することを促していく。さらに、サプライチェーン・リスク等の新たな脅威を先取りした対応を推進し、組織の壁を越えたサプライチェーン全体でセキュリティを向上するための方策を講じていく。そのために、内閣官房は、大規模事業者等だけではなく中小事業者等も含めた重要インフラ事業者等がBCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等を効果的に整備できるように、その重要性や取組方針について示す。また、重要インフラ所管省庁と連携し、重要インフラ事業者等がこれらを整備できるように、各重要インフラ分野に属する組織に合った支援策を検討する。

また、サービス障害に係るリスクは分野や事業者によって異なるといった課題がある。そのため、組織ごとにリスクを把握し、自組織に最適な防護対策を実施しなければならない。内閣官房は、重要インフラ事業者等の自組織のリスクに応じた最適な防護対策を推進していく。その一環として、経営層のリーダーシップの下での体制整備、最新のサイバー攻撃の手口や被害の状況等を踏まえた有効な対策等について、サイバーセキュリティに係るガイドライン等により重要インフラ事業者等に対して啓発していく。さらに、対策の際の課題、ベストプラクティス、最新の脅威情報やインシデント情報等の共有のため、サイバーセキュリティについて知見を有する独立行政法人、ISAC(Information Sharing and Analysis Center)を含むインシデント情報共有・分析機能を有する機関等を積極的に活用しつつ、情報共有のためのプラットフォーム構築等、民民間・官民間における一層の情報共有網の拡充を進める。

(1) BCP/IT-BCP

重要インフラ事業者等は、任務保証を実施する観点から、リスクマネジメントの中で、事業継続計画(BCP)及びIT固有の事業継続計画(IT-BCP)を整備し、維持することが必要である。サイバーインシデントを未然に防止するための方策や方針の策定に加え、事業継続に関する悪影響を許容範囲内に抑制するためのBCPの一部としてIT-BCPを策定する。システム障害が組織全体にエスカレーションする際、当初IT-BCPが機能し、ある時点からBCPへ円滑に移行していくことが求められる。自組織のBCPの整備においては、シームレスにIT-BCPとBCPの連携をするように整備することが必要である。

(2) CSIRT の効果的な運用

重要インフラ事業者等は、CSIRTを整備し、通常時からインシデントに的確に対処できる体制を充実・強化することが求められる。CSIRTは、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。加えて、障害が発生した場合など有事の際の対応を行うだけではなく、サイバーセキュリティインシデントの未然防止や情報収集、障害の検知等を行う。

(3) 安全基準等の活用

重要インフラ事業者等は、重要インフラ分野のガイドライン等を参考にすることで、自組織の内部規定の見直しを進める。これにより、組織の体制の底上げにつながることが期待される。詳細は「2.安全基準等の整備及び浸透」で記載する。

(4) 情報共有体制の強化

個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化に取り組む。詳細は「3.情報共有体制の強化」で記載する。

(5) リスクマネジメントの活用

重要インフラ事業者等は組織の特性に応じたリスクを把握し、現在の状況を踏まえ、改善目標を設定し、継続的な改善を行う仕組みを機能させる必要がある。詳細は「4.リスクマネジメントの活用」で記載する。

(6) 障害発生に関する対応

障害発生時においては、リスクマネジメントを経て顕在化した課題を元に策定した、BCP/IT-BCPやコンティンジェンシープランを実行することが重要である。加えて、昨今のサイバーセキュリティを取り巻く環境変化の速さの観点から、想定外の危機における対応も考慮する必要がある。重要インフラ事業者等においては、リスクマネジメントと危機管理の一体的な対応を実施することが期待される。

また、障害発生時の対応を適切かつ迅速に行うためには、関係者間での情報伝達による不整合を起こさないことが求められる。したがって、日々のコミュニケーションを充実させることを推進する。

さらに、システム担当者の運用で得られた最新の脅威や脆弱性は、防護対策における評価や改善につなげることができる。重要インフラ事業者等は、発見した脅威や脆弱性に関するリスクを払拭するような管理策を適用することが求められる。

(7) 監査検証

重要インフラ事業者等は、自組織の重要インフラサービスに係る障害対応体制の運用

状況やリスクアセスメントに基づく適切な管理策の整備の状況を検証するために、監査検証が必要である。

監査については、監査実施主体に応じて内部監査や外部監査があり、トップマネジメントの一環として、自組織に有効的と考えられる監査を決定し、実施する。特に内部監査においては、自組織の障害対応体制の改善を援助できるように、監査部門で担う役割を明確化することを推進する。

重要インフラ事業者等においては、検証結果を経営層等に報告し、必要に応じて体制の改善を実施することが期待される。

(8) その他取組

その他、重要インフラ事業者等が実施する障害対応体制の強化に資する取組として、演習、人材育成、国際連携等がある。これらについては「5. 防護基盤の強化」で記載する。

1.3 官民一体となった障害対応体制の強化

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、特に情報通信、電力、金融など、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる。

我が国を取り巻く安全保障環境は厳しさを増しており、サイバーセキュリティ戦略(令和3年9月28日閣議決定)では、サイバー攻撃に対する国家の強靭性を確保し、サイバー攻撃から国家を防御する力(防御力)、サイバー攻撃を抑止する力(抑止力)、サイバー空間の状況を把握する力(状況把握力)をそれぞれ高めつつ、政府全体としてシームレスな対応を抜本的に強化していくことが重要とされている。重要インフラ防護において、これらを具現化していく。

防御力については、任務保証の観点から政府機関及び重要インフラ事業者等におけるコミットメントの確保や、重要インフラ事業者等が自組織に最適な防護対策に取り組めるよう、本行動計画において、一層の改善を図るものとする。

脅威の高まりに対して的確に対応するためには、効果的な抑止力の確保が重要となる。このため、官民の相互信頼に基づく協業を通じ、状況把握力を一層高めるとともに、攻撃者を特定し責任を負わせるためにサイバー攻撃を検知・調査・分析する能力を引き続き高め、抑止力を強化する。そのためにも関係機関の役割に応じた相互連携を機動的に行い、安全保障の観点からの取組を強化する。

1.4 重要インフラに係る防護範囲の見直し

任務保証を目的とした重要インフラ防護を実現するためには、重要インフラ分野間の相互依存関係や外部サービス（既存の重要インフラ事業者等でない外部委託先等の周辺事業者等が提供するサービス）への依存等の実態及び新たな技術の発展・拡大による社会経済システム全体へのリスクの拡散や被害の深刻化という環境変化に対応するため、サプライチェーンを含めた「面としての防護」を確保する必要がある。

既存の重要インフラ分野におけるセプター未加入事業者に対する加盟促進や、当該分野が依存している外部サービスに関する実態把握と防護範囲の見直しに取り組む中、複数の分野において、新たにセプターへ加盟する事業者や新たに内閣官房から情報の一部（公開情報を取りまとめて紹介するニュースレター等）を受け取る複数の業種が生じるとともに、既存の事業領域を超える連携等を模索する動きが生じるなどの進展が見られる。今後も、社会環境の変化に柔軟に対応しながら、重要インフラサービスを安全かつ持続的に提供するための「面としての防護」を実現するため、防護範囲見直しの取組を継続する。

また、国民生活及び社会経済活動の防護等において安全保障上の観点を踏まえる必要性が高まっているため、内閣官房は、関係主体と連携し、防護対象として情報共有等を推進すべき重要インフラ分野についての取組強化や、新たな重要インフラとして位置付けるべきサービスを適切に防護できるよう、重要インフラ分野の見直し等の継続的な取組を行っていく。

2. 安全基準等の整備及び浸透

重要インフラを取り巻く環境の変化や脅威の多様化を踏まえ、重要インフラ事業者等が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ことが必要である。そのため、関係主体は、安全基準等の整備及び浸透に取り組むことが期待される。

安全基準等に関する体系を図 2に示す。具体的には、内閣官房は、重要インフラ所管省庁の協力のもとに、各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」(以下「安全基準等策定指針」という。)として策定している。さらに、安全基準等策定指針で定めた手順等を具体的に示すための手引書(以下「手引書」という。)及び個別の対処方法、留意点等を示すガイダンス等の関連文書を策定している。安全基準等策定指針、手引書等を踏まえ、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、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」、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(以下「安全基準等」という。)が策定されている。

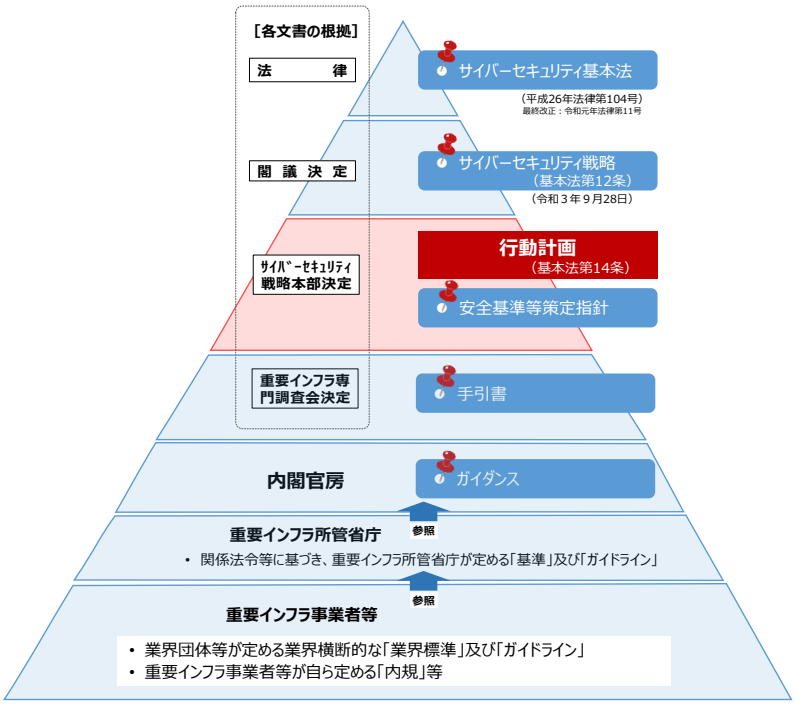


図 2 重要インフラ防護に関する安全基準等に係る体系

2.1 安全基準等策定指針の継続的改善

内閣官房は、特に障害対応体制の強化の観点から、安全基準等策定指針及び手引書の見直しを行う。安全基準等策定指針及び手引書の見直しについては、3年に1度の実施を

原則とする。他方、社会動向の大きな変化等、現行の安全基準等策定指針及び手引書では十分ではない事象が発生した場合は、この限りでない。さらに、安全基準等策定指針及び手引書の関連文書であるガイダンス等については、昨今のランサムウェアによる攻撃の増加を一例とする周辺環境の激変やインシデント等に速やかに対応できるよう、運用等から得られた知見を踏まえて適時に改定する。また、国際標準や海外の指針のうち日本でも参考にすべきものがあれば適宜採り入れることを検討する。

本行動計画期間中に新たに整備を行う安全基準等策定指針に係る事項は以下のとおりとする。

(1) 組織統治に関する基準の整備

組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく、「サイバーセキュリティ関係法令Q&Aハンドブックver1.0」（令和２年３月２日）で規定している①内部統制システムとサイバーセキュリティとの関係、②サイバーセキュリティと取締役等の責任、③サイバーセキュリティ体制の適切性を担保するための監査等、④サイバーセキュリティと情報開示、を活用するなどして、安全基準等策定指針の記載を充実させる。

(2) サプライチェーンに関する基準の整備

サプライチェーンに起因する重要インフラサービス障害の連鎖に係るリスク、例えば、①サプライチェーンの過程で製品に不正機能等が埋め込まれるリスク、②政治経済情勢による機器・サービスの供給途絶のリスク、③クラウドサービス等の外部サービスにおける情報の取扱い・可用性に係るリスク等の高まりを踏まえ、サプライチェーン・リスクへの対応について安全基準等策定指針の記載を充実させる。

(3) 自組織に適した継続的改善のための基準の整備

自組織に適した対策に係る基本的な考え方を安全基準等策定指針に盛り込み、具体的な実施手法を示す関連文書等の作成を実施する。

(4) その他基準の整備

プラントや工場等の制御システムへのサイバー攻撃等の脅威に迅速に対応するため、ITとOTの横断的な組織整備や、OTのセキュリティ人材の育成の重要性を訴求する。

2.2 安全基準等の継続的改善

重要インフラ所管省庁は、自らが安全基準等の策定主体の場合には、安全基準等策定指針の改定等を踏まえて、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。重要インフラ事業者等は、自らが安全基準等の策定主体の場合には、関係法令の要求事項を遵守できるよう、安全基準等策定指針の改定等を

踏まえつつ、継続的に安全基準等を改善する。

具体的には、各重要インフラ事業者等の対策の経験から得た知見等をもとに、サイバーセキュリティの確保に向けた取組の運用、内部監査・外部監査、サイバーセキュリティに係る環境変化の調査・分析の結果、演習・訓練、重要インフラサービス障害対応等から課題を抽出し、リスク評価を経て、安全基準等がそれぞれの重要インフラ分野及び各組織に最適なものとなるよう取り組む。安全基準等の検証に際しては、安全基準等策定指針及び内閣官房が公表した社会動向の変化・新たな知見を用いることとする。

内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。

2.3 安全基準等の浸透

重要インフラ事業者等において有効な障害対応体制の構築がなされているかを精緻に把握することを目的に、内閣官房は、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段について調査分析する。結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。

重要インフラ分野・組織ごとのリスクの多様化・複雑化に伴い、組織に応じた対策状況や、経営層の関与状況等の実態をより正確に把握することが重要になってきている。そのため、重要インフラ事業者等における自主的な取組を促進できる調査方法へ変更する必要がある。内閣官房は、新たな調査方法について重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を検討し、2023年度中を目処に具現化する。

具体的には、重要インフラ事業者等において、①サイバーセキュリティの現状に係る自己評価、②自組織における本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施、を繰り返すことで、サイバーセキュリティの確保に資する継続的な改善を図ることができる合理的・効果的な調査手法を検討する。

2.4 安全基準等の文書の明確化

内閣官房は、安全基準等策定指針、安全基準等の理解を促進するため、その一覧をまとめ、また、文書間の関係性を明確化する。

3. 情報共有体制の強化

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の動向が刻々と変化する中、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、単独で取り組むセキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組むことが必要である。また、重要インフラサービス障害に係る情報及び脅威や脆弱性情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じることは、当該脅威や脆弱性による被害を最小限にとどめるだけでなく、新たなサイバー攻撃の抑止やシステムの不具合の発生の防止にもつながる。こうした背景を踏まえ、これまでの行動計画でも円滑な情報共有を促進するための取組を進めており、本行動計画においても引き続き、本件取組の意義・必要性の理解を深め、その活性化を図るための施策を推進することが重要である。

このため、個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化に取り組む。

なお、自助ありきの共助、自助と共助(互助)を促進させるための公助であることを念頭に、重要インフラ事業者等の自主的な取組の活性化を前提とし、情報共有における共助を推進する。

3.1 本行動計画期間における情報共有体制

これまでの行動計画で構築された情報共有体制が関係主体の間で定着していることも踏まえ、これを引き続き継承・発展させ、内閣官房では、情報共有体制の運営及び必要に応じた見直し等に取り組み、重要インフラ事業者等は共有された情報をリスクマネジメントや事案対処等へ積極的に活用していくものとする。

重要インフラ事業者等は重要インフラ所管省庁を経由して内閣官房へ情報連絡を行い、内閣官房は重要インフラ所管省庁及びセプターを経由して重要インフラ事業者等へ情報提供を行うことを基本としている。予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象を重要インフラ所管省庁に報告することで、政府機関からの指導等につながるのではないかといった懸念を払拭できず、情報共有の活性化を阻害する一因ともなっていたと考えられることから、重要インフラ事業者等が重要インフラ所管省庁に直接報告する形態に加え、法令等で報告が義務付けられていない事象については、セプター事務局経由で情報連絡元の匿名化等を行った上で重要インフラ所管省庁に報告することも可能としている。これらにより、重要インフラ事業者等は、内容に応じて自らの判断でどのように連絡をするかを選択でき、報告が義務付けられていない事象であっても心理的障壁なく情報連絡を行えるようになる。あわせて、各セプター事務局に情報が集約され、必要に応じた分野内での速やかな展開も可能となり、セプターの機能強化にもつながることが期待される。

さらに、緊急時における内閣官房と重要インフラ事業者等の間のホットライン構築に

より、迅速かつ効率的な情報共有の実現が期待される。

加えて、サイバーセキュリティ関係機関は、企業から独立した中立的な観点から、国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっており、このことを踏まえれば、内閣官房及び重要インフラ事業者等とサイバーセキュリティに関する知見を有する同機関とが密に連携することは有効かつ望ましい姿であると言える。あわせて、同機関については、連絡元の了解が得られた情報の匿名化等を行い、積極的に関係主体と共有するなど、我が国の情報共有体制におけるメインプレーヤーのひとつとしての活動が期待される。

なお、サイバーセキュリティ戦略本部長がサイバーセキュリティ基本法第28条第3項の規定に基づき、同法第32条(資料提供等)又は第33条(資料の提出その他の協力)の規定に基づき重要インフラ所管省庁の長又は重要インフラ事業者等の長若しくは代表者からサイバーセキュリティ戦略本部に提供された重要インフラ事業者等のサイバーセキュリティに関する資料、情報等に基づき、重要インフラ所管省庁の長に勧告できる等の仕組みを、その事務を行う内閣官房(内閣サイバーセキュリティセンター)は適切に運用する。

また、災害やテロ等に起因する大規模重要インフラサービス障害が発生した場合、「緊急事態に対する政府の初動対処体制について」(平成15年11月21日閣議決定)に基づき、本行動計画にのっとって関係主体が適切に情報共有を行うなど、関係主体間での密接な連携を図るものとする。

これらを踏まえ、本行動計画期間中の体制を「別紙4-1　情報共有体制(通常時)」及びその延長線上にある「別紙4-2　情報共有体制(大規模重要インフラサービス障害対応時)」に、各関係主体の役割を「別紙4-3　情報共有体制における各関係主体の役割」に示す。また、重要インフラ分野の重要システムや重要インフラサービス障害の事例等について、「別紙1　対象となる重要インフラ事業者等と重要システム例」及び「別紙2　重要インフラサービスとサービス維持レベル」に表す。

以上の取組を着実に進めるとともに、分野をまたがるサイバーセキュリティ上の脅威や脆弱性についても迅速かつ的確に対応できるよう、重要インフラサービス障害に係る情報及び脅威や脆弱性情報を内閣官房に分野横断的に集約し、分析の上、関係主体と共有する仕組みの構築を進める。

3.2 情報共有の更なる促進

共有すべき情報について、これまでの行動計画における定義を継承して「重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報(以下「システムの不具合等に関する情報」という。)」とし、「別添：情報連絡・情報提供について」及び「別紙３　情報連絡における事象と原因の類型」の考え方のとおりとする。情報システムのうち、エアギャップを有し、外部との接続がないとして安全と考えられていた制御システム等においてもサイバー攻撃が確認されている。普及が進んでいるIoTを含め、

これらに対する脅威や脆弱性等についても共有すべき情報の対象である。

本行動計画期間においては、関係主体間で別添に従って情報連絡・情報提供を行い、情報共有の推進を図る。また、環境変化等が生じた場合には、適宜その見直しに取り組む。

なお、内閣官房は、ナショナルサート[3]の枠組みの強化の検討と整合性を保ち、その整備の一環として、サイバーセキュリティ協議会等との連携を一層推進する。

3.3 重要インフラ事業者等の活動の更なる活性化

重要インフラ事業者等の活動を更に活性化するに当たり、重要インフラ事業者等の自らの活動に加え、セプター内、セプター間における情報共有の充実が期待される。

具体的には、重要インフラ事業者等においては、自ら積極的に情報共有に取り組むとともに、経営層のリーダーシップの下、サプライチェーン等に関わる事業者を含め、CSIRT等の重要インフラサービス障害対応体制を構築・強化することが期待される。なお、自ら情報収集を行うことにより情報への理解とその効果的な活用が進むと考えられることから、重要インフラ事業者等の情報収集の活性化が期待される。また、セプターにおいては、これまでの行動計画期間に引き続き、内閣官房が提供する情報の取扱いに関する取決め、機密保持及び構成員外への情報提供に関し、構成員間で合意されたルールが適用され、緊急時に各構成員及び構成員外との連絡が可能な窓口(PoC[4])が設定されている状況において、内閣官房が提供する情報を共有することの継続が期待される。

加えて、セプター内の情報集約及び情勢判断を行うコーディネータの設置、予兆情報や平時の重要インフラサービス障害事例の共有、セプター間やセプターカウンシル等との情報共有に必要な機能の充実を通じた活動の更なる活性化が期待される。また、一部の事業者間ではISACを設置し、ISAC内でサイバーセキュリティの確保に資する情報の共有・調査・分析、さらには海外のISAC等との情報共有等も進められている。ISAC連携等による自動化を含めた分野間・官民連携の枠組みの整備を検討するなど、ISACへの参画やISAC間の情報共有を促進することで、更なる事業者間の情報共有の活発化やサイバーセキュリティの確保に係る積極的な取組が期待される。

なお、セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体であることから、各セプターの主体的な判断により、情報を相互に連携するものである[5]。

このように、各セプターの積極的な参画により、重要インフラ事業者等におけるサービスの維持・復旧能力の向上に資する自発的かつ幅広い取組を通じて、セプター間の情

[3] 国として、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。

[4] PoC：Point of Contact。

[5] セプターカウンシル設立趣意書(セプターカウンシル創設準備会及びNISC)による。

報共有の一層の充実等、重要インフラ事業者等の活動の更なる活性化が期待される。

3.4 セプター訓練

内閣官房は、各分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施する。

実施に際して、セプター訓練では多くの重要インフラ事業者等の参加実績があることを踏まえ、必要に応じて分野横断的演習との連携を検討し、緊急時における情報連絡体制・手段の検証等、セプターや重要インフラ所管省庁からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有訓練の実現を目指す。

4. リスクマネジメントの活用

リスクマネジメントは、重要インフラ防護の目的である重要インフラサービスの継続的提供を不確かにするリスクに対して組織的に対応するために必要な活動である。

関係主体は、本行動計画期間中に「IV 1.2 障害対応体制の強化に向けた取組」を具体化するため、リスクマネジメントを適切に活用していくものとする。また、内閣官房は、各重要インフラ事業者等において最適な防護対策を継続的に改善するためのガイダンス等を作成し、これを支援するものとする。

昨今の環境変化、技術革新等、重要インフラサービス障害に係るリスクが動的に変化してきている状況において、リスクに的確に対処し、許容できる範囲に抑えるようにするためには、経営層の関与が不可欠である。このため、重要インフラサービスの継続的提供の停止が、経営に与えるインパクトを自組織で適切に認識し、組織全体で取り組む意識の醸成と継続的な取組の推進、監視、測定を通じて可視化することにより、その改善を行うことが重要である。

4.1 リスクマネジメントの推進

重要インフラ事業者等がリスクマネジメントに的確に取り組むためには、まず自組織の特性（プロファイル）を把握し、さらに自組織に適した防護対策については、計画、実施、評価・改善を繰り返し、継続的な取組（プロセス）を推進することが求められる。

特に、DXの進展により、重要インフラを取り巻く環境やリスクは今後も大きく変化することが明らかな状況にあり、重要インフラサービスの継続的提供を行いながら、継続的な改善を効果的に実施していくためには、自組織が直面するリスクとその程度を把握し、自組織の重要インフラサービス提供に係る特性(プロファイル)の明確化に着手することから新たな改善をスタートさせる必要がある。

(1) 自組織に適した防護対策の実現に向けた方向性

① 自組織のプロファイルの明確化

プロファイルとは、重要インフラサービスの継続的提供に係る自組織のビジネス方針、戦略、情報資産等の特性のことである。

プロファイルについては、これまでのリスクマネジメントの取組と融合させることで、自組織が直面するリスクを明確にすることが容易となることから、改善計画の範囲とその程度を決定するための基礎データとなる。

通常、プロファイルは、実態把握と将来像を明らかにするためのものである。

- 現段階における防護対策の実施状況等の実態把握(As Is)
- 目標とする将来像(To Be)

② 改善項目の拾い出しと適用の程度の決定

目標と実態のかい離を埋めるためには、改善項目を拾い出す必要があるが、以下の

観点等からアプローチすることで、実施すべき防護対策を検討し、その適用の程度については、自組織における評価基準等をもって、優先順位付けすることが必要となる。

i. 情報資産のリスクに関する改善
ii. 確実なサービス提供に関する改善
iii. 障害等の発生検知に関する改善
iv. 障害等の対処に関する改善
v. 障害等によって阻害された機能の復旧に関する改善

この際、防護対策を数多く実施することやリスク対応の優先度を高レベルに引き上げることを目標に計画等の作成を進めるのではなく、最終的な目標は、自組織に適したリスクの低減と、適切な防護対策の実現に焦点を当てる必要がある。

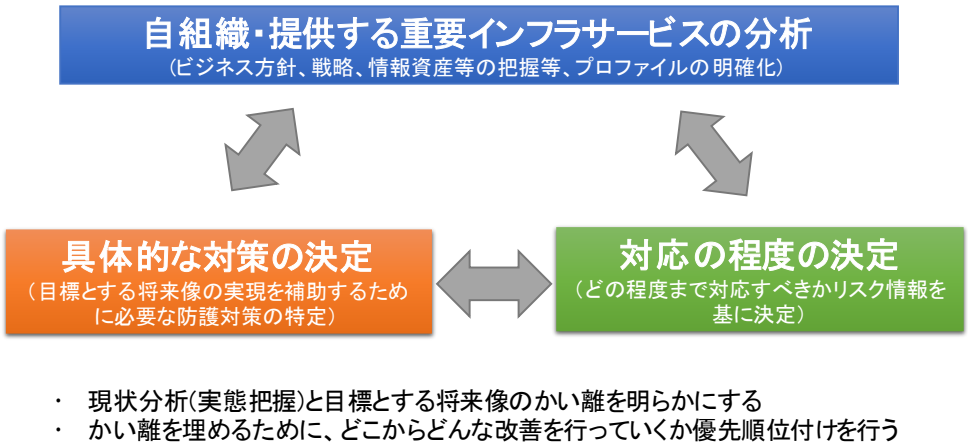


図 3 自組織に適した防護対策の実現（概念図）

図 3 に示すように、重要インフラ事業者等の自組織の現状分析を行うことによって、重要インフラサービスの継続的提供に係る対応すべきリスクを明確にし、対応の程度にメリハリをつけ、効果的な自組織に適した具体的な対策の決定を行うことが可能となる。こうした考え方は、柔軟で再現性があり、自組織におけるリスクの特定、評価及び管理について、より一層の強化に資するもので、これまで取り組んできているリスクマネジメントを更に発展させる狙いがある。

(2) 自組織に適した防護対策の具現化

内閣官房は、前号に示した重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンス等を整備する。これらガイダンス等は、関係主体が自組織に適した防護対策の実現に向けて、その改善を迅速かつ的確に行えるようパフォーマンスベースとし、達成状況が監視、測定可能なものとする。なお、これらガイダンス等は、自組織で活用するほか、必要に応じて関係業界や、重要インフラ所管省庁等とともに改善していくなど考慮するものとする。

(3) リスクマネジメントに関するこれまでの取組の継続

重要インフラ事業者等は、自組織におけるリスクマネジメントの各取組が自組織に適した防護対策の実現等に有効かつ効果的に機能しているかどうか、自組織が主体的に行う監査等の取組において、継続して確認する必要がある。

内閣官房は、重要インフラ事業者等に対してセプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会を引き続き充実させる。また、内閣官房は、東京大会に向けて官民が連携してリスクマネジメントの取組を進めたことなどにより、東京大会の円滑な運営に寄与した。こうした経験やノウハウについて、重要インフラ事業者等に対しても積極的に活用することとし、その具体的な手法や手順についての検討を行う。

4.2 環境変化におけるリスク把握

サイバー空間において提供される多様なサービスは、サプライチェーンの複雑化等に伴い、関係主体間での「相互連関・連鎖性」が一層深化していくことが想定される。さらに、コロナ禍等により不連続な形で起こる変化は、予期しない形でリスクを顕在化させるおそれがあり、社会を取り巻く環境は常に変化していることを認識する必要がある。そのため、社会全体としての対処の最適化を目指すために環境変化に対するリスクを把握することが求められる。

内閣官房は、以下のとおり、環境変化に対するリスクの把握及び「相互連関・連鎖性」の把握に関する調査を実施し、その結果等については、重要インフラ事業者等に提供する。あわせて、本行動計画の取組の改善に活用する。

(1) 環境変化調査

デジタル改革を踏まえたDXの進展によるサイバー空間の変容は、従来では想定し得なかったリスクも同様に拡大し得る。内閣官房は、中長期的な重要インフラ分野への浸透が予想される新しい技術・システムや関連する制度等を対象として、環境変化の実態調査及び環境変化に伴う新たなリスク源・リスクの分析を行う。また、当該調査・分析は、時間経過や環境変化に応じて行うことでより良い結果を得られることから、その対象や範囲を柔軟に捉えつつ、継続的に行う。

(2) 相互依存性調査

内閣官房は、分野を越えたリスクを把握するといった重要インフラ事業者等の抱える課題を払拭すべく、重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を実施する。相互依存性に関する調査の実施に当たっては、内閣官房、重要インフラ所管省庁、重要インフラ事業者等が互いに必要な情報を連携し、協力して活動を進める必要があり、内閣官房は、相互依存性の解析について、より有効な手法、手順について整理する。

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の動向が刻々と変化する中、国全体のサイバーセキュリティに関する水準を向上させるためには、国民一人一人がサイバーセキュリティに対する意識を高めていくとともに、重要インフラ事業者等における障害対応体制の強化や、幅広い層に向けた人材育成等を通して、我が国のサイバーセキュリティ全体の底上げを進めることが重要である。

サイバーセキュリティの有効性の確保に向けては、図１「重要インフラ事業者等の対策例」と「政府機関等の施策例」で示したとおり、基本方針の策定、人材育成・キャリアパスの整備・人材配置、サイバーセキュリティの確保に向けた取組状況の対外説明、環境変化に伴う新たなリスク源・リスクに対する課題抽出等、本行動計画の全体を支える共通基盤的な取組の強化が必要である。

このため、本行動計画期間においては、内閣官房は、重要インフラ分野全体における障害対応体制の有効性の検証や、重要インフラ防護能力の維持・向上に資する人材育成を推進するとともに、第4次行動計画に引き続き、「セキュリティ・バイ・デザイン」の推進、国際連携、他の関係主体と協力しつつ広報広聴活動等に取り組む。

特に、障害対応体制の有効性検証においては、内閣官房が分野横断的演習を実施することで、関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくことを目指す。

さらに、本行動計画の他施策に資することを目的に、本施策の実施にて得た知見を他施策に提供していく。

5.1 障害対応体制の有効性検証

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

内閣官房は、重要インフラサービスの継続的提供の強靭性の確保を念頭に、引き続き、分野横断的演習を実施する。分野横断的演習は、内閣官房と重要インフラ所管省庁等が連携して実施し、重要インフラ事業者等に対して組織全体の障害対応体制の有効性を継続的に検証・改善する機会として提供する。

(1) 分野横断的演習による障害対応体制の改善

内閣官房は、重要インフラ事業者等が日頃より強化に取り組む障害対応体制を意識した演習を準備することで、重要インフラ事業者等の障害対応体制に対してその有効性の検証を行う。演習の準備では、これまでの演習運営を通じて得た知見・課題、他施策や重要インフラサービス障害を引き起こす要因であるリスク源に係る最新動向等を踏まえ

つつ、重要インフラ事業者等が職務・役職横断的に実施する演習シナリオを企画する。

なお、重要インフラ事業者等による自主的な取組を促すことを目的に、分野横断的演習の一部を疑似的に体験できる演習プログラム等の提供に取り組む。

また、障害対応体制の強化に資することを目的に、演習を通じて得た知見・課題を参考資料として本行動計画の他施策に提供する。

重要インフラ事業者等においては、演習への備えとして自組織におけるリスク等の把握に努め、演習に参加し、その事後においては、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマネジメント等が有効に機能しているかの見直しとその改善に取り組む必要がある。このため、重要インフラ事業者等は、分野横断的演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証・改善することが期待される。また、重要インフラ事業者等は、有効性検証を円滑に行うことを目的に、分野横断的演習のシナリオ・実施方法・検証課題等の企画、分野横断的演習の実施への協力が期待される。

(2) 重要インフラ全体への分野横断的演習の成果の浸透

内閣官房は、これまでの演習において蓄積してきた演習参加者におけるグッドプラクティスや、演習中における反省点等を共有し、更なる重要インフラ全体への演習成果の普及・浸透を行う。

また、各重要インフラ分野から重要インフラ事業者等の演習参加を促進することを目的に、演習中の役割等を経験することで得られるメリットや、演習参加における事前準備、事後の改善の場面を通じて経営層との対話の機会としても有効に活用できる等といったメリットの説明資料についても作成・公表する。

(3) 重要インフラ所管省庁等との連携

重要インフラ所管省庁やISAC等の民間機関が実施する重要インフラ防護に資する演習・訓練は、内閣官房が実施する分野横断的演習と期待される効果が異なるが、それぞれが実施する演習における主な対象者や検証目的の明確化及び相互連携の在り方等を踏まえつつ、必要に応じて分野横断的演習と相互に連携・補完しながら実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図っていくことが期待される。

なお、重要インフラサービス障害対応に当たっては、各府省庁や各重要インフラ事業者等のサイバーセキュリティを担当する部門だけでなく防災・危機管理部門との情報共有を要する可能性もあるため、内閣官房及び重要インフラ所管省庁は、関係主体からのニーズも踏まえ、必要に応じて当該部門との連携に取り組む。

さらに、重要システムの維持に密接に関連する関係主体、重要インフラサービスを支える重要インフラ分野以外の事業者等の参画も視野に入れた演習の企画立案に取り組む。

5.2 人材育成等の推進

関係主体において、サイバーセキュリティ戦略(令和3年9月28日閣議決定)等に基づく取組を推進する。具体的には、人材育成に関する次の施策を講じる。

(1) 戦略マネジメント層の育成

サイバー攻撃が複雑化・巧妙化する中、重要インフラ事業者等が任務保証を実現するためには、組織全体を通じたサイバーセキュリティへの意識の底上げと組織内の適切な連携が重要となる。

内閣官房は、組織に応じたセキュリティ管理策の実装や、障害対応体制の強化における組織統治の必要性について意識を高めていくとともに、障害対応体制改善のプロセス等を通して、サイバーセキュリティ関連のリスクに起因する経営・事業上の脅威に対するマネジメントや、経営層等と緊密な連携を行えるよう、戦略マネジメント層の育成を推進する。

(2) 部門間連携の推進

昨今の制御システムを対象とする攻撃等の脅威を鑑み、ITの管理部門に限らず、OTの管理部門や法務部門、広報部門等においてもサイバーセキュリティの確保の必要性を意識することが重要である。

内閣官房は、様々な役割や能力を持つ人材が組織横断的に連携し、サイバーセキュリティの確保を可能とする体制の構築を推進する。

重要インフラ事業者等においては、体制の構築に当たり、組織内の人事異動や配置の状況等を踏まえ、組織全体を通じたサイバーセキュリティへの意識の浸透及び底上げに取り組むことが期待される。

(3) 産学官の連携の推進

内閣官房は、産学官が互いに連携し、必要なセキュリティ人材像の定義、実践的な対処能力を持つ実務者層・技術者層の育成、サイバーセキュリティに係る演習・訓練、資格取得等の具体的な人材育成策を推進する。重要インフラ事業者等においては、自組織のセキュリティ人材が幅広く知見を得られるよう、組織内の活動以外でも、様々な演習・訓練や情報共有の機会等を積極的に活用することが期待される。

5.3 「セキュリティ・バイ・デザイン」の推進

安全・安心なIoT環境を実現していくためには、システムのライフサイクル(企画・設計・開発・運用・廃棄)における企画段階からサイバーセキュリティの観点を意識し、システム仕様にセキュリティ要件を適切に組み込むことが求められる。昨今新たなITビジネスの展開において重大なセキュリティインシデントが繰り返し発生していること等を踏まえ、サイバーセキュリティを業務、製品・サービス等のシステムの企画・設計段階

から確保する「セキュリティ・バイ・デザイン」の実装が必須となっている。

内閣官房は、新たなビジネス展開時に「セキュリティ・バイ・デザイン」が実装できるよう考え方の普及に努めるとともに、重要インフラ事業者等において的確な情報収集及び知見の活用が可能な組織体制の整備に加え、「セキュリティ・バイ・デザイン」の良好事例の共有を推進する。

また、各重要インフラ事業者等においては、「セキュリティ・バイ・デザイン」の実装を念頭に置き、システムのライフサイクル全般にわたりサイバーセキュリティの確保に向けた取組を実践することが期待される。

5.4 国際連携の推進

国際社会の変化の加速化・複雑化が進展している中で、高度なサイバー能力を有する組織等が他国の重要インフラへのサイバー攻撃を行ったとされている事例が指摘される等、国際的な観点からもサイバー空間における脅威が高まっている。このような中で、各国において同盟国・同志国との協力・連携を強化する重要性が認識されている。

このため、内閣官房は、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携して、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進する。具体的には、我が国の分野横断的演習の取組紹介、米豪印やASEAN等との多国間の枠組みや米国その他同志国等との二国間による協議、CSIRT間連携や海外のサイバーセキュリティ政策担当者向けの講演等を通じて、我が国の特徴的な施策を積極的に発信することにより、サイバー攻撃関連情報、海外の脅威情報、インシデント対応事例、ベストプラクティスの共有等の基盤となる協力関係を強化するとともに、国際的な重要インフラ防護能力の向上にも寄与する。これによって海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。

重要インフラ事業者等においては、国際連携を推進できる人材を確保し、サイバーセキュリティに係る取組の海外同業他社への展開や国際会議への参加等を通じた海外の動向把握、海外ISAC等との情報共有等により、多角的・多面的な国際連携に取り組むことが期待される。

5.5 サイバー犯罪対策等の強化

サイバー空間の公共空間化を踏まえ、サイバーセキュリティ戦略(令和3年9月28日閣議決定)では、サイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図るとされており、警察は、警察庁にサイバー事案に係る政策を一元的に担うサイバー警察局と国の捜査部隊としてのサイバー特別捜査隊を創設し、地域に密着した活動を展開する都道府県警察と合わせて警察全体としてセキュリティ確保に向けた取組を推進している。

内閣官房は、警察庁と連携し、警察による重要インフラ事業者等との協力等の必要な取組を支援し、重要インフラ事業者等を取り巻くサイバー空間の安全性・信頼性の確保

を図る。

5.6 デジタル庁と連携したセキュリティ確保

デジタル庁の設置に伴いデジタル社会の形成が進む一方で、クラウド技術やゼロトラストアーキテクチャーに対応したサイバーセキュリティに対する意識の向上や、サイバー空間を構成する技術基盤やデータ等に対する信頼の醸成も重要となる。

内閣官房は、デジタル庁と連携し、先進的でセキュリティ確保が適切に講じられた重要インフラサービスの提供の実現や、地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の必要な取組を行う。

5.7 広報広聴活動の推進

(1) 国民へのわかりやすい情報発信

重要インフラサービス障害の影響を可能な限り極小化するためには、重要インフラ事業者等によるサイバーセキュリティの水準の向上のみならず、サプライチェーンを担うその他の企業や国民を含め社会全体が状況を踏まえて冷静に対応できることも重要である。このため、関係主体は、国民による冷静な対応に資することを目的に、行動計画の枠組みや取組について国民への積極的な発信を行う。

内閣官房は、Webサイト、SNS、ニュースレター、講演等を通じ、本行動計画の取組を広く認識・理解し得るよう引き続き努めるとともに、より効果的な広報チャネルや、より国民にとってわかりやすい発信の在り方についても検討を進める。

(2) 関連文書及び関連規格の整備

重要インフラのサイバーセキュリティの有効性の確保において、関係主体がその検討を行う上で、関連文書や関連規格を必要なときに参照できるようにすることが重要である。

このため、内閣官房は、重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的とした重要インフラ防護に係る関連規程集の発行や、他の関係主体との協力の下、国内外で策定される関連規格の整理及び明示を行う。

(3) 広聴活動の推進

デジタル経済の浸透及びデジタル改革の推進に伴い、新たな技術の活用や、新たなデジタルサービスが次々と生み出され社会に浸透していく一方で、サイバー攻撃の組織化・洗練化や、その手法が多様に変化・高度化していくこと等が考えられる。

内閣官房は、このように複雑化・巧妙化するサイバー攻撃への適切な対応を推進するため、各種調査やセミナー等を通じて各分野の状況把握や技術動向等の情報収集に努め、随時施策に反映させる。

V. 関係主体において取り組むべき事項

1. 内閣官房

(1)「障害対応体制の強化」に関する事項

① 組織統治の在り方について規定化。

② 重要インフラ事業者等のBCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。

③ 重要インフラ事業者等におけるISAC等のインシデント情報共有・分析機能を有する機関等活用の推進。

④ 脅威の検知・調査・分析に関する能力の向上。

⑤ 防御力、抑止力、状況把握力の向上。

⑥ 任務保証のための「面としての防護」を念頭に、サプライチェーンを含めた防護範囲見直しの取組を継続するとともに、関係府省庁(重要インフラ所管省庁に限らない)の取組に対する協力・提案を継続。

(2)「安全基準等の整備及び浸透」に関する事項

① 本行動計画で掲げられた各施策の推進に資するよう、安全基準等策定指針の改定を実施し、その結果を公表。

② 必要に応じて社会動向の変化及び新たに得た知見を踏まえてガイダンス等の関連文書を適時に改定し、その結果を公表。

③ 上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。

④ 重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。

⑤ 重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査を実施し、結果を公表。重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を速やかに検討し具現化。

⑥ 上記⑤の調査結果を、本行動計画の各施策の改善に活用。

⑦ 安全基準等の整備に係る文書一覧について整理し、文書間の関係性を明確化。

(3)「情報共有体制の強化」に関する事項

① 通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運営及び必要に応じた見直し。

② 重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供。

③ 国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっ

ているサイバーセキュリティ関係機関との協力。

④ サイバーセキュリティ基本法に規定する勧告等の仕組みを適切に運用。

⑤ 重要インフラサービス障害に係る情報及び脅威や脆弱性情報を分野横断的に集約する仕組みの構築を進め、運用に必要となる資源を確保。

⑥ ナショナルサート の枠組みの強化の検討との整合性保持

⑦ 重要インフラ所管省庁の協力を得つつ、各セプターの機能・活動状況等を把握するための定期的な調査・ヒアリング等の実施、先導的なセプター活動の紹介。

⑧ 情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。

⑨ セプターカウンシルに参加するセプターと連携し、セプターカウンシルの運営及び活動に対する支援の実施。

⑩ セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の整備。

⑪ 必要に応じてサイバー空間関連事業者との連携を個別に構築し、重要インフラサービス障害発生時に適時適切な情報提供を実施。

⑫ 新たに情報共有範囲の対象となる重要インフラ分野内外の事業者に対する適時適切な情報提供の実施。

⑬ 重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプターの情報疎通機能の確認(セプター訓練)等の機会を提供。

(4) 「リスクマネジメントの活用」に関する事項

① 重要インフラ事業者等におけるリスクアセスメントへの利活用のための既存の手引書の見直し及び新たなガイダンス等の作成。

② 重要インフラ事業者等に対して、セプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会の提供。

③ 東京大会の経験やノウハウについて、重要インフラ事業者等に対する積極的な活用及びその具体的な手法・手順について検討。

④ 本施策における調査等の結果を重要インフラ事業者等におけるリスクマネジメントの実施や安全基準等の整備等に反映する参考資料として提供。

⑤ 本施策における調査等の結果を本行動計画の他施策に反映する参考資料として利活用。

(5) 「防護基盤の強化」に関する事項

① 障害対応体制の有効性の検証が可能な分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。

② 職務・役職横断的な全社的に行う演習シナリオを企画。

③ 分野横断的演習の改善策の検討。
④ 重要インフラ事業者等による自主的な取組を促すため、分野横断的演習の一部を疑似的に体験できる演習プログラム等を提供。
⑤ 分野横断的演習の機会を活用して、障害対応体制の有効性の検証等を実施。
⑥ 分野横断的演習で得られた重要インフラ防護に関する知見の普及・浸透。
⑦ 他省庁や民間機関の重要インフラサービス障害対応の演習・訓練の情報を把握し、連携の在り方を検討。
⑧ 戦略マネジメント層の育成、部門間連携、産学官の連携等による人材育成等の推進。
⑨ 重要インフラ事業者等に対する「セキュリティ・バイ・デザイン」の実装の推進。
⑩ 各国政府等との協力・連携を強化し、知見の共有や能力構築支援等の推進。
⑪ 警察庁と連携し、警察による重要インフラ事業者等との協力等の必要な取組を支援。
⑫ デジタル庁と連携し、先進的でセキュリティ確保が適切に講じられた重要インフラサービスの提供の実現や、地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の必要な取組を実施。
⑬ Webサイト、SNS、ニュースレター及び講演会を通じた広報を実施。
⑭ 重要インフラ防護に係る関連規定集の発行及び関連規格の整理、可視化。
⑮ 各種調査やセミナー等を通じた広聴を実施。

2. 重要インフラ所管省庁

(1) 「障害対応体制の強化」に関する事項

① 重要インフラ事業者等のBCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。
② 脅威の検知・調査・分析に関する能力の向上。
③ 防御力、抑止力、状況把握力の向上。
④ 任務保証のための「面としての防護」を確保するための取組を継続。
⑤ 重要インフラ分野内において実際に取組を行う対象である「重要インフラ事業者等」の範囲について継続的に見直し。

(2) 「安全基準等の整備及び浸透」に関する事項

① 安全基準等策定指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。
② 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。
③ 重要インフラ分野ごとの安全基準等の分析・検証を支援。
④ 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等

の浸透に向けた取組を実施。

⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。

⑥ 毎年、内閣官房が実施する重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査方法の検討及び実施に協力。

(3) 「情報共有体制の強化」に関する事項

① 内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

② 重要インフラ事業者等との緊密な情報共有体制の維持と必要に応じた見直し。

③ 重要インフラ事業者等からのシステムの不具合等に関する情報の内閣官房への確実な連絡。

④ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。

⑤ セプターの機能充実への支援。

⑥ セプターカウンシルへの支援。

⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。

⑧ セプター事務局や重要インフラ事業者等における情報共有に関する活動への協力。

⑨ 内閣官房が情報疎通機能の確認(セプター訓練)等の機会を提供する場合の協力。

(4) 「リスクマネジメントの活用」に関する事項

① リスクアセスメントの実施に際し、内閣官房、重要インフラ事業者等その他の関係主体が実施する取組への協力。

② 内閣官房により提供されたガイダンス等の重要インフラ事業者等への展開その他リスクアセスメントの浸透に資する内閣官房への必要な協力。

③ 重要インフラ事業者等のリスクコミュニケーションの支援。

④ 重要インフラ事業者等が実施するモニタリング及びレビューの必要に応じた支援。

⑤ 本施策における調査等に関し、当該調査等に関する情報及び必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査・分析が本施策における調査等と関連する場合には、必要に応じて内閣官房と連携。

⑥ 本施策における調査等を施策へ活用。

(5) 「防護基盤の強化」に関する事項

① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。

② セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。

③ 分野横断的演習への参加。

④ 必要に応じて、分野横断的演習成果を施策へ活用。
⑤ 分野横断的演習の改善策の検討への協力。
⑥ 分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。
⑦ サイバーセキュリティに係る演習や教育等により、サイバーセキュリティ人材の育成を支援。
⑧ 重要インフラ事業者等に対する「セキュリティ・バイ・デザイン」の実装の推進。
⑨ 内閣官房と連携し、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進。
⑩ 内閣官房と連携し、関連規格の整理、可視化。

3. サイバーセキュリティ関係省庁

(1) 「障害対応体制の強化」に関する事項

① 脅威の検知・調査・分析に関する能力の向上。
② 防御力、抑止力、状況把握力の向上。

(2) 「情報共有体制の強化」に関する事項

① 内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。
② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。
③ セプターカウンシル等からの要望があった場合、意見交換等を実施。

4. 事案対処省庁及び防災関係府省庁

(1) 「障害対応体制の強化」に関する事項

① 脅威の検知・調査・分析に関する能力の向上。
② 防御力、抑止力、状況把握力の向上。

(2) 「情報共有体制の強化」に関する事項

① 内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。
② 被災情報、テロ関連情報等の収集。
③ 内閣官房に対して、必要に応じて情報連絡の実施。
④ セプターカウンシル等からの要望があった場合、意見交換等を実施。

(3) 「防護基盤の強化」に関する事項

① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施

への協力。

② 重要インフラ事業者等からの要望があった場合、重要インフラサービス障害対応能力を高めるための支援策を実施。

③ 分野横断的演習の改善策の検討への協力。

④ 必要に応じて、分野横断的演習と事案対処省庁及び防災関係府省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。

5. 重要インフラ事業者等

(1) 「障害対応体制の強化」に関する事項

① 経営層、CISO、戦略マネジメント層、システム担当者の役割と責任に基づく、組織一丸となった対応。

② リスクマネジメントと危機管理の一体的な対応。

③ BCP及びIT-BCP 、CSIRT等、インシデントの発生時に対処できる体制の整備。

④ 日々の運用で、発見した脅威や脆弱性を払拭するような管理策の実施。

⑤ 自組織に有効的と考えられる監査の実施とその結果の活用。

(2) 「安全基準等の整備及び浸透」に関する事項

① 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。

② 自らが安全基準等の策定主体である場合は、毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。

③ 安全基準等を踏まえ、サイバーセキュリティの確保の取組やそのための環境整備を検討。

④ サイバーセキュリティの確保の現状について自己評価を行い、自組織における本来あるべき状況や要件との差異を分析すること、さらに、分析結果をもとに自組織に不足している対策の優先順位付けとその実施を繰り返すことによる安全基準等の継続的改善。

⑤ 毎年、内閣官房が実施する調査に協力。

(3) 「情報共有体制の強化」に関する事項

① セプターカウンシル、セプター、重要インフラ所管省庁及び内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

② システムの不具合等に関する情報連絡を実施。

③ 攻撃手法及び復旧手法に関する情報等の収集。

④ サイバーセキュリティ関係機関との合意に基づく補完的な情報共有。

⑤ セプターカウンシルにおける活動の実施。

⑥ 内閣官房が提供する情報疎通機能の確認(セプター訓練)等を活用するなどして、自らの情報共有体制を強化。

(4) 「リスクマネジメントの活用」に関する事項

① 自組織に適した防護対策について、計画、実施、評価、改善(PDCA)のサイクルを繰り返し、継続的な改善の実施。

② 自組織が直面するリスクとその程度の把握及び自組織の重要インフラサービス提供に係る特性(プロファイル)の明確化に着手。

③ 自組織におけるリスクマネジメントの各取組が自組織に適した防護対策の実現等に有効かつ効果的に機能しているかどうか、自組織が主体的に行う監査等の取組において、継続した確認の実施。

④ セプターカウンシルへの参加や分野横断的演習等を活用し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの充実。

⑤ 本施策における調査等に関し、当該調査等に関する情報及び必要な情報の内閣官房への提供等の協力。

⑥ 本施策における調査等の結果として提供される情報の自組織のリスクマネジメントへの活用。

(5) 「防護基盤の強化」に関する事項

① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。

② 分野横断的演習への備えとして、自組織におけるリスク等の把握を実施。

③ 分野横断的演習への参加。

④ 分野横断的演習の事後において、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマネジメント等が有効に機能しているかの見直しとその改善を実施。

⑤ 分野横断的演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証し改善を実施。

⑥ 分野横断的演習の改善策の検討への協力。

⑦ 組織内の人事異動や配置の状況等を踏まえた、組織全体を通じたサイバーセキュリティへの意識の浸透及び底上げに資する人材育成。

⑧ 自組織のセキュリティ人材が幅広く知見を得られる人材育成。

⑨ 「セキュリティ・バイ・デザイン」の実装を念頭に置いたシステムのライフサイクル全般にわたるサイバーセキュリティの確保。

⑩ 国際連携を推進できる人材を確保し、サイバーセキュリティに係る取組の海外同業他社への展開や海外の動向把握等により、多角的・多面的な国際連携を促進。

⑪ 内閣官房と連携し、関連規格の整理、可視化。

6. セプター及びセプター事務局

(1) 「障害対応体制の強化」に関する事項

① 任務保証のための「面としての防護」を念頭に、サプライチェーンを含めた防護範囲見直しの取組に対する積極的な協力。

(2) 「情報共有体制の強化」に関する事項

① セプターカウンシル、重要インフラ事業者等、重要インフラ所管省庁及び内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

② 内閣官房等からの情報提供について、セプター内の情報取扱いルールにのっとって重要インフラ事業者等への情報提供を実施。

③ 重要インフラ事業者等からの情報連絡について、必要に応じてセプター事務局で匿名化等を行った上で重要インフラ所管省庁に報告するとともに、セプター構成員への展開等、情報共有体制を強化。

④ サイバーセキュリティ関係機関との合意に基づく補完的な情報共有の実施。

⑤ セプターの機能強化・充実。

⑥ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。

⑦ セプターカウンシルへの参加。

⑧ 情報疎通機能の定期的な確認。

(3) 「リスクマネジメントの活用」に関する事項

① 自セプターを構成する重要インフラ事業者等の主体的な取組を支援。また、必要に応じて、内閣官房、重要インフラ所管省庁、他のセプターその他の関係主体への協力。

(4) 「防護基盤の強化」に関する事項

① 重要インフラ事業者等の分野横断的演習への参加を支援。

② 必要に応じて分野横断的演習への参加。

③ 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開を支援。

7. セプターカウンシル

(1) 「情報共有体制の強化」に関する事項

① 各セプターと連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

② 共有対象とする情報及びその共有方法の整理の実施。

③ 相互理解及びベストプラクティス等の具体的な事例の共有による分野横断的な情報共有の推進。

④ 関係主体との協力関係を深めるため、政府機関等からの要請又は自らの発意により、両者の状況認識等の共有を進めるための意見交換等の実施。

(2) 「防護基盤の強化」に関する事項

① 必要に応じて分野横断的演習への参加。

8. サイバーセキュリティ関係機関

(1) 「情報共有体制の強化」に関する事項

① 内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。

② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。

③ 重要インフラ事業者等又はセプターとの合意に基づく補完的な情報共有に加え、連絡元の了解が得られた場合は匿名化等を行った上で関係主体との間でも情報共有を実施。

④ 内閣官房が実施する分析機能の強化の検討に対しての協力。

⑤ セプターカウンシルから要望があった場合、意見交換等を実施。

(2) 「リスクマネジメントの活用」に関する事項

① 自セプターを構成する重要インフラ事業者等の主体的な取組を支援。また、必要に応じて、内閣官房、重要インフラ所管省庁、他のセプターその他の関係主体への協力。

(3) 「防護基盤の強化」に関する事項

① 分野横断的演習に必要となる重要インフラサービス障害の事例等に関する情報を内閣官房に提供。

② 内閣官房と連携し、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進。

9. サイバー空間関連事業者

(1) 「情報共有体制の強化」に関する事項

① 内閣官房が行う共有対象とする情報とその共有方法を整理するための取組に対する協力。

② 内閣官房に対して、通常時及び大規模重要インフラサービス障害対応時における積極的な情報連絡の実施。

VI. 評価・検証

本行動計画の評価・検証は、次の二つの視点で行う。

○「成果(アウトカム)を測る視点」からの評価

本行動計画に基づく取組を通じて、社会が実際にどの程度「理想とする将来像」に近付いたのかという視点での評価を行う。本行動計画の「評価」とは、「理想とする将来像」に照らして本行動計画に基づく取組の妥当性を確認し、施策の改善に向けた課題の抽出を行うことをいう。

○「結果(アウトプット)を測る視点」からの検証

本行動計画に基づく取組を着実に進め、また継続的に改善させていくために、各取組がどのような結果をもたらしたのかという視点での検証を行う。本行動計画の「検証」とは、各年度において各取組の進捗状況に係る客観的事実を確認し、翌年度以後の取組の方針を定めることをいう。

1. 本行動計画の評価

1.1 評価運営

「成果(アウトカム)を測る視点」からの評価(本行動計画の評価)は、「Ⅰ. 総論　2. 理想とする将来像」に照らして行う。この際、本行動計画に基づく様々な取組が相互に関連して成果をなすものであることを考慮し、本行動計画の施策それぞれに対して行うのではなく、重要インフラ防護に資する取組の全体、すなわち本行動計画の枠組みに対して総合的に行うこととする。

なお、本行動計画の評価は、サイバーセキュリティ戦略本部が実施し、そのために必要な調査・検討は重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行うものとする。

行動計画の評価運営は、行動計画の性質上、毎年の変化を追っても直ちに改善策を検討することが困難であることから、3 年に 1 度の実施を原則とする。また、社会動向の大きな変化等、本行動計画が想定し得なかった事象が発生した場合は、3 年に 1 度の実施は、その限りとしない。

1.2 補完調査

本行動計画の評価を行う際には、各施策群の個別の成果からは把握しきれない状況についても適切に把握し、総合的な評価を行うことが重要である。このため、補完的な情報を収集するための調査を原則として各年度において実施する。なお、調査結果については、可能な範囲で公表する。

2. 本行動計画の検証

2.1 検証運営

「結果(アウトプット)を測る視点」からの検証(各年度における進捗状況の確認)は、「Ⅳ. 計画期間内の取組」に示した施策群ごと(以下「本行動計画の各施策」という。)に、その進捗状況の確認として行う。

なお、本行動計画の検証は、サイバーセキュリティ戦略本部の主管の下、重要インフラ事業者等及び重要インフラ所管省庁の協力を得て各年度に内閣官房が行い、重要インフラ専門調査会での審議を経て、サイバーセキュリティ戦略本部に付議するものとする。

2.2 「重要インフラ事業者等による対策」の検証

重要インフラ事業者等は、重要インフラサービスの安全かつ持続的な提供に責任を負うものとして、日々サイバーセキュリティの確保に取り組んでいる。この取組を継続し、かつ、着実な改善を期すために、また重要インフラ事業者等の取組に対する政府の支援策をより効果的なものへと改善させていくためには、サイバーセキュリティの確保の結果を客観的に検証することが重要である。

対策の結果検証は、重要インフラ防護の目的である「重要インフラサービスの安全かつ持続的な提供を実現すること」を踏まえ、重要インフラ分野ごとの重要インフラサービス障害への対策・対応状況を検証することとする。

なお、「重要インフラ事業者等による対策」の評価については、個別の重要インフラ事業者等の取組は各々の経営判断に基づく自主的な取組を含むものである以上、各々の重要インフラ事業者等が自ら改善に取り組むことが適当である。また、重要インフラ事業者等は、重要インフラサービス障害への対策の状況を検証するとともに、実際に重要インフラサービス障害を被った場合には、その重要インフラサービス障害への対処の内容を自己評価し、可能であれば、これらの実施状況を明らかにすることが望ましい。

2.3 「政府機関等による施策」の検証

本行動計画の政府機関等による各施策は、いずれも重要インフラ事業者等におけるサイバーセキュリティに関し、自主的な取組の促進その他の必要な施策を講ずるものである。

施策の結果検証は、重要インフラ事業者等によるサイバーセキュリティの確保に対する本行動計画の各施策による寄与の状況を検証することとする。

VII. 本行動計画の見直し

本行動計画の見直しは、本行動計画の評価を踏まえ、サイバーセキュリティ戦略本部において実施し、そのために必要な調査・検討は、重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行う。

行動計画の見直しについては、行動計画の評価と併せて3年に1度の実施を原則としているが、社会動向の大きな変化等、本行動計画が想定し得なかった事象が発生した場合は、その限りでない。

別添：情報連絡・情報提供について

1. システムの不具合等に関する情報

重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システム[6]の不具合等に関する情報」という。）には、①重要インフラサービス障害の未然防止、②重要インフラサービス障害の拡大防止・迅速な復旧、③重要インフラサービス障害の原因等の分析・検証による再発防止の３つの側面が含まれ、政府機関等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間及び相互依存性のある重要インフラ分野間においてはこうした情報を共有する体制を強化することが必要である。なお、予兆・ヒヤリハットでは事象が顕在化していないものの、顕在化した際には複数の重要インフラ分野や重要インフラ事業者等の重要インフラサービス障害に至ることも考えられることから、システムの不具合と同様に、情報共有の対象とすることが必要である。

したがって、本行動計画における情報共有の範囲は、図に示すものとする。

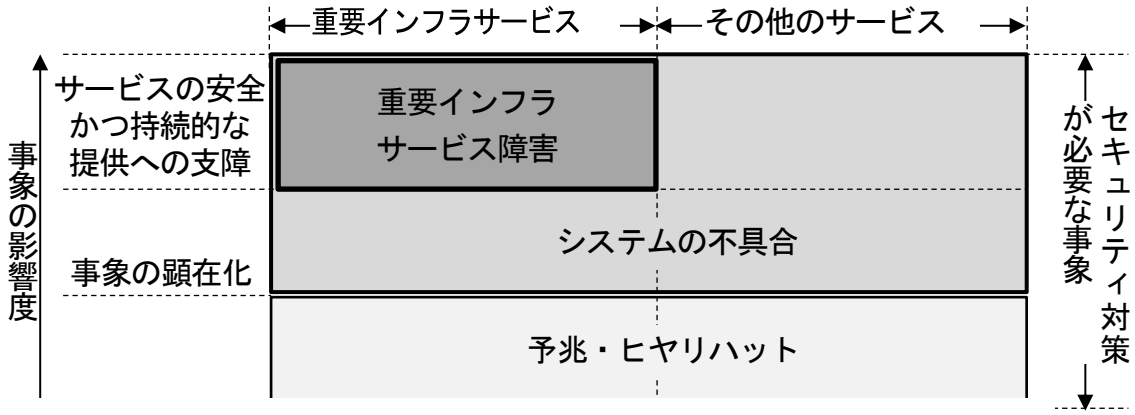


図　情報共有の対象範囲

[6] ここでいうシステムには、いわゆる情報系システムに限らず、各重要インフラ分野のプラントやシステム監視等でも用いられる制御システムや、普及が進んでいる IoT 等も含まれることに留意。

2. 重要インフラ事業者等からの情報連絡

2.1 情報連絡を行う場合

システムの不具合等に関する情報[7]のうち、以下のいずれかのケースに該当する場合、重要インフラ事業者等は情報連絡を行うものとする。情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとし、全容が判明する前の断片的又は不確定なものであっても差し支えない。

① 法令等で重要インフラ所管省庁への報告が義務付けられている場合。
② 関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合。
③ そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合。

なお、上記に該当するかどうか不明な場合については、重要インフラ所管省庁又は内閣官房に対して相談することが望ましい。

2.2 情報連絡の仕組み

重要インフラ事業者等から重要インフラ所管省庁を通じて内閣官房に至る情報連絡の手順は以下のとおりとする。

① 重要インフラ事業者等は、「別紙３　情報連絡における事象と原因の類型」により当該事象とその原因を類型化した上で、「別紙４－１　情報共有体制(通常時)」及びその延長線上にある「別紙４－２　情報共有体制(大規模重要インフラサービス障害対応時)」に示す連絡体制に基づき重要インフラ所管省庁に連絡する。
② 重要インフラ所管省庁において所管分野ごとに選任された内閣官房併任者(リエゾン)は、該当分野の重要インフラ事業者等から受けた連絡を内閣官房に連絡する。
③ 内閣官房は、連絡された情報を適切に管理し、情報連絡元が指定する情報共有の可能な範囲で取り扱う。
④ 特に緊急性を有する場合には、①～②の手順にかかわらず、重要インフラ事業者等は重要インフラ所管省庁に連絡するとともに、内閣官房にも同報する。

なお、別紙4-1及び別紙4-2に示すとおり、予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象を報告する場合、重要インフラ事業者等はセプター事務局等を経由して情報連絡元の匿名化等を行った上で連絡することも可とする。

2.3 情報連絡された情報の取扱い

情報連絡された情報の取扱いについて、内閣官房及び連絡を受けた重要インフラ所管省庁は、法令等に定めがある場合又は連絡を行う重要インフラ事業者等の了承がある場合を除き開示しない。当該情報は、「行政機関の保有する情報の公開に関する法律(平成11年法律第42号)」第5条第2号ロに規定する情報として取り扱う(不開示情報)。なお、当該情報が同号ただし書に規定する情報[8]に該当する場合には、公開されることがある。また、「3.1 情報提供を行う場合」に該当する場合はこの限りではない。

[7] 重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報を指す。
[8] 人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報

3. 重要インフラ事業者等への情報提供

3.1 情報提供を行う場合

重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者及び重要インフラ事業者等から提供される幅広いシステムの不具合等に関する情報を集約、分析等した上で、以下のいずれかのケースに該当する場合、内閣官房は積極的に情報提供を行うものとする[9]。

① セキュリティホールやプログラム・バグ等に関する情報を入手した場合等であって、他の重要インフラ事業者等においてもその情報に関係する重大な問題を生じるおそれがあると認められる場合。

② サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合。

③ そのほか重要インフラ事業者等のサイバーセキュリティの確保に有効と考えられる場合。

なお、内閣官房では、情報の提供元が特定されないよう、情報を加工するなど、不利益を被らないための適切な措置を講じた上で情報提供を行う。

また、内閣官房から重要インフラ事業者等への情報提供の範囲は、情報の提供元があらかじめ示す情報共有可能な範囲のうち、内閣官房が当該情報に関係すると考える重要インフラ分野とする。なお、情報の提供元が示す情報共有可能な範囲を越えて情報共有する必要があると内閣官房が認める場合には、その共有範囲の変更について情報の提供元との間で調整を行う。

3.2 情報提供の仕組み

内閣官房から重要インフラ所管省庁を通じて重要インフラ事業者等に至る情報提供の手順は以下のとおりとする。

① 内閣官房が情報提供を行う場合は、重要インフラ所管省庁のリエゾンを通じて行う。その際、情報提供を受けた者が、その情報を容易に活用できるようにするため、重要度や内容等に応じた情報の分類及び取扱い範囲が一目で認識できるよう、適切な識別方法を設ける。

② 重要インフラ所管省庁のリエゾンはセプターの窓口(PoC)に対して情報を伝達する。

③ セプターは、セプターを構成する重要インフラ事業者等に対して情報を伝達する。

④ 早期警戒情報等であって特に緊急性を有する場合には、①～③の手順にかかわらず、内閣官房から直接セプター又は個別重要インフラ事業者等へ提供するとともに、重要インフラ所管省庁のリエゾンに同報する。ただし、識別方法の適正化については、①の手順に準ずる。

3.3 情報提供のための連携体制

内閣官房は、重要インフラ所管省庁を通じて重要インフラ事業者等に提供する情報の集約及び重要インフラ事業者等への情報提供において、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者

[9] 提供する情報については、情報を突き合わせることによる精度の向上、重要インフラ分野のサービス停止・低下が原因で発生した重要インフラサービス障害や各分野間に共通するリスク源により発生した重要インフラサービス障害に関する他の重要インフラ分野への影響予測を行うなど、質の向上を図る。

等と以下のとおり連携する。

① サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁及びサイバーセキュリティ関係機関から提供される幅広い情報の集約。

② サイバー空間関連事業者から必要に応じて、重要インフラサービス障害に関する付加情報等の集約。

③ 情報の集約・分析においては、必要に応じ、サイバーセキュリティ関係機関及びサイバー空間関連事業者に連携等を要請。

④ 大規模重要インフラサービス障害に関する情報については、通常時の情報共有体制に加え、内閣官房、事案対処省庁、防災関係府省庁から構成される情報共有体制の下で情報を集約及び共有。

別紙１　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野	対象となる重要インフラ事業者等(注１)	対象となる重要システム例(注２)
情報通信	・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融　銀行等 生命保険 損害保険 証券 資金決済	・銀行、信用金庫、信用組合、労働金庫、農業協同組合等 ・資金清算機関 ・電子債権記録機関 ・生命保険 ・損害保険 ・証券会社 ・金融商品取引所 ・振替機関 ・金融商品取引清算機関 ・主要な資金移動業者 ・主要な前払式支払手段(第三者型)発行者　　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・金融機関相互ネットワークシステム ・電子債権記録機関システム ・保険業務システム ・証券取引システム ・取引所システム ・振替システム ・清算システム
航空	・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
空港	・主要な空港・空港ビル事業者	・警戒警備・監視システム ・フライトインフォメーションシステム ・バゲージハンドリングシステム
鉄道	・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
ガス	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・地方公共団体	・地方公共団体の情報システム
医療	・医療機関 （ただし、小規模なものを除く。）	・診療録等管理システム ・診療業務支援システム ・地域医療支援システム
水道	・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム
物流	・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学	・主要な石油化学事業者	・プラント制御システム
クレジット	・主要なクレジットカード会社 ・主要な決済代行業者 ・指定信用情報機関　　等	・クレジット(包括信用購入あつせん及び二月払購入あつせん)に係る決済システム ・信用情報提供・収集システム
石油	・主要な石油精製・元売事業者	・受発注システム ・生産管理システム ・生産出荷システム
港湾	・主要な港湾運送事業者・港湾管理者等	・ターミナルオペレーションシステム（TOS）

注１　ここに掲げているものは、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びITへの依存度の進展等を踏まえ、対象とするものの見直しを行う。
注２　ここに掲げているものは、例であり全てではない。

別紙２　重要インフラサービスとサービス維持レベル

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
情報通信		・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること（電気通信事業法第2条）	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障	・電気通信事業法（業務停止等の報告）第28条 ・電気通信事業法施行規則（報告を要する重大な事故）第58条 【サービス維持レベル】 ・電気通信設備の故障により、役務提供の停止・品質の低下が、３万以上の利用者に対し２時間以上継続する事故が生じないこと
		・放送	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第113条、第122条 ・放送法施行規則（報告を要する重大な事故）第125条 【サービス維持レベル】 ・基幹放送設備の故障により、放送の停止が15分以上継続する事故が生じないこと ・特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が15分以上（中継局の無線設備にあっては、２時間以上）継続する事故が生じないこと
		・ケーブルテレビ	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第137条 ・放送法施行規則（報告を要する重大な事故）第157条 【サービス維持レベル】 ・有線一般放送の業務に用いられる電気通信設備の故障により、放送の停止を受けた利用者の数が３万以上、かつ、停止時間が２時間以上の事故が生じないこと
金融	銀行等	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ（銀行法第10条第1項第１号） ・資金の貸付け又は手形の割引（銀行法第10条第１項第２号） ・為替取引（銀行法第10条第１項第３号）	・預金の払戻しの遅延・停止 ・融資業務の遅延・停止 ・振込等資金移動の遅延・停止	・主要行等向けの総合的な監督指針 ・中小・地域金融機関向けの総合的な監督指針 ・系統金融機関向けの総合的な監督指針

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
		・資金清算	・資金清算（資金決済に関する法律第２条第10項）	・資金清算の遅延・停止	・清算・振替機関等向けの総合的な監督指針
		・電子記録等	・電子記録（電子記録債権法第56条） ・資金決済に関する情報提供（電子記録債権法第62条及び第63条）	・電子記録、資金決済に関する情報提供の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（12 電子債権記録機関関係）
	生命保険	・保険金等の支払	・保険金等の支払請求の受付（保険業法第97条第1項） ・保険金等の支払審査（保険業法第97条第1項） ・保険金等の支払（保険業法第97条第1項）	・保険金等の支払の遅延・停止	・保険会社向けの総合的な監督指針
	損害保険	・保険金等の支払	・事故受付（保険業法第97条第1項） ・損害調査等（保険業法第97条第1項） ・保険金等の支払（保険業法第97条第1項）	・保険金等の支払の遅延・停止	・保険会社向けの総合的な監督指針
	証券	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引（金融商品取引法第２条第８項第１号） ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理（金融商品取引法第２条第８項第２号） ・有価証券等清算取次ぎ（金融商品取引法第2条第８項第5号）	・有価証券売買等の遅延・停止	・金融商品取引業者等向けの総合的な監督指針
		・金融商品市場の開設	・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務（金融商品取引法第2条第14項及び第16項、第80条並びに第84条）	・有価証券の売買、市場デリバティブ取引等の遅延・停止	・金融商品取引所等に関する内閣府令第112条
		・振替業	・社債等の振替に関する業務（社債、株式等の振替に関する法律第８条）	・社債・株式等の振替等の遅延・停止	・社債、株式等の振替に関する法律（事故の報告）第19条 ・一般振替機関の監督に関する命令（事故）第17条 ・清算・振替機関等向けの総合的な監督指針

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
		・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
	資金決済	・資金移動業	・為替取引（資金決済に関する法律第２条第２項）	・決済サービスの遅延・停止 ・振込等資金移動の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（14資金移動業者関係）
		・第三者型前払式支払手段の発行	・第三者型前払式支払手段の発行（資金決済に関する法律第3条第1項及び第５項）	・決済サービスの遅延・停止	・事務ガイドライン第三分冊：金融会社関係（５前払式支払手段発行者関係）
航空		・旅客、貨物の航空輸送サービス ・予約、発券、搭乗・搭載手続 ・運航整備 ・飛行計画作成	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条） ・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・搭乗、航空貨物の搭載 ・航空機の点検・整備 ・飛行計画の作成、航空局への提出	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空分野における情報セキュリティ確保に係る安全ガイドライン
空港		・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港分野における情報セキュリティ確保に係る安全ガイドライン
鉄道		・旅客輸送サービス ・発券、入出場手続	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業（鉄道事業法第２条） ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告） 第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第5条 ・鉄道分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
電力	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条第１項第８号） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条第１項第14号）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第3条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス	・一般ガス導管事業 ・ガス製造事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項） ・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第2条第９項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第2条第2項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン
物流	・貨物自動車運送事業 ・船舶運航事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期にわたる製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	・クレジットサービス	・クレジット（包括信用購入あつせん及び二月払購入あつせん）に係る決済サービス（割賦販売法第2条第3項及び第35条の16第2項） ・特定信用情報提供業務（割賦販売法第35条の3の36）	・クレジットサービスの遅延・停止 ・カード情報又は信用情報の大規模漏えい	・割賦販売法（後払分野）に基づく監督の基本方針 ・クレジットCEPTOARにおける情報セキュリティガイドライン
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油分野における情報セキュリティ確保に係る安全ガイドライン
港湾	・TOSによるターミナルオペレーション	・陸上輸送によるコンテナ貨物の搬入・搬出、コンテナターミナル内におけるコンテナ貨物の一時保管、海上輸送のための船舶へのコンテナ貨物の積卸し	・荷捌きの効率低下、停止によるコンテナ貨物の搬入・搬出の停滞、停止	・港湾分野における情報セキュリティ確保に係る安全ガイドライン

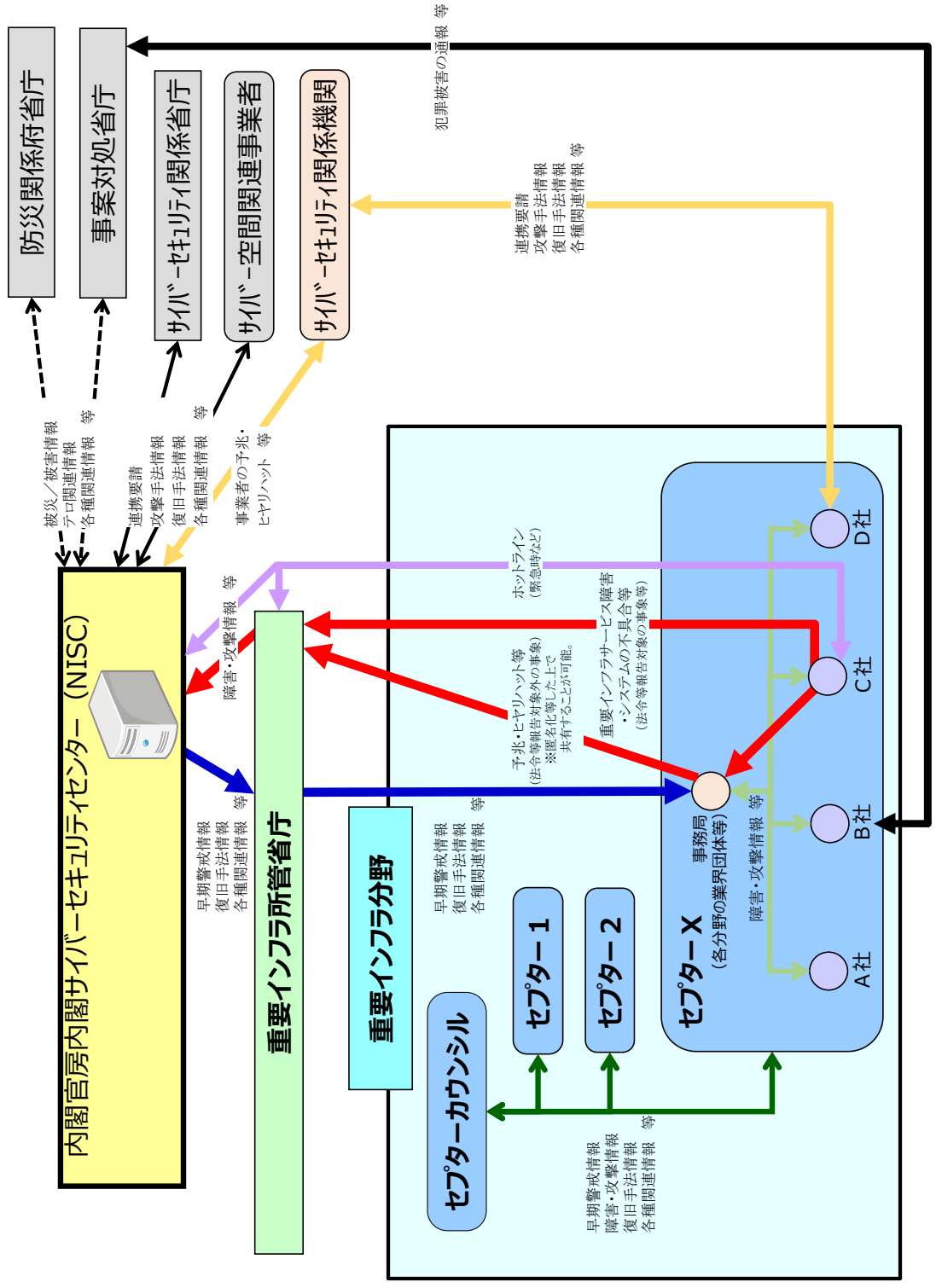
注１　ITを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。

別紙３　情報連絡における事象と原因の類型

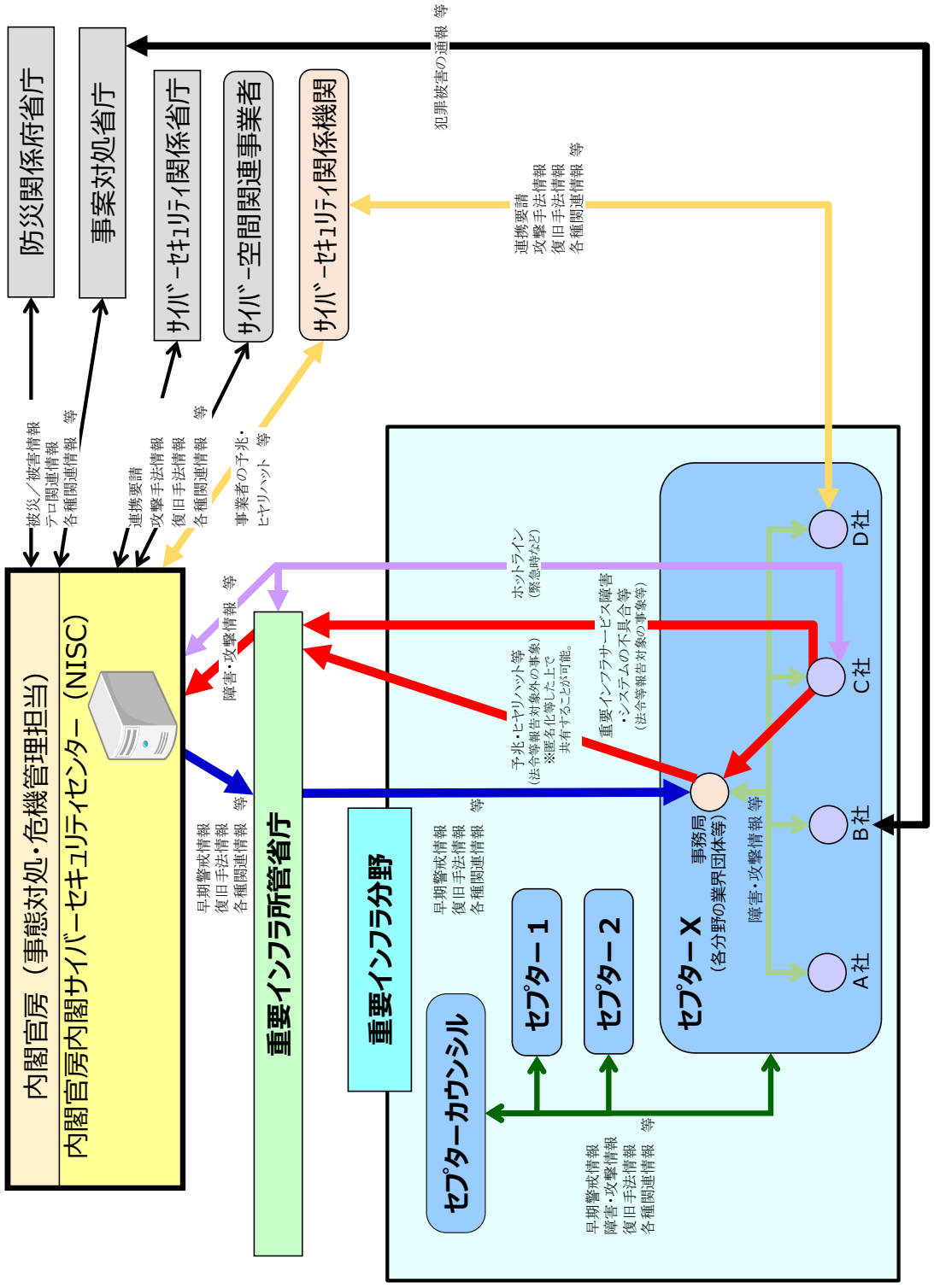
事象の類型		事象の例	説明
未発生の事象		予兆・ヒヤリハット	サイバー攻撃の予告などの予兆や、事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信などによるヒヤリハットの発生
発生した事象	機密性を脅かす事象	情報の漏えい	組織の機密情報等の流出など、機密性が脅かされる事象の発生
	完全性を脅かす事象	情報の破壊	Webサイト等の改ざんや組織の機密情報等の破壊など、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やWebサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記につながる事象	マルウェア等の感染	マルウェア等によるシステム等への感染
		不正コード等の実行	システム脆弱性等をついた不正コード等の実行
		システム等への侵入	外部からのサイバー攻撃等によるシステム等への侵入
		その他	上記以外の事象

原因の類型	原因の例
意図的な原因	不審メール等の受信、ユーザＩＤ等の偽り、DDoS攻撃等の大量アクセス、情報の不正取得、内部不正、適切なシステム等運用の未実施等
偶発的な原因	ユーザの操作ミス、ユーザの管理ミス、不審なファイルの実行、不審なサイトの閲覧、外部委託先の管理ミス、機器等の故障、システムの脆弱性、他分野の障害からの波及等
環境的な原因	災害や疾病等
その他の原因	上記以外の脅威や脆弱性、原因不明等

別紙４－１　情報共有体制(通常時)



別紙４－２　情報共有体制(大規模重要インフラサービス障害対応時)



別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における[注]各関係主体の役割
○ 内閣官房 （事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房 （ＮＩＳＣ）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣから受領したシステムの不具合等に関する情報を該当するセプターに提供する。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。
○ セプターカウンシル	セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。 主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。
○ セプター事務局	重要インフラ所管省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。
○ 重要インフラ事業者等	システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、「別添：情報連絡・情報提供について」に基づき重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。

注　災害やテロ等に起因する大規模重要インフラサービス障害が発生した場合、当該緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）に基づき、関係府省庁間で情報を集約及び共有する。

別紙５　定義・用語集

CISO	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。
CSIRT	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。
IT-BCP 等	重要インフラサービスの提供に必要な情報システムに関する事業継続計画(関連マニュアル類を含む。)その他の事業継続計画。
安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、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」、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」等の総称。ただし、安全基準等策定指針は含まない。
安全基準等策定指針	安全基準等の策定・改定に資することを目的として、サイバーセキュリティの確保において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。サイバーセキュリティ戦略本部決定による。
関係主体	内閣官房、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター及びセプター事務局、セプターカウンシル、サイバーセキュリティ関係機関並びにサイバー空間関連事業者。
コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。
サービス維持レベル	任務保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。
サイバーセキュリティ	サイバーセキュリティ基本法第 2 条に規定するサイバーセキュリティをいう。電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。
サイバーセキュリティ関係機関	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)。
サイバーセキュリティ関係省庁	警察庁、デジタル庁、総務省、外務省、経済産業省、原子力規制庁(※)及び防衛省。 ※原子力発電所の安全の観点からサイバーセキュリティに取り組む省庁
サイバー空間関連事業者	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。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。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。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
システムの不具合	重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。

重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する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で、重要インフラ分野に属するもの。
重要インフラサービス	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。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
重要インフラ事業者	サイバーセキュリティ基本法第 3 条第 1 項に規定する重要社会基盤事業者をいう。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に関する事業を行う者。具体的には、重要インフラ分野に属する事業を行う者のうち、「別紙１　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの(地方公共団体を除く)。
重要インフラ事業者等	サイバーセキュリティ基本法第 12 条第 2 項第 3 号に規定する重要社会基盤事業者等をいう。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。
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省及び国土交通省。
重要インフラ分野	重要インフラについて業種ごとに指定する分野であり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス(地方公共団体を含む)」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の 15 分野。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、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。
情報共有	システムの不具合等に関する情報(重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報)やサイバーセキュリティの確保に資する情報について、関係主体間で相互に提供し、共有すること。情報連絡及び情報提供の双方を含む。
情報システム	事務処理等を行うシステム、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の IT を用いたシステム全般。
情報提供	サイバーセキュリティの確保に資するための情報を、内閣官房から重要インフラ事業者等へ提供すること等。
情報連絡	重要インフラ事業者等におけるシステムの不具合等に関する情報(重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報)を、重要インフラ事業者等から内閣官房に連絡すること等。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
大規模重要インフラサービス障害	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。
ナショナルサート	国として、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。
防災関係府省庁	災害対策基本法(昭和 36 年法律第 223 号)第 2 条第 3 号に基づく指定行政機関等の、災害時の情報収集に関係する府省庁。
予兆・ヒヤリハット	システムの不具合が生じておらず、又は生じなかったものの、システムの不具合につながるおそれがあり、又はそのおそれがあった事象。

「重要インフラのサイバーセキュリティに係る行動計画」概要

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

重要インフラ所管省庁

- 金融庁
  ［金融］
- 総務省
  ［情報通信、行政］
- 厚生労働省
  ［医療］
- 経済産業省
  ［電力、ガス、化学、クレジット、石油］
- 国土交通省
  ［航空、空港、鉄道、水道、物流、港湾］

重要インフラ(全１５分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾

関係機関等

- サイバーセキュリティ関係省庁
  ［総務省、経済産業省等］
- 事案対処省庁
  ［警察庁、防衛省等］
- 防災関係府省庁
  ［内閣府、各省庁等］
- サイバーセキュリティ関係機関
  ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者
  ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

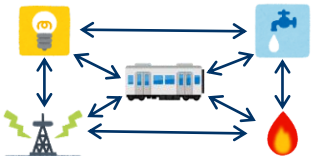
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

行動計画の基本的考え方・要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、
①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等をリスクとして捉え、リスクを許容範囲内に抑制すること
②重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ること
の両面から、強靱性を確保し、国民生活や社会経済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こと。

2. 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成26年法律第104号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。
- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

3. 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

4. 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を明確にする。
- サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

行動計画の取組①： 障害対応体制の強化

重要インフラ事業者等は組織全体としてサイバーセキュリティの確保に取り組んだ上で、官民の相互連携を密にした障害対応体制の強化を推進する。

取組のポイント

- ✓ 組織統治の一部としての障害対応体制の整備
- ✓ サプライチェーンも含めた包括的な対応

行動計画期間中の取組

（1）組織統治の一部としての障害対応体制

- 経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者を含めた障害対応体制の強化を推進

（2）障害対応体制の強化に向けた取組

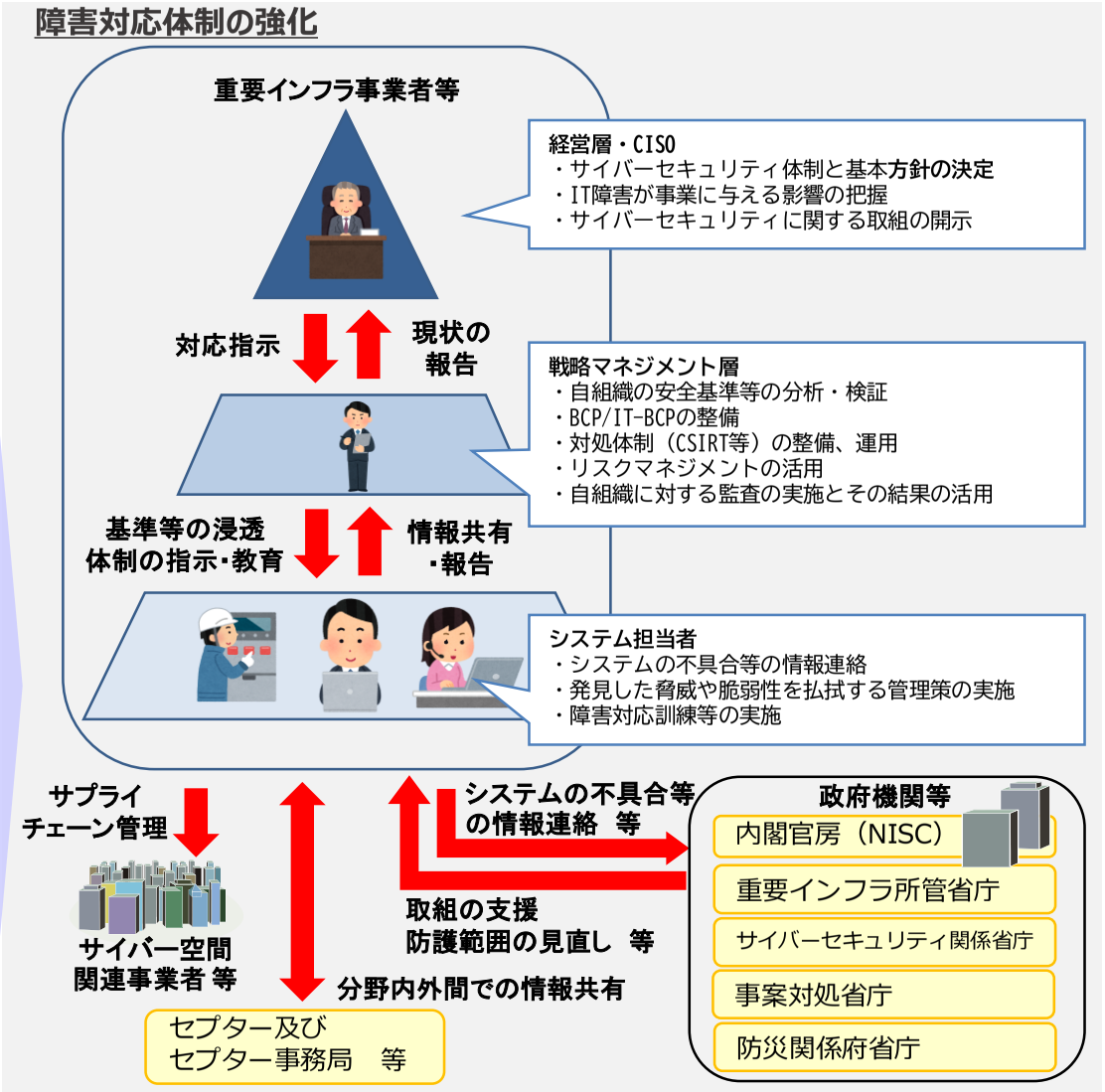
- 障害対応体制を強化するため、BCP/IT-BCP、CSIRT、監査体制等の効果的な取組を推進

（3）官民一体となった障害対応体制の強化

- 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討

（4）重要インフラに係る防護範囲の見直し

- 環境変化に対応するため、サプライチェーンを含めた「面としての防護」の確保及び国の安全等の確保の観点からの取組



行動計画の取組②： 安全基準等の整備及び浸透

自組織に最適な防護対策を実施するため、重要インフラ事業者等の関係主体における「安全基準等」の整備及び浸透の取組を推進する。

※ 安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称

取組のポイント

- ✓ 社会動向や周辺環境の変化に適応した、自組織に適した安全基準等の整備
- ✓ 監査や演習等によるリスク評価を経た安全基準等の継続的な改善

行動計画期間中の取組

（1）指針の継続的改善

- **組織統治の一部としてサイバーセキュリティを取り入れる**方策の強化や、サプライチェーンに関する基準の整備
- 自組織に適した継続的改善のための基準の整備

（2）安全基準等の継続的改善

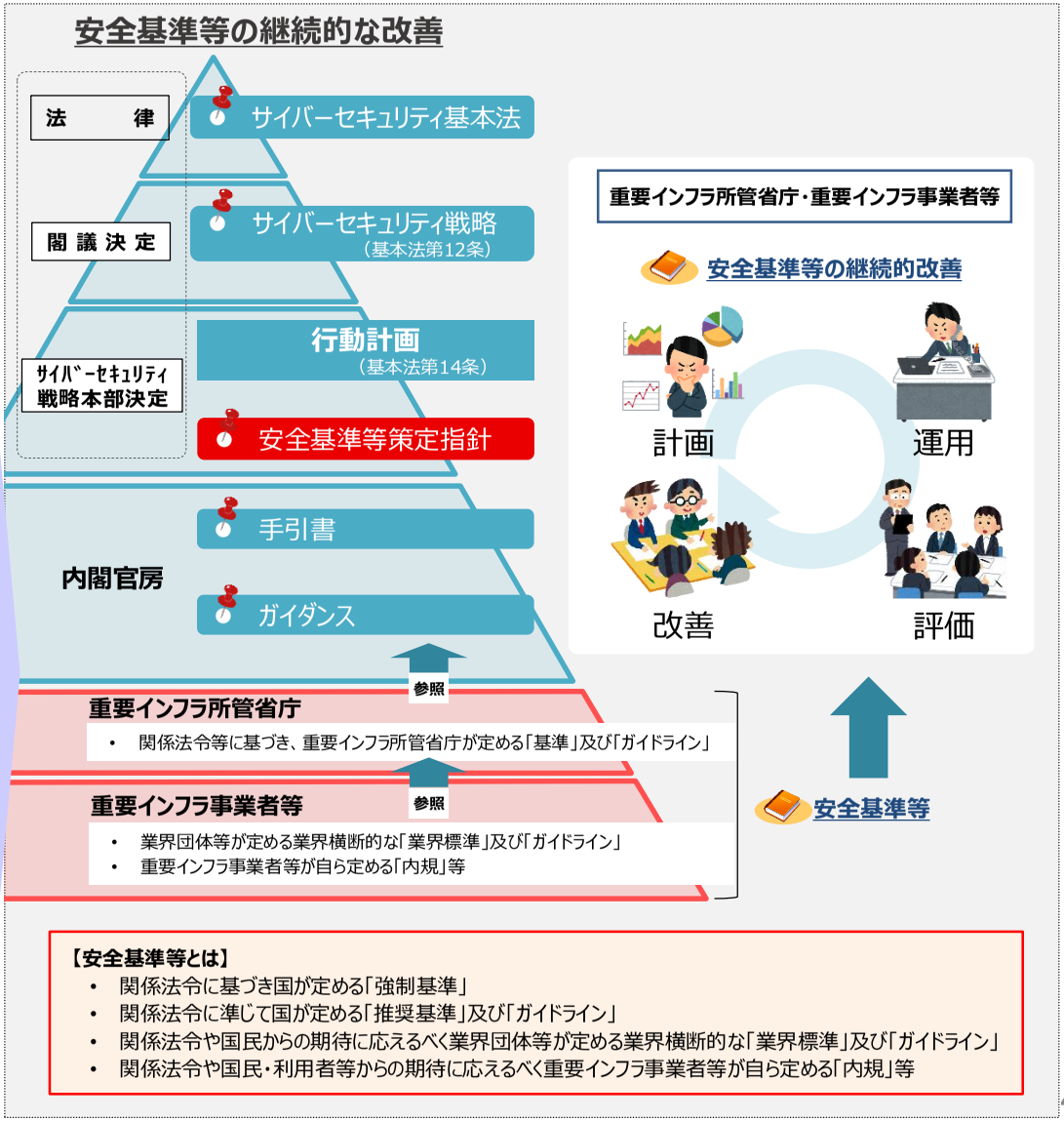
- **内部・外部監査**や演習への参加等による**リスク評価**を経た、安全基準等の継続的な改善
- 重要インフラ所管省庁による安全基準等の改善状況を調査

（3）安全基準等の浸透

- 重要インフラ事業者等におけるサイバーセキュリティ確保に向けた取組について、実態把握のための調査

（4）安全基準等の文書の明確化

- 安全基準等策定指針、安全基準等の理解促進のため、文書の一覧化や文書間の関係性を明確化



行動計画の取組③： 情報共有体制の強化

個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化に取り組む。

取組のポイント

- ✓ これまでの行動計画で構築され定着している情報共有体制の継承・発展
- ✓ 重要インフラ事業者等の自主的な取組の活性化

行動計画期間中の取組

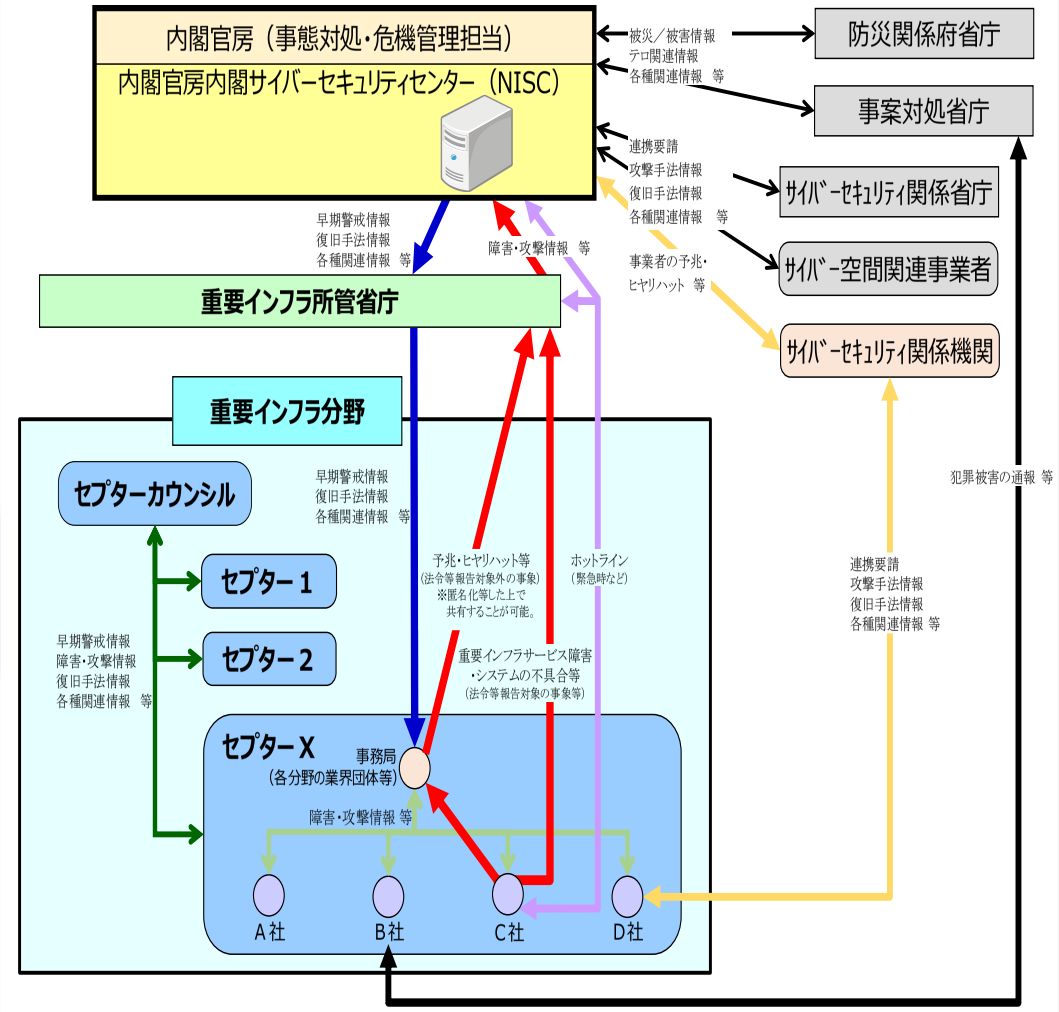
（１）情報共有の更なる促進

- 共有された情報のリスクマネジメント等への積極的な活用
- 重要インフラサービス障害に係る情報及び脅威や脆弱性情報の集約、分析、共有
- 共有すべき情報の明確化（情報系だけでなく制御系やIoTシステムも対象となること等を明示）
- 環境変化等が生じた場合における適時適切な見直し

（２）重要インフラ事業者等の活動の更なる活性化

- 経営層のリーダーシップの下、障害対応体制の構築・強化
- セプター内、セプター間の情報共有の更なる充実
- ISACへの参画及びISAC間の情報共有の促進
- より実態に即した形でのセプター訓練の実施

重要インフラにおける情報共有体制



行動計画の取組④： リスクマネジメントの活用

重要インフラサービスの継続的提供の強靭性確保のため、自組織に適した防護対策の計画・実施、評価・改善の繰り返しによる継続的な取組を推進する。

取組のポイント

- ✓ 自組織に適した防護対策の実現
- ✓ 環境変化による新たなリスク・リスク源の把握
- ✓ 重要インフラ分野間の相互依存性の解析

行動計画期間中の取組

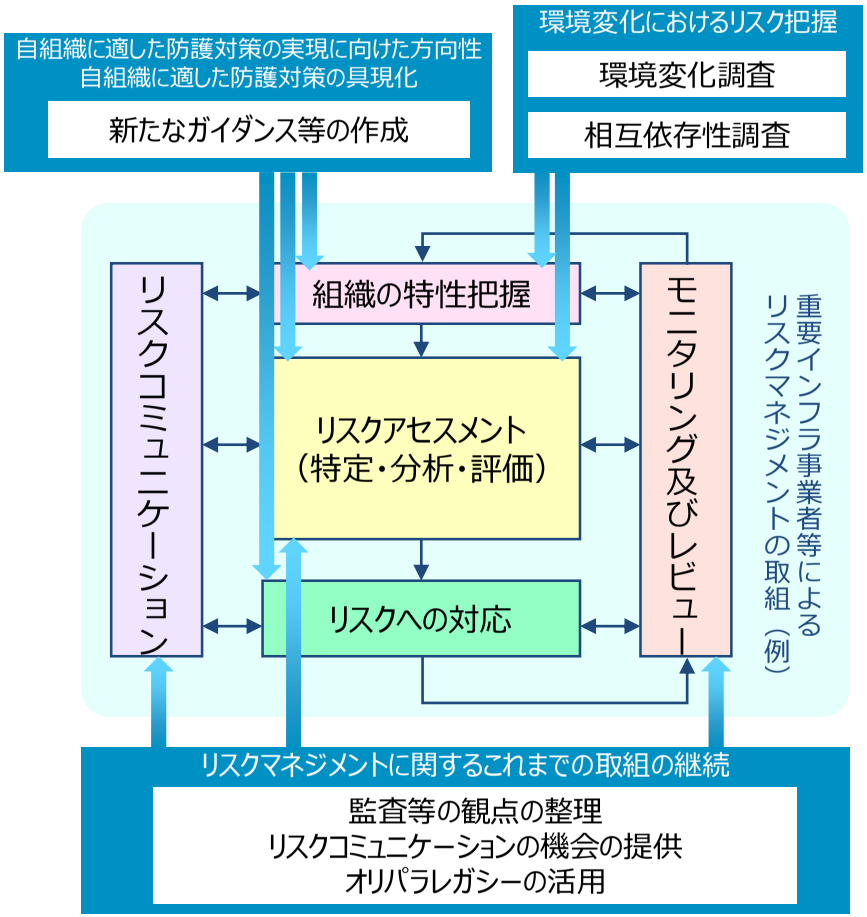
（1）リスクマネジメントの推進

- 自組織のプロファイルを明確化し、自組織に適した防護対策の実現に向けた取組の推進
- 有効な対策や既存の基準類の活用方法について検討し、手引書の見直し、新たなガイダンス等を整備する

（2）リスクに関する調査・分析

- デジタル化を伴うDXの進展によるサイバー空間の変容等によるリスクに対応するため、環境変化調査を実施する
- 重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を実施する。

リスクマネジメントの活用



行動計画の取組⑤： 防護基盤の強化

重要インフラの防護基盤の強化のため、障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組を推進する。

取組のポイント

- ✓ 障害対応体制の有効性検証の実施
- ✓ IT部門だけでなく、幅広い部門の人材育成
- ✓ 効果的な広報チャネルを活用した情報発信　　等

行動計画期間中の取組

（1）障害対応体制の有効性検証
- 分野横断的演習による障害対応体制の検証
- 演習で得た課題を活用した障害対応体制の改善

（2）人材育成等の推進
- 経営層と緊密な連携を行えるよう、戦略マネジメント層の育成
- IT部門に限らない、組織全体の意識向上

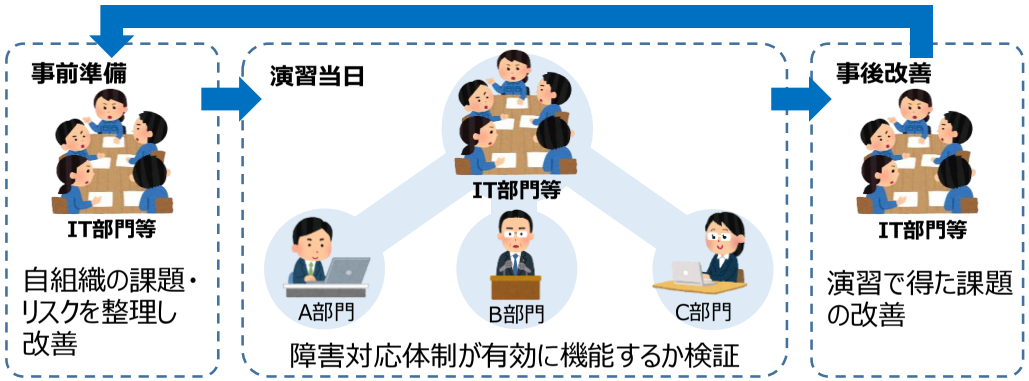
（3）国際連携の推進
- 政府間や事業者間の様々な枠組みを活用した多面的・多角的な国際連携の推進

（4）警察・デジタル庁との連携強化
- サイバー犯罪や、DXに伴う新たな技術に対する意識向上による全体としてのセキュリティ確保の推進

（5）広報広聴活動の推進
- 行動計画の枠組みや取組の国民への積極的な発信
- 関連文書及び関連規格の整備

防護基盤の強化に向けた取組

障害対応体制の有効性検証



人材育成等

- 戦略マネジメント層の育成
- 組織全体の意識向上

国際連携

asean　MERIDIAN Connecting and Protecting

二国間、地域間、多国間の連携

警察・デジタル庁との連携強化

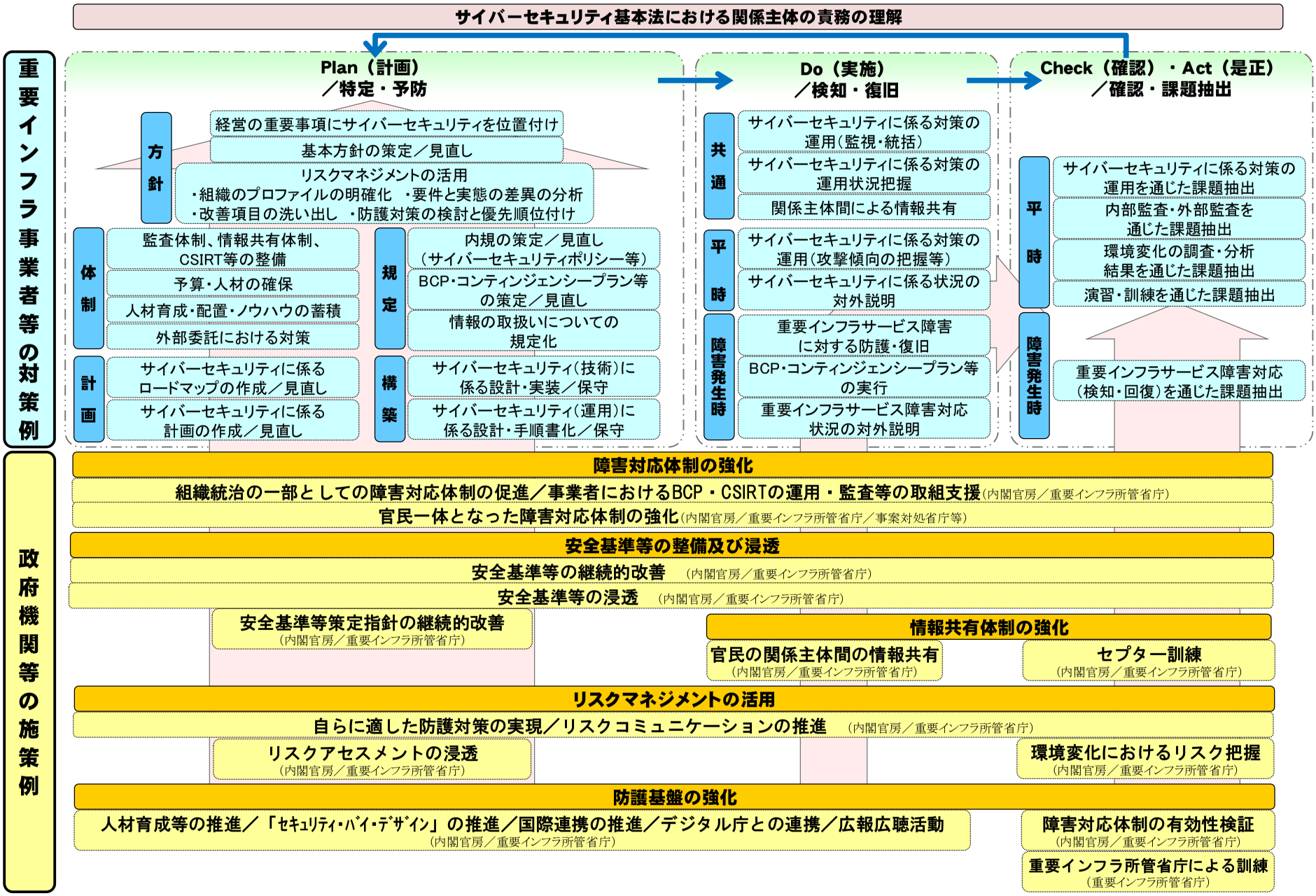
警察庁 National Police Agency　デジタル庁

- サイバー犯罪の警察への通報等
- DXに伴う新技術への意識向上を通じたサイバー空間の安全確保

広報広聴活動

Webサイト、SNS、ニュースレター、講演等を通じた発信

「重要インフラ事業者等による対策例」と各対策に関連する「政府機関等の施策例」



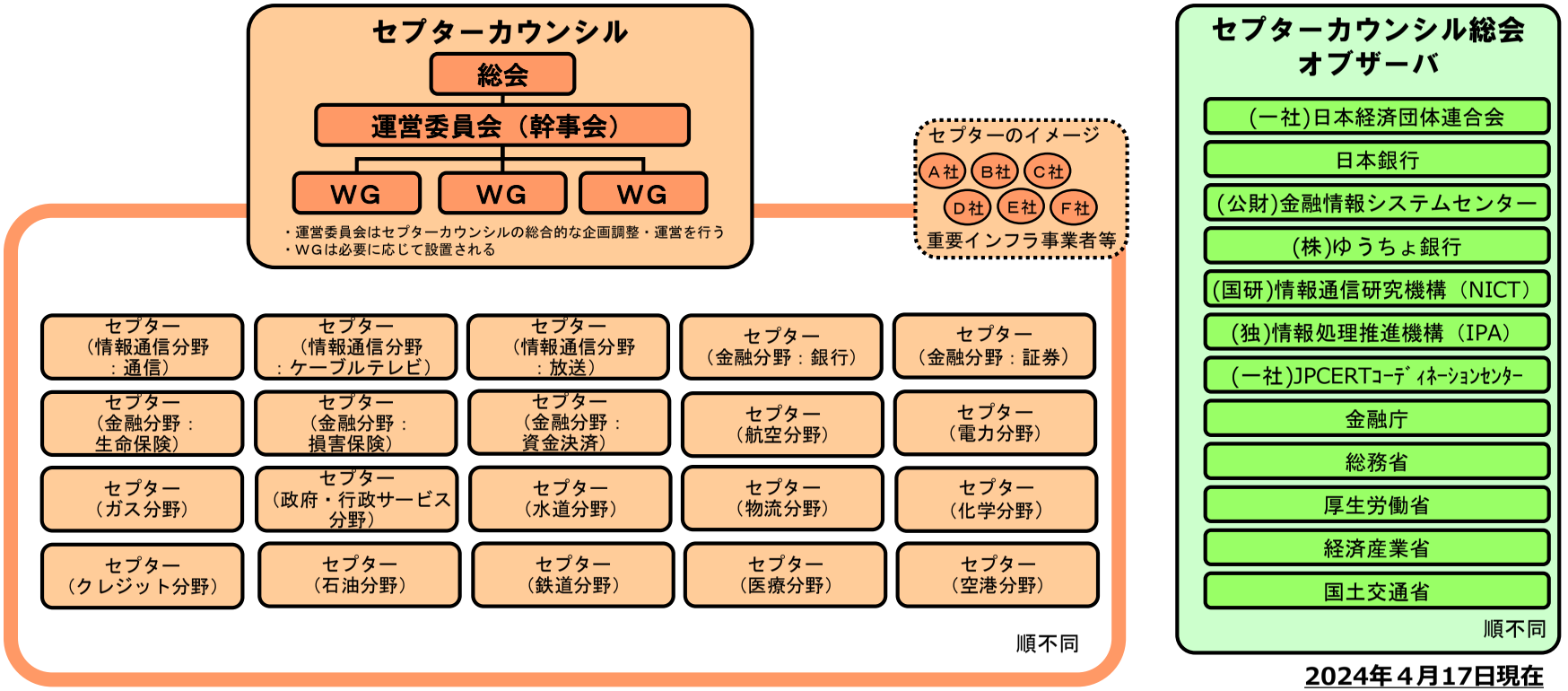
セプターとセプターカウンシル

セプター（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）

- 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。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。
  これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。
  政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、2009年２月26日に創設。



2024年４月17日現在

セプター 一覧

［2024年９月末日現在］

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油	港湾
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油	港湾
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会					航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR	港湾CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	資金決済CEPTOAR													
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟 日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部	(一社)日本損害保険協会 IT企画部	(一社)日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟	(一社)日本港運協会
構成員 (のべ数)	28社 1団体	303社 1団体	194社 2団体	1,228社	276社 7機関	41社	49社	190社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	12社	49社	10社	30社 9団体 7地方公共団体
構成員以外の情報展開先	403社・団体	336社	13社	8社・団体	9社 1機関	–	10社	8社	–	–	–	25社・機関	194社・団体	–	385社・団体	内容に応じ1,314事業体へ展開	–	–	–	–	–

既存事業領域を越える連携等	情報通信（ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟）、金融（金融ISACにおいて、加盟金融機関間で情報共有・活動連携）、航空・空港・鉄道・物流（交通ISACにおいて、参加事業者間で情報共有・活動連携）、電力（電力ISACにおいて、加入する電気事業者間で情報共有・活動連携）、化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者と情報共有・活動連携）、J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報CISTA（JPCERT/CC: セキュリティ情報全般）

重要インフラのサイバーセキュリティに係る
安全基準等策定指針

2023年７月４日
サイバーセキュリティ戦略本部

目次

1. 目的及び位置付け

1.1. 重要インフラにおけるサイバーセキュリティの確保の重要性

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

経営層[1]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、リスクマネジメントによる事前対応と、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サイバーセキュリティの確保に取り組むことが重要である。

1.2. 「安全基準等」とは何か

各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。本文書（以下「安全基準等策定指針」という。）においては、サイバーセキュリティの確保に関して、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「安全基準等」と呼ぶ。

安全基準等は、次の①～④に分類される。

① 関係法令に基づき国が定める「強制基準」

② 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」

③ 関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」

④ 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

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

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

1.3. 安全基準等策定指針の位置付け

安全基準等策定指針は、「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日サイバーセキュリティ戦略本部決定）（以下「行動計画」という。）に基づき、安全基準等の策定・改定を支援するために策定される。

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

安全基準等策定指針には、各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を整理・記載する。これらの取組は原則として安全基準等に規定されることを期待しているが、組織状況に応じて採否が検討されうる取組は推奨事項として「～することが望ましい」「～することが望まれる」という表現にしている。

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

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

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

2. 総則

次に掲げる項目を安全基準等に規定することが望まれる。

2.1. 策定目的

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

2.2. 対象範囲

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

2.3. 関係主体の役割

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

[2] 行動計画「Ⅰ総論 1. 重要インフラ防護の目的」参照。

3. 組織統治におけるサイバーセキュリティ

重要インフラのサイバーセキュリティの確保には、任務保証の観点から取り組むべきである。任務保証とは、サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方」である。

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

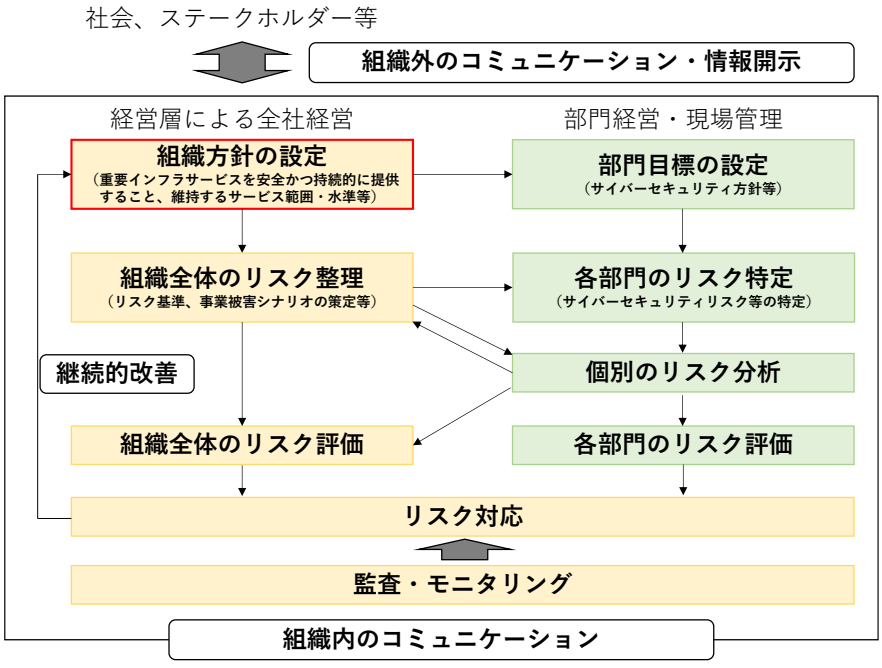


図　組織統治とサイバーセキュリティのイメージ

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

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

3.1. 組織方針

3.1.1. 組織方針とサイバーセキュリティ

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

3.1.2. サイバーセキュリティ方針

組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定する。

- セキュリティ対策の目的や方向性
- 関係主体等からの要求事項への対応
- 経営層によるコミットメント

3.2. 組織内外のコミュニケーション

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

組織内のガバナンスや内部統制、その他のリスクマネジメントにおけるコミュニケーションの一部として、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設ける。

セキュリティ・バイ・デザインを共通の価値として認識し、製品・サービス企画時等の内部協議プロセスの関係者にサイバーセキュリティを担当する部署を加えることが望ましい。

組織内外の関係者間でサイバーセキュリティに関する役割、責任分担、情報共有の体制等について意見交換を行うことが望ましい。

3.3. 経営リスクとしてのサイバーセキュリティリスクの管理

組織全体[5]のリスクマネジメントの一部として、サイバーセキュリティリスク及びそれが事業運営に及ぼす影響について経営層が理解し評価できる体制を整備する。すなわち、組織方針を踏まえ、サイバーセキュリティを確保できないことによって組織の情報システム及び情報を活用する事業、事業者としての信頼、その他の経営リスクがどのような影響を受けるのかといった視点からもリスクを管理し、個々の情報システム及び情報自体のセキュリティに関する視点においてもリスクを分析する。また、

[5] 経営層、CISO（「3.4. 責任及び権限の割当て」を参照）、戦略マネジメント層、担当者層といった縦の階層のほか、情報システム部門、事業部門、広報部門といった横方向にも留意。

自組織にとどまらず、ビジネスパートナーや委託先等、サプライチェーン全体にわたるセキュリティ対策への目配り[6]を行う。

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

3.4. 責任及び権限の割当て

サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てる[7]。特に、サイバーセキュリティに関する責任者（CISO 等）を任命すべきであり、その任命にあたっては、経営層の責任において実施する[8]。当該責任者は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと直接コミュニケーションできる者として位置付けられるべきであり、経営層に相当する者の中から任命されることが望ましい。

---

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

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

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

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

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

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

3.5. 資源の確保

経営層は、セキュリティ対策に必要な資源（予算・人材等）について、組織の価値を維持・増大していく上で、組織活動におけるコストや損失を減らすために必要不可欠な投資[9]であるとの考え方[10]のもとで配分する。

3.6. 監査・モニタリング

情報セキュリティ監査、システム監査等の監査[11]（難しい場合には少なくとも自己点検）を経営層の責任において実施する。現状のシステムやセキュリティ対策の問題点を検出するために、脆弱性診断、ペネトレーションテスト等を実施することが望ましい。

セキュリティ対策の導入・運用に伴うリスクの状況変化（事象の発生頻度の変化や、事象の結果の影響度の変化等）を定期的に確認する。また、サイバーセキュリティ方針に基づき設定した目標の達成状況、サイバーセキュリティ方針・各種計画の有効性・妥当性等について、定期的に、又は状況変化に応じて確認する。

3.7. 情報開示

国民の安心感の醸成を図る観点から、組織内の既存の情報開示体制を活用し、可能な範囲でサイバーセキュリティに関する取組を開示[12]する。サイバーセキュリティに関する次の情報を開示することが望ましい。

- 組織方針・サイバーセキュリティ方針
- 維持するサービス範囲・水準
- リスク管理体制
- サイバーセキュリティに関する責任者の知見
- 資源の確保
- リスクの把握と対応計画策定
- 緊急対応体制・復旧体制
- インシデントの発生状況

---

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

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

[11] 内部監査を担当する部局は、組織トップの下に設けられることが多いが、その場合でも、事案の性質に応じて、報告先は組織トップとする場合と監査役等とする場合とを使い分けることとすべきである（デュアルレポートライン。経済産業省「グループ・ガバナンス・システムに関する実務指針」〔2019 年 6 月 28 日〕72 頁以下）。

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

3.8. 継続的改善

サイバーセキュリティに関する監査・モニタリングの結果や、最新のセキュリティ動向も踏まえ、組織統治の枠組みの継続的改善を行う。サイバーセキュリティを担当する部署においては、経営層からの指示、モニタリング・レビュー、危機管理、演習・訓練等を踏まえ、サイバーセキュリティ方針、各種計画等の継続的改善を行う。

改善を継続的に実施することで、サイバーセキュリティも含めたリスクマネジメントの考え方が組織に浸透し、組織風土に定着するよう努めることが望ましい。

4. リスクマネジメントの活用と危機管理

リスクマネジメントによる事前対応と、危機管理の両面からサイバーセキュリティの確保に取り組むことが重要である。

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

4.1. 組織状況の理解

重要インフラサービスに関する外部環境（政治、経済、社会等）及び内部環境（組織体制、戦略、能力等）の状況について、近い将来の状況も含めて整理する。また、関係法令[13]、契約等に規定された義務、供給者・委託先が提示する制限事項等、関係者からの要求事項を整理する。任務保証の観点から次のような組織の特性を理解することが望ましい。

- 自組織が果たすべき役割・機能と、それを踏まえて維持・継続することが必要なサービス
- 最低限提供するサービスの範囲・水準
- サービス提供を維持するために必要な業務や経営資源

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

4.2. リスクアセスメント

情報システム、ソフトウェア、情報等の資産を特定する。組織状況と資産を踏まえ、任務保証の考え方に基づくリスクアセスメントを実施する。重要インフラサービスの継続提供を不確かなものとするシナリオを作成し、リスク分析を実施することが望ましい。

- 重要インフラサービスの継続的提供を不確かなものとするリスクとしては、自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等があり、リスクの特性に応じたリスク分析手法を選択する。
- 制御システム[14]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[15]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

[13] 例えば、重要インフラの事業法、個人情報の保護に関する法律（平成 15 年法律第 57 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（令和４年法律第 43 号）等。NISC「サイバーセキュリティ関係法令 Q&A ハンドブック」を参照。

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

スメントを実施する[16]。
- 情報システムの運用中も、サイバー攻撃に関する新たな脅威の発生等の環境変化に応じて適宜リスクアセスメントを実施する。
- 本来あるべき状況や要件を検討し、目標とする将来像を決定する。

4.3. サイバーセキュリティリスク対応

4.3.1. リスク対応の決定

目標とする将来像と実態のかい離を埋めるために実施すべきセキュリティ対策を検討する。セキュリティ対策の程度については、成熟度モデルを活用しつつ、自組織における評価基準等をもって優先順位付けする。

リスク対応により、重要インフラサービス障害の発生を抑止するのみならず、発生した障害が経済社会に与える影響を許容範囲内に抑制するための検知・対応・復旧の各機能を実現する。

4.3.2. 個別方針の策定

リスク対応の中で決定した個々のセキュリティ対策において遵守すべき行為や判断等の基準を個別方針（例：アクセス制御方針、情報分類方針等）としてまとめ、組織内へ伝達する。また、必要に応じて委託先に対しても伝達する。

4.3.3. リスク対応計画の策定

サイバーセキュリティに関するリスク対応計画を策定する。計画には次を記載することが望ましい。
- 目標とする将来像
- 実施事項
- 必要な資源
- 責任者
- 達成期限
- 結果の評価方法

4.4. サプライチェーン・リスクマネジメント

対応すべき代表的なサプライチェーン[17]に係る脅威は次のとおり。
- 不正機能等の埋め込み
- サービスの供給途絶
- 外部サービスにおける情報の不適切な取扱い

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

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

・ 海外拠点、グループ組織、取引先等を経由したサイバー攻撃

自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行う。

サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。海外拠点については、現地の法令、文化等も踏まえた対応を行う。

直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。さらに、リスクに応じて直接の供給者に連なる供給者への関与の程度を決定しつつ、各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。また、セキュリティ対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めることが望ましい。

4.5. 事業継続計画等

サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針（コンティンジェンシープラン、事業継続計画[18]、事業復旧計画[19]等）にサイバーセキュリティを組み入れる。事業継続計画等には、サプライチェーンに係る脅威への対応を盛り込む。事業継続計画とあわせて、情報システムに係る記載を詳細化した対応方針（IT-BCP 等）[20]も策定することが望ましい。システム障害の影響が組織全体に波及する際、IT-BCP から事業継続計画へ円滑に移行していくことが望ましい。

4.6. 人材育成・意識啓発

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

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

---

[18] 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）

[19] 平時のサービス水準までの完全復旧対応の方針。

[20] サイバーセキュリティ基本法（平成 26 年法律第 104 号）におけるサイバーセキュリティの定義には、情報システムの安全性及び信頼性の確保のために必要な措置も含まれる。

4.7. CSIRT 等の整備

CSIRT[21]としての機能を持つ体制を整備する。CSIRT 等は、役割分担や対応手順等を関連部門と合意する。特に、制御システムを保有する場合には、制御システム関連部門と連携できる体制を整備することが望ましい。

4.8. 平時の運用

4.8.1. セキュリティ対策の導入、運用プロセスの確立・実行

リスク対応計画を踏まえ、セキュリティ対策の導入、運用プロセスの確立・実行、CSIRT 等の運用を行う。重要インフラサービス障害に繋がる可能性のある事象（サイバー攻撃、情報システムの異常状態等）を早期検知する仕組みを構築するとともに、関係部署等との情報共有、トリアージ[22]等の運用プロセスを確立することが望ましい。

4.8.2. 情報共有

NISC「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月８日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）も踏まえ、組織内外と情報共有を実施する。

収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行う。

- ISAC 等の分野専門性の高い情報共有活動に参加し、情報収集することが望ましい。
- 連絡体制が最新の情報に更新されているか確認することが望ましい。
- 有益な情報を得るには自ら適切な情報提供を行う必要があることを自覚し、組織内外に情報提供を行うことが望ましい。

4.9. 危機管理

サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施する。また、重要インフラサービス障害が発生した場合、事業継続計画等に従った初動・復旧対応を実施する。サイバーセキュリティを担当する部署は、初動・復旧対応に関する経営層の意思決定を支援するとともに、組織内外と情報共有を実施する。

4.10. 演習・訓練

リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効

[21] 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。

[22] 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。

性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行う。経営層も交え、組織全体での演習・訓練[23]を実施することが望ましい。また、他の重要インフラ事業者、サプライチェーンに係る事業者等と合同の演習・訓練、過去のインシデント対応事例の研究等を実施することが望ましい。

[23] 例えば、NISC が主催する「分野横断的演習」。

5. 対策項目

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

5.1. 組織的対策

5.1.1. 資産の管理

5.1.1.1. 資産に対する責任

- 情報システム、ソフトウェア、情報等の資産を特定し、各資産の管理責任者や利用制限（利用が許される範囲）等を明確化した資産目録を作成・維持管理する。
- 情報システム又はその運用を外部サービスによって代替する場合には、利用する外部サービスの一覧を作成・維持管理する。
- ネットワーク構成図、データの流れ図等を作成する。
- 未承認の資産がネットワークに接続・運用されていないか監視し、対処する。

5.1.1.2. 情報分類と取扱い

- 機密性、完全性、可用性の観点から、情報を格付けし、情報媒体（紙、電子）へのラベル付け等により管理する。
- 情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を実施する。

5.1.1.3. データ管理

- システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う。
- 事業環境の変化を捉え､インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。

5.1.2. 供給者管理

- 供給者やその再委託先等が重要インフラ事業者等の資産にアクセスするリスクを低減するためのセキュリティ要求事項を整理し、あらかじめ供給者と合意する。
- 供給者のサービス提供に係る契約等の合意事項について定期的に確認するとともに、供給者が作成した報告書のレビューや監査等を実施する。
- 供給者が提供するサービスの変更に対する管理を行う。
- 供給者が提供するサービスにおけるインシデント発生時や、機器の脆弱性を把握した際に、供給者と速やかに情報を共有し対応できる体制を構築する。

5.1.3. 運用の管理

5.1.3.1. 運用の手順及び責任

- 情報システム等の運用に関連する手順書を整備する。
- 手順書を共有し、作業誤りやセキュリティ基準違反を抑止する。
- 情報システム等の更新に関する事前承認手続きを定める。
- 運用環境と開発・試験環境を分離する。

5.1.3.2. マルウェアからの保護

- マルウェアを検出及び予防する仕組みを整備し、マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。

5.1.3.3. バックアップ

- システムイメージやデータ等に対するバックアップの方針及び手順を整備し、定期的なバックアップリカバリー検査を実施する。

5.1.3.4. ログ取得

- 情報システムのイベントログや運用担当者の作業ログを記録・管理する。
- ログが悪意を持った人物やマルウェア等によって故意に改ざん、消去されないよう管理する。例えば、ログの性質に応じた定期的な検査によって、ログに対する不正行為の有無を確認する。

5.1.3.5. 運用ソフトウェアの管理

- 情報システムで利用するソフトウェアの個々の設定について可能な限り把握・理解し、安全性の確保に努める。
- ソフトウェアのサポート対象バージョンへの更新を計画的に実施する。サポート対象バージョンへの更新が困難な場合には、補完的な措置を講じる。

5.1.3.6. 脆弱性の管理

- 脆弱性情報を収集し、運用中の情報システムに対する影響の有無を確認する。
- 定期的な脆弱性スキャンを実施する。
- 情報システムへのパッチ適用に関する作業方針・内容を確立する。パッチ適用が困難な場合には、情報システムに対する監視を強化するなどの補完的な措置を講じる。

5.1.4. システムの取得・開発・保守

- 情報システムの取得・開発・改善に係る要求事項にサイバーセキュリティに関する事項を含める。必要に応じて、第三者認証を受けた情報システムや、セキュリティ対策の十分な実績があり対策状況を公開しているといった信頼できる事業者

の製品等を活用する。
- 情報システムの取得・開発・改善時にサイバーセキュリティを確保するための手順、環境等を整備する。情報システムの重要度に応じて、情報システムの受け入れ確認時に脆弱性診断を実施する。
- システム開発を外部委託する場合には、サイバーセキュリティに配慮した開発方針の遵守状況を委託先に対して定期的に確認する。

5.1.5. インシデント管理
- インシデントの管理責任者を定める。
- 組織内外へのインシデント報告や証拠収集等の手順を整備する。
- インシデントへの対応を通じて得た知識を、将来のインシデントへの備えとして活用するための仕組みを確立する。

5.2. 人的対策
5.2.1. 従業員の管理
- 重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理する。

5.2.2. 委託先管理
- 委託先との契約書等に、委託先の従業員に関する要求事項[24]や委託終了後も遵守すべき事項を盛り込む。
- 委託先の取組状況を定期的に確認し、必要な改善を求める。

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

5.2.4. エスカレーション
- 従業員が発見した又は疑いを持ったセキュリティ事象を、適切なエスカレーションにより速やかに報告するための仕組みを設ける。

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

[24] 自組織の従業員の管理に関する事項と同等の内容が考えられる。

5.3.2. 災害による障害の発生しにくい設備の設置及び管理

・ 災害による障害が発生しにくい設備配置とする等の災害対策を実施する。

5.3.3. 装置の管理

・ 傍受や損傷の可能性を考慮して通信・電源ケーブルを配線する。
・ 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る事前承認の仕組みを整備する。

5.4. 技術的対策

5.4.1. 利用者アクセスの管理

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

5.4.2. 情報システム等のアクセス制御

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

5.4.3. 暗号を活用した情報管理

・ 暗号の利用方針や暗号鍵の管理方針を策定する。

5.4.4. 通信のセキュリティ

・ 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知等によってネットワークのセキュリティを確保する。
・ 重要な情報を通信手段により転送するにあたり、セキュリティ確保に係る取組方針や手順を整理し、転送相手と合意する。

5.4.5. 多層防御

・ 重要業務を行う端末、ネットワーク、システム又はサービスには、多層防御を導入する。

5.5. 動向を踏まえた対策

5.5.1. ランサムウェア対策

- 速やかなパッチ適用等による脆弱性対策を講じる。
- 海外拠点、サプライチェーンを含めて資産管理をする。
- システムソフトウェア及びデータのバックアップを行い、バックアップから復旧可能なことを定期的に確認する。
- バックアップデータをネットワークから隔離し保存する。
- 役割等に基づいてネットワークを分割する。
- 攻撃を受けた後に調査できるようにログなどを保存する。
- ベンダーなどの関係者と協力関係を構築する。
- 攻撃を受けた際は所管省庁や警察に連絡し、逐次時系列で状況を保存する。
- ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むことが望ましい。

5.5.2. クラウドサービス利用時の対策

- 利用するクラウドサービスの仕様を確認し理解を深める。
- 責任共有モデル[25]を理解し、クラウドサービス提供者との責任範囲等を明確にする。
- 情報公開等の設定にミスがないか確認する。
- サービス仕様が変わる際には影響を確認する。
- 多岐にわたるステークホルダーを把握し、情報共有体制・インシデント対応体制を構築する。
- クラウドサービスの利用終了時に、クラウドサービス上のデータの取扱いについて確認する。

25 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。

重要インフラのサイバーセキュリティ部門における
リスクマネジメント等手引書

2023年７月４日

内閣官房内閣サイバーセキュリティセンター

目次

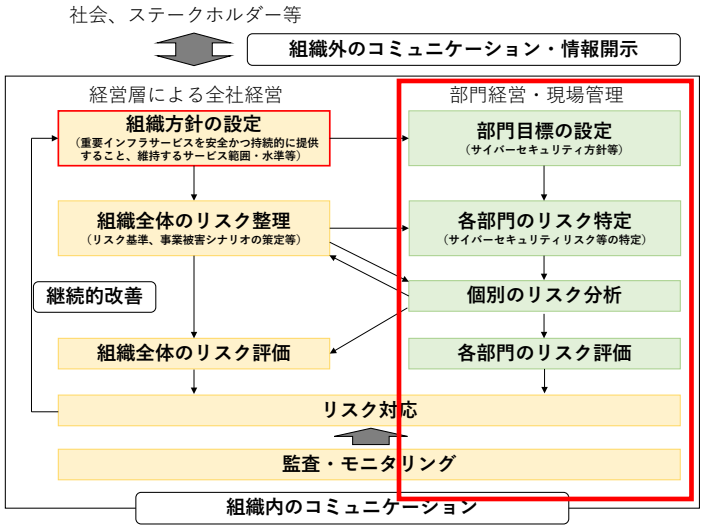
1. はじめに

1.1. 手引書策定の目的

- 情報通信技術の進歩や複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず変容かつ増大している。新しいサービスの創出機会等も拡大している一方で、サイバー攻撃等による情報漏えいやサービス停止の被害が増加するなど、サイバーセキュリティに関するリスクも拡大している。
- 「重要インフラのサイバーセキュリティに係る行動計画」（2022 年６月 17 日サイバーセキュリティ戦略本部決定）（以下「行動計画」という。）では、「国民生活や経済社会活動の基盤となるサービスを提供する重要インフラ事業者等においては、経営の重要事項としてサイバーセキュリティを取り込み、重要インフラを取り巻く情勢（システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まり等）を鑑みて、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応をより一層促進する」こととされた。
- 本手引書は、サイバーセキュリティ部門（戦略マネジメント層、担当者層）向けに、安全基準等策定指針で示すセキュリティ確保に向けた取組についての参考情報を提供する。

1.2. 手引書の記載範囲

- 本手引書では、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（仮称）のうち、「4. リスクマネジメントの活用と危機管理」におけるリスクマネジメント等の主要なプロセス（下図の赤枠箇所）及び「5. 対策項目」における主なセキュリティ対策について、サイバーセキュリティ部門における取組を念頭に記載する。



図：組織統治とサイバーセキュリティのイメージ

1.3. 手引書の適用範囲

1.3.1. 対象とする事業者等

・ 本手引書は、重要インフラ事業者等による利活用を想定している。各事業分野や事業領域に特化したリスクマネジメント手法が既に確立している場合は、既存の手引書やガイドライン等を優先して利活用しつつ、必要に応じて本手引書の記載内容を補完的に利活用することが望まれる。

1.3.2. リスクマネジメントの対象

・ 本手引書におけるリスクマネジメントでは、重要インフラ事業者等が、そのサービス提供に必要な業務の遂行のために所有、使用又は管理する情報資産等に係る事象の結果（自然災害、サイバー攻撃等に起因する障害）から認識されるリスクを対象とする[1]。

[1] 重要インフラ事業者等においては、サイバーセキュリティに関するリスク以外のリスクがあることも考えられる。本手引書では、スコープを限定したリスクマネジメントの手法を紹介しているが、実際にリスクの評価やリスク対応の選択肢の同定に係る意思決定を行う際には、サイバーセキュリティに関するリスク以外についても勘案し、総合的に考慮することが重要である。

2. リスクマネジメントのフレームワーク

2.1. 全体像

- NISC「機能保証のためのリスクアセスメント・ガイドライン」、NIST「重要インフラのサイバーセキュリティフレームワーク（CSF)」[2]、ISO/IEC27001 をベースに構成している。
- 対象を従来のリスクアセスメントからリスクマネジメント全体に拡大し、コミュニケーション及び協議、モニタリング及びレビュー等に係る取組を追記した。
- 組織の状況把握からリスク対応の決定・改善に至る一連の取組[3]について、NIST CSF をベースに追記した。

2.2. 前提

- リスクの捉え方について、「目的に対する不確かさの影響」をリスクと捉える（ISO 31000:2018 における定義に準拠。)。

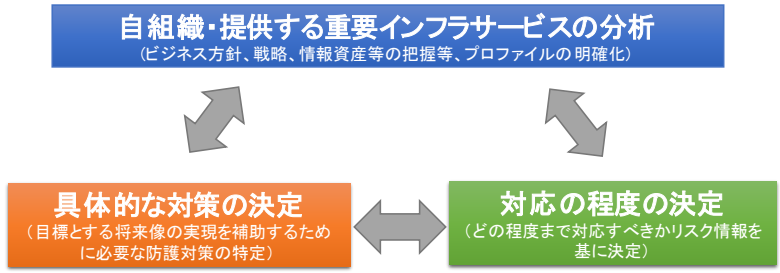
[2] NIST において、NIST CSF の改定に向けた検討がなされている。
[3] NIST CSF では、「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つセキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用対効果の高いアプローチ」とされている。

3. コミュニケーション及び協議

- リスクマネジメントのプロセスの初期段階において、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。
- リスクマネジメントにおけるコミュニケーション及び協議には、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なうことに留まらず、リスクマネジメントの各ステップの活動を行う為に必要な分析に使用する最新の情報や手法に加えて、ステークホルダーの価値観等のリスク特定や評価に重要な情報の共有を行なうことも含まれる。
- ステークホルダーとのコミュニケーション及び協議により、実施しているリスクマネジメントへの安心を高め、参加意識を高めることもできる。

4. 組織の状況の特定

- 自組織が直面するリスクとその程度を把握し、自組織の重要インフラサービス提供に係る特性の明確化に着手することから新たな改善をスタートする。
- 任務保証の考え方を踏まえ、自組織の特性を明確化する。
- 自組織の内部状況、外部状況及び関係主体の要求事項等について把握した情報は、従業員のセキュリティ意識向上の観点から、整理したものを組織内に共有する。



- 現状分析(実態把握)と目標とする将来像のかい離を明らかにする
- かい離を埋めるために、どこからどんな改善を行っていくか優先順位付けを行う

図：自組織に適した防護対策の実現（概念図）

4.1. 組織の状況及び特性の理解

- 組織全体のリスクマネジメントの一部として整理される組織内外の状況及び特性を理解する。
- 必要に応じて、サイバーセキュリティの視点から組織の状況及び特性の更なる明確化を行う。

4.1.1. 内部状況の理解

- 次に例示するような組織内部の現状をサイバーセキュリティの視点から理解する。
  - ＊ 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
  - ＊ セキュリティリスクに対する、部署や立場による認識の差異
  - ＊ 従業員のセキュリティリテラシー

1） ビジョン、使命及び価値観

2) 組織統治、組織体制、役割及びアカウンタビリティ
3) 戦略、目的及び方針
4) 組織の文化
5) 組織が採用する規格、指針及びモデル
6) 資源及び知識として理解される能力（例えば、資本、時間、人員、知的財産、プロセス、システム、技術）
7) データ、情報システム及び情報の流れ
8) 内部ステークホルダーの認知及び価値観を考慮に入れた、内部ステークホルダーとの関係
9) 契約上の関係及びコミットメント
10) 相互依存及び相互関連

ISO 31000:2018 より、内部状況の例

4.1.2. 外部状況の理解

・ 次に例示するような組織外部の現状をサイバーセキュリティの視点から理解する。
  * 自組織が関連する法令の改正状況（事業法、個人情報保護法等）
  * 所管省庁や規制当局における基準の策定、改正状況
  * 関連団体における基準やガイドラインの策定、改正状況
  * 景気、為替、経済リスクが与えるセキュリティ投資への影響
  * 国外に拠点のある事業者における現地の法令、情勢等の状況
  * セキュリティ投資による優遇措置や市場競争におけるイニシアチブ
  * 重要インフラサービスの利用者に与える影響
  * 国内外におけるセキュリティインシデントの発生事例や、その報道等による社会からのセキュリティ認識の広まり
  * 外部取引先との契約における、セキュリティに関する要求事項
  * 自組織が任務保証を達成するために必要な他の重要インフラサービス
  * 自組織と他組織の相互依存関係

1) 国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因
2) 組織の目的に影響を与える、鍵となる原動力及び傾向
3) 外部ステークホルダーとの関係、並びに外部ステークホルダーとの認知、価値観、必要性及び期待
4) 契約上の関係及びコミットメント
5) ネットワークの複雑さ、及び依存関係

ISO 31000:2018 より、外部状況の例

4.1.3. 重要インフラサービス継続に係る特性の理解

・ 内部状況及び外部状況を踏まえ、次に例示するような自組織の重要インフラサービス継続に係る特性を理解する。
  * 自組織のサービス停止が経済社会に与える影響
  * サービス継続に係る重要なシステムや機能
  * 重要なシステムや機能を支える業務
  * 業務を支える資源及び知識（予算、人員、設備、技術、資産の脆弱性情報）
  * 他の重要インフラとの相互依存関係
  * 重要インフラサービス障害時における、復旧までの許容可能な時間

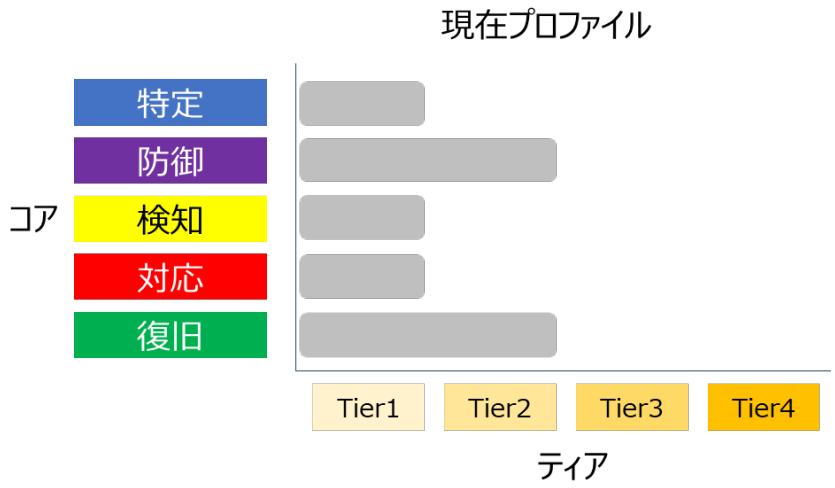
4.2. 現在プロファイルの特定

・ 現段階における自組織のサイバーセキュリティ対処態勢等の実態を把握するに当たり、一例として、現在プロファイルの特定が考えられる。
・ 現在プロファイルの特定に当たっては、NIST サイバーセキュリティフレームワーク（CSF)、英国サイバーアセスメントフレームワーク（CAF)、サイバーセキュリティ能力成熟度モデル（C2M2)、CIS Controls 等が参考となる。NIST CSF では、サイバーセキュリティの確保に当たり、コアと呼ばれる５つの区分（特定・防御・検知・対応・復旧)のセキュリティ対策と、ティアと呼ばれる対策の程度を例示している。
・ 経済産業省 のサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）は、NIST CSF など国外の主要な規格との整合性を確保しており、国外の規格を踏まえた各国の認証制度との相互承認を進めていくことができる内容となっている。

【プロファイルの特定について】

セキュリティ対策の状況把握について、NIST CSF ではプロファイルという考え方が説明されている。

プロファイルには対策の区分であるコアと、対策の程度を示すティアの２つの要素があり、プロファイルを特定するためには、まずこれらを自組織用に整理する必要がある。



図：現在プロファイルの特定の概念図

NIST CSF にはコアを細分化した 23 のカテゴリ及び 108 のサブカテゴリが例示されている。これらのカテゴリ全てについて対応するのではなく、自組織にとって必要な項目を採用し、整理を行う。

対策の程度を示すティアについても４つの段階が例示されているが、ティアの段階についても自組織向けに設定できる。適切なティアを判断するに当たり、成熟度モデル等、既存のガイダンスの活用を検討することが考えられる。また、リスクの許容度がティアに反映される場合もある。

成熟度モデルは、組織において現在取り組んでいる対策や手法等に能力レベルを評価し、目標や改善のための優先順位を設定するためのベンチマークとなる。

代表的な成熟度モデル

- サイバーセキュリティ能力成熟度モデル（C2M2）
- サイバーセキュリティ成熟度モデル認証（CMMC）

表：ティア（対応の程度）の例

Tier1	**・セキュリティ対策が未対応の状態。** ・リスクマネジメントの枠組みが定められておらず、リスク対処は場当たり的。 ・セキュリティリスクに関して意識が不足している。 ・情報共有のプロセスが存在しない。 ・ステークホルダーとは協力関係にない。
Tier2	**・セキュリティ対策は整備しているが、運用化まではできていない。** ・リスクマネジメントの枠組みは経営層に承認されているが、組織全体のポリシーにはなっていない。 ・サプライチェーン・リスクは把握しているものの対応はできない。
Tier3	**・セキュリティ対策は整備できており、定期的に見直しができる状態。** ・リスクマネジメントの枠組みが自組織のポリシーとなっており、また定期的に見直されている。 ・従業員は割り当てられた役割と責任を果たすための知識とスキルを持っている。 ・セキュリティ担当の役員と他の役員が定期的に他の役員とコミュニケーションを取っている。 ・ステークホルダーと協力関係にある。 ・サプライチェーン・リスクの対処ができる。
Tier4	**・セキュリティ対策は整備できており、適時に見直しができる状態。** ・組織全体のサイバーセキュリティマネジメントのアプローチが確立されている。 ・セキュリティリスクマネジメントが組織文化の一部となっている。 ・役員が示したビジョンを実践し、システムレベルでリスク分析を行っている。 ・事業目的、ミッションの変更に迅速かつ効果的に対処できる。 ・サプライチェーン・リスクをリアルタイムに近い情報で対処している。

出典：NIST CSF

5. リスクアセスメント

5.1. リスクアセスメントの実施

・ 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、次のような手順によってセキュリティリスクアセスメントを実施する。

①リスクアセスメントの対象の特定

絶えず変化する自組織を取り巻く状況及び関係主体等のニーズを踏まえ、重要インフラサービスの提供に必要な業務の範囲・水準等を明らかにするとともに、当該業務の遂行に必要な情報システム等の経営資源を特定する。

②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。

③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「事象の発生可能性」等を評価軸として策定されるリスク基準を活用して、特定されたリスクの大きさを確認する。

④リスク評価

基準値以上の大きさのリスクを抽出するとともに、個別事情も考慮してリスク対応の対象とするリスクを抽出する。

・ リスク分析に当たっては、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[4]を念頭に分析することが重要である。
・ 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、セキュリティリスクに加えて、HSE[5]等の観点からのリスクも特定し、分析・評価を行う事も求められる。HSE 等の観点として、例えば、重要インフラサービスの提供を担う従業員等の労働安全・衛生の確保や、重要インフラサービスの利用者の安全・健康の確保、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。
・ 上記手法においてリスク対応の対象として抽出しなかったリスクも管理が必要である。所管部署の責任において当該リスクを管理させる場合には、各部署の管理状

[4] 重要インフラ分野等の間の「相互連関・連鎖性」が一層深化していくことが予想される。NISC において、重要インフラサービス障害等が生じた場合の影響の波及に関する調査（相互依存性調査）を実施予定である。

[5] 健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.2.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。

況（セキュリティ管理策の導入有無等）を適時確認可能とする仕組みを整備する。

・ リスクアセスメントの具体的なプロセスについては、NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0 版」等を参考にしながら、リスクの特性に応じたリスク分析手法によってリスクを評価する。

5.2. 制御システムのリスクアセスメント

・ 制御システムにおいては IPA「制御システムのセキュリティリスク分析ガイド」、ISO/IEC 62443「制御システムセキュリティに関する国際規格」、NIST-SP 800-82「産業用制御システム（ICS）セキュリティガイド」等を踏まえ、資産ベースに加え、事業被害ベースの脅威を想定したリスクアセスメントを実施する。

・ 制御システム関連のインシデント事例について情報収集し、リスクを評価することが重要である。

・ 一般的に、制御システムは可用性（安全、安定稼働）が最優先される。パッチ適用やバージョンアップ、暗号化などのリスク低減策の実施が、制御システムの安定稼働に影響を与えると判断できる場合には、ログや通信の監視等の代替策の実施によりリスク低減を図る。

・ 制御システムに関するセキュリティ責任者を設置し、情報システムと制御システムの担当者間で適切なコミュニケーションをとる。

・ セキュリティリスクを考慮し外部ネットワークに接続していない環境で運用していても、災害、自然故障、管理不良等により制御システムの可用性が低下するリスクがある。

【リスク分析の手法について】

リスク分析のアプローチとして、資産ベースのリスク分析と、事業被害ベースのリスク分析がある。

○ **資産ベースのリスク分析**

保護すべきシステムを構成する資産群を明確にし、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

○ **事業被害ベースのリスク分析**

回避したい事業被害を明確にし、事業被害を引き起こすと想定される脅威について、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

	資産ベースのリスク分析	**事業被害ベースのリスク分析**
長所	全ての資産を単体で網羅的にリスク分析と対策の検討が可能	事業被害をもたらす攻撃ツリーに対する多層防御的な観点で、対策を検討することが可能
限界／短所	資産を一律に評価するので、事業上の対策優先順位付けに考慮が必要	想定（対象）外の攻撃の入口や、攻撃ツリーで経由しない資産や、経由した資産での直接の攻撃（不正アクセスや操作等）以外の攻撃に対する対策の検討は、見落とされる可能性がある。

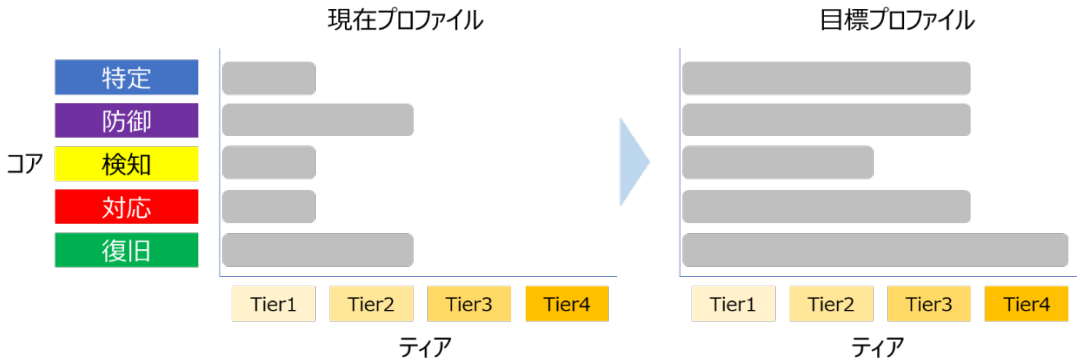
組織の状況によって選択する分析手法は異なる場合があるが、組織が保有する資産（情報システムやネットワーク構成、データフロー図等）が明確化されていることが前提である。

出典：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」

6. リスク対応

6.1. 目標プロファイルの作成

- 重要インフラ事業者等は、リスクアセスメントの結果や、自組織の目標、組織の状況、ステークホルダーからの要求事項等を踏まえ、目標とする将来像を決定する。目標とする将来像を決定するに当たり、一例として目標プロファイルの作成が考えられる。
- 現在プロファイルの特定と同様、目標とするティアを設定する。目標とするティアは、自組織の方針に見合うものであり、任務保障の観点からサイバーセキュリティのリスクを自組織にとって許容可能な程度まで低減できるものである必要がある。
- 発生した障害等への対応については、障害等の発生の予防・検知と比べて多くの費用、人材等を要する傾向にあることから、予防・検知の徹底が重要となる。



図：目標プロファイルの概念図

6.2. ギャップ分析と優先順位付け

- 現在プロファイルと目標プロファイルの差異について分析する。
- 差異を解消し、目標プロファイルに近づけるための取組について、組織方針に基づく動機、リスク、セキュリティ対策の費用対効果等を踏まえ、優先順位付けを行う。

6.3. リスク対応計画

- 優先順位付けを踏まえ、現在プロファイルと目標プロファイルの差異に対して実施すべき取組をまとめたリスク対応計画を作成し、実施する。

6.4. サプライチェーン・リスク対応

- 製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理する。
- 不正機能等の埋め込みに係る脅威に対応する。
  （リスク管理策例）
  * 調達過程における一貫した品質管理が担保できることの選定基準への盛り込み
  * 指定したセキュリティ要件が実装されているか、不正プログラムが混入していないかを確認する検査体制の構築
  * 委託先が再委託先を監督し責任を負うことが可能な体制であるかの確認
  * 再委託の禁止、又は再委託前に委託元の許可を得ることの契約要件への盛り込み
- サービスの供給途絶に係る脅威に対応する。
  （リスク管理策例）
  * 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応する。
  （リスク管理策例）
  * 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応する。
  （リスク管理策例）
  * 第三者による評価検証結果の活用
  * サプライチェーンとのネットワーク接続点におけるセキュリティの確認
- 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）におけるリスク管理措置の例や、NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」が参考になる。
- 発注者となる組織においては、独占禁止法及び下請法を考慮したパートナーシップ体制を構築する[6]。

[6] 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/hontai_1028.pdf

7. コンティンジェンシープラン及び事業継続計画の策定

初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画」を策定する（又はこれらと同等の方針を定めた計画を策定する）とともに、当該計画の実行に必要な組織体制を整備する 。なお、事業継続計画を整備済みの重要インフラ事業者等においては、目標復旧水準から平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（事業復旧計画）も別途策定する。

策定に当たり、「【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」が参考となる。

7.1 コンティンジェンシープランの策定

- 重要インフラサービス障害の発生又はそのおそれがあることを認識した際に、経営層や職員等がまず実施すべき対応を明確にし、迅速に行動することが求められる。そこで、初動対応（緊急時対応）の方針、手順、態勢等を定めた「コンティンジェンシープラン」の策定が必要となる。

7.2 事業継続計画（BCP）の策定

- 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、態勢等を定めた「事業継続計画」の策定が必要となる。
- 重要インフラサービスに影響を与える要素として、サプライチェーン・リスクが含まれる場合があることも考慮し、事業継続計画を策定する。

8. 運用

8.1. 人材育成

- サイバーセキュリティの推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を確保・維持する観点から、これらのセキュリティ人材の重要インフラ事業者内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検討する。
- 重要インフラ事業者等の従業員がセキュリティ方針及びセキュリティ管理策の個別方針に基づく義務と責任を果たせるようにするため、従業員に対して、サイバーセキュリティに関連する十分な教育・トレーニングを実施する（必要に応じて委託先にも実施）。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やセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練への参加、「情報処理安全確保支援士」等の資格取得等も期待される。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。
- サイバーセキュリティリスクについて可能な限り理解できるよう、経営層に対してセキュリティ教育を実施する[7]。
- 制御システムのサイバーセキュリティの確保に当たっては、制御システムを熟知した上でサイバーセキュリティの知見を高めることが重要である。制御システムに関するセキュリティ人材を確保する取組としては、産業サイバーセキュリティセンター（ICSCoE）による中核人材育成プログラムを活用することが考えられる。

8.2. CSIRT 等の整備

- サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画の実行に必要な組織体制の一つとして、CSIRT[8]（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。CSIRT 等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。
  特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス要害発生時の対応に OT 関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。

---

[7] NISC では経営層や DX を推進する部課長向けに、プラス・セキュリティ知識として、参考となるカリキュラムを公開している。https://security-portal.nisc.go.jp/dx/plussecurity.html

[8] Computer Security Incident Response Team の略。サイバー攻撃による情報システムの不具合など、コンピュータセキュリティに係るインシデントに対処するための組織のこと。なお、事業者によって CSIRT を組織として常設している場合とインシデント発生時のみ設置する場合がある。

また、サイバー攻撃に迅速に対処する観点から、サイバーセキュリティの専門知識を持つ組織を含めた対処体制を平時から整備する。例えば、サイバー空間関連事業者及びサイバーセキュリティ関係機関との提携が有効である。

・ その他、セキュリティ確保の取組を推進するため、次のような役割が考えられる。
    * 脅威情報等の収集及び関係主体との情報共有担当
    * コンティンジェンシープラン及び事業継続計画の実行担当
    * セキュリティ対策の取組全般に対する内部監査担当
    * サプライチェーン（供給者、委託先等）におけるセキュリティ対策の取組の管理担当
    * セキュリティ人材の職能要件の管理及び教育・研修担当
    * 情報システム（ネットワークを含む）の運用担当
    * 各資産（情報システム、ソフトウェア、情報等）の管理担当
    * 物理的セキュリティが要求される施設の管理担当

8.3. 平時におけるリスク対応

・ 「リスク対応計画」に基づき、リスク対応において決定したセキュリティ管理策の導入を進めるとともに、それらを効果的かつ確実に運用するためのプロセスを確立し、実行する。
・ 重要インフラサービスの提供に係る情報システム等の運用状態を示すデータについて、アラートやログ等の複数の監視結果を相互に組み合わせて、重要インフラサービス障害につながる可能性のある事象（サイバー攻撃、情報システムの異常状態等）を早期検知する仕組みを構築するとともに、検知後に続く関係部署等との事象の共有、トリアージ（サイバー攻撃等の事象の影響分析及び対応の優先順位付け）等の運用プロセスを確立する。
・ 日頃からサイバーセキュリティ関係機関等が提供する脅威情報やそれらの分析・対策情報を確認する。行動計画に基づく情報共有については、NISC『「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書』の運用に則り積極的な情報共有を実施する。
・ ISAC 等の分野専門性が高い情報共有活動への参加し情報収集を行う。
・ サイバーセキュリティ関係機関等からの情報提供や収集した脅威情報等を踏まえ、必要に応じて追加のリスクアセスメント及びリスク対応を実施し、重要インフラサービスの強靭化を図る。

8.4. 危機管理

・ 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析（情報システム等へのフォレンジックを含む）、関係主体等との情報共有・調

整（顧客向け広報活動を含む）、被害拡大の防止、サービスの復旧等の対応を実施する。

また、重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

・ 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、経営層の意志決定を支援するため、経営層が理解できるように事象の内容、影響及び現在の対応状況等を説明する必要がある。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、初動及び復旧の対応について経営リスクの観点から経営層へエスカレーションを行う。

8.5. 演習・訓練

・ リスクマネジメントによる事前対応と、障害発生時の危機管理の両面から、体制や取組の有効性を検証するため、定期的に演習・訓練を実施する。重要インフラ全体の防護能力の観点からは、同業の重要インフラ事業者等やサプライチェーン、関係主体等との合同での演習・訓練やケーススタディ（他事業者の過去のインシデント対応事例の研究）の実施も期待される。なお、合同での演習・訓練には、内閣サイバーセキュリティセンターが主催する「分野横断的演習」や、重要インフラ所管省庁やサイバーセキュリティ関係機関等の関係主体が主催するものがある。

9. モニタリング及びレビュー

9.1. モニタリング実施計画の策定と実施

- サイバーセキュリティ確保の取組の効果について、継続的に改善を行うため、リスク対応計画や、人材育成の進捗状況等をモニタリングする。継続的に実施するため、モニタリング及びレビューのプロセスを計画に組み込む。
- サイバーセキュリティ確保の取組により、リスクをどの程度回避、軽減が出来たかを測定・評価する。現状のシステムやセキュリティ対策の問題点を検出するために、脆弱性診断、ペネトレーションテスト等の手段がある。
- リスクの管理レベルが社会からの要求事項の変化に沿うよう、日々改善する。

9.2. 内部監査の実施

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

9.3. モニタリング及びレビュー結果の反映方針の策定

- モニタリング及び監査結果から、改善や見直しが必要な箇所を認識する。レビューに際し、内部環境、外部環境の変化や、関係主体からの要求事項も確認する。

10. 記録及び報告

10.1. 記録

・ リスクマネジメントの検証、改善のため、各プロセスにおいて、記録を作成する。記録の作成に当たっては次の事項を考慮する。
  * 記録の作成及び維持管理の費用及び労力
  * 閲覧方法、検索の容易性及び保存媒体
  * 保有期間
・ 記録を取ることを目的にするのではなく、利用目的に合わせて記録することが重要なことに留意する。

10.2. 報告

・ ステークホルダーとのコミュニケーションの質を高めたり、経営層の意思決定を補助したりするために報告を実施する。報告に当たっては次の事項を考慮する。
  * それぞれのステークホルダーに特有の情報の必要性及び要求事項
  * 報告の費用、頻度及び適時性
  * 報告の方法
  * 情報と組織の目的及び意思決定との関連性

11. 対策項目

・ 以下に個別の対策例を示す。各リスク評価の結果、重要度に応じて組織ごとにリスク対応を行うことが前提であることに留意。

11.1. 組織的対策

11.1.1. 資産管理

・ 組織全体の資産目録を作成し、定期的に維持管理する。制御システムについても作成する。重要な機器やサービス業務の機能維持・レジリエンス向上のため、全ての重要な資産の現在の詳細構成を記述した文書を策定し、維持管理する。
・ 全てのシステム・ネットワーク構成を記述した文書（システム・ネットワーク構成図）を作成し、維持管理する。制御システムについても文書を作成する。構成図は定期的なレビューと更新を実施する。
・ 新しいハードウェア、ソフトウェア、ファームウェアを導入する前に、承認を必要とする仕組みとし、組織の情報資産の可視性を高める。技術的に可能な場合、承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する。

11.1.2. 情報分類と取扱い

・ 重要インフラサービスの提供に係る情報及びその他の関連資産を適切に保護するため、情報の取扱い手順を整備する。情報は機密性、完全性、可用性及び関連する利害関係者の要求事項に基づき分類及び情報媒体へのラベル付けを行う。
・ 自組織の業務上の要求事項に対処できるよう、情報の分類体系はアクセス制御に関する方針と整合させる。
・ 自組織が採用した情報分類体系に従って、情報のラベル付けに関する手順を策定し、情報の分類、伝達、処理、管理を適切に行う。ラベル付けは物理的、電子的手段等があるが、デジタル情報についてはメタデータを活用する手法がある。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の手順を定める。

11.1.3. 運用管理

11.1.3.1. 運用の手順及び責任

・ サイバーセキュリティに関する脅威情報を収集し、意思決定等に活用できるよう分析する。
・ インターネットに接続されたシステムの既知の脆弱性（CVE 情報等）を、重要な資産から優先的にパッチ適用等により緩和する。パッチ適用が不可能又は可用性や安全性を損なうおそれのある制御システムについては、ネットワークの

分離や監視等の代替手段を使用し、当該システムがインターネットからアクセスできないようにする。

・ 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにする。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

11.1.3.2. マルウェアからの保護

・ 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。
・ マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトの利用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の導入を検討する。
・ 被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、IPS[9]/プロキシサーバ（不審な外部通信の遮断）、EDR[10]（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)等がある。

11.1.3.3. バックアップ

・ 運用に必要なシステムについて、年 1 回以上の定期的なバックアップを実施する。
・ バックアップデータはバックアップ元のシステムと異なるセグメントにすることやオフラインにする等、切り離して保管し、データの重要度に応じて保存方法、保存期間を定める。また、定期的に復旧テストを実施する。
・ 制御システムについては、設定、役割、PLC ロジック、設計図面、ツールについてもバックアップする。

11.1.3.4. ログ管理

・ システム及びネットワーク機器等のアクセス・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などセキュリティの確保に必要なログを、検知及びインシデント対応で使用するために収集し、保存する。

---

[9] Intrusion Prevention System の略。ネットワークやサーバへの通信を監視し、不正なアクセスを検知して通信を遮断する不正侵入防止システム。
[10] Endpoint Detection and Response の略。従業員が利用する端末やサーバにおける不審な挙動を検知し、迅速に対応するためのセキュリティ対策の一種。

・ 定期的又は適宜、保存したログの点検及び分析を行う。
・ ログを改ざん、削除から保護するための対策を行う。また、イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の制御システムについては、制御システムとの間の通信ログを収集する。
・ 収集したログはツールや中央システム（SIEM 等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。

11.1.3.5. 運用ソフトウェアの管理

・ 重要インフラサービスに係る運用ソフトウェアを、セキュリティを保って管理するための手順及び対策を実施する。
運用ソフトウェアの更新は、管理層の認可に基づき適切に実施する。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。
・ 外部供給ソフトウェアについては、供給者がサポートするバージョンを維持する。供給者は古いバージョンのサポートを終了していくため、重要インフラ事業者はサポートのないソフトウェアに依存するリスクを考慮し、リスク管理策を検討する。
・ 安全に関する要求事項を優先する等の理由により、セキュリティ要求事項を完全には満たしていない場合において、採用するセキュリティ管理策を文書化し、正式に承認を得る。

11.1.3.6. 情報の転送

重要インフラサービスの提供に係る重要情報等を、電子メールや電子データ交換、インスタントメッセージ等の通信手段を活用して情報転送する場合には、あらかじめ機密性や完全性等のセキュリティ確保に係る取組方針や手順を整理するとともに、それらについて転送相手となる関係主体等の合意を図る。

11.1.4. システムの取得・開発・保守

・ 重要インフラサービスの提供に係る情報システムを新たに取得・開発する際や、既存の情報システムを改善する際には、「セキュリティ・バイ・デザイン」の考え方を踏まえ、システムの要求事項に情報セキュリティについての要求も含めて検討を行う（必要に応じて、前述の HSE 等の観点からの要求も含めて検討を行う）。重要インフラの分野によっては、情報システムのセキュリティ確保に

係る国際標準に則した第三者認証制度が存在するため、必要に応じて、認証された情報システムの活用等も検討する。

・ また、情報セキュリティに配慮した開発や構築を実現するための方針や手順、環境等を整備する。特に、情報システムの受け入れ確認の際には、情報セキュリティ関連の要求事項の確認に加えて、情報システムの重要度に応じて、脆弱性診断の実施要否を検討する。さらに、システム開発を外部委託する場合には、情報セキュリティに配慮した開発方針の遵守状況を委託先に対して定期的に確認する。

11.1.5. インシデント管理

・ インシデント管理責任者を定め、責任者に対しセキュリティ事象を報告できる方法を確立する。(関連 11.2.4. エスカレーション)
・ 管理、文書化、検知、優先順位付け、分析、伝達及び利害関係者の調整等を含む、自組織がセキュリティインシデントを管理するためのプロセスを確立する。
・ 一般的な脅威シナリオ及び自組織固有の脅威シナリオに対応するセキュリティインシデント対応計画を策定する。制御システムを保有する場合は制御システムも対象とした脅威シナリオにも対応したセキュリティインシデント対応計画を策定する。策定した対応計画については年 1 回以上訓練を実施し、訓練で得られた教訓をもとにセキュリティインシデント対応計画を更新する。
・ インシデント対応計画には、次の活動が含まれる場合がある。
  * 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、供給者並び顧客など、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

11.2. 人的対策

11.2.1. 経営層の訓練及び従業員の管理

・ 組織の全ての従業員を対象としたトレーニングを年１回以上実施する。フィッシング、ビジネスメール詐欺、パスワードセキュリティなどの基本的な概念を網羅し、サイバーセキュリティに関する組織内文化を醸成する。
・ サイバーセキュリティの基本的なトレーニングに加え、制御システムの運用、維持、保全の担当者は、制御システムに特化したサイバーセキュリティのトレーニングを年１回以上実施する。
・ 雇用の終了又は変更後も有効なセキュリティに関する責任及び義務を定めて、従業員はその要求事項を遵守する。外部委託等の利害関係者に対しても同様の要求事項を伝達する。

11.2.2. 委託先管理

・ 重要インフラサービスに係る業務の外部委託選定の際には、事業場の要求事項に加えて、アクセスされる情報の分類や認識されたリスク等を考慮する。
自組織と委託先との業務委託契約書等には、委託先が自組織のセキュリティの要求を満たすセキュリティ対策に取り組む責任、従業員に対する意識向上の教育・訓練を実施する責任、委託終了後もなお有効なセキュリティに関する責任及び義務等について盛り込む。
なお、継続的に取り組むリスクアセスメントの結果次第では、契約文言の見直しが必要な場合も想定されるため、セキュリティ部門や法務部門等による情報交換の場を定期的に設けることが期待される。
・ 委託期間中においては、委託先に対するセキュリティに関する要求事項が確実に遂行されるよう、委託先の取組状況を定期的に確認し、必要な改善を求める。

11.2.3. テレワーク・遠隔制御

・ 組織の施設外から従業員が作業し、組織内の情報にアクセスする際に行われるテレワークにおいては、以下に例示するトピックについて方針を定め、従業員が遠隔作業している場合のセキュリティ対策を実施する。
  * テレワークサイトにおける、他者（家族、友人等）からの情報又は資源への認可されていないアクセスの脅威
  * 公共の場所にいる他者からの情報又は資源への認可されていないアクセスの脅威
  * 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項、制限事項
  * ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用
  * システムを遠隔で制御し初期化するためのセキュリティに配慮した仕組み
  * テレワークが終了したときの、権限及びアクセス権の失効

11.2.4. エスカレーション

・ 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにする。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

11.3. 物理的対策

・ 情報システムを収容する建物の屋根、壁、天井及び床を強固な構造物とし、外部に接する全ての扉を施錠する。入退室時におけるアクセスカード、生体認証等による認証の仕組みや、警備員、侵入者警報、監視カメラ等による監視システムを構築する。これにより、認可された要員だけが管理領域に入退できるようにする。
・ また、悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。
・ 火災、洪水、地震等の自然災害や、爆発物、武器等による人的災害についてリスクアセスメントを実施し、災害対策や、ランダムな物品検査を実施する。

11.3.1. 装置の管理

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

11.3.2. 電源管理

・ 重要システムが稼働する施設について、雷対策や定期的な計画停電のスケジュールを管理して対応する。
・ 重要システムへ供給する電源系統を複数にすることや、無停電電源装置等を使用し

可用性を考慮した対策を実施する。

11.4.技術的対策

11.4.1. 利用者アクセスの管理

- ユーザーアカウントに管理権限を割り当てず、管理権限も用途ごとに設定する（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 離職者のアカウント管理として、全てのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有する全てのユーザーアカウントと、組織情報へのアクセスを無効にする。

11.4.2. 情報システム等のアクセス制御

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

11.4.2.1. アカウントロック

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

11.4.2.2. パスワード管理

- ハードウェア、ソフトウェア等を使用する前に、製造元のデフォルトパスワードを変更する。制御システムについても、新規又は将来の全てのデバイスのデフォルト認証情報を変更する方針とする。これは、実現が容易なだけでなく、

将来的にサイバー攻撃手法が変化した場合の潜在的なリスクも軽減される。ハードコードされている等、デフォルトパスワードの変更が不可能な場合、代替セキュリティ管理策を実施し、ログインのアクセスログを監視する。

- 自組織の情報資産に対して、パスワードの用途ごとに最小パスワード長及び複雑さを設定する。パスワードの用途は、「ログインパスワード」「パスワードロックされた圧縮ファイルや文書ファイル」「無線アクセスポイントへの接続」等がある。アカウントロックや多要素認証等、他の管理策との組み合わせを考慮して、パスワード長及び複雑さを設定する。
- 自組織のサービスや資産に関して、一意かつ個別のパスワードを設定する。利用者に対し、アカウント、アプリケーション、サービス等でパスワードを再利用させないようにする。

11.4.2.3. 多要素認証の活用

- ハードウェアベースの多要素認証技術が利用可能な場合は有効にする。利用できない場合にはソフトウェアベースを利用する。SMS による多要素認証は、やむを得ない場合を除きできるだけ避けるようにする。

11.4.3. 技術的脆弱性の管理

- 運用する情報システムのソフトウェア及びその他の技術に関して、関連する技術的脆弱性を特定し、組織の情報資産とあわせて整理する。
- 外部から取得した情報システムの場合には、供給者に脆弱性の報告や取扱い及び開示を実施することを要求する。
- 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」、「ロールバックの手順を定める」等、適切な対策を実施する。
- 適用可能な更新、パッチ等がない又はその他の理由により修復が困難な場合には、次のような管理策を検討する。
  - ＊ 提供元が提案する回避策の適用
  - ＊ その脆弱性に関係するサービス又は機能の停止
  - ＊ ネットワーク境界におけるアクセス制御
  - ＊ 適切なトラフィックフィルタ（仮想パッチ）の適用による攻撃からの保護
  - ＊ 実際の攻撃を検知するために、監視を強化

11.4.4. 暗号化を活用した情報管理

11.4.4.1. 機微なデータの取り扱い

・ 個人情報及び認証情報を含む機微なデータは、暗号化して保存され、許可された管理者のみがアクセスできるようにする。

11.4.4.2. 暗号化通信及び電子署名

・ 転送中のデータを保護するために、適切な TLS 暗号化を導入する。
  * 非推奨や、脆弱な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。
  * 制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行う。
  * 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照する。なお、暗号技術に係る国内外の法令及び規制の存在について留意する。
  * 完全性が求められる情報を取り扱う情報システムについては、STARTTLS 等の通信経路の暗号化機能や、DMARC 等の電子署名の付与及び検証を行う機能を設ける必要性の有無を検討する。

11.4.5. 多層防御

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

【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。

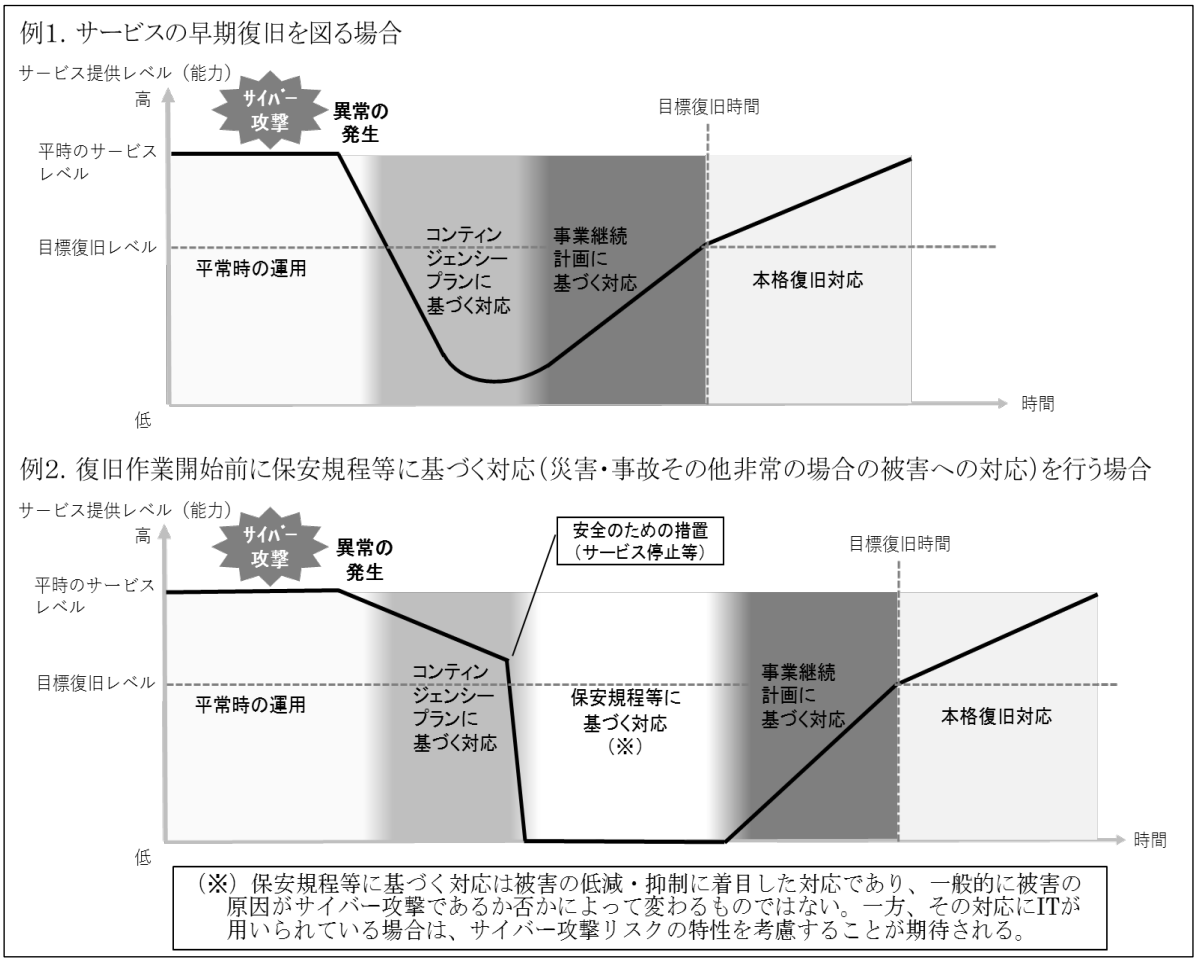
ＣＰ及びＢＣＰの名称や記載の範囲、発動のタイミング等は分野や事業者等によって異なる場合があるため、次頁以降の特性等を考慮して策定・改定すべき対象ドキュメント（以下、適用対象）は各事業者等の状況に応じて検討される必要がある。

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、JPCERT/CC 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の発動に備えた平時の対策）

- 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の発動に備えた平時の対策）

- 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、ネットワークセグメント分割（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[1]（影響範囲の特定と被害端末の隔離）等がある。

[1] Endpoint Detection and Response の略。

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の発動に備えた平時の対策）

- 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の発動に備えた平時の対策）

- 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の発動に備えた平時の対策）

- 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、平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、調査のために平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の発動に備えた平時の対策）

- 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。

参考文献

（マネジメント関連）

- 米国国立標準技術研究所(NIST:National Institute of Standards and Technology). 重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.1 版. 独立行政法人 情報処理推進機構. 2019-01. https://www.ipa.go.jp/security/publications/nist/
- 内閣官房 内閣サイバーセキュリティセンター. 企業経営のためのサイバーセキュリティの考え方. 2016-08-02. https://www.nisc.go.jp/pdf/council/cs/jinzai/dai03/03shiryou01.pdf
- 経済産業省, 独立行政法人情報処理推進機構. サイバーセキュリティ経営ガイドライン Ver3.0. 経済産業省. 2023-03. http://www.meti.go.jp/policy/netsecurity/mng_guide.html
- JIS Q 27014:2015, 情報技術 – セキュリティ技術 – 情報セキュリティガバナンス.
  【対応国際規格】
  ISO/IEC 27014:2013, Information technology – Security techniques – Governance of information security.
- JIS Q 31000:2019, リスクマネジメント – 指針.
  【対応国際規格】
  ISO 31000:2018, Risk management – Guidelines.
- JIS Q 27001:2014, 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム – 要求事項.
  【対応国際規格】
  ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- JIS Q 22301:2013, 社会セキュリティ – 事業継続マネジメントシステム – 要求事項.
  【対応国際規格】
  ISO 22301:2012, Societal security – Business continuity management systems – Requirements.
- JIS Q 19011:2012, マネジメントシステム監査のための指針.
  【対応国際規格】
  ISO 19011:2011, Guidelines for auditing management systems.
- リスクマネジメント規格活用検討会, 編集委員長 野口和彦. ISO 31000:2018 リスクマネジメント 解説と適用ガイド. 日本規格協会. 2019-06-27.

- 米国エネルギー省. Cybersecurity Capability Maturity Model(C2M2) Ver2.1. 2022-06.
  https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
- 米国サイバーセキュリティ社会基盤安全保障庁(Cybersecurity and Infrastructure Security Agency). Cross-Sector Cybersecurity Performance Goals Ver1.0.1. 2023-03.
  https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- 内閣官房 内閣サイバーセキュリティセンター. サイバーセキュリティ関係法令 Q&A ハンドブック Ver.1.0. 2020-03-02.
  https://security-portal.nisc.go.jp/guidance/law_handbook.html
- 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. 2022-07-19.
  https://www.meti.go.jp/policy/economy/keiei_innovation/keizaihousei/corporategovernance/guideline.html
- 株式会社東京証券取引所. コーポレートガバナンス・コード. 2021-06-11.
  https://www.jpx.co.jp/equities/listing/cg/index.html
- 英国国家サイバーセキュリティセンター(National Cyber Security Center). Cyber Assessment Framework Ver3.1. 2022-04.
  https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
- Center for Internet Security (CIS). CIS Controls V8. 2021-05.
  https://www.cisecurity.org/controls
- 経済産業省. 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). 2019-04-18.
  https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
- 米国国防総省. Cybersecurity Maturity Model Certification(CMMC) 2.0. 2021-11.
  https://dodcio.defense.gov/CMMC/Documentation/

（リスクアセスメント関連）

- 独立行政法人情報処理推進機構 技術本部 セキュリティセンター. 制御システムのセキュリティリスク分析ガイド第２版. 2023-03.
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
- 内閣官房 内閣サイバーセキュリティセンター. 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. 2023-03.
  https://www.nisc.go.jp/policy/group/cyber/policy.html

- NIST. SP 800-82 Rev.2 Guide to Industrial Control Systems (ICS) Security. 2015-05.
  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

（サプライチェーン・リスクマネジメント関連）

- 内閣官房 内閣サイバーセキュリティセンター. 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. 2016-10-25.
  https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
- 経済産業省. IT 製品の調達におけるセキュリティ要件リスト. 2018-02-28.
  http://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf
- 独立行政法人情報処理推進機構 セキュリティセンター. IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック. 2018-02-28.
  https://www.ipa.go.jp/security/it-product/guidebook.html
- 内閣官房 内閣サイバーセキュリティセンター. 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. 2022-07-29.
  https://www.nisc.go.jp/pdf/policy/general/SBD_manual.pdf

（事業継続計画関連）

- 内閣官房 内閣サイバーセキュリティセンター. 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）～. 2021-04.
  https://www.nisc.go.jp/pdf/policy/general/itbcp1-1_3.pdf
- 内閣府. 事業継続ガイドライン. 2023-03.
  https://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline202303.pdf

（CSIRT 関連）

- 一般社団法人 JPCERT コーディネーションセンター. インシデントハンドリングマニュアル. CSIRT マテリアル 運用フェーズ. 2021-11-30.
  https://www.jpcert.or.jp/csirt_material/operation_phase.html
- 一般社団法人 JPCERT コーディネーションセンター. CSIRT マテリアル.
  https://www.jpcert.or.jp/csirt_materi

（対策関連）

- サイバーセキュリティ戦略本部. 政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）. 2023-07-04.
  https://www.nisc.go.jp/policy/group/general/kijun.html

- ISO/IEC 27002:2022, Information Security, cybersecurity and privacy protection – Information security controls.
- 一般財団法人 日本情報経済社会推進協会. CSMS 認証基準（IEC62443-2-1）Ver2.0. 情報マネジメントシステム認定センター. 2016-10-04. https://isms.jp/csms/std/index.html
- 一般財団法人 日本情報経済社会推進協会. CSMS ユーザーズガイド －CSMS 認証基準（IEC62443-2-1）対応－Ver1.2. 情報マネジメントシステム認定センター. 2015-05. https://isms.jp/csms/std/index.html
- 経済産業省. 情報セキュリティ管理基準（平成 28 年改正版）. 2016-03-01. http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html
- IoT 推進コンソーシアム, 総務省, 経済産業省. IoT セキュリティガイドライン ver1.0. 2016-07. http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
- 内閣官房 内閣サイバーセキュリティセンター. 政府機関等の対策基準策定のためのガイドライン（令和５年度版）. 2023-7-4. https://www.nisc.go.jp/policy/group/general/kijun.html
- 一般社団法人 JPCERT コーディネーションセンター. 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. 2022-05-23. https://www.jpcert.or.jp/research/apt-loganalysis.html
- 一般社団法人 JPCERT コーディネーションセンター. 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて. 2016-04-21. https://www.jpcert.or.jp/research/apt-guide.html

「重要インフラのサイバーセキュリティに係る行動計画」に基づく
情報共有の手引書

令　　和　　６　　年　　７　　月

内閣官房　内閣サイバーセキュリティセンター

更新履歴

日付	内容	文書番号
令和　２年　３月 31 日	制定	閣サ第 275 号
令和　４年　10 月 14 日	行動計画改定等に伴う改定	閣サ第 770 号
令和　５年　10 月 31 日	他の情報共有体制との関係追加等に伴う改定	閣サ第 733 号
令和　６年　７月 10 日	行動計画改定に伴う改定	閣サ第 592 号

目次

Ⅰ．前書き

１．目的

重要インフラとは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものです。

「重要インフラのサイバーテロ対策に係る特別行動計画」（平成１２年１２月情報セキュリティ対策推進会議決定）において情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）の７分野を重要インフラ分野の対象とし、また、本特別行動計画に基づき平成１３年１０月に官民の連絡・連携体制を構築し、情報共有に取り組んできました。

現在は、「サイバーセキュリティ基本法」（平成２６年法律第１０４号）（以下「法」という。）第１４条において「重要社会基盤事業者等におけるサイバーセキュリティ確保の推進」として情報の共有を講ずることとしているほか、法第１２条の規定に基づき定めている「サイバーセキュリティ戦略」において重要インフラの防護に関し情報共有体制を拡充していくこととしています。

また、法の基本理念にのっとり、これまで数次にわたって策定されてきた「重要インフラのサイバーセキュリティに係る行動計画」（２０２２年６月１７日サイバーセキュリティ戦略本部決定、２０２４年３月８日サイバーセキュリティ戦略本部改定）（以下「行動計画」という。）において、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油及び港湾の１５分野を重要インフラ分野と指定しています。本行動計画において情報共有体制について規定しており、政府内において、重要インフラ事業者からの情報連絡や重要インフラ事業者等への情報提供を行っています。

本手引書は、重要インフラに係る情報共有の具体的内容、手続等を明示することにより、重要インフラ事業者等が行動計画に基づく情報共有を円滑に行うための参考にしていただくことを目的にしています。

なお、本手引書に記載している内容は一例を示したものであり、ＣＳＩＲＴの構築・改善等、重要インフラ事業者等の自発的な活動を妨げるものではありません。

２．使用上の注意

本手引書は、業務をわかりやすく解説することを念頭にしているため、法令用語等の言い換えを行っている場合もあり、必ずしも正確ではない場合があります。厳密な法令解釈が必要な場合は、法及び行動計画が優先します。

Ⅱ．行動計画に基づく情報共有

１．情報共有について

１．１　情報共有の意義

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の動向が刻々と変化する中、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、単独で取り組むセキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組むことが必要です。また、重要インフラサービス障害に係る情報及び脅威や脆弱性情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じることは、当該脅威や脆弱性による被害を最小限に留めるだけでなく、新たなサイバー攻撃の抑止やシステムの不具合の発生防止にもつながります。

１．２　情報共有の全体像

行動計画に基づく情報共有は、重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システムの不具合等に関する情報」という。）を重要インフラ事業者等から重要インフラ所管省庁に連絡し、それを重要インフラ所管省庁がＮＩＳＣに連絡する情報連絡と、サイバーセキュリティ対策に資するための情報をＮＩＳＣから重要インフラ所管省庁に提供し、それを重要インフラ所管省庁が（所管する）重要インフラ事業者等に対して提供する情報提供から成ります。情報共有の流れの概念はそれぞれ図１及び図２に示すとおりです。本枠組は、サイバーセキュリティ基本法に基づいて構築しているものですが、法令等で義務付けられているものではなく、法第６条に重要社会基盤事業者の責務として規定されている「自主的かつ積極的にサイバーセキュリティの確保に努める」、「サイバーセキュリティに関する施策に協力するよう努める」ということから重要インフラ事業者の協力の下、取り組んでいるものとなります。

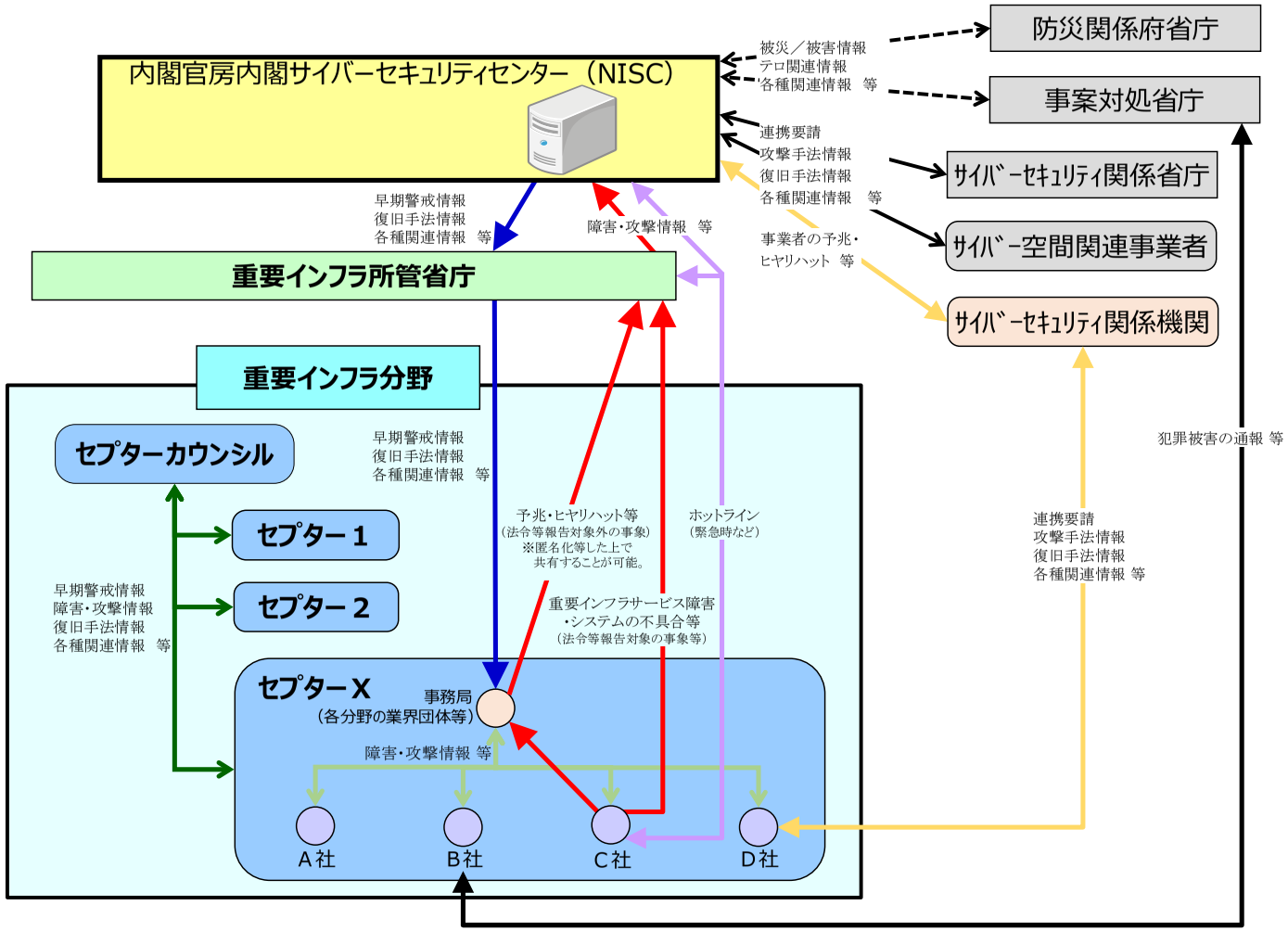


図 1　情報共有体制（通常時）

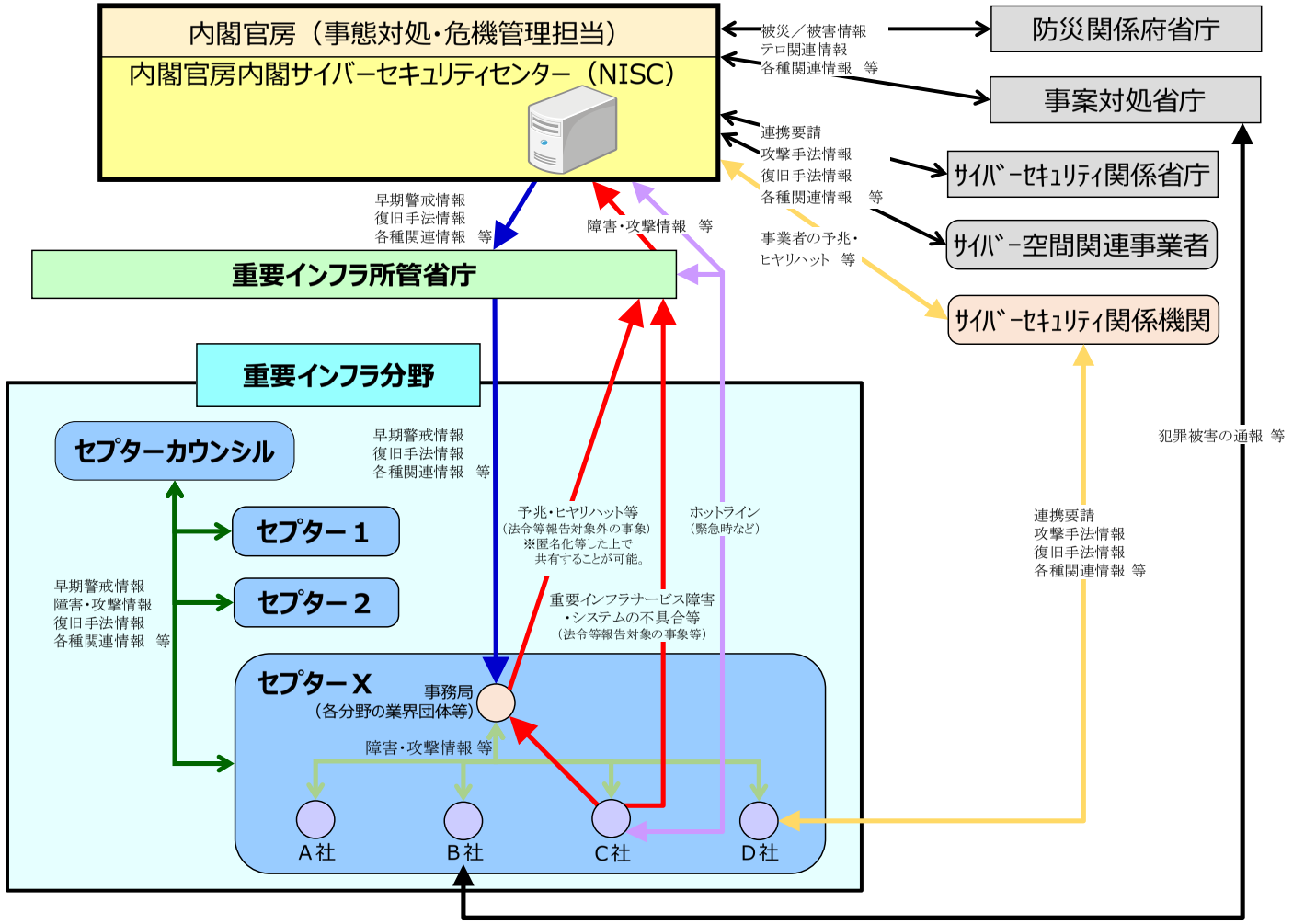


図２　情報共有体制（大規模重要インフラサービス障害対応時）

１．３　情報共有の対象

行動計画に基づく情報共有は「システムの不具合等に関する情報」を対象としており、行動計画中以下のとおり規定しています。なお、ここでいう「システム」には、いわゆる情報系システムに限らず、各重要インフラ分野のプラントやシステム監視等でも用いられる制御システムや IoT 等も含むことに留意してください。

行動計画　別添：情報連絡・情報提供について

1.　システムの不具合等に関する情報

重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システムの不具合等に関する情報」という。）には、①重要インフラサービス障害の未然防止、②重要インフラサービス障害の拡大防止・迅速な復旧、③重要インフラサービス障害の原因等の分析・検証による再発防止の３つの側面が含まれ、政府機関等は重要インフラ事業者等に対して適宜・適切に提供し、また重要インフラ事業者間及び相互依存性のある重要インフラ分野間においてはこうした情報を共有する体制を強化することが必要である。

なお、予兆・ヒヤリハットでは事象が顕在化していないものの、顕在化した際には複数の重要インフラ分野や重要インフラ事業者等の重要インフラサービス障害に至ることも考えられることから、システムの不具合と同様に、情報共有の対象とすることが必要である。

したがって、本行動計画における情報共有の範囲は、図に示すものとする。

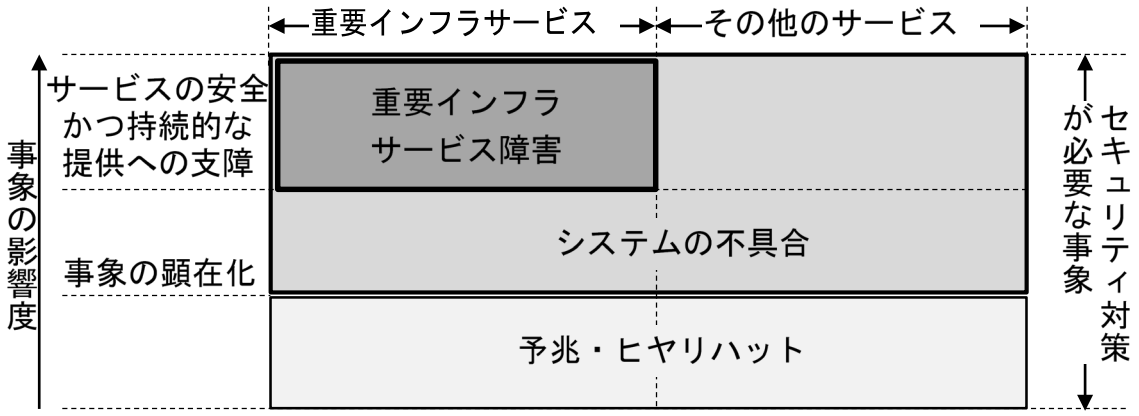


図　情報共有の対象範囲

「図　情報共有の対象範囲」に示されているとおり、情報共有の対象としているものは事象（結果）であり、その原因については限定をしていません。事象の原因について把握し、分析することが必要かつ重要であることから、情報共有における原因について

は、その対象はサイバー攻撃のみならず、情報システムに関係するものとしています。①サイバー攻撃等の「意図的な原因」、②操作ミス等の「偶発的な原因」、③災害や疾病等の「環境的な原因」、④「その他の原因」の４つに分類しています。これは、行動計画に基づき策定されている安全基準等において、重要インフラサービスの安定的供給や事業継続等への影響がないように、顕在化する可能性が高いＩＴ障害を想定した上で、そのＩＴ障害の原因を各重要インフラ分野及び各重要インフラ事業者等の特性等を可能な限り具体的に考慮し規定しているものと同じものです。

①～④の具体的な内容については、各重要インフラ分野が策定している安全基準等において規定している内容を用いることで満たされると考えられます。参考として、その例を表１に示します。

表１　情報連絡における原因の例

原因の類型	原　因	説　明
意図的な原因	不審メール等の受信	標的型攻撃メールやフィッシングメールなどの受信
	ユーザＩＤ等の偽り	パスワードリスト攻撃やＩＤ・パスワードの総当たり攻撃などによるなりすまし
	DDoS 攻撃等の大量アクセス	オープンリゾルバやボットネット等の利用などによる大量アクセス
	情報の不正取得	中間者攻撃やなりすまし等による情報の窃取など
	内部不正	システム運用者等による権限の濫用、盗難や退職者等の権限解除失念等よる不正利用
	適切なシステム等運用の未実施	運用規程等の不遵守、逸脱や適切な規程等の未整備など
偶発的な原因	ユーザの操作ミス	メール誤送信や不適切な権限での情報開示、設定ミスなど
	ユーザの管理ミス	PC や外部記憶媒体(USB メモリ等)等の紛失、盗難など
	不審なファイルの実行	マルウェアに感染した外部記憶装置等の接続やメールの添付ファイル等の閲覧など
	不審なサイトの閲覧	改ざんされたサイトやフィッシングサイト等の悪意あるサイトの閲覧など
	外部委託先の管理ミス	外部委託先による不適切な情報管理やシステム等の運用など
	機器等の故障	ネットワーク機器、ハードウェア機器等の故障（脆弱性以外のソフトウェアの不具合を含む）
	システムの脆弱性	SQL インジェクション等につながる脆弱なコーディング、システムのバグやパッチの未適用などに起因する脆弱性
	他分野の障害からの波及	通信の途絶や停電等の他の重要インフラ分野で発生した障害による影響など
環境的な原因	災害や疾病	地震や台風等による災害やインフルエンザ等の疾病など
その他の原因	その他	上記以外の脅威や脆弱性
	不明	原因を未確認もしくは原因が不明

なお、ここで述べている重要インフラサービスは、重要インフラ事業者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です。各重要インフラ分野における対象となる重要インフラ事業者等と重要システムの例を表２に、重要インフラサービスとその障害の例を表３に示します。

表２　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野	対象となる重要インフラ事業者等(注１)	対象となる重要システム例(注２)
情報通信	・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融　銀行等 生命保険 損害保険 証券 資金決済	・銀行、信用金庫、信用組合、労働金庫、農業協同組合等 ・資金清算機関 ・電子債権記録機関 ・生命保険 ・損害保険 ・証券会社 ・金融商品取引所 ・振替機関 ・金融商品取引清算機関 ・主要な資金移動業者 ・主要な前払式支払手段(第三者型)発行者　　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・金融機関相互ネットワークシステム ・電子債権記録機関システム ・保険業務システム ・証券取引システム ・取引所システム ・振替システム ・清算システム
航空	・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
空港	・主要な空港・空港ビル事業者	・警戒警備・監視システム ・フライトインフォメーションシステム ・バゲージハンドリングシステム
鉄道	・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
ガス	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・地方公共団体	・地方公共団体の情報システム
医療	・医療機関 （ただし、小規模なものを除く。）	・診療録等管理システム ・診療業務支援システム ・地域医療支援システム
水道	・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム
物流	・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学	・主要な石油化学事業者	・プラント制御システム
クレジット	・主要なクレジットカード会社 ・主要な決済代行業者 ・指定信用情報機関　　等	・クレジット(包括信用購入あつせん及び二月払購入あつせん)に係る決済システム ・信用情報提供・収集システム
石油	・主要な石油精製・元売事業者	・受発注システム ・生産管理システム ・生産出荷システム
港湾	・主要な港湾運送事業者・港湾管理者等	・ターミナルオペレーションシステム（TOS）

注１　ここに掲げているものは、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びITへの依存度の進展等を踏まえ、対象とするものの見直しを行う。
注２　ここに掲げているものは、例であり全てではない。

表３　重要インフラサービスとサービス維持レベル

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
情報通信		・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること（電気通信事業法第2条）	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障	・電気通信事業法（業務停止等の報告）第28条 ・電気通信事業法施行規則（報告を要する重大な事故）第58条 【サービス維持レベル】 ・電気通信設備の故障により、役務提供の停止・品質の低下が、３万以上の利用者に対し２時間以上継続する事故が生じないこと
		・放送	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第113条、第122条 ・放送法施行規則（報告を要する重大な事故）第125条 【サービス維持レベル】 ・基幹放送設備の故障により、放送の停止が15分以上継続する事故が生じないこと ・特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が15分以上（中継局の無線設備にあっては、２時間以上）継続する事故が生じないこと
		・ケーブルテレビ	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第137条 ・放送法施行規則（報告を要する重大な事故）第157条 【サービス維持レベル】 ・有線一般放送の業務に用いられる電気通信設備の故障により、放送の停止を受けた利用者の数が３万以上、かつ、停止時間が２時間以上の事故が生じないこと
金融	銀行等	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ（銀行法第10条第1項第１号） ・資金の貸付け又は手形の割引（銀行法第10条第１項第２号） ・為替取引（銀行法第10条第１項第３号）	・預金の払戻しの遅延・停止 ・融資業務の遅延・停止 ・振込等資金移動の遅延・停止	・主要行等向けの総合的な監督指針 ・中小・地域金融機関向けの総合的な監督指針 ・系統金融機関向けの総合的な監督指針

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
		・資金清算	・資金清算（資金決済に関する法律第２条第10項）	・資金清算の遅延・停止	・清算・振替機関等向けの総合的な監督指針
		・電子記録等	・電子記録（電子記録債権法第56条） ・資金決済に関する情報提供（電子記録債権法第62条及び第63条）	・電子記録、資金決済に関する情報提供の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（12 電子債権記録機関関係）
	生命保険	・保険金等の支払	・保険金等の支払請求の受付（保険業法第97条第1項） ・保険金等の支払審査（保険業法第97条第1項） ・保険金等の支払（保険業法第97条第1項）	・保険金等の支払の遅延・停止	・保険会社向けの総合的な監督指針
	損害保険	・保険金等の支払	・事故受付（保険業法第97条第1項） ・損害調査等（保険業法第97条第1項） ・保険金等の支払（保険業法第97条第1項）	・保険金等の支払の遅延・停止	・保険会社向けの総合的な監督指針
	証券	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引（金融商品取引法第２条第８項第１号） ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理（金融商品取引法第２条第８項第２号） ・有価証券等清算取次ぎ（金融商品取引法第2条第８項第5号）	・有価証券売買等の遅延・停止	・金融商品取引業者等向けの総合的な監督指針
		・金融商品市場の開設	・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務（金融商品取引法第2条第14項及び第16項、第80条並びに第84条）	・有価証券の売買、市場デリバティブ取引等の遅延・停止	・金融商品取引所等に関する内閣府令第112条
		・振替業	・社債等の振替に関する業務（社債、株式等の振替に関する法律第８条）	・社債・株式等の振替等の遅延・停止	・社債、株式等の振替に関する法律（事故の報告）第19条 ・一般振替機関の監督に関する命令（事故）第17条 ・清算・振替機関等向けの総合的な監督指針

重要インフラ分野		重要インフラサービス（手続を含む）(注１)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注２)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
		・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
	資金決済	・資金移動業	・為替取引（資金決済に関する法律第２条第２項）	・決済サービスの遅延・停止 ・振込等資金移動の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（14資金移動業者関係）
		・第三者型前払式支払手段の発行	・第三者型前払式支払手段の発行（資金決済に関する法律第3条第1項及び第５項）	・決済サービスの遅延・停止	・事務ガイドライン第三分冊：金融会社関係（５前払式支払手段発行者関係）
航空		・旅客、貨物の航空輸送サービス ・予約、発券、搭乗・搭載手続 ・運航整備 ・飛行計画作成	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条） ・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・搭乗、航空貨物の搭載 ・航空機の点検・整備 ・飛行計画の作成、航空局への提出	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空分野における情報セキュリティ確保に係る安全ガイドライン
空港		・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港分野における情報セキュリティ確保に係る安全ガイドライン
鉄道		・旅客輸送サービス ・発券、入出場手続	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業（鉄道事業法第２条） ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告） 第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第5条 ・鉄道分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
電力	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条第１項第８号） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条第１項第14号）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第3条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス	・一般ガス導管事業 ・ガス製造事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項） ・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第2条第９項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第2条第2項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン
物流	・貨物自動車運送事業 ・船舶運航事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス(手続を含む)(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等(サービス維持レベル(注2))
	呼称	サービス(手続を含む)の説明(関連する法令)		
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期にわたる製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	・クレジットサービス	・クレジット(包括信用購入あつせん及び二月払購入あつせん)に係る決済サービス(割賦販売法第2条第3項及び第35条の16第2項) ・特定信用情報提供業務(割賦販売法第35条の3の36)	・クレジットサービスの遅延・停止 ・カード情報又は信用情報の大規模漏えい	・割賦販売法(後払分野)に基づく監督の基本方針 ・クレジットCEPTOARにおける情報セキュリティガイドライン
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油分野における情報セキュリティ確保に係る安全ガイドライン
港湾	・TOSによるターミナルオペレーション	・陸上輸送によるコンテナ貨物の搬入・搬出、コンテナターミナル内におけるコンテナ貨物の一時保管、海上輸送のための船舶へのコンテナ貨物の積卸し	・荷捌きの効率低下、停止によるコンテナ貨物の搬入・搬出の停滞、停止	・港湾分野における情報セキュリティ確保に係る安全ガイドライン

注１　ITを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。

２．ＮＩＳＣへの情報連絡

２．１　情報連絡の流れ

重要インフラ事業者等において重要インフラサービス障害をはじめとするシステムの不具合等が発生した際において、以下のいずれかのケースに該当する場合、重要インフラ事業者等は重要インフラ所管省庁を通じてＮＩＳＣへ情報連絡を行います。

①法令等で重要インフラ所管省庁への報告が義務付けられている場合。

②関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合。

③そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合。

予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象であるときにも、重要インフラ事業者等から重要インフラ所管省庁に報告を行い、重要インフラ所管省庁がＮＩＳＣへ情報連絡しますが、その他セプター事務局経由で情報連絡元の匿名化等を行った上で重要インフラ所管省庁に報告することも可能です。

情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとし、全容が判明する前の断片的又は不確定なものであっても差し支えありません。

重要インフラ所管省庁は、重要インフラ事業者等あるいはセプター事務局からシステムの不具合等に関する報告のあったものについて、情報連絡様式を用いてＮＩＳＣに情報連絡を行います。ＮＩＳＣは、情報連絡を受領した際には識別番号を採番し、提出を行った重要インフラ所管省庁に識別番号を通知します。

情報連絡の流れを図 3 に示します。

ＮＩＳＣへの情報連絡は電子メールを基本としますが、ファイル転送システム、ＦＡＸ及び電話による情報連絡も可能です。

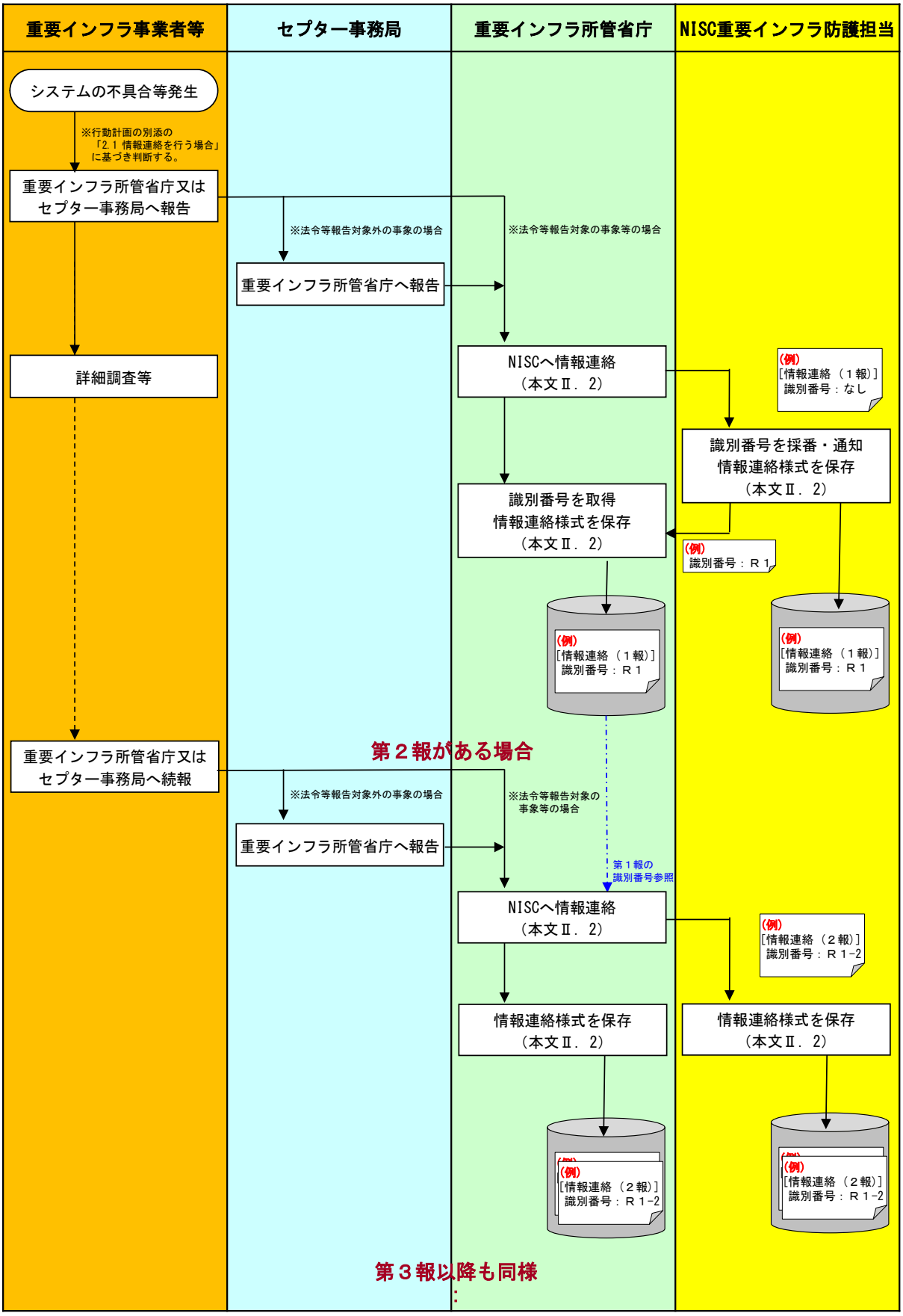

重要インフラ事業者等
セプター事務局
重要インフラ所管省庁
NISC重要インフラ防護担当
システムの不具合等発生
※行動計画の別添の「2.1 情報連絡を行う場合」に基づき判断する。
重要インフラ所管省庁又はセプター事務局へ報告
※法令等報告対象外の事象の場合
※法令等報告対象の事象等の場合
重要インフラ所管省庁へ報告
詳細調査等
NISCへ情報連絡（本文Ⅱ．2）
(例) [情報連絡（１報)] 識別番号：なし
識別番号を採番・通知情報連絡様式を保存（本文Ⅱ．2）
識別番号を取得情報連絡様式を保存（本文Ⅱ．2）
(例) 識別番号：Ｒ１
(例) [情報連絡（１報)] 識別番号：Ｒ１
(例) [情報連絡（１報)] 識別番号：Ｒ１
第２報がある場合
重要インフラ所管省庁又はセプター事務局へ続報
※法令等報告対象外の事象の場合
※法令等報告対象の事象等の場合
重要インフラ所管省庁へ報告
第１報の識別番号参照
NISCへ情報連絡（本文Ⅱ．2）
(例) [情報連絡（２報)] 識別番号：Ｒ１-2
情報連絡様式を保存（本文Ⅱ．2）
情報連絡様式を保存（本文Ⅱ．2）
(例) [情報連絡（２報)] 識別番号：Ｒ１-2
(例) [情報連絡（２報)] 識別番号：Ｒ１-2
第３報以降も同様

図３　情報連絡の流れ

２．２　情報連絡様式

情報連絡様式を図４に、記載例及び記載上の注意を図５に示します。

情報連絡様式に記載する事項は、次のとおりです。

・報数（当該情報連絡が第何報であるか）
・情報連絡を行う日時
・情報連絡を行う重要インフラ所管省庁担当者の情報
・情報共有範囲
・発生した事象の類型
・発生した事象における原因の類型
・別紙の有無
・分野名
・事象が発生した重要インフラ事業者等の名前
・発生した事象の概要
・重要インフラサービス等への影響に関し、サービス維持レベルの逸脱の有無、他の事業者等への波及の可能性の有無
・当該事象に係る推移等
・今後の予定
・その他、得られた教訓等

原則、重要インフラ所管省庁がこれらの記載を行います。ただし、予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象の際で、重要インフラ事業者等、あるいはセプター事務局が様式への記載を行った方が正確な内容となりえると考えられる場合については、この限りではありません。なお、ＮＩＳＣへの情報連絡の際の様式については、管理上の問題から、図４に示す様式のとおり、欄外も含め変更しないでください（非表示は可）。

また、迅速な情報連絡を行うことを優先する観点から、得られた情報の範囲で情報連絡様式を作成、必要に応じて資料を添付するものとし、情報の追加や更新の都度、続報を発信するものとします。特に、セプター事務局からの情報連絡については、事業者名をはじめとして匿名化された情報が含まれている場合もあるため、記載可能な範囲で記載することとします。

☐ 警報　☐ 注意喚起　☐ 参考情報

（重要インフラ所管省庁→内閣官房）

情報連絡様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号*　＿＿＿＿＿＿＿＿＿＿（※第1報の識別番号は空欄）

情報連絡日時*　　年　　月　　日　　時　　分

情報連絡元*	省庁名：		担当者名：	
	部局名：			
	電話番号：		FAX番号：	
	電子メールアドレス：			
情報共有範囲*	☐ RED = 宛先限り （NISC重要インフラ防護担当(※1)限り） ☐ AMBER + STRICT = 特定分野・組織内関係者限り （NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り） ☐ AMBER = 特定分野・関係者限り （NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り） ☐ GREEN = 重要インフラ関係主体限り （NISC、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者、セプター及び重要インフラ事業者等に属する者限り） ☐ CLEAR = 公開情報			
	特記事項：			

※1：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行う。

①発生した事象の類型

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	☐
発生した事象	機密性を脅かす事象	情報の漏えい （組織の機密情報等の流出など）	☐
	完全性を脅かす事象	情報の破壊 （Webサイト等の改ざんや組織の機密情報等の破壊など）	☐
	可用性を脅かす事象	システム等の利用困難 （制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	☐
	上記につながる事象(※3)	マルウェア等の感染 （マルウェア等によるシステム等への感染）	☐
		不正コード等の実行 （システム脆弱性等をついた不正コード等の実行）	☐
		システム等への侵入 （外部からのサイバー攻撃等によるシステム等への侵入）	☐
		その他	☐

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の類型

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	☐
	ユーザID等の偽り	☐
	DDoS攻撃等の大量アクセス	☐
	情報の不正取得	☐
	内部不正	☐
	適切なシステム運用等の未実施	☐
偶発的な原因	ユーザの操作ミス	☐
	ユーザの管理ミス	☐
	不審なファイルの実行	☐
	不審なサイトの閲覧	☐
	外部委託先の管理ミス	☐
	機器等の故障	☐
	システムの脆弱性	☐
	他分野の障害からの波及	☐
環境的な原因	災害や疾病等	☐
その他の原因	その他	☐
	不明	☐

◆情報連絡の内容(※4)　　（別紙有無*：☐有　☐無 ）

項　目	情報の内容
③分野名*(※5)	
④事象が発生した重要インフラ事業者等名	
⑤概　要	判明日時：　年　月　日　時　分 （発生日時：　年　月　日　時　分 ） 事象が発生したシステム・委託先業者等： 発生事象の概要： システムの稼働状況：☐影響なし　☐停止中　☐一部稼働中　☐復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：☐有　☐無 他の事業者等への波及の可能性：☐有　☐無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 （補足情報） 対外的な対応状況 報道発表、報道等への掲載：☐済　☐予定有　☐無　（済・予定有では日時・件名を記入） 個人情報保護委員会への連絡：☐済　☐予定有　☐確認中　（済では日時・件名を記入） その他NISC以外に連絡を行った先：
⑧今後の予定	☐事象継続中 （続報あり） ☐事後調査実施中 （続報あり） ☐今後の対応策を継続検討 （続報なし） ☐対応完了 （続報なし）
⑨その他 ・得られた教訓等	

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラのサイバーセキュリティに係る行動計画」に定める「重要インフラ分野」を指す。
※6：「重要インフラのサイバーセキュリティに係る行動計画」に定める「サービス維持レベル」を指す。

図４　情報連絡様式

記載例

☐ 警報　☐ 注意喚起　■ 参考情報

（重要インフラ所管省庁→内閣官房）

記載例　：青字
記載上の注意：赤字

情報連絡様式

（第　1　報*）

（*が付与された項目は必須事項）

西暦で記載

24時間表記で記載

識別番号*	（※第1報の識別番号は空欄）
情報連絡日時*	2023 年　8 月　19 日　13 時　15 分

いつ時点での内容かの日付・時間を記載。（記載するとセルの色は白に変化）

情報連絡元*	省庁名：	XX省	担当者名：	連絡　太郎
	部局名：	YY課		
	電話番号：	03-XXXX-YYYY	FAX番号：	03-XXXX-YYYY
	電子メールアドレス：	renraku.taro@xx.go.jp		

情報共有範囲*

☐ RED = 宛先限り
（NISC重要インフラ防護担当(※1)限り）

☐ AMBER + STRICT = 特定分野・組織内関係者限り
（NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り）

☐ AMBER = 特定分野・関係者限り
（NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り）

■ GREEN = 重要インフラ関係主体限り
（NISC、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者、セプター及び重要インフラ事業者等に属する者限り）

☐ CLEAR = 公開情報

選択したＴＬＰ（情報共有範囲）に関する補足情報を記載。

特記事項：
企業名・該当サービス等、企業が特定される事項を除いて他分野への情報提供可。

※1：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行う。

①発生した事象の類型

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	☐
発生した事象	機密性を脅かす事象	情報の漏えい（組織の機密情報等の流出など）	☐
	完全性を脅かす事象	情報の破壊（Webサイト等の改ざんや組織の機密情報等の破壊など）	■
	可用性を脅かす事象	システム等の利用困難（制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	☐
	上記につながる事象(※3)	マルウェア等の感染（マルウェア等によるシステム等への感染）	☐
		不正コード等の実行（システム脆弱性等をついた不正コード等の実行）	☐
		システム等への侵入（外部からのサイバー攻撃等によるシステム等への侵入）	☐
		その他	☐

最初に明らかとなった事象について、１つだけ■を選択する。

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の類型

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	☐
	ユーザID等の偽り	☐
	DDoS攻撃等の大量アクセス	☐
	情報の不正取得	☐
	内部不正	☐
	適切なシステム運用等の未実施	☐
偶発的な原因	ユーザの操作ミス	☐
	ユーザの管理ミス	☐
	不審なファイルの実行	☐
	不審なサイトの閲覧	☐
	外部委託先の管理ミス	☐
	機器等の故障	☐
	システムの脆弱性	☐
	他分野の障害からの波及	☐
環境的な原因	災害や疾病等	☐
その他の原因	その他	☐
	不明	■

発生原因について■を選択する。複数選択可。

◆情報連絡の内容(※4)　（別紙有無*：☐ 有　■ 無）

項　目	リストから選択 情報の内容
③分野名*(※5)	○○分野
④事象が発生した重要インフラ事業者等名	○○株式会社
⑤概　要	判明日時：　2023 年　8 月　18 日　20 時　0 分 （発生日時：　2023 年　8 月　19 日　2 時　59 分　（サーバログ等より推測）） 事象が発生したシステム・委託先業者等： 会社情報管理サービス（https://example.com/top.php） ・会員がアクセスし、個人情報の変更やサービス申込等を実施。 発生事象の概要： ・○○株式会社の会員情報管理サービスのWEBサイトが改竄された。 ・閲覧したユーザにウイルス感染の恐れがあり、現在、当該サイトを一時閉鎖しサービス停止中。 ・多数の個人情報流出が確認されており、被害の詳細を調査中。 システムの稼働状況：　☐ 影響なし　■ 停止中　☐ 一部稼働中　☐ 復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：　☐ 有　■ 無 他の事業者等への波及の可能性：　☐ 有　■ 無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 XX/XX 00:00 / 外部より○○株式会社のHPがおかしいと匿名メールを受信。 XX/XX 01:00 / サーバ運用ベンダへ連絡。サーバログ等の調査をし、HPが改ざんされていることを確認。 XX/XX 03:00 / アクセスした利用者にウィルス感染のおそれがあるためサーバを停止。 （必要に応じて行を追加して経緯を記載。） （補足情報） ・XX月XX日現在、○○件の個人情報流出を確認。 （名前、住所、電話番号、メールアドレスが漏えい。） ・コンテンツ管理システムYYYYのv99.99の脆弱性を突かれたものと想定される。 （報道発表等がある場合は、別紙として添付する、あるいは掲載ページのアドレス等を記載。） 対外的な対応状況 報道発表、報道等への掲載：　■ 済　☐ 予定有　☐ 無　（済・予定有では日時・件名を記入） XX/XX 09:00頃　○○株式会社のトップページにニュースリリースを掲載。 （https://example.com/newsXXXX） 個人情報保護委員会への連絡：　☐ 済　☐ 予定有　■ 確認中　（済では日時・件名を記入） 現在のところ、個人情報漏洩の事実は確認されていない。 NISC以外に連絡を行った先： XX/XX 10:00頃　○○県警へ通報
⑧今後の予定	■ 事象継続中　（続報あり） ☐ 事後調査実施中　（続報あり） ☐ 今後の対応策を継続検討　（続報なし） ☐ 対応完了　（続報なし）
⑨その他 ・得られた教訓等	・現時点での得られた教訓は、経営層への情報のエスカレーション体制を普段から確認し、迅速な判断ができるようにすること。

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラのサイバーセキュリティに係る行動計画」に定める「重要インフラ分野」を指す。
※6：「重要インフラのサイバーセキュリティに係る行動計画」に定める「サービス維持レベル」を指す。

図５　情報連絡様式記載例

２．３　情報連絡様式中の具体的記載について

本項では、情報連絡様式中、補足説明が必要と考えられるものについて解説します。

(1) 重要度

情報連絡様式において、対策を実施する主体※がとるべき対応に応じて重要度をあらかじめ警報、注意喚起、参考情報の３段階に定義しています。重要度は次に示す表４の説明を参考に適切なものを選択します。

※対策を実施する主体：情報連絡を受領し、その内容に対して対策を行う者。

すなわち情報連絡の場合、重要インフラ所管省庁からＮＩＳＣへの連絡ですので、各重要インフラ所管省庁が当該情報連絡の内容をどの程度の重要度として捉えているのかを示す項目になります。

表４　情報連絡の重要度及びその説明

重要度	説明
警報	対策を実施する主体において、直ちに対応について検討することが推奨される情報
注意喚起	対策を実施する主体において、対応について検討することが推奨される情報
参考情報	対策を実施する主体に対するサイバーセキュリティ対策への参考情報

(2) 情報共有範囲（Traffic Light Protocol：ＴＬＰ）

情報連絡に記載する情報には、企業情報や、情報の拡散により脅威が増大するおそれのある機微情報等が含まれることから、情報発信者※は、適切なＴＬＰを設定する必要があり、情報を受け取った側では、設定されたＴＬＰを必ず守らねばなりません。

※重要インフラ事業者等が重要インフラ所管省庁に報告する際にあっては、重要インフラ事業者等。セプター事務局が重要インフラ所管省庁に報告する際にあっては、セプター事務局。重要インフラ所管省庁がＮＩＳＣに情報連絡する際にあっては、重要インフラ所管省庁。

ＴＬＰによる情報の共有範囲は、

・RED＝宛先限り、すなわちＮＩＳＣ重要インフラ防護担当及び重要インフラ所管省庁（情報提供先又は情報提供元の所管省庁）限り

・AMBER+STRICT＝特定分野・組織内関係者限り、すなわちＮＩＳＣ重要インフラ防護担当並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者（その組織の職員）

で、かつ業務の遂行に当たって、その情報を知る必要がある者限り

・AMBER＝特定分野・関係者限り、すなわちＮＩＳＣ重要インフラ防護担当並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）で、かつ業務の遂行に当たって、その情報を知る必要がある者限り

・GREEN＝重要インフラ関係主体限り、すなわちＮＩＳＣ、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り

・CLEAR＝公開情報

上記に加えて、

・情報発信者が、上記の情報共有範囲に含まれない対象の追加を求める場合は、当該対象を共有範囲に含めることができます。

・ＮＩＳＣ重要インフラ防護担当においては、事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行います。

であり、その定義は表５に示すとおりです。

情報連絡様式中にあらかじめＴＬＰの欄を設定しているので、そこから適切なものを選択します。ただし、例えば、RED を選択した場合であっても、事象が発生した重要インフラ事業者等がウェブサイトでその内容を発表しており、その内容については共有可能であるなど、ＴＬＰによらない部分的に共有が可能な範囲などがある場合には、その内容を特記事項に記載するようにしてください。

表５　情報共有範囲

区　分	情報共有可能な範囲(※1)	定義
RED 宛先限り	・　ＮＩＳＣ（重要インフラ防護担当）※2 ・　重要インフラ所管省庁（情報提供先又は情報提供元の所管省庁）	情報発信者と、情報受信者の２者間に限定する。
AMBER+STRICT 特定分野・組織内関係者限り	・　ＮＩＳＣ（重要インフラ防護担当）※2 ・　重要インフラ所管省庁（直接関係する分野） ・　セプター（直接関係する分野） ・　セプターを構成する重要インフラ事業者等（直接関係する分野）	左記の情報共有範囲に属する者（その組織の職員）で、かつ業務の遂行に当たって、その情報を知る必要がある者に限る。
AMBER 特定分野・関係者限り	・　ＮＩＳＣ（重要インフラ防護担当）※2 ・　重要インフラ所管省庁（直接関係する分野） ・　セプター（直接関係する分野） ・　セプターを構成する重要インフラ事業者等（直接関係する分野）	左記の情報共有範囲に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）で、かつ業務の遂行に当たって、その情報を知る必要がある者に限る。
GREEN 重要インフラ関係主体限り	・　ＮＩＳＣ ・　重要インフラ所管省庁 ・　事案対処省庁 ・　サイバーセキュリティ関係省庁 ・　防災関係府省庁 ・　サイバーセキュリティ関係機関 ・　サイバー空間関連事業者 ・　セプター ・　重要インフラ事業者等	左記の情報共有範囲に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）に限る。
CLEAR 公開情報	・　限定なし	要機密情報としての扱いは要さない。著作権を適性に扱う限りにおいて、分配、出版、インターネット上での公開及び放送に供することも可能とする。

※１：情報発信者が、上記の情報共有範囲に含まれない対象の追加を求める場合は、当該対象を共有範囲に含めることができるものとする。

※２：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行う。

(3) 別紙

発生した事象に関し、報道発表・ウェブサイトでの発表等を行っている場合には、リンク先の明示や当該資料を別紙として添付することが望まれます。

また、発生した事象に係る検体等（届いた電子メール、添付されていたファイル等）は攻撃者に係る情報、対策の検討等に有益なものです。このため、それらをＮＩＳＣが必要と判断する場合、重要インフラ所管省庁及び重要インフラ事業者等と調整の上、提供いただく場合があります。

２．４　情報連絡の取扱いについて

(1) 秘匿性の確保

情報連絡は機微情報を含むことから秘匿性を確保するものとします。ＮＩＳＣは、付番、公開範囲等に基づき体系的に管理し、保存し、必要な時にいつでも参照できるようにします。

(2) 検体等

ＮＩＳＣが検体等を受領した際には、ＮＩＳＣにおいて分析を行うほか、あらかじめ連携を要請したサイバーセキュリティ関係機関と共有し、分析等を依頼することもあります。

３．ＮＩＳＣからの情報提供

３．１　情報提供の流れ

ＮＩＳＣは、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者及び重要インフラ事業者から提供される幅広いシステムの不具合等に関する情報を集約、分析等した上で、以下のいずれかのケースに該当する場合に情報提供を行います。

①セキュリティホールやプログラム・バグ等に関する情報を入手した場合等であって、他の重要インフラ事業者等においてもその情報に関係する重大な問題を生じるおそれがあると認められる場合。

②サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合。

③そのほか重要インフラ事業者等のサイバーセキュリティの確保に有効と考えられる場合。

ＮＩＳＣは、情報の提供元が特定されないよう、情報を加工するなど、不利益を被らないための適切な措置を講じた上で情報提供を行います。

また、ＮＩＳＣから重要インフラ事業者等への情報提供の範囲は、情報の提供元があらかじめ示す情報共有可能な範囲のうち、ＮＩＳＣが当該情報に関係すると考える重要インフラ分野とします。なお、情報の提供元が示す情報共有可能な範囲を越えて情報共有する必要があるとＮＩＳＣが認める場合には、その共有範囲の変更について情報の提供元との間で調整を行います。

ＮＩＳＣから重要インフラ事業者等への情報提供は、重要インフラ所管省庁へ行い、情報提供を受領した重要インフラ所管省庁がセプター事務局、あるいは必要に応じて直接重要インフラ事業者等に展開することにより実施します。

情報提供の流れを図６に示します。

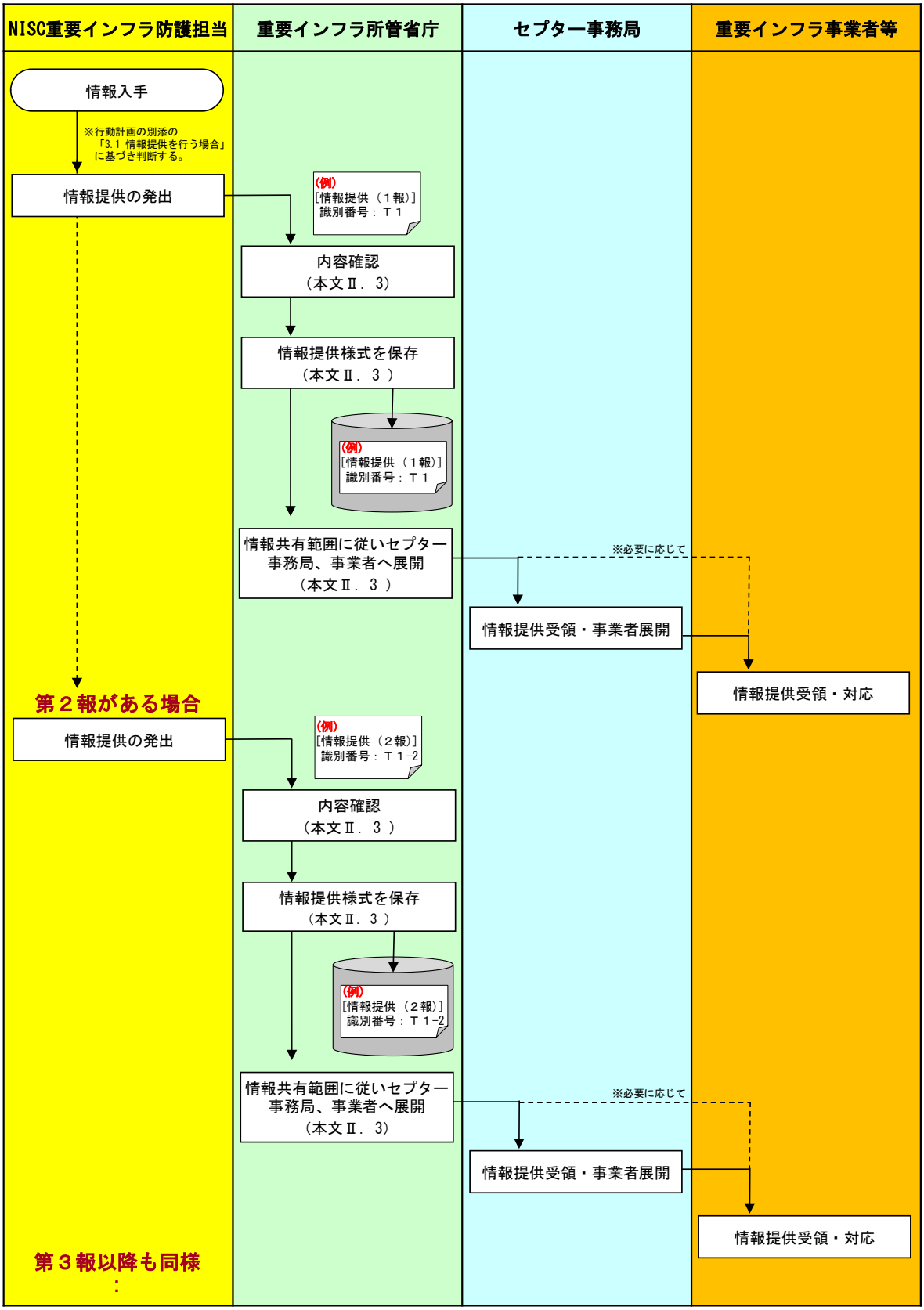

NISC重要インフラ防護担当
重要インフラ所管省庁
セプター事務局
重要インフラ事業者等
情報入手
※行動計画の別添の「3.1 情報提供を行う場合」に基づき判断する。
情報提供の発出
(例)
[情報提供（1報)]
識別番号：T1
内容確認
（本文Ⅱ．3）
情報提供様式を保存
（本文Ⅱ．3 ）
(例)
[情報提供（1報)]
識別番号：T1
情報共有範囲に従いセプター事務局、事業者へ展開
（本文Ⅱ．3 ）
※必要に応じて
情報提供受領・事業者展開
情報提供受領・対応
第２報がある場合
情報提供の発出
(例)
[情報提供（2報)]
識別番号：T1-2
内容確認
（本文Ⅱ．3 ）
情報提供様式を保存
（本文Ⅱ．3 ）
(例)
[情報提供（2報)]
識別番号：T1-2
情報共有範囲に従いセプター事務局、事業者へ展開
（本文Ⅱ．3）
※必要に応じて
情報提供受領・事業者展開
情報提供受領・対応
第３報以降も同様
：

図６　情報提供の流れ

３．２　情報提供様式

情報提供様式及びその記載例をそれぞれ図７及び図８に示します。

ＮＩＳＣは、本様式に必要事項を記入し重要インフラ所管省庁に対し情報提供を行います。補足すべき事項等がある場合には別紙にてその内容の説明を行います。

なお、情報提供におけるＮＩＳＣへの問合せは、情報共有範囲内の重要インフラ所管省庁に限ります。

☐ 警報　☐ 注意喚起　☐ 参考情報

（内閣官房→重要インフラ所管省庁）

情報提供様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号*

情報提供日時*　　年　　月　　日

情報提供先* （所管省庁名及び分野名）	
情報共有範囲*	☐ RED = 宛先限り （情報提供先の重要インフラ所管省庁限り） ☐ AMBER + STRICT = 特定分野・組織内関係者限り （情報提供先の直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り） ☐ AMBER = 特定分野・関係者限り （情報提供先の直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り） ☐ GREEN = 重要インフラ関係主体限り （重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者限り） ☐ CLEAR = 公開情報
	特記事項：

◆情報提供の内容　　**（別紙有無*：☐ 有　　☐ 無 ）**

項　目		情報の内容
脅威等の内容	①概　要	
	②対　象	
③対処方針		
④その他		

本件問合せ先（重要インフラ所管省庁からの問合せに限る。）
内閣サイバーセキュリティセンター
重要インフラ防護担当：
電話番号 ：
FAX番号 ：
電子メールアドレス ：

図７　情報提供様式

☐ 警報　☐ 注意喚起　■ 参考情報

記載例　：青字

（内閣官房→重要インフラ所管省庁）

情報提供様式

（第　1　報*）

（*が付与された項目は必須事項）

識別番号*	Txxxxxx
情報提供日時*	2022 年　XX 月　XX 日　13:00

情報提供先* （所管省庁名及び分野名）	XX省（ZZ分野）、YY省（ZZ分野）、…
情報共有範囲*	☐ RED = 宛先限り （情報提供先の重要インフラ所管省庁限り） ☐ AMBER + STRICT = 特定分野・組織内関係者限り （情報提供先の直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り） ☐ AMBER = 特定分野・関係者限り （情報提供先の直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り） ■ GREEN = 重要インフラ関係主体限り （重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者限り） ☐ CLEAR = 公開情報
	特記事項： 特になし

◆情報提供の内容　（別紙有無*：☐ 有　■ 無 ）

項　目		情報の内容
脅威等の内容	①概　要	大手サイトfunifuniにおいてサイト改ざんが行われ、当該サイトへのアクセスに伴いマルウェア（悪意のあるソフトウェア）感染のおそれがあります。
	②対　象	XX年XX月XX日以降に http://example.co.jp/top(.)html にアクセスした場合。
③対処方針		○Webアクセスログ等の確認を行う。 ○マルウェアの通信先である次のIP及びドメインをブロックする。 XX.XX.XX.XX、ZZ.ZZ.ZZ.ZZ、example.com
④その他		特になし

本件問合せ先（重要インフラ所管省庁からの問合せに限る。）
内閣サイバーセキュリティセンター
重要インフラ防護担当：提供　花子
電話番号：　03-xxxx-xxxx
FAX番号：　03-xxxx-xxxx
電子メールアドレス：　teikyo.hanako@xx.go.jp

図８　情報提供様式記載例

３．３　情報提供様式中の具体的記載について

本項では、情報提供様式中、補足説明が必要と考えられるものについて解説しますが、本項は前述の情報連絡様式における説明と基本的に同様です。

(1) 重要度

情報提供様式において、対策を実施する主体※がとるべき対応に応じて重要度をあらかじめ警報、注意喚起、参考情報の３段階に定義しています。重要度は次に示す表４の説明を参考に適切なものを選択します。

※対策を実施する主体：情報提供を受領し、その内容に対して対策を行う者。

すなわち情報提供の場合、ＮＩＳＣから重要インフラ所管省庁への連絡ですので、ＮＩＳＣ側で当該情報連絡の内容をどの程度の重要度として捉えているのかを示す項目になります。

表４　情報提供の重要度及びその説明

重要度	説明
警報	対策を実施する主体において、直ちに対応について検討することが推奨される情報
注意喚起	対策を実施する主体において、対応について検討することが推奨される情報
参考情報	対策を実施する主体に対するサイバーセキュリティ対策への参考情報

(2) 情報共有範囲（Traffic Light Protocol：ＴＬＰ）

情報提供に記載している情報には、企業情報や、情報の拡散により脅威が増大するおそれのある機微情報等が含まれることから、情報発信者※は、適切なＴＬＰを設定する必要があり、情報を受け取った側では、設定されたＴＬＰを必ず守らねばなりません。

※この場合、情報発信者はＮＩＳＣになります。

ＴＬＰによる情報の共有範囲は、

・RED＝宛先限り、すなわちＮＩＳＣ重要インフラ防護担当及び重要インフラ所管省庁（情報提供先又は情報提供元の所管省庁）限り

・AMBER+STRICT＝特定分野・組織内関係者限り、すなわちＮＩＳＣ重要インフラ防護担当並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者（その組織の職員）で、かつ業務の遂行に当たって、その情報を知る必要がある者限り

・AMBER＝特定分野・関係者限り、すなわちＮＩＳＣ重要インフラ防護担当並び

に直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）で、かつ業務の遂行に当たって、その情報を知る必要がある者限り

・GREEN＝重要インフラ関係主体限り、すなわちＮＩＳＣ、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属するもの限り

・CLEAR＝公開情報

上記に加えて、

・情報発信者が、上記の情報共有範囲に含まれない対象の追加を求める場合は、当該対象を共有範囲に含めることができます。

・ＮＩＳＣ重要インフラ防護担当においては、事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行います。

であり、その定義は表５に示すとおりです。

情報提供様式中にあらかじめＴＬＰの欄を設定しているので、そこから適切なものを選択し、情報提供を行います。ただし、RED が選択されている場合であっても、RED である内容が限定的であり、その他については共有可能であるなど、ＴＬＰによらない部分的に共有が可能な範囲などがある場合には、その内容を特記事項に記載して情報提供を行います。

Ⅲ．他の情報共有体制との関係

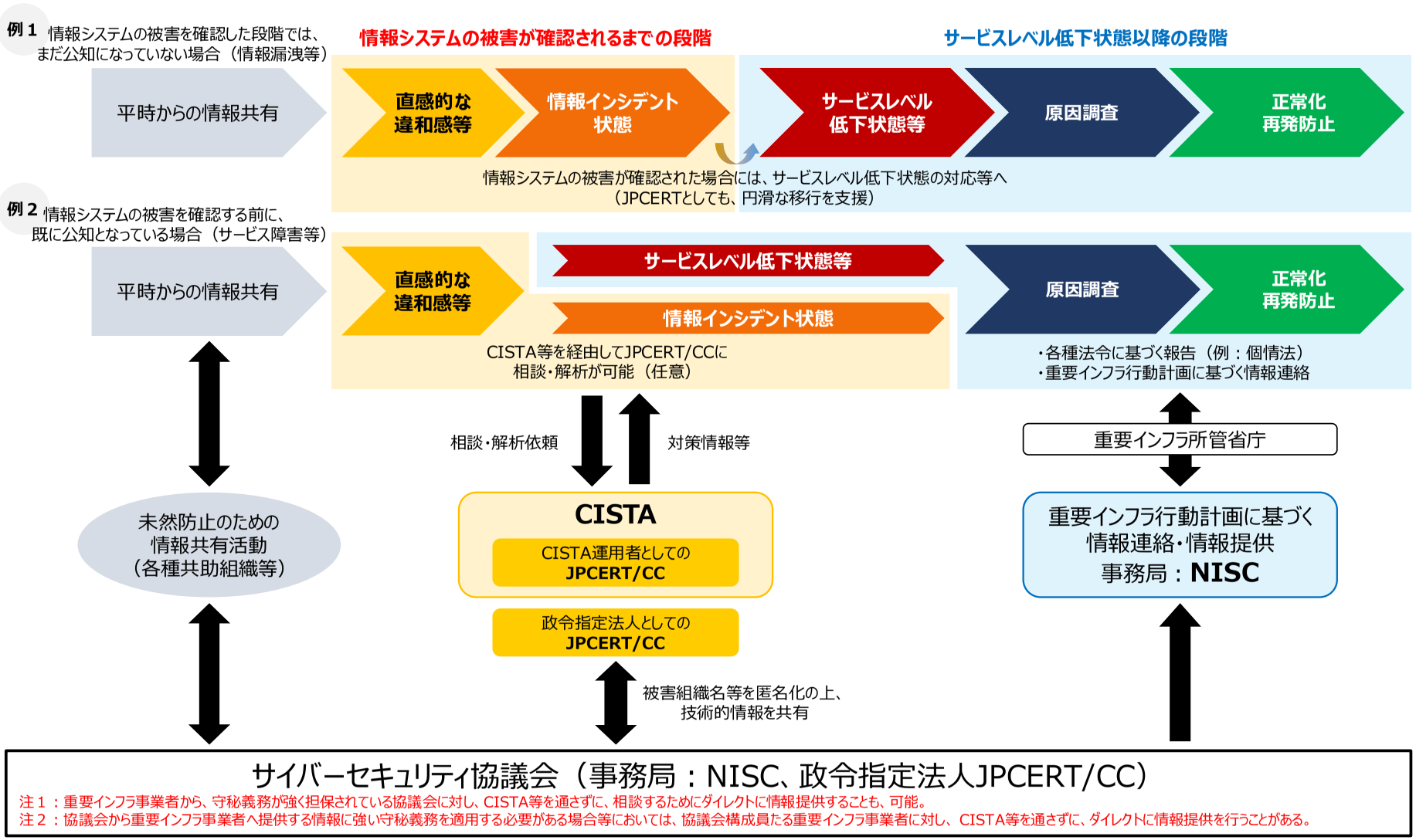
１．サイバーセキュリティ協議会

サイバーセキュリティ協議会は、サイバーセキュリティ基本法の規定に基づき平成３１年４月１日に創設された枠組みです。官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うものであり、主として、脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行うものです。協議会に加入し構成員となることにより対策情報等の受領ができるほか、情報インシデント状態の際に相談・解析依頼等を行うことができます。本枠組みにおいては法令で守秘義務を規定していることから、これまで外部に提供することがためらわれた情報の共有を図りやすいという利点があります。

本枠組みと行動計画に基づく情報共有との関係を図示すると図９のとおりです。

すなわち、通常業務を行う中で「いつもと何か違う」といった直感的な違和感が生じた段階やサイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態（情報インシデント状態）といった、情報システムの被害が確認されていない早期の段階では、罰則により担保された守秘義務の下、安心して協議会に対し相談等を行うことが考えられます。その後、情報システムの被害が確認され、平常時（情報システムによるサービスが安全かつ持続的に提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティエンジェンシープラン等に基づく対応を行っている状態（サービスレベルが低下状態）へ移行（※）した場合には、行動計画に基づく情報共有体制を活用することになります。

（※）なお、情報システムの被害を確認する前の段階で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まります。



※「情報インシデント状態」：ここでは、サイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態をいう。
※「サービスレベル低下状態」：ここでは、平常時（情報システムによるサービスが安全かつ持続的に提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティエンジェンシープラン等に基づく対応を行っている状態をいう。なお、情報システムの被害を確認する前の段階（そもそも攻撃の存在を検知・認知していないケースを含む。）で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合（上記「例２」）においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まることとなる。
※「CISTA」：経済産業省予算事業「CISTA・検体分析機能の実用性調査及び開発」事業で運用する、情報共有・検体解析ポータルシステムをいう。
※「行動計画に基づく情報連絡」：ここでは、重フラ行動計画「2.1 情報連絡を行う場合」の対象となる情報のうち、事業者における事案発生の疑いの段階での事案の連絡、相談を気兼ねなく安心して行うことができる情報共有体制における取扱いが適すると考えられる情報（例：事業者等が検知した情報で非公知のもの、特定分野間に限定されるもの、機微性が高いもの、詳細な内容のものなどをいう。）を除いたものの情報連絡をいう。
※協議会が重要インフラ以外の主体から得られた情報等に基づき重要インフラ分野においても早期対処が必要と判断した場合には、提供者の同意を得た上で行動計画側等に提供することがあり得る。これに対し、行動計画側等から協議会側に早期対処の情報連絡を行う必要が生じるケースは、現実的にほぼ想定されない。

図９　協議会との関係

２．ＣＩＳＴＡ（Collective Intelligence Station for Trusted Advocates）

ＣＩＳＴＡ（シスタ）は、一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」という。）と早期警戒情報受信組織との間で、脅威情報や分析結果及びそれらに対するフィードバック情報等の共有を行うシステムであり、JPCERT/CC が受信組織に対して脅威情報や分析結果、技術レポート等を提供し、受信組織が JPCERT/CC に対してフィードバックや検体等の提供を行うことにより、脅威情報を共有し、インシデントの未然防止や被害拡大の抑止を図るとともに、情報インフラ全体のリスク低減を目的としたものです。

３．サイバー情報共有イニシアティブ「Ｊ－ＣＳＩＰ」

Ｊ－ＣＳＩＰ（Initiative for Cyber Security Information sharing Partnership of Japan）は、独立行政法人情報処理推進機構（以下「ＩＰＡ」という。）が情報の中継点・相談役として、国内の重要産業等に対するサイバー攻撃への対策を、各業界での自主的・互助的に行う情報共有活動です。ＩＰＡは、提供・共有された情報が重要な攻撃情報と判断した場合には、情報提供元組織に対して、所管省庁等への報告を勧めることがあります。また、この際ＩＰＡの見解やアドバイスが求められた場合は、相談対応の一環として可能な範囲で対応します。

４．ＪＩＳＰ（Japan cyber security Information Sharing Partnership）

ＪＩＳＰ（ジスプ）は、サイバーセキュリティ対策を政府が積極的に支援する官民連携の取組。民間団体、地方公共団体、政府関係組織、情報セキュリティ関係機関等が、サイバーセキュリティに関する脅威情報、インシデント情報等をワンストップで共有でき、参加組織からの要請に応じて助言及び対処支援調整を行うパートナーシップです。2019 年４月から 2020 年東京オリンピック/パラリンピック競技大会のサイバーセキュリティの取組として運用を開始し、2022 年４月から、サイバーセキュリティ協議会の枠組みの中での取組として活動を継承しました。社会経済を支えるサービスを提供する組織を対象に加え、社会全体のサイバーセキュリティの確保に向け、持続的なサイバーセキュリティ対策の推進を目的としています。

５．サイバーセキュリティ対処調整センター

サイバーセキュリティ対処調整センター（以下「CS 対処調整センター」という。）は、サイバーセキュリティ協議会の枠組みの中の JISP の運営事務局です。サイバーセ

キュリティ基本法（平成 26 年法律第 104 号）に基づくサイバーセキュリティ戦略（令和３年９月 28 日閣議決定）にのっとり、2025 年日本国際博覧会（以下「大阪・関西万博」という。）に係るサイバーセキュリティ上の脅威・事案情報の収集・提供及びインシデント発生時の対処支援調整を行う中核的役割を担っている組織であり NISC が中心となって運営を行っています。

大阪・関西万博に関するサイバー事案の関連情報共有と対処支援調整は、全体としては CS 対処調整センターが担当します。とりわけ、大阪・関西万博の安全・円滑な準備及び運営並びに持続性の確保のため、大阪・関西万博を支える重要なサービスを提供する事業者である「重要サービス事業者等」に対して、大阪・関西万博のサイバーセキュリティに係る脅威・インシデント情報を共有するとともに、必要があるときにはインシデント対処に対する支援調整を行います。

行動計画に基づく情報共有（①）と CS 対処調整センターを中心とした情報共有（②）との関係を図示すると図 10 のとおりです。重要サービス事業者等である重要インフラ事業者等は、①、②それぞれに情報連絡を行うことも可能ですが、事業者側における業務負担の軽減を図る観点から、いずれか一方のみへの連絡も可能です。

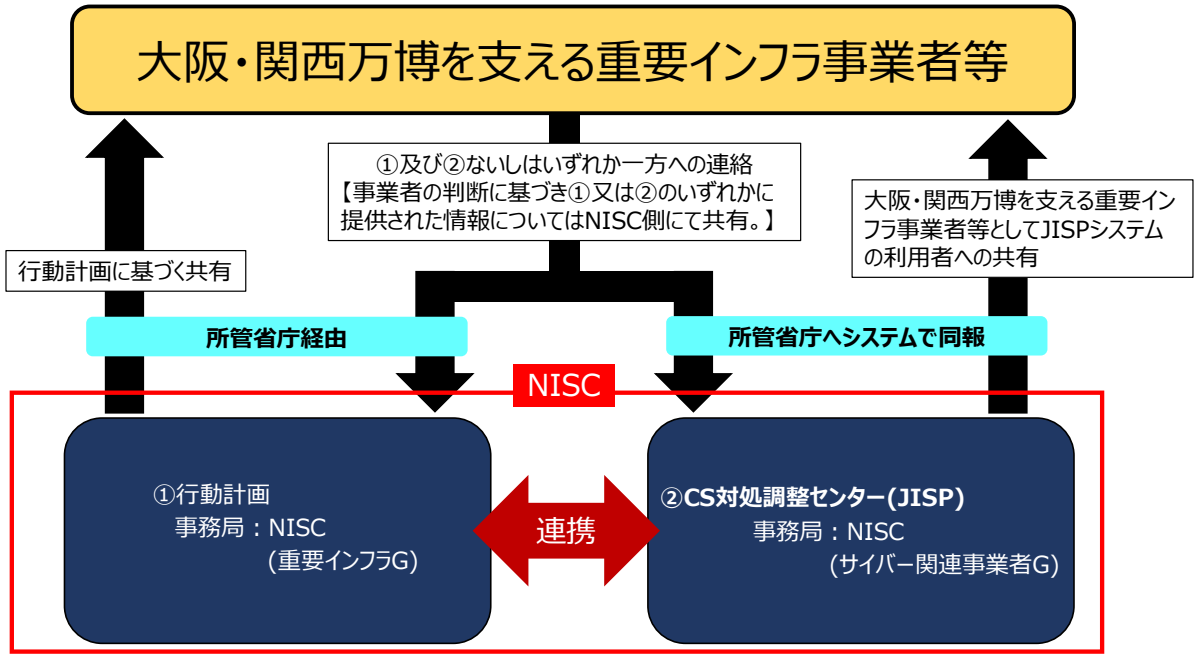


図 10　サイバーセキュリティ対処調整センターとの関係

Ⅳ. インシデント対応に資する情報等について

１．通常時から逐次確認すべき情報

１．１　ソフトウェア会社からの定例的なアップデート情報

(1) マイクロソフト株式会社

https://msrc.microsoft.com/blog/categories/japan-security-team/
で公開される月例のセキュリティ更新プログラム（年月日によって URL は変化）
https://msrc.microsoft.com/blog/2024/04/202404-security-update/

セキュリティ更新プログラムは、ソフトウェアの脆弱性を修正するセキュリティ更新プログラムは、通常、米国時間の毎月第２火曜日に公開される。日本では、時差の関係上、毎月第２火曜日の翌日（第２水曜又は第３水曜）の公開となる。

ただし、脆弱性の危険性が高いと判断した場合は例外措置を採り、セキュリティ更新プログラムは可能な限り迅速に公開される。

(2)アドビシステムズ株式会社（Adobe Acrobat Reader）

https://helpx.adobe.com/jp/acrobat/release-note/release-notes-acrobat-reader.html

以下のセキュリティアップデートが公開される。リリースの時期については明言されていない。

・Continuous リリース（C）：新機能と機能拡張のほか、新しいセキュリティアップデート、既存機能のバグの修正、以前にリリースされた不定期のパッチの更新を含む機能リリース。

・四半期ごとのアップデート（Q）：機能の向上、新しいセキュリティアップデート、以前にリリースされた不定期のパッチ更新を含む定期的なアップデートです。Reader では、このようなアップデートが完全なインストーラーとして提供される場合があります。

・不定期のパッチ（OOC）：セキュリティの問題の修正を目的としたアップデート。

その他の Adobe 製品については以下を参照。
https://helpx.adobe.com/jp/security.html

１．２　サイバーセキュリティ関係機関からの情報

(1) JPCERT/CC

https://www.jpcert.or.jp/

注意喚起として、深刻かつ影響範囲の広い脆弱性などの情報が告知される。情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内 CSIRT 業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等を対象にしている。

(2) IPA

https://www.ipa.go.jp/security/index.html

重要なセキュリティ情報が、Web 上で公開される。

重要なセキュリティ情報とは、放っておくと不正アクセスやデータが盗まれるなどの危険性が高いセキュリティ上の問題と対策について伝えるもので、インターネットを使っている多くの利用者が影響を受けるセキュリティ対策情報を対象にしている。

このほか、Web ページで脆弱性対策情報（JVN）、他組織からの情報が掲載されている。

２．ＣＳＩＲＴ構築に資する情報

２．１　CSIRT マテリアル（JPCERT/CC）

https://www.jpcert.or.jp/csirt_material/

２．２　CSIRT 構築ガイド（日本シーサート協議会）

https://www.nca.gr.jp/activity/pub_doc/wtda.html

Ⅴ．関係法令等
１．関係法令
〇サイバーセキュリティ基本法（平成２６年法律第１０４号）
（定義）
第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（基本理念）
第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（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に関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。
２～６　（略）

（重要社会基盤事業者の責務）
第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（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促進）
第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

〇重要インフラのサイバーセキュリティに係る行動計画（2022 年６月 17 日　サイバーセキュリティ戦略本部決定）
Ⅱ．本行動計画の要点（抄）
①「重要インフラ防護」の目的
　重要インフラにおいて、任務保証の考え方を踏まえ、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等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を

行い、迅速な復旧を図ることの両面から、強靱性を確保し、国民生活や社会経済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こと。

② 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成 26 年法律第 104 号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。
- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

③ 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

④ 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を経営の重要事項としてサイバーセキュリティを取り込む。
- サイバーセキュリティの確保には、サイバーセキュリティ基本法第 2 条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

Ⅲ. 計画期間内の取組（抄）

3. 情報共有体制の強化

3.3 重要インフラ事業者等の更なる活性化

重要インフラ事業者等の活動を更に活性化するに当たり、重要インフラ事業者等の自らの活動に加え、セプター内、セプター間における情報共有の充実が期待される。

具体的には、重要インフラ事業者等においては、自ら積極的に情報共有に取り組むとともに、経営層のリーダーシップの下、サプライチェーン等に関わる事業者を含め、

CSIRT 等の重要インフラサービス障害対応体制を構築・強化することが期待される。なお、自ら情報収集を行うことにより情報への理解とその効果的な活用が進むと考えられることから、重要インフラ事業者等の情報収集の活性化が期待される。また、セプターにおいては、これまでの行動計画期間に引き続き、内閣官房が提供する情報の取扱いに関する取決め、機密保持及び構成員外への情報提供に関し、構成員間で合意されたルールが適用され、緊急時に各構成員及び構成員外との連絡が可能な窓口(PoC)が設定されている状況において、内閣官房が提供する情報を共有することの継続が期待される。

２．用語の定義

CISO	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。
CSIRT	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。
IT-BCP 等	重要インフラサービスの提供に必要な情報システムに関する事業継続計画(関連マニュアル類を含む。)その他の事業継続計画。
安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、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」、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」等の総称。ただし、安全基準等策定指針は含まない。
安全基準等策定指針	安全基準等の策定・改定に資することを目的として、サイバーセキュリティの確保において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。サイバーセキュリティ戦略本部決定による。
関係主体	内閣官房、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター及びセプター事務局、セプターカウンシル、サイバーセキュリティ関係機関並びにサイバー空間関連事業者。
コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。
サービス維持レベル	任務保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。
サイバーセキュリティ	サイバーセキュリティ基本法第 2 条に規定するサイバーセキュリティをいう。電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。
サイバーセキュリティ関係機関	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)。
サイバーセキュリティ関係省庁	警察庁、デジタル庁、総務省、外務省、経済産業省、原子力規制庁(※)及び防衛省。 ※原子力発電所の安全の観点からサイバーセキュリティに取り組む省庁
サイバー空間関連事業者	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。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。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。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
システムの不具合	重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。

重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する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で、重要インフラ分野に属するもの。
重要インフラサービス	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。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
重要インフラ事業者	サイバーセキュリティ基本法第 3 条第 1 項に規定する重要社会基盤事業者をいう。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に関する事業を行う者。具体的には、重要インフラ分野に属する事業を行う者のうち、「別紙１　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの(地方公共団体を除く)。
重要インフラ事業者等	サイバーセキュリティ基本法第 12 条第 2 項第 3 号に規定する重要社会基盤事業者等をいう。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。
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省及び国土交通省。
重要インフラ分野	重要インフラについて業種ごとに指定する分野であり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス(地方公共団体を含む)」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の 15 分野。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、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。
情報共有	システムの不具合等に関する情報(重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報)やサイバーセキュリティの確保に資する情報について、関係主体間で相互に提供し、共有すること。情報連絡及び情報提供の双方を含む。
情報システム	事務処理等を行うシステム、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の IT を用いたシステム全般。
情報提供	サイバーセキュリティの確保に資するための情報を、内閣官房から重要インフラ事業者等へ提供すること等。
情報連絡	重要インフラ事業者等におけるシステムの不具合等に関する情報(重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報)を、重要インフラ事業者等から内閣官房に連絡すること等。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
大規模重要インフラサービス障害	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。
ナショナルサート	国として、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。
防災関係府省庁	災害対策基本法(昭和 36 年法律第 223 号)第 2 条第 3 号に基づく指定行政機関等の、災害時の情報収集に関係する府省庁。
予兆・ヒヤリハット	システムの不具合が生じておらず、又は生じなかったものの、システムの不具合につながるおそれがあり、又はそのおそれがあった事象。

【最終ページ】

☐警報　☐注意喚起　☐参考情報

（重要インフラ所管省庁→内閣官房）

情報連絡様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号*　（※第1報の識別番号は空欄）

情報連絡日時*　　年　　月　　日　　時　　分

情報連絡元*	省庁名：		担当者名：	
	部局名：			
	電話番号：		FAX番号：	
	電子メールアドレス：			
情報共有範囲*	☐ RED = 宛先限り （NISC重要インフラ防護担当(※1)限り） ☐ AMBER + STRICT = 特定分野・組織内関係者限り （NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り） ☐ AMBER = 特定分野・関係者限り （NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り） ☐ GREEN = 重要インフラ関係主体限り （NISC、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者、セプター及び重要インフラ事業者等に属する者限り） ☐ CLEAR = 公開情報			
	特記事項：			

※1：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を行

①発生した事象の類型

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	☐
発生した事象	機密性を脅かす事象	情報の漏えい （組織の機密情報等の流出など）	☐
	完全性を脅かす事象	情報の破壊 （Webサイト等の改ざんや組織の機密情報等の破壊など）	☐
	可用性を脅かす事象	システム等の利用困難 （制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	☐
	上記につながる事象(※3)	マルウェア等の感染 （マルウェア等によるシステム等への感染）	☐
		不正コード等の実行 （システム脆弱性等をついた不正コード等の実行）	☐
		システム等への侵入 （外部からのサイバー攻撃等によるシステム等への侵入）	☐
		その他	☐

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の類型

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	☐
	ユーザID等の偽り	☐
	DDoS攻撃等の大量アクセス	☐
	情報の不正取得	☐
	内部不正	☐
	適切なシステム運用等の未実施	☐
偶発的な原因	ユーザの操作ミス	☐
	ユーザの管理ミス	☐
	不審なファイルの実行	☐
	不審なサイトの閲覧	☐
	外部委託先の管理ミス	☐
	機器等の故障	☐
	システムの脆弱性	☐
	他分野の障害からの波及	☐
環境的な原因	災害や疾病等	☐
その他の原因	その他	☐
	不明	☐

◆情報連絡の内容(※4)　　（別紙有無*：☐有　☐無 ）

項　目	情報の内容
③分野名*(※5)	
④事象が発生した重要インフラ事業者等名	
⑤概　要	判明日時：　　年　月　日　時　分 （発生日時：　　年　月　日　時　分 ） 事象が発生したシステム・委託先業者等： 発生事象の概要： システムの稼働状況：☐影響なし ☐停止中 ☐一部稼働中 ☐復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：☐有 ☐無 他の事業者等への波及の可能性：☐有 ☐無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 （補足情報） 対外的な対応状況 報道発表、報道等への掲載：☐済 ☐予定有 ☐無 （済・予定有では日時・件名を記入） 個人情報保護委員会への連絡：☐済 ☐確認中 ☐不要 （済では日時・件名を記入） その他NISC以外に連絡を行った先：
⑧今後の予定	☐事象継続中　（続報あり） ☐事後調査実施中　（続報あり） ☐今後の対応策を継続検討　（続報なし） ☐対応完了　（続報なし）
⑨その他 ・得られた教訓等	

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラのサイバーセキュリティに係る行動計画」に定める「重要インフラ分野」を指す。
※6：「重要インフラのサイバーセキュリティに係る行動計画」に定める「サービス維持レベル」を指す。

記載例

□警報　□注意喚起　■参考情報

（重要インフラ所管省庁→内閣官房）

記載例　：青字
記載上の注意：赤字

情報連絡様式

（第　1　報*）

（*が付与された項目は必須事項）

西暦で記載

24時間表記で記載

識別番号*	（※第1報の識別番号は空欄）
情報連絡日時*	2023 年　8 月　19 日　13 時　15 分

いつ時点での内容かの日付・時間を記載。（記載するとセルの色は白に変化）

情報連絡元*	省庁名：	XX省	担当者名：	連絡　太郎
	部局名：	YY課		
	電話番号：	03-XXXX-YYYY	FAX番号：	03-XXXX-YYYY
	電子メールアドレス：	renraku.taro@xx.go.jp		

情報共有範囲*

□ RED = 宛先限り
（NISC重要インフラ防護担当(※1)限り）

□ AMBER + STRICT = 特定分野・組織内関係者限り
（NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り）

□ AMBER = 特定分野・関係者限り
（NISC重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り）

■ GREEN = 重要インフラ関係主体限り
（NISC、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者、セプター及び重要インフラ事業者等に属する者限り）

□ CLEAR = 公開情報

選択したＴＬＰ（情報共有範囲）に関する補足情報を記載。

特記事項：
企業名・該当サービス等、企業が特定される事項を除いて他分野への情報提供可。

※1：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を

①発生した事象の類型

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	□
発生した事象	機密性を脅かす事象	情報の漏えい（組織の機密情報等の流出など）	□
	完全性を脅かす事象	情報の破壊（Webサイト等の改ざんや組織の機密情報等の破壊など）	■
	可用性を脅かす事象	システム等の利用困難（制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	□
	上記につながる事象(※3)	マルウェア等の感染（マルウェア等によるシステム等への感染）	□
		不正コード等の実行（システム脆弱性等をついた不正コード等の実行）	□
		システム等への侵入（外部からのサイバー攻撃等によるシステム等への侵入）	□
		その他	□

最初に明らかとなった事象について、１つだけ■を選択する。

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の類型

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	□
	ユーザID等の偽り	□
	DDoS攻撃等の大量アクセス	□
	情報の不正取得	□
	内部不正	□
	適切なシステム運用等の未実施	□
偶発的な原因	ユーザの操作ミス	□
	ユーザの管理ミス	□
	不審なファイルの実行	□
	不審なサイトの閲覧	□
	外部委託先の管理ミス	□
	機器等の故障	□
	システムの脆弱性	□
	他分野の障害からの波及	□
環境的な原因	災害や疾病等	□
その他の原因	その他	□
	不明	■

発生原因について■を選択する。複数選択可。

◆情報連絡の内容(※4)　（別紙有無*：☐ 有　■ 無 ）

項　目	リストから選択 情報の内容
③分野名*(※5)	○○分野
④事象が発生した重要インフラ事業者等名	○○株式会社
⑤概　要	判明日時：　2023 年　8 月　18 日　20 時　0 分 （発生日時：　2023 年　8 月　19 日　2 時　59 分　（サーバログ等より推測）） 事象が発生したシステム・委託先業者等： 会社情報管理サービス（https://example.com/top.php） ・会員がアクセスし、個人情報の変更やサービス申込等を実施。 発生事象の概要： ・○○株式会社の会員情報管理サービスのWEBサイトが改竄された。 ・閲覧したユーザにウイルス感染の恐れがあり、現在、当該サイトを一時閉鎖しサービス停止中。 ・多数の個人情報流出が確認されており、被害の詳細を調査中。 システムの稼働状況：　☐ 影響なし　■ 停止中　☐ 一部稼働中　☐ 復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：　☐ 有　■ 無 他の事業者等への波及の可能性：　☐ 有　■ 無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 XX/XX 00:00 / 外部より○○株式会社のHPがおかしいと匿名メールを受信。 XX/XX 01:00 / サーバ運用ベンダへ連絡。サーバログ等の調査をし、HPが改ざんされていることを確認。 XX/XX 03:00 / アクセスした利用者にウィルス感染のおそれがあるためサーバを停止。 （必要に応じて行を追加して経緯を記載。） （補足情報） ・XX月XX日現在、○○件の個人情報流出を確認。 （名前、住所、電話番号、メールアドレスが漏えい。） ・コンテンツ管理システムYYYYのv99.99の脆弱性を突かれたものと想定される。
（報道発表等がある場合は、別紙として添付する、あるいは掲載ページのアドレス等を記載。）	対外的な対応状況 報道発表、報道等への掲載：　■ 済　☐ 予定有　☐ 無　（済・予定有では日時・件名を記入） XX/XX 09:00頃　○○株式会社のトップページにニュースリリースを掲載。 （https://example.com/newsXXXX） 個人情報保護委員会への連絡：　☐ 済　☐ 予定有　■ 確認中（済では日時・件名を記入） 現在のところ、個人情報漏洩の事実は確認されていない。 NISC以外に連絡を行った先： XX/XX 10:00頃　○○県警へ通報
⑧今後の予定	■ 事象継続中　（続報あり） ☐ 事後調査実施中　（続報あり） ☐ 今後の対応策を継続検討　（続報なし） ☐ 対応完了　（続報なし）
⑨その他 ・得られた教訓等	・現時点での得られた教訓は、経営層への情報のエスカレーション体制を普段から確認し、迅速な判断ができるようにすること。

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラのサイバーセキュリティに係る行動計画」に定める「重要インフラ分野」を指す。
※6：「重要インフラのサイバーセキュリティに係る行動計画」に定める「サービス維持レベル」を指す。

クラウドを利用した
システム運用に関するガイダンス
（詳細版）

令和４年４月５日

内閣官房内閣サイバーセキュリティセンター

改定履歴

改定年月日	改定箇所	改定内容
2021 年 11 月 30 日	―	・初版決定
2022 年 4 月 5 日	3.4 8	・利用規約に注釈を追加 ・用語集を一部修正

目次

1. はじめに

本ガイダンスは、増加するクラウドサービスの選定や利用、サービスを使った環境の構築や運用などを行うに当たり、クラウドサービスの「利用者[1]」（以下「利用者」という。）がクラウドサービスの基本を理解し、クラウドサービスにおけるインシデント（利用者にとって好ましくない事象や出来事）の発生を可能な限り抑制することや、インシデントが発生した際の対応及びステークホルダー（利害関係者）の連携によって事態の解決を図る重要性など、クラウドサービスの安全な運用に重点を置いた利用者向けの基本的なガイダンスの詳細版です。

昨今、個別の動作環境（ハードウェアやソフトウェア）を準備して、自らコントロールする「オンプレミス」のシステムに代わり、クラウドサービスを活用したシステム構築や運用が主流となってきています。確かに、利用者にとってクラウドサービスを利用することは、調達や導入の負荷軽減に寄与しますが、利用者からシステム運用や責任そのものがなくなるわけではありません。クラウドサービスでは、クラウド事業者が提供する動作環境を活用していることから、利用者が制御できない環境や領域が存在するため、利用者の目に見えないところでクラウドサービスの更新や仕様変更が行われます。

そのため、クラウド事業者の作業によってインシデントが発生する場合もあり、利用者はクラウド事業者からWebサイトへの公開等により提供される情報の把握や変更管理などを適切に行う必要があります。インシデントによってはクラウド事業者にもその原因が分からず、約款や利用規約などの取り決めにもない想定外の事態が発生する場合もあります。その場合は、クラウドサービスに係る全てのステークホルダー、関係機関や、サイバーセキュリティコミュニティが協力しながら、事案対応を行う必要があります。

クラウドサービスは約款による契約に基づいて提供されることから、利用者がクラウドサービスを活用し、顧客に対して何らかのサービス等を提供する事業を行っている場合、その顧客から見れば、利用者が当該サービスの提供元となります。このため、クラウド事業者側に起因するインシデントが発生した際、クラウド事業者は基本的には約款や利用規約で定めている範囲で責任を負う一方、それ以外の範囲については、利用者に責任が問われる場合があります。クラウドサービス利用に関して、初期導入の容易さや負荷軽減のメリットがある一方、オンプレミスと同等に利用者の責任は存在することから、システムの運用・維持体制の整備が不可欠であることを認識することが重要です。

我が国では、利用者が様々な情報技術を活用する場面において、自組織のみで対応が完結することは少なく、システムの構築や運用の全体や一部を外部に委託しているのが現状です。そのため、情報システム子会社やシステムインテグレータ（以下「SIer」という。）をはじめとしたステークホルダーを把握して、我が国全体（Cybersecurity for All）で対応することが欠かせません。

「デジタル・トランスフォーメーション」や「クラウド・バイ・デフォルト」が叫ばれている昨今において、クラウドサービスの活用は、事業継続や成長の観点からも欠かすことができません。利用者はクラ

[1] クラウドサービスを利用する事業者のほか、地方公共団体も含む。

ウドサービスの活用を一層推進する一方で、クラウドサービスの構造や責任範囲などについて理解を深めておく必要があります。また、クラウド事業者は、情報の非対称性を踏まえ、情報の公開や提示を実施し、我が国全体でクラウドサービスを安心・安全に使える社会にしていくよう努める必要があります。

2. クラウドサービスの基本理解

2.1. クラウドサービスを利用する背景

以前は、組織が利用するシステムは、自分たちで全てのハードウェアやソフトウェア(OS、ミドルウェアやアプリケーション)などを調達しなければなりませんでした。しかし、それでは初期投資に費用がかかることや、企画や設計からかなりの長い歳月を隔てなければシステム利用、そして事業そのものが開始できませんでした。それでは、変化の激しい現代社会において、大きな遅れをとることになります。そこで注目され、昨今の主流となっているのがクラウドサービスを活用した事業やシステムの展開です。

クラウドサービスと言ってもその形態は様々です。利用者はどのようなクラウドサービスを活用するのか適切に選定する必要があります。NIST SP800-145[2]などでも定義されているように、ハードウェアや仮想化ソフトウェアなどの基盤となる環境を整備しているのが「IaaS(Infrastructure as a Service)」、そしてOSやアプリケーションを制御、支援するミドルウェアまでの環境を整備しているのが「PaaS(Platform as a Service)」、さらにアプリケーションまでの環境を整備しているのが「SaaS(Software as a Service)」です。クラウドサービスは後者になればなるほど、クラウド事業者が提供する範囲が広がり、利用者はより早く活用することが可能です。

利用者は各社が提供しているクラウドサービスがどの分類に当てはまる(又は折衷的に提供している)サービスなのかを理解した上でクラウドサービスを活用し、利用者の責任範囲を明確にする必要があります。

また、これまで 3 つの分類で語られることが多かったクラウドサービスですが、昨今ではさらに細分化されています。例えば、様々な環境で利用可能なアプリケーションの開発ができるCaaS(Container as a Service)や、サーバレスでアプリケーション開発ができるFaaS(Function as a Service)等の形態が存在し、それらを組み合わせてシステムが構築されるようになり、より複雑化しています。

2.2. クラウドサービスのメリット・デメリット(リスク)

クラウドサービスは導入や構築が素早く行え、拡張性が高い一方で、外部の資源を活用しているので、組織のリスク管理そのものに影響し、自組織だけでは完結しがたい状況になります。また、これまで我が国のクラウドサービスは、事業継続性の観点だけではなく、初期導入面のコス

[2] NIST(アメリカ国立標準技術研究所)によるクラウドコンピューティングの定義
https://www.ipa.go.jp/files/000025366.pdf

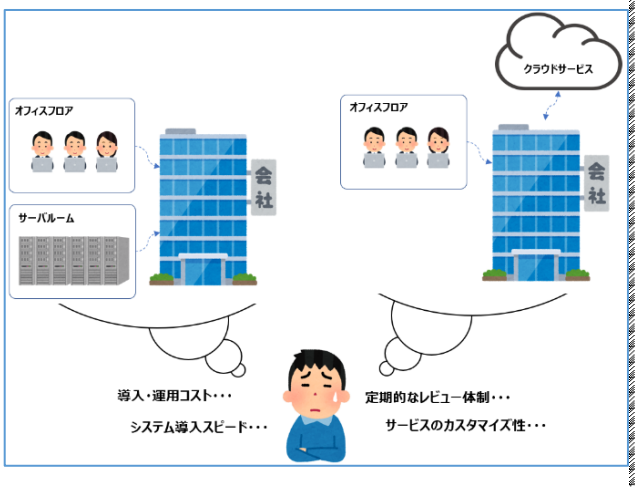
ト低減の視点から価格面が注目され、導入が進んでいる現状にあります。忘れてはならないのは、クラウドサービスであったとしてもシステムを運用し続けているという意識を持つことです。むしろクラウドサービスはクラウド事業者のタイミングで仕様や約款などの変更が行えるため、新たな仕様の確認や、設定の再確認等、運用にはそれ相応のコストがかかります。図１にまとめたメリットやデメリットを理解した上でクラウドサービスを活用しましょう。

メリット	デメリット
・導入や構築が素早く行える ・利用状況に応じた拡張性の高さ ・自組織で調達しない範囲の運用負荷の軽減 （※作業は軽減されても運用責任は残る） ・拡張機能が追加され続ける	・自組織のシステムやサービス意識の低下 ・カスタマイズ性が低い ・ステークホルダーが多く、リスク管理が自組織で完結し難い ・特定のクラウドサービスの専門知識が必要 ・仕様変更や機能拡張のたびにレビューしなければならない

図１ クラウドサービスのメリット・デメリット

コラム：クラウドサービスの必要性

クラウドサービスの特徴として、仕様の変更や機能の追加がしばしば行われます。利用者はそれらの機能を理解し、変更される仕様に対して都度レビューをしなければなりません。進化し続けるクラウドサービスは非常に大きな強みですが、それは利用者の負担とも考えられます。システムの調達や刷新を行う際、本当にクラウドサービスを活用するのが適しているのか、というポイントから検討するのが望ましいと言えます。政府はクラウド・バイ・デフォルトの考え方を提唱しておりますが、まずクラウドサービスを候補として検討するという考え方であり、クラウドサービスだけが選択肢であるものではありません。導入サービスの内容や組織体制によってはクラウドサービスが不向きなこともあり得ますので、オンプレミスの構成も十分に検討するのがよいでしょう。



コラム：セキュリティ担保の取組

利用者環境のセキュリティを実装するには利用者が責任をもって担保するべきものです。脆弱性診断のパッケージツールや SI サービス、ペネトレーションテストの SI サービスなど様々ありますが、ツールやサービスに一任するのではなく、明確な目的と意図をもってそれらのツール等を活用するべきです。

クラウド事業者側も、サービスの設定値やログを監視するツール等を提供しており、クラウドサービス側の仕様変更があった際に設定値の簡易的な確認が行えます。

しかし、どのような対策を講じてもセキュリティインシデントのリスクをゼロにすることはできません。許容できないインシデントリスクに対しては、サイバーリスク保険も選択肢のひとつとして検討することが考えられます。

3. クラウド事業者や利用者などのステークホルダーの責任等の理解

3.1. クラウドサービス活用におけるステークホルダーの理解

利用者にとっては、クラウド事業者からクラウドサービスを直接調達する場合や、販売者や構築者を介して調達する場合など、クラウドサービスの活用には様々なステークホルダーが存在します。利用者はステークホルダーを把握し、締結された契約の相手方、その契約内容(約款、利用規約等[3])及び契約に基づく責任範囲を把握する必要があります。クラウドサービスにおいては、その利便性から、クラウド上のデータのみを取り扱い、システム運用には関わらない事業者が存在する場合もあります。システム上のステークホルダー(表１)に加え、データを取り扱うステークホルダー(表２)についても把握する必要があります。なお、以下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(利用者とクラウド事業者のみの)場合もあります。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す[4] 。

表１ システム視点でのステークホルダー例

項目	説明
利用者	クラウドサービスやシステムを利用する組織
販売者	クラウドサービスやシステムを販売する組織
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 SIer 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 (SIer や SIer 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 (SIer や SIer の委託企業など)
クラウド事業者	クラウドサービスを提供している組織 ※組織によっては日本国内には販売拠点や一時的なサポートを行う体制しかない場合があり、最終的なサポートの判断や解決策の提供などは、国外の拠点から行う場合もあるため、ステークホルダーはクラウド事業者の国内外の体制の確認を行うとともに、クラウド事業者は体制について開示する必要があります。
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

さらに、昨今はシステム視点だけではなく、「データ」の視点も欠かすことができません。そもそもクラウドサービスを活用している時点で、オンプレミス型とは異なり、既にクラウド事業者がデータを保管しています。

[3] 約款、利用規約、利用条件等があり、取引条件を記載した文書を指す。

[4] 自治体の SNS 利用と個人情報へのアクセス
https://cio.go.jp/sites/default/files/uploads/documents/dp2021_04.pdf

クラウドサービスを利用し、利用者自身が作成した文書や資料であれば「保有者」であり、データの主体と言えます。また多重下請け構造に鑑みると、保有者が作成した文書や資料などについて、必ずしもシステムには依存せずに、クラウドサービス外においても、販売者、構築者、設置者、運用者がデータを保存している場合があります。データの保存者も保有者のデータの所在を明確にしておくなど、適切にデータを守らなければなりません。またクラウド事業者は保有者のデータを保管する者として、データの棄損や消失などがないよう保管しておく必要があります。なお、データの使用者や加工者は、保有者との利用契約等に基づいて（許諾を得る場合を含む。）、使用や加工を行います。

クラウドサービスに限られた話ではなく、昨今のシステム活用に当たっては、このようにデータ視点でのステークホルダーの理解も欠かすことができません。

表 2 データ視点でのステークホルダー例

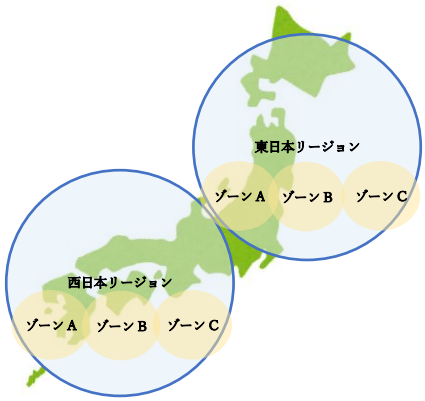
項目	説明
保有者	クラウドサービスに保存するデータを保有している者（独自にデータを作成した者等）
保存者	保有者のデータを保存している者（所有者の業務や作業などの委託事業者）
保管者	保有者のデータを保管している者（クラウド事業者）
使用者	保有者のデータを利用する者（情報収集者や所有者の許諾を得て利用する者）
加工者	保有者のデータを編集・修正する者

コラム：データセンターとリージョンについて

データセンターは、サーバやネットワーク等の装置を設置・運用することに特化した施設のことです。災害時に設備に極力支障が出ないよう耐震・免震構造となっており、24 時間 365 日安定した電力供給、安定した通信が行えるよう設計されています。クラウドサービスはハードウェアを意識せずに利用できますが、実体となるハードウェアはどこかのデータセンターで稼働しています。

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ります。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等が考えられます。情報の開示が懸念される場合は、機関等の管理する暗号鍵で暗号化するなどの措置の検討や、クラウド事業者へデータ保護の措置等についての確認を行うようにしましょう[5]。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必要があります。

リージョン(region)とは地域、領域といった意味の英語で、クラウドの分野では地理的・ネットワーク的に独立したエリアのことを意味します。東日本リージョン、北米リージョンというように、クラウドサービスがどのリージョンで運用されているのかを表すのに使用されます。激甚災害等に備えるには、複数のリージョンで運用されるサービスを選択する必要があります。リージョン内をロケーションごとに分割したエリアのことをゾーンと呼びます。なお、クラウド事業者によってリージョンやゾーンの用語の定義や範囲に違いがあることにご留意ください。

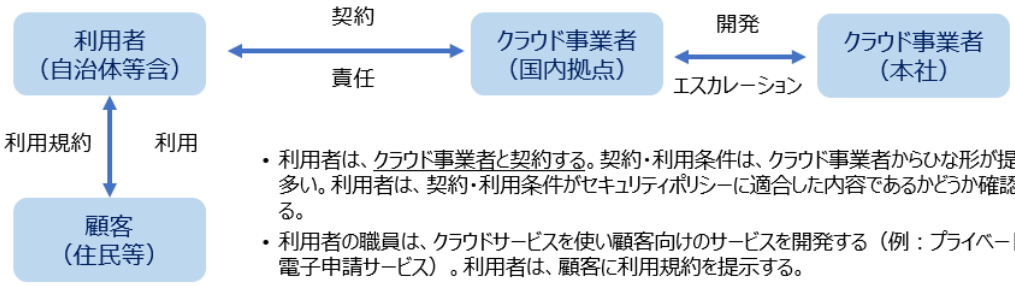


[5] 政府機関等の対策基準策定のためのガイドライン(令和３年度版)
https://www.nisc.go.jp/active/general/pdf/guider3.pdf
遵守事項 4.2.1(3)(e) 「国内法以外の法令及び規制が適用されるリスク」について

コラム：クラウドサービスのステークホルダー例

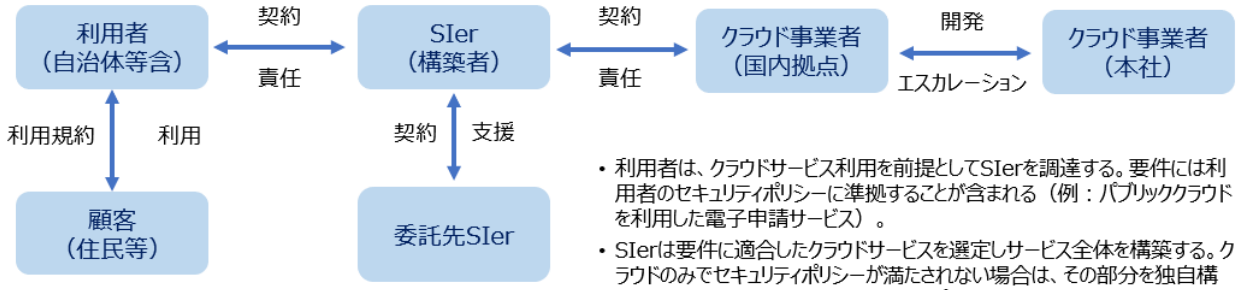
以下にクラウドサービスにおけるステークホルダーの例を示します。クラウド事業者やSIer（構築者）はそれぞれの間における契約や利用規約に基づき事業を行っています。利用者は関連する事業者等がどのような契約関係にあるのかに留意する必要があり、また顧客に対して提供するサービス自体の説明責任は利用者が負うものであることを認識する必要があります。

利用者がクラウドサービス契約者



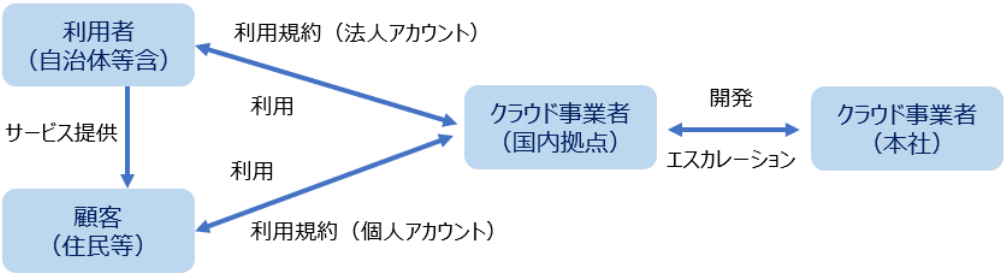
- 利用者は、クラウド事業者と契約する。契約・利用条件は、クラウド事業者からひな形が提供される場合が多い。利用者は、契約・利用条件がセキュリティポリシーに適合した内容であるかどうか確認したのち契約する。
- 利用者の職員は、クラウドサービスを使い顧客向けのサービスを開発する（例：プライベートクラウドを使った電子申請サービス）。利用者は、顧客に利用規約を提示する。

SIerがクラウドサービス契約者



- 利用者は、クラウドサービス利用を前提としてSIerを調達する。要件には利用者のセキュリティポリシーに準拠することが含まれる（例：パブリッククラウドを利用した電子申請サービス）。
- SIerは要件に適合したクラウドサービスを選定しサービス全体を構築する。クラウドのみでセキュリティポリシーが満たされない場合は、その部分を独自構築する（例：データの保存場所をオンプレに作る等）。
- SIerは、クラウド事業者と契約し、利用規約等の変更について監視を怠らないようにする。

利用者、顧客がクラウドサービス契約者



- 利用者は、クラウドサービスの利用規約に同意し、法人アカウントを開設する（約款による利用）。利用者は、利用規約がセキュリティポリシーに合致するか確認したのち利用する。
- 顧客は、クラウドサービスの利用規約に同意し、個人アカウントを開設する（約款による利用）。
- 利用者は、クラウドサービスを利用して、サービスを顧客に提供する（例：メールマガジン配信、チャットによる問合せ対応）。
- 利用者は、クラウドサービスの利用規約の変更を監視し、セキュリティポリシーに合致しなくなった場合は、利用を停止する。

3.2. クラウド事業者における「責任共有モデル」

クラウドサービスを活用する際、「責任共有モデル(Shared Responsibility Model)」の理解が大前提となります。これは、利用者とクラウド事業者が、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です。図 2 は基本的な責任共有モデルの考え方ですが、各クラウド事業者やサービスによって責任共有モデルの考え方が異なる場合があります。

しかし、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)データなどの取扱は、概ね利用者側の責任です。また、先に述べたとおり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ります[6]。そのため、責任共有モデルは構築者や設置者などのステークホルダーを踏まえた上で理解する必要があります。

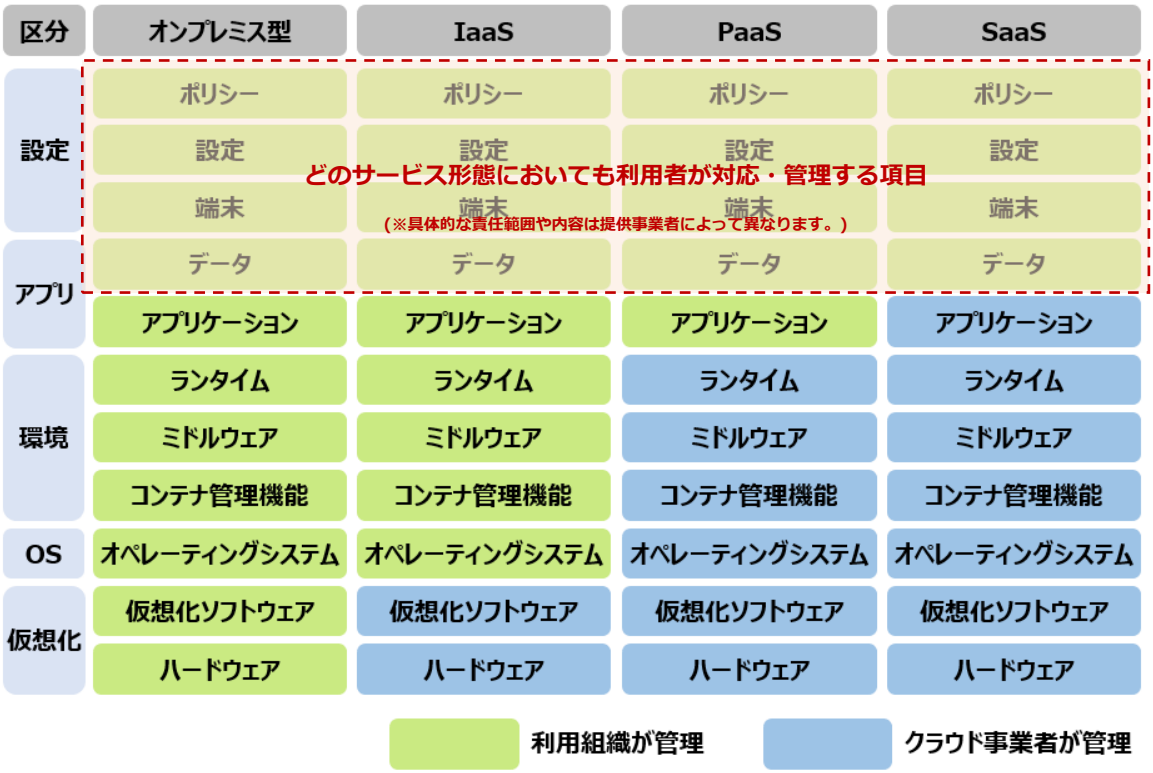


図 2 クラウドサービスの責任共有モデル(例)

[6] 近年のクラウドサービスでは、マネージド・サービスという運用を自動化するサービスが広がってきていますが、運用の責任は利用者側にあることを認識する必要があります。

コラム：クラウドサービスの類型

クラウドの基礎概念解説のため、サービスの分布や責任共有モデルを IaaS、PaaS、SaaS の類型で示しましたが、多くの組織では単一の類型でクラウドサービスを利用することは非常に稀です。IT のサービスは様々な要素の組み合わせであり、例えばデータベースは PaaS、Web サーバは IaaS、認証の仕組みは SaaS、といったように外から見たら一つのサービスでも、中身は複数の要素が組み合わさっており、サービスのニーズに合わせてこうした組合せを行う”設計”が重要となります。また、場合によっては複数のクラウドサービスを連携させて自社のサービスとして組み込むことも一般的です。

クラウド事業者によっては設計のデザインパターンや設計原則などの資料を公開しており、ベストプラクティスを学ぶことでより良いサービスを使うことができます。

複数社のクラウドサービスを組み合わせた構成を SIer が構築する場合などにおいても、利用者は利用サービスに関連する事業者ごとに責任範囲の明確化と理解が求められます。

クラウドサービスを安全に利用していくためには、責任範囲を区別する責任分界点の明確化、インシデント発生時の対応等をあらかじめ検討する必要があります。こうした背景を踏まえ、米国 NSA[7]は 2020 年 1 月にクラウドサービスの脅威・脆弱性と責任共有モデルを示し、「設定」「アプリケーション/データ」「環境」「オペレーティングシステム」「仮想化」といた大枠の区分で表記をしています。しかし昨今、クラウドサービスはより複雑な構造となっており、各クラウドサービスの領域そのものも不明瞭にもなってきています。

図 2 のとおり、クラウドサービスを利用する場合においても、オンプレミス型同様に様々な運用や管理が求められており、ここでは「ポリシー」「設定」「端末」「データ」の４つに細分化して、利用者側の必要な対応について概説します。

まず、それぞれの組織には、粒度や量は異なっても組織の指針やルールなどが存在します。それらの現存する指針やルール(顧客サービスの方針やセキュリティポリシー等)と照らし合わせた上で、組織としてクラウドサービスをどのように構築し、活用するのか、組織としての「ポリシー(組織的な指針)」は事前に確認、検討を行い、(状況によっては)変更し、見直しをしながら運用します。またそのポリシーを踏まえた上で、システム自体のポリシー(製品やサービスの基本となる指針)も決定、設定し、運用し続ける必要があります。

また、利用者の責任範囲として、セキュリティの基本となるアクセス管理やアカウント管理、システムの詳細設定など、活用する上でのシステム上の「設定」も欠かすことができません。この設定をシステム活用当時から対応しておかないと、いわゆる「設定不備」によるインシデントが発生します(クラウド事業者の仕様変更があった場合も同様です。)。なお、クラウド事業者は、導入や運用の様々な段階においても、情報の非対称性を深く考慮し、利用者だけではなく、販売者・構築者・設置者・運用者に対して、設定に関する情報を丁寧に開示し、説明する必要があります。

さらに、クラウドサービスに接続する端末のマルウェア感染などのインシデントが発生しないように、又はシステム側に波及しないように、アクセスする端末のセキュリティ対策も行う必要があります。なお、テレワークを実施している組織においては、物理的な端末の盗難等のリスクも含め、テレワーク未実施の組織よりも厳格なセキュリティ上の配慮が必要です。

組織に元々あるデータやシステムによって生み出されたデータは、保管場所としてはクラウド事業者側にありますが、データそのものは保有者の情報資産であり、運用や活用の責任は保有者(≒利用者)にあります。昨今、バックアップの重要性が高まっており、重要な情報資産であればあるほど、マルチクラウドやオフラインでのバックアップなどを検討し、事業継続のためのデータ管理を考える必要があります。その一方で、クラウド事業者においては、利用者が設定、運

[7] アメリカ国家安全保障局(National Security Agency)

用しているデータに対するアクセスコントロールや権限、手段、機能等が変わることのないように考慮した上で仕様変更を行い、データを安心・安全に活用できる環境整備を行います。もし、クラウド事業者による仕様変更によって、データや利用者全体に悪影響が及ぼすことが判明した場合は、即座に応急処置や緩和策などの提示を行い、利用者に対応を促す必要があります。

3.3. 責任共有モデルを踏まえた販売者、構築者、設置者、運用者の責任と役割

特に我が国の場合は、クラウド事業者と利用者の間に様々なステークホルダーが存在します。また「責任共有モデル」の箇所で述べたようなポリシーからデータまでの領域についても、利用者の管理領域であったとしても利用者だけで対応が完結せず、それぞれのステークホルダーからの支援を受けている場合があります。そのため、再委託先や再々委託先などを含めた全てのステークホルダーを把握し、普段の業務やインシデント時の業務、責任範囲などについて、事前及び継続的に協議を行い、組織間の運用の落とし穴にならないよう、体制を整えておく必要があります。例えば、特に重要なシステムについては再委託や再々委託を認めないようにするなど、ステークホルダーをあらかじめ限定的にしておくことも、利用者としては検討する必要があります。

また、クラウド事業者としては IaaS や PaaS のサービスを販売者や構築者などに提供し、その組織が SaaS として利用者にクラウドサービスを提供している場合があります。この場合は特にクラウド事業者や販売者、構築者などにおいても事前の協議を行い、クラウドサービスを提供する事業者として対応や責任の範囲の明確化を行い、インシデント発生時には円滑に対応できる体制の確保が必要です。利用者は活用するクラウドサービスの構造について理解に努めることが大切です。

さらに、クラウド事業者のデータセンターが海外にある場合などは、上記のステークホルダーの責任と役割だけでなく、当該国の法令や政府機関の対応等にも細心の注意を払う必要があります。

3.4. ステークホルダーとの契約形態等の理解

クラウドサービスを利用するに当たって、ステークホルダーによって契約の形態、締結対象、組織数なども異なります。

例えば、IaaS を提供しているクラウド事業者のサービスを用いて、構築者が SaaS を構築し、販売者が対象の SaaS を販売しているとします。この場合、クラウド事業者と構築者はクラウドサービス利用のために契約を締結し、構築者は販売者との販売店としての契約を締結し、販売者と利用者は購入や利用に関する契約を締結しています。

表面上、利用者は販売者としか契約を締結していないように見えるかもしれませんが、当該契約が、販売者と構築者及び構築者とクラウド事業者のそれぞれの契約を踏まえた内容になって

いる場合や、利用者が、構築者又はクラウド事業者との間にて別途契約を締結することが前提条件になっている場合、クラウド事業者が公表している約款等への同意が必要とされている場合などがあります。そのため、どの組織とどのような契約を締結していることになるのか、販売者以外の組織とはどのような関係が構築されるのかといった契約状況を把握する必要があります。なお、契約は利用者、事業者ともに対等な立場で同意のもと締結されるものです。利用者は、自組織が一方的に不利な契約内容とならないよう、十分に留意する必要があります。クラウド事業者においても、サービス利用約款や利用規約の策定や更新の際、利用者に不利な内容にならないようにしなければなりません。

契約時に特に確認すべきポイントは、平常時の支援内容、インシデント発生時の支援内容、データの取扱（バックアップや破棄などを含む。）に関する内容、そして損害賠償などに関する内容です。クラウドサービスを使うということは、自組織だけでリスク管理や対応が行えるわけではありません。インシデントが発生した時点で利用者が契約内容や約款を見直しても遅いため、必ず契約時に確認をしなければなりません。また、クラウド事業者の約款変更は定期又は不定期に更新されるため、継続的な確認体制も欠かすことができません。

なお、2020 年に施行された改正民法の規定を踏まえ、利用者はまずクラウド事業者と行う取引が「定型取引」に該当するものなのかを確認し、サービス利用約款や利用規約等に定型約款の規定が適用されるのか否かを確認する必要があります。いずれの契約形態であっても、契約締結後、利用約款等の変更が利用者にとって利益になる場合も、不利益になる場合もあります。想定される事態に適切に対処するために契約内容について法務部門等と相談していただくことが望まれます。

クラウド事業者においても、提供するクラウドサービスが不特定多数との取引を目的とした定型取引としての性質を有するのであれば、サービス利用約款が定型約款に該当する可能性があることを忘れてはなりません。

コラム：契約の類型について

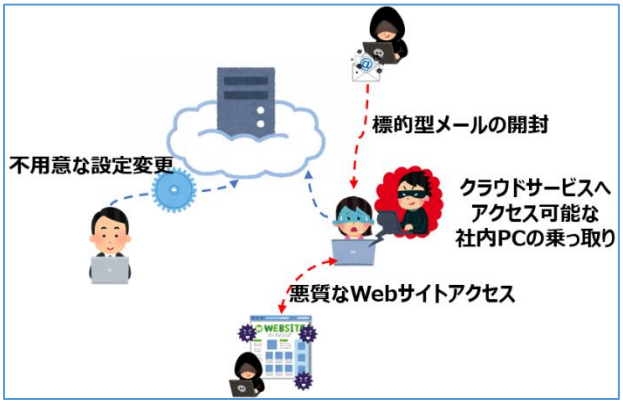
クラウドサービスを利用する際の契約形態は、多数の利用者と同一内容の契約を結ぶことが多いため、利用規約、利用条件、利用契約等の取引条件を記載した文書(以下「利用規約[8]」という。)が用意されていることがほとんどです。利用規約にはクラウドサービスの形態によって民法上の定型約款に該当するものと該当しないものとがあります。定型約款に該当する場合は不当条項規制や変更手続の規定が適用されますが、定型約款に該当しない場合は利用規約が契約に組み入れられているかどうかによって異なります。

また、クラウドサービスは手軽に利用できるものも多く、利用規約の内容について利用者が把握していないケースも見受けられますが、サービスの利用を開始したり、支払いの登録をしたりした段階で利用者は利用規約に同意したと認められる場合があります。

トラブルが発生した際のクラウド事業者とのやりとりには利用規約が土俵となります。クラウドサービスの利用の際には情報システム部門だけでなく、法務部門とも連携して内容について理解するようにしましょう。

コラム：サイバー攻撃の侵入口

セキュリティ対策が強固なクラウドサービスを実現しても、利用者の操作(設定、メール開封、Web サイト訪問など)次第では攻撃者が侵入できる可能性が高まります。特に設定については、既定の設定がどのような動作なのか、といった観点も踏まえて設計を行う必要があります。メール開封や Web サイト訪問については、無害化するソリューションの活用が対策例として考えられます。



サイバー攻撃を可能にしてしまう例

[8] 利用規約には、以下の合意書やポリシーが含まれる場合があります。
- 「クラウドサービスレベル合意書 (Cloud SLA)」
- 「利用ポリシー (Acceptable User Policy)」
- 「セキュリティポリシー (Security Policy)」
- 「データ保護ポリシー (Data Protection Policy)」
- 「事業継続ポリシー (Business Continuity Policy)」
- 「アップグレードポリシー (Upgrade Policy)」
- 「終了ポリシー (Termination Policy)」

4. クラウド利用(環境構築、運用など)の注意点

クラウドサービスをはじめ様々な環境や技術の活用はあくまでも手段の 1 つに過ぎないため、まずは組織としてクラウドサービスをなぜ利用するのか、目標や目的、情報技術を活用する理由を明確にします。その上で最もふさわしいクラウドサービスを選定します。

4.1. 構築時の注意点

＜選定・設計＞

4.1.1. どのような形式のクラウドサービスを活用するのか

まず利用者は、自組織の現状把握が欠かせません。特に既存のシステムや環境が、構築者や設置者などへ依存している場合は、支援を受けている構築者や設置者などと協議を行い、クラウドサービスを活用できる現状であるのか、移行するためにはどのような作業が生じるのかなど、自組織で現状を把握しなければなりません。その上で、自組織に合ったクラウドサービスはどのような形式のものであるか、IaaS・PaaS・SaaS に代表されるような様々なカテゴリの中から構築の仕方を検討していきます。

4.1.2. どのクラウド事業者・サービスを選定するのか

クラウド事業者の選定に当たっては、大きく 3 つのポイントがあります。

共存・共栄できる事業者

まずは、クラウドサービスを提供する事業者として適切な管理体制があるのか、関連する認証を取得しているのか、利用実績数や事例、品質に対する考え方など、クラウド事業者そのものの信頼性の確認です。具体的には、有事の際のインシデント対応において共に連携できること、利用者がクラウドを活用して提供するサービスの重要度に応じてクラウド事業者側のログデータ(ログの種類、保存期間など)等のインシデント対応に必要な情報を即座に提供できること、その情報の入手フローの確認を含め、想定外のインシデントでも問題解決のための提案ができること等、クラウド事業者のサポート方針やサポートレベルを見極める必要があります。

クラウドサービスの信頼性

2 つ目は、サービスの稼働率やこれまでの障害の発生状況、クラウドサービスのセキュリティ対策、データの保管やバックアップの体制など、サービスそのものの信頼性の確認です。SaaS の機密性やデータ安全に関して、ISMAP(日本)や FedRAMP(米国)といった認定制度があり、選定の際の参考となります。

情報開示方針

3 つ目は情報開示の明瞭性です。規約や約款などの契約面における適切な記載はもちろんのこと、サービス自体やそのサポート内容の公開方法や公開項目、そして障害発生時の情報開示の方法や体制など、目に見える形でクラウド事業者が情報公開に努めている様子があるのかなどを確認します。なお、総務省においては利用者向けのクラウドサービスの比較・評価・選択等を目的とした「クラウドサービスの安全・信頼性に係る情報開示指針」を公表

しています[9]。

4.1.3. 既存の方針や規程のままで対応が可能か

クラウドサービス利用に当たって、組織が運用している方針や規程(セキュリティポリシー等)と抵触が生じないかを確認します。例えば、これまで組織で定義している「重要な情報については外部に持ち出したり保存したりしてはならない。」といったポリシーを運用している組織で、クラウドサービスを活用して、外部で重要な情報についても保管や保存ができるようにする場合、既存の方針や規程に抵触している場合があります。そのため、方針や規程を確認し、クラウドサービス活用に当たって、抵触が生じないか確認します。

＜実装＞

4.1.4. 選定したクラウドサービスの理解を深める

実装に向けて注意すべきことは、サービスの概要を理解することはもちろんのこと、設定の不備によるインシデントが起きないように設定方法の理解を深めることや、そもそもの設計思想を理解することも大切です。特にシステム的な視点だけではなく、利用者が守らなければならないデータがより安全な状態を維持するためにはどのようにしたらよいのか、クラウドサービスを提供している事業者はどのように考えているのかを確認し、理解を深めます。クラウド事業者が構築や運用に関するガイドを提供している場合は、対象の文書に目を通し、加えてクラウドサービスのサポート情報やFAQなどを確認しましょう。また、それでも不明な点がある場合は、直接サポート窓口に確認することも大切です。

なお、自組織ではなく外部への委託や支援を受けて実装を考えている場合は、この設計思想などのクラウドサービスを実装する初期段階から共に理解を深めることが望ましいです。

クラウドシステムの急速な広まりから、組織内の基幹システム等にも幅広くクラウドサービスを活用する利用者が増加しています。組織におけるクラウドシステムへの依存度の高まりに伴い、クラウドサービスの障害は事業継続や可用性の観点から、組織に与える影響は大規模化しています。3.2.でもデータ面について述べたとおり、重要な情報資産であればあるほど、マルチクラウドやオフラインでのバックアップなどを検討し、事業継続を見据えた設計及び実装をする必要があります。

4.1.5. 実装は誰が行うのかを明確にする(構築者・設置者・運用者など)

全ての設定や実装作業を利用者のみで行えるケースは少なく、SIer やコンサルティング企業などの外部支援を受けて実装している組織が多いのが現状です。忘れてはならないのはクラウドサービスの利用主体は利用者にあり、根本的な実装責任は(クラウド事業者側の仕様変更などを除いて)利用者にあることです。外部の支援を受けることは決して悪くはないですが、利用者が自ら具体的な実装は行わないような場合でも、より主体的に実装に携わ

[9] 総務省「クラウドサービスの安全・信頼性に係る情報開示指針」
https://www.soumu.go.jp/main_content/000475596.pdf

らなければならないということです。その上で、構築者や設置者などはクラウド事業者から取得している情報を開示し、インシデントが起きにくく、利用しやすい環境の構築に努める必要があります。ステークホルダーの対応範囲を明確にし、実装における不備を抑制するためにも、役割分担を明確にしておく必要があります。

＜検証＞

4.1.6. ポリシーや設定など、適切な構築や設定が行えているのか

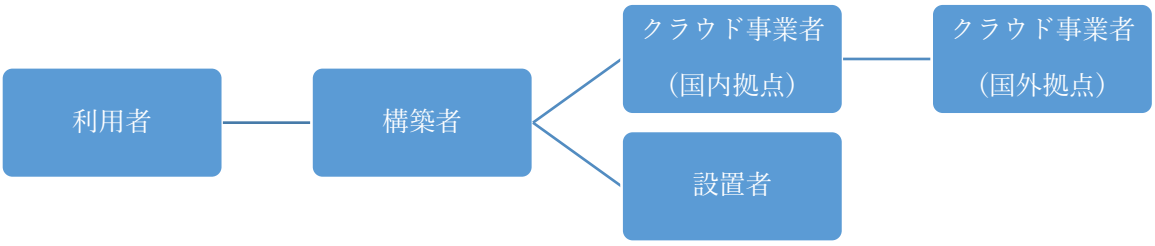
利用者が主体となり、構築者や設置者が実装した環境が、クラウド事業者が提供している情報に基づき適切に構築できているのかどうかを検証します。利用できる状況になったら直ちに利用を開始するのではなく、オンプレミス型のシステム同様に検証のプロセスを忘れてはなりません。できる限り第三者に依頼し、安全に設定できているのかどうか、設定不備や脆弱性に係る診断、ペネトレーションテストなどの実施により、インシデントが発生しない状況にあるのかどうかを確認します。なお、先にも述べたとおり、クラウドサービスは定期的にクラウド事業者側での仕様変更が行われています。そのため、このような検証は運用段階になっても定期的に実施するのが望ましいです。

4.2. 運用時の注意点

4.2.1. 体制

これまで述べてきたとおり、クラウドサービスを活用するからといって、利用者のシステム運用がなくなるわけではありません。クラウドサービスを活用して事業やサービスを展開していれば、その責任は利用者にあります。また前述のとおり、責任共有モデルを理解した上で、自組織の対応範囲を確認し、特に双方に責任がある領域においては、協議を行い、対応を事前に確認し、体制を確立しておく必要があります。利用者とクラウド事業者だけではステークホルダーは完結せず、構築者や設置者、運用者などがそれぞれいる場合や、さらにはクラウド事業者側の対応として、国外の拠点が対応に関係する場合もあります。このため、ステークホルダーを含めた体制の構築が必要です。

【代表的なステークホルダーの例示】



運用体制の確保は、まずは相談や連絡が可能な窓口を把握することから始まります。

そして、クラウドサービスを含むシステム運用に関する責任者を任命します。これはインシデントが発生したときに対象のサービスやシステムを利用停止する判断を行ったり、重

要な更新などが生じた場合に判断を行ったりするための指揮系統を明確にするためです。その上で、実際の作業や指示を行う担当者を任命します。主に利用者のステークホルダーとの連携や、確認した情報の展開や具体的な作業の現場監督のような役割を担います。

さらに、これまで述べてきたとおり、クラウドサービスは事業者側の仕様や約款などの変更が利用者側の変更のタイミングと合わせて行われるわけではなく、定期又は不定期に更新されます。また、昨今クラウドサービス上でのインシデントも発生していることから、脅威情報や脆弱性情報など、クラウドサービスに関連する情報を収集し、展開する担当者を任命しておくと、より安全な活用が可能です。

上記それぞれに責任者や担当者を任命することが難しい場合は、兼任であったとしても組織としての任命をする必要があります。

4.2.2. 対応

クラウドサービスに関する対応として、平常時とインシデント発生時の 2 つに分けて解説します(インシデント発生時については「6.インシデント発生時のステークホルダー連携の在り方」で後述。)。

平常時においては、システムやサービスの設定が適切に行われているか、クラウド事業者が公開しているガイドなどを参照し、見直しを行います。また新しいバージョンの公開やサービスの更新が行われた場合には、変更点や影響の確認を行います。不明な点は契約を行っている運用者やクラウド事業者などに確認を行います。また組織が活用しているシステムやサービスに影響がある脅威情報や脆弱性情報が公開されていないかを確認します。一方で、運用者やクラウド事業者も情報提供を積極的に行い、利用者の確認に対して真摯に対応します。

5. クラウド利用に当たってのコミュニケーションの在り方

5.1. 普段からのコミュニケーションの方法や注意点

クラウドサービスを利用するに当たっては、①利用者と運用者、②運用者とクラウド事業者、③クラウド事業者と利用者の間では、定期的に協議を行い、窓口・連絡先の把握や信頼関係の構築に努める必要があります。

特にコミュニケーションが大切なタイミングは、クラウド事業者側の仕様や約款の変更が行われたときです。クラウド事業者は、利用者に対して、(エグゼクティブサマリをまとめるなど)分かりやすく情報提供し、また運用者や構築者、設置者に対してはより具体的に情報(ガイドやFAQ など)を提供し、変更に対する説明責任を果たす必要があります。以下に、ステークホルダーのコミュニケーションの例について記します。

5.1.1. 利用者と運用者(又は構築者や設置者)

運用者はクラウド事業者から取得した情報を基に、取得情報そのものの提供や提供するサービスの更新予定・内容などについて利用者と協議します。サービスを更新する場合は、更新理由や更新によって変更する点、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双方で行います。また運用者は利用者に対してサービス更新時の影響を説明し、利用者は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検討する必要があります。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ようにしましょう。

5.1.2. 運用者(又は構築者や設置者)とクラウド事業者

運用者はクラウド事業者から提供されている情報を注視しておきます。クラウド事業者も積極的に運用者に対して情報を開示し、また開示されている情報も国内外で差異が生じないように情報の提供に努める必要があります。クラウド事業者が提供する重要な情報については、一般公開される前に運用者が情報を取得できるような体制や関係性を構築しておく必要があります。また技術的な側面だけではなく、約款などの法律的な側面においても確認、協議することを忘れてはなりません。5.1.1 と同様に協議内容は保管し続けるようにしましょう。

5.1.3. クラウド事業者と利用者

クラウド事業者は運用者に提供している情報と同等の情報を利用者に提供できるように努める必要があることに加え、情報の非対称性があることを理解した上で、より分かりやすく利用者に伝える必要があります。またクラウド事業者と利用者の間においても、できる限り定期的に協議を行うよう努める必要があります。利用者も、自らが活用しているクラウドサービスについては、定期的に更新情報の収集に努める必要があります。特に利用者は、確認したサポート情報や約款などは、サービスを利用している間は保管し、適切に振り返りが行えるようにしましょう。

5.2. インシデント発生を想定した準備

クラウドサービス活用に限らず、利用者はインシデントを想定し、備える必要があります。発生しうる代表的なインシデントは、「システムやサービスの脆弱性を狙った攻撃」、「OSINT 等を活用した攻撃」、「装置故障などによるシステム障害」、「クラウドサービスの故障」、そして「設定の不備」が挙げられます。先にも述べたとおり、クラウド事業者や構築者、運用者等のインシデントであったとしても、組織が提供している事業やサービスそのものにインシデントが波及した場合は、顧客に被害や迷惑が生じ、組織としての責任が問われる可能性があります。

まず、利用者や構築者などは、過去にクラウド事業者(できればクラウド事業者の競合企業を含め)に発生したインシデントを確認します。新しいインシデント発生は誰にも予測できませんが、できる限り「想定内のインシデント」とするように努め、事前に対応や対策を練ることが大切です。

また利用者は、クラウド事業者や運用者などが提供しているサポート(保守・運用)契約について確認し、追加費用などのオプションサービスについてもあらかじめ確認をしておく必要があります。構築者や運用者、そしてクラウド事業者も限られた資源の中でサービスを提供しており、有償の契約であれば 24 時間 365 日のサポートが受けることができる契約や、SLA(Service Level Agreement)や SLO(Service Level Objective)がより明確になったサポート、オンサイト(訪問対応が可能な)サポートなどの契約を準備している場合があります。特に重要なシステムにおいてクラウドサービスを活用する場合は、事前に経営層を含めて当該サポート契約の締結について協議し、クラウド事業者や運用者と契約を行うことが望ましいでしょう。

さらにインシデントが発生すると、利用者や運用者、構築者などは、原因究明に努める必要があります。組織でインシデント対応が行えるように、あらかじめクラウド事業者が提供可能なログやその内容について確認しておくとよいでしょう。例えば、ログの種類や、どれくらいの期間のログが提供可能なのか、またそもそも提供に当たって費用がかかるのか、分析や対応のための教育があるのかなどです。これらの対応は費用に関係するため、クラウドサービスを検討している段階で確認する必要があります。

最後に基本的な内容ですが、どこに問い合わせればいいのか、連絡先を事前に把握し、組織内に共有をしておく必要があります。なお、インシデント発生時にどこの組織に調査や解析などをお願いするのか、事前に見当をつけておくことも大切です。

クラウドサービスは提供しているクラウド事業者がよりサービスを理解しており、「クラウド事業者＞構築者・設置者・運用者＞販売者>利用者」の情報の非対称性があります。そこでインシデント発生時にはエグゼクティブサマリなどの分かりやすい情報提供ができる体制の整備に努め、我が国のシステムや事業がより安心・安全に利用できるように努める必要があります。

コラム：SLA

SLA(Service Level Agreement)とはクラウドサービスの品質に関する合意内容で、クラウド事業者と利用者との契約に含まれる内容となります。SLA の内容は情報漏えい等の法的リスク、損害賠償の内容と関連する契約条項といえますので、情報システム部門だけでなく法務部門とも連携して検討することが望ましいと言えます。

SLA は多くのクラウドサービスでサービス稼働率として表記されます。利用者は SLA に基づき、サービスの停止時間を想定し、許容することとなります。

SLA における許容停止時間の一覧表

SLA	停止時間(週)	停止時間(月)	停止時間(年)
99%	1.68 時間	7.2 時間	3.65 日
99.9%	10.1 分	43.2 分	8.76 時間
99.95%	5 分	21.6 分	4.38 時間
99.99%	1 分	4.32 分	52.56 分
99.999%	6 秒	25.9 秒	5.26 分

稼働率を例示しましたが、クラウドサービスによって SLA の内容は様々です。特定のシステム要件を満たすことを SLA の前提条件とする場合もあります。使用を検討しているクラウドサービスごとに SLA の詳細を確認することが必要です。

コラム：外部認証制度、評価制度

情報セキュリティマネジメントシステム(ISMS)は組織の情報資産のセキュリティ管理体制で、ISO/IEC 27001 として標準化されておりますが、クラウドサービスに対応した情報セキュリティ管理体制は、ISO/IEC 27017 として規格標準化されています。

クラウド事業者は ISO/IEC 27001 と ISO/IEC 27017 の両方の認証を取得し、クラウドサービスセキュリティへの取組を対外的にアピールしています。

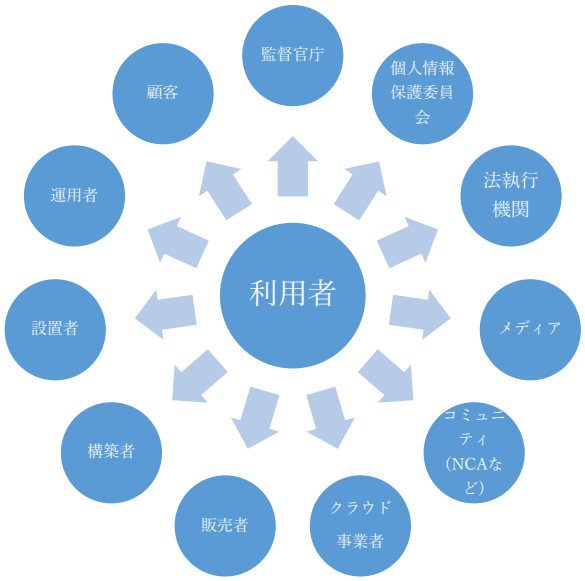
また日本政府では、令和 2 年 6 月に「政府情報システムのためのセキュリティ評価制度」(ISMAP)を立ち上げ、国際基準等を踏まえ策定したセキュリティ基準に基づき、クラウドサービスを第三者が評価を行い、クラウドサービスの調達に活用しています。

米国においても「クラウドサービスに関するセキュリティ評価・認証の統一ガイドライン」(FedRAMP)を採用し、米国政府の導入するクラウドサービスの採用に役立てています。

しかし、これらはあくまでセキュリティ管理体制、セキュリティ対策の実装状況評価等を行っているものであり、利用者はセキュリティインシデントへの対応体制を整備する必要があります。

6. インシデント発生時のステークホルダー連携の在り方

インシデント発生後は、先のステークホルダーに加えて、監督官庁や法執行機関、(個人情報の漏えい・滅失・毀損に関する場合は)個人情報保護委員会などとの連携が加わります。また、メディアからの問合せや法的解釈が求められる場合に備え、広報や法務に関係する部門や担当者とも連携を行います。そのため、先に述べたクラウド事業者や運用者などの窓口把握だけではなく、自組織の広報や法務に関係する窓口についても事前に把握し、いつでも連携できる体制を整備します。さらに、自組織やシステムの関係者だけではなく、国内外の研究者や技術者から連絡を受けることにより、インシデントが発見される場合があります。状況によってはこのようなステークホルダーとの連携が追加されることも認識しておくことが大切です。



また、複雑化、巧妙化するサイバー攻撃や、クラウドサービスの活用が進んでいる現状において、インシデントが発生したときに、一組織だけで対応するのは難しいのが現実です。そこで日本シーサート協議会(NCA)などのコミュニティに、利用者だけではなく、販売者、構築者、設置者、運用者、そしてクラウド事業者も含め参画し、ステークホルダーが連携しやすい体制の確保を行います。そこでは、他組織でのインシデント発生状況や自組織のインシデント情報の共有などを行い、協力してインシデントの解決に取り組む必要があります。

以下に、インシデントが発生したときの対応概要について記します。

＜サイバー攻撃の場合＞

- 影響範囲に応じて、システムの停止を検討します。
- クラウド事業者からログの取得を行い、利用者や運用者又は他の調査機関で分析を行います。
- 個人情報の漏えい・滅失・毀損に関する場合は、速やかに監督官庁や個人情報保護委員会に報告を行います[10]。

＜脆弱性や設定不備の場合＞

上記、サイバー攻撃の場合に加えて、以下のようなポイントを追加して検討、対応します。

- クラウド事業者のサポート(サービス)情報を確認し、最新の情報を確認します。
- クラウド事業者からガイドやFAQなどが公開されている場合は、参照します。
- 特にゼロデイ攻撃の場合、緩和策や回避策があるか確認し、公開されている場合は、組織内で対応を実施するか検討します。
- 新たなモジュールやパッチが公開されたら、できる限り速やかに適用や更新を行います。

上記のように、インシデントがどのようなインシデントなのか、発生の早い段階で、状況や性質などが理解できればよいですが、クラウド事業者や運用者などステークホルダーから情報開示や共有が行われていない場合、利用者はインシデント対応が難しくなる場合があります。そのため、情報共有や連携を行うコミュニティの活用は欠かすことができず、社会全体でインシデントの早期解決に努める必要があります。

[10] 個人情報の保護に関する法律（個人情報保護法）については、2022年4月1日から改正法が施行されます。当該施行後、個人情報取扱事業者、国の行政機関及び独立行政法人等においては、個人の権利利益を害するおそれが大きい個人データの漏えい等事態（サイバー攻撃を受けた場合等も想定しつつ、不正の目的をもって行われたおそれがある個人データの漏えい等事案等、対象となる事態を個人情報保護委員会規則や「個人情報の保護に関する法律についてのガイドライン（通則編）」等で規定）について、個人情報保護委員会等への報告（同委員会から事業所管大臣に委任されている個人情報取扱事業者に関する報告の受理権限に基づき、当該大臣に報告する場合も含む）及び本人への通知を行う必要があります。なお、地方公共団体の機関及び地方独立行政法人については、改正法が別に施行予定の2023年春頃より個人情報保護委員会への報告及び本人への通知が必要になります。

＜情報が不足している、又はインシデントの特定ができない場合＞

- ステークホルダーは、日本シーサート協議会(NCA)などのインシデントの事前・発生時・事後の連携が行えるコミュニティに参画します。また、クラウド事業者もコミュニティに参画し、事前又はインシデント発生時には、より積極的に情報提供や連携を行うなど、コミュニティを活用します。
- 情報共有ルール(チャタムハウスルールや TLP(Traffic Light Protocol)など)を理解し、ルールに則って、情報を共有します。
- 情報が共有されたコミュニティでは、加盟している組織のインシデント発生状況を確認します。
- 複数の組織で同様の、又は類似したインシデントが発生している場合は、コミュニティと事業者との契約の有無に関わらず、クラウド事業者の窓口に通報や相談を行います。
- クラウド事業者は当該通報や相談に対し、現状把握、調査、回答を行います。
- クラウド事業者も国内外で差が生じることのないよう情報を提供し、インシデント対応が完了するまで支援を続けます。
- 特にコミュニティに対しては、利用者に限らずクラウド事業者も積極的に情報共有や連携を行う必要があります。
- また影響範囲を鑑みて、コミュニティは内閣サイバーセキュリティセンター(NISC)などの政府機関に共有を行い、官民連携して問題の解決に当たります。
- インシデント対応が完了後、官(関係省庁)、民(コミュニティ(利用者・運用者など)、クラウド事業者)の関係者が参集し、振り返りや勉強会を実施することが望ましいです。

自組織で発生したインシデントを共有することに抵抗感のある組織も多いですが、インシデントは、早期の共有が、早期の解決をもたらします。特に原因の特定ができないインシデントや、ステークホルダーでの対応者が不明瞭になる「狭間のインシデント」は、共有が遅くなればなるほど解決が遠くなります。インシデントの発生は決して恥ずかしいことではなく、早期に共有し合わなければ解決できない時代に突入していることを、(特に経営者が)理解する必要があります。

特に、想定外のインシデントが発生した際に、リスク情報の提供などがステークホルダーにおいて必要なときには、クラウド事業者は秘密保持に配慮しつつ、事業遂行に係る社会的責任を踏まえた対応として、利用者とその顧客に情報の提供や連携を行う必要があります。

コラム：2022 年 4 月 1 日から施行される個人情報保護法

個人情報の保護に関する法律(個人情報保護法)について、民間分野における個人情報を取り扱う事業者(個人情報取扱事業者)に関する改正が 2020 年 6 月に成立・公布され、2022 年 4 月 1 日から全面施行されます[11]。これに合わせ、「個人情報の保護に関する法律についてのガイドライン(通則編)」及びその Q&A の改正等が行われており、個人情報取扱事業者がクラウドサービスを利用する場合に留意すべき点として以下の 2 点があります。

1 点目は、利用者である個人情報取扱事業者がクラウドサービスを利用する場合であっても、契約条項によってクラウド事業者がそのサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている等、クラウド事業者がサーバに保存された個人データを取り扱わないこととなっている場合には、クラウド事業者への個人データの第三者提供や個人データの取扱の委託には該当しない点です。この場合、利用者である個人情報取扱事業者は、個人データに係る本人が被る権利利益の侵害の大きさを考慮し、その個人データの取扱状況(個人データを取り扱う期間、取り扱う個人データの性質及び量を含む。)等に起因するリスクに応じ、自ら果たすべき適切な安全管理措置を講じる必要があります。

2 点目は、以上の場合において、個人データが保存されるサーバが外国にある場合については、利用者である個人情報取扱事業者が外国において個人データを取り扱うこととなるため、基本的には、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要がある点です。さらに、個人情報の取扱に関する透明性を通じて本人関与の実効性を確保するため、クラウド事業者が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称、それら外国の制度等を把握した上で講じた安全管理措置の内容等を本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置く必要があります。なお、クラウド事業者によっては、個人データが保存されるサーバが所在する国を特定等できない場合があるため、この場合には、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となるべき情報として、例えば、サーバが所在する外国の候補が具体的に定まっている場合における当該外国の名称等を本人の知り得る状態に置く必要があります。

以上とは別に、利用者たる個人情報取扱事業者から外国(日本と同等の水準にあると認められる個人情報の保護に関する制度を有する外国として個人情報保護委員会規則で定める EU 及び英国を除く。)に所在するクラウド事業者への個人データの第三者提供や個人データの取扱の委託に該当する場合については、利用者たる個人情報取扱事業者において、クラウド事業者への提供等を認める旨の本人からの事前同意の取得が必要となり、当該取得時に、クラウド事業者が所在する外国の名称、当該外国における個人情報の保護に関する制度、クラウド事業者が講ずる個人情報の保護のための措置その他本人に参考となるべき情報を本人に提供する必要があります。また、クラウド事業者が日本における個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制を整備している

[11] これに加えて、デジタル社会の形成を図るための関係法律の整備に関する法律による個人情報保護法の改正等のうち、国の行政機関及び独立行政法人等に関する部分が 2022 年 4 月 1 日から施行し、地方公共団体の機関及び地方独立行政法人に関する部分が 2023 年春頃に施行予定となっています。これらの機関等がクラウドサービスを利用する場合に留意すべき点については、個人情報保護法のほか、「個人情報の保護に関する法律についてのガイドライン（行政機関等編)」等も参照する必要があります。

場合については、利用者たる個人情報取扱事業者において、本人からの事前同意の取得は不要ですが、クラウド事業者による相当措置の継続的な実施を確保するために必要な措置を講じるとともに、本人の求めに応じて当該措置に関する情報を本人に提供する必要があります。さらに、クラウド事業者への個人データの取扱の委託に該当する場合は、委託先となるクラウド事業者に対する必要かつ適切な監督を行う必要もあります。

諸外国においても EU の一般データ保護規則(GDPR)、カリフォルニア州消費者プライバシー法(CCPA。なお、2023 年 1 月から改正されたカリフォルニアプライバシー権法(CPRA)が適用)など、プライバシー保護規制は拡大しております。国外に拠点をもつ利用者はこれらの法律にも対応しなければなりません。

諸外国におけるプライバシー関連法令

（参考）個人情報保護委員会　https://www.ppc.go.jp/

7. おわりに

本文書はクラウドサービスの基本的な内容や姿勢を明記したものであり、今後このガイダンスは利用者、クラウド事業者などの全てのステークホルダーの連携によって、より一層安全性の確保のために研鑽していくことが大切です。技術や活用方法など様々な変化が生じれば、このガイダンスも継続的に見直していく必要があり、完成に向けた継続的な議論や取組が必要です。

既にクラウドサービスなしでは事業が継続できないほど依存している組織も多く、これからの時代はクラウドサービスの活用は欠かせません。このような時代であるからこそ、普段から、そして特にインシデントが発生したときは、コミュニティを含む全てのステークホルダーが健全に連携し合う必要があります。クラウドサービスのステークホルダー連携こそが我が国のサイバー空間の安全に貢献できると言っても過言ではありません。

「Cybersecurity for All」、誰も取り残すことなく、全てのステークホルダーがクラウドサービスの理解に努める一方で、情報の非対称性を理解した上でそれぞれが説明責任を果たし、誰もが安心・安全にクラウドサービスを活用できる社会を実現していくよう努める必要があります。

8. 用語集

クラウドコンピューティング

利用者がサーバやストレージ等のリソースを物理的、仮想的に共用し、インターネットを介してサーバ、アプリケーション等にどこからでも必要に応じて利用可能とするコンピュータ活用方式。実装方式として、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド等がある。

クラウドサービス

クラウドコンピューティングを活用して提供されるサービス。基礎的なサービスモデルとして IaaS/PaaS/SaaS がある。

パブリッククラウド

クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。

プライベートクラウド

クラウドサービスの提供方式のひとつ。クラウド事業者が 1 つの組織に対してクラウドサービスを提供するものであり、当該組織外のユーザは利用することができない、その組織専用に実装されるクラウドコンピューティング方式。

ハイブリッドクラウド

パブリッククラウド、プライベートクラウド等、複数の提供方式を組み合わせて実装されるクラウドコンピューティング方式。パブリッククラウドで Web サービスを構成し、認証情報はプライベートクラウドに保管して Web サービスの認証処理を行うといった例が挙げられる。

マルチクラウド

利用者が複数のクラウドサービスを併用する運用形態。ハイブリッドクラウドが複数のクラウドサービスを組み合わせ、単一のシステムを構築するクラウドコンピューティングの実装方式であるのに対し、マルチクラウドはそれぞれ独立したまま活用する運用の形態。バックアップ・リカバリ体制の構築等で活用されることが多い。

オンプレミス

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

IaaS(Infrastructure as a Service)

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

PaaS(Platform as a Service)

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

SaaS(Software as a Service)

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

SLA(Service Level Agreement)

サービスレベル合意書。クラウド事業者と利用者との合意事項で、クラウド事業者は SLA に含まれるサービスレベル(稼働率や性能等)を満たすことを利用者に保証する。そのため SLA を満たせなかった場合は違約規程として返金規約等がある。

SLO(Service Level Objective)

サービスレベル目標。クラウド事業者が、合意した SLA を履行するために、稼働率、セキュリティ、サポートといった項目ごとに、パフォーマンスの目標値を設定したもの。クラウド事業者が設定する目標値のため SLO には違約規程がなく、SLO の内容について利用者に開示されない場合もある。

TLP(Traffic Light Protocol)

情報共有の促進を目的に作られた、適切な組織または人に共有するための標示。情報共有の範囲を 4 色で示す。

TLP:RED	公開不可、関係者限定
TLP:AMBER	限定公開、関係者が所属する組織とそのクライアントのみで共有可能
TLP:AMBER+STRICT	限定公開、関係者が所属する組織のみで共有可能
TLP:GREEN	限定公開、コミュニティ内で共有可能
TLP:CLEAR	制限なく共有可能

デジタル・トランスフォーメーション

企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

クラウド・バイ・デフォルト

情報システム構築の際に、クラウドサービスの利用を第一候補として、その検討を行うものとする考え。

チャタムハウスルール

会議における情報の公開と共有を促すルール。会議出席者は、発言者を匿名化した上で、会議中に得た情報を自由に使用できる。

「政府情報システムのためのセキュリティ評価制度」(ISMAP)

政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。

クラウドサービスに関するセキュリティ評価・認証の統一ガイドライン(FedRAMP)

米国政府におけるクラウドサービスの調達プログラム。米国政府にクラウドサービスを提供するクラウド事業者はFedRAMP準拠を証明する必要がある。

オープン・ソース・インテリジェンス(OSINT)

一般に公開された利用可能な情報をもとにする情報収集の手段。OSINT(オシント)と読む。
インターネット情報をはじめ、インタビュー記事や企業のプレスリリースといった情報等を分析して情報収集する。サイバーセキュリティ分野においても、諜報活動を目的としたサイバー攻撃や、サイバー犯罪捜査、分析といった攻防の両面からOSINTの活用が進んでいる。

本ガイダンス執筆協力一覧(五十音順：敬称略)

アマゾン ウェブ サービス ジャパン合同会社
株式会社エヌ・ティ・ティ・データ
グーグル・クラウド・ジャパン合同会社
クラスメソッド株式会社
グローバルセキュリティエキスパート株式会社
シスコシステムズ合同会社
株式会社セールスフォース・ジャパン
株式会社ディー・エヌ・エー
一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会
日本マイクロソフト株式会社
弁護士　北條　孝佳
楽天グループ株式会社
株式会社ラック
立命館大学 情報理工学部 情報理工学科　教授　上原　哲太郎

以上

２　戦略

サイバーセキュリティ戦略

令和３年９月 28 日

この戦略は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 12 条第５項において準用する同条第４項の規定に基づき、国会に報告するものである。

目次

1. 策定の趣旨・背景

2020 年代を迎えた最初の 1 年に、世界はコロナ禍の影響による不連続な変化に直面した。世界各地でロックダウンや外出制限が行われ、人々のくらしや様々な経済活動の基盤となる日常空間は、当たり前に享受できるものではなく、至るところに脆弱な側面を抱えているものであることが浮き彫りとなった。一方で、このような危機への対応を通じ、結果として人々のデジタル技術の活用は加速し、サイバー空間は、我々の生活におけるある種の「公共空間」として、より一層の重みを持つようになってきている。

また、この変化は、長い時間軸でみた大きな潮流を反映したものとも捉えられる。平成の時代を通じたデジタル経済の浸透は留まることなく、令和の時代に入り、デジタル庁を司令塔として、加速していくことが想定される。2020 年代は、2030 年に向けた国際的目標である SDGs[1]への貢献も期待される中、我が国の経済社会が、サイバー空間と実空間が高度に融合した Society5.0[2]の実現へと大きく前進する「Digital Decade」となり得ると考えられる。

一方で、足元では政治・経済・軍事・技術を巡る国家間の競争の顕在化を含む国際社会の変化の加速化・複雑化、情報通信技術の進歩や、複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間をとりまく不確実性は絶えず変容し、かつ増大している。

サイバー空間の「自由、公正、安全」が所与のものではなく、むしろその確保が危機に直面している中、我々はサイバーセキュリティに対し、常に変化を重ねていくことこそが確保すべき価値の不変性に繋がるとする「不易流行」の精神[3]で取り組んでいかなければならない。その礎として、我が国としての戦略があらためて求められている。

1.1. 2020 年代を迎えた日本をとりまく時代認識　～「ニューノーマル」とデジタル社会の到来～

(1) デジタル経済の浸透、デジタル改革の推進

インターネットの登場によりサイバー空間という新たな空間が創出され、平成の時代を通じデジタル経済が大きく進展し、デジタル経済の影響は、人々の生活そのものに波及している。我が国のインターネット利用者は 8 割を超え[4]、インターネットの平均利用時間は 1 日当たり 2 時間を超えた[5]。また、IoT[6]や AI、5G[7]、クラウドサービス等の利用

---

[1] Sustainable Development Goals の略。2001 年に策定されたミレニアム開発目標（MDGs）の後継として、2015 年 9 月の国連サミットで加盟国の全会一致で採択された「持続可能な開発のための 2030 アジェンダ」に記載された、2030 年までに持続可能でよりよい世界を目指す国際目標。17 のゴール・169 のターゲットから構成され、地球上の「誰一人取り残さない（leave no one behind）」ことが示されている。

[2] 狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上 5 番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略 2017（2017 年 6 月 9 日閣議決定））

[3] 熟語の出自は、松尾芭蕉が俳諧の本質を捉えるための理念として提起したものとされる。「不易」は時代の新古を超越して不変なるもの、「流行」はその時々に応じて変化していくものを意味するが、両者は本質的に対立するものではなく、真に「流行」を得ればおのずから「不易」を生じ、また真に「不易」に徹すればそのまま「流行」を生ずるものだと考えられている。（出典：小学館「日本大百科全書（ニッポニカ）」）

[4] 総務省「令和 2 年 通信利用動向調査」（2021 年 6 月 18 日）インターネット利用者の割合は全体の 83.4%。高齢者の利用者の割合も 5 割を超えている。

[5] 総務省情報通信政策研究所「令和元年度 情報通信メディアの利用時間と情報行動に関する調査報告書」（2020 年 9 月 30 日）

[6] Internet of Things の略。

[7] 第 5 世代移動通信システム。2015 年 9 月、国際電気通信連合（ITU）において、5G の主要な能力やコンセプトをまとめた「IMT ビジョン勧告（M.2083）」が策定され、その中で、5G の利用シナリオとして、「モバイルブロードバンドの高度化（eMBB：enhanced

拡大、テレワークの定着、教育における ICT 活用等の実施など人々の行動が変容しており、サイバー空間はあらゆる人にとって経済社会活動の基盤となりつつある。このような変化の潮流は、確かな推進力として、サイバー空間と実空間が高度に融合した Society5.0 の実現を後押しすることが期待される。

一方で、デジタル化の推進に向けては悪用・乱用からの被害防止やリテラシーの涵養、公的機関・民間双方のデジタル化の遅れなど、諸課題への的確な対応が必要となる。このため、2021 年 9 月に設置されたデジタル庁をデジタル社会の形成に向けた司令塔とし、「誰一人取り残さない、人に優しいデジタル化」の実現を目指して「デジタルの活用により、一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」をビジョンに掲げ、デジタル改革を強力に推進していく[8]こととしている。

(2) SDGs への貢献に対する期待

我が国として強力に推進する Society5.0 の実現を通じて、更なるデータ活用が可能となり、それによって防災や気候変動、環境保護、女性のエンパワーメントなど、SDGs でも重点事項として挙げられている様々な分野において、地球規模課題の解決に寄与することも期待される。

特に、我が国における「2050 年カーボンニュートラル」[9]に伴う「グリーン成長」の実現に向けては、スマートグリッドや製造自動化をはじめ、強靱なデジタルインフラが不可欠であるとされている[10]。

(3) 安全保障環境の変化

我が国が享受してきた既存の秩序の不確実性は急速に増している。政治・経済・軍事・技術を巡る国家間の競争の顕在化を含め、国際社会の変化の加速化・複雑化が進展しており、サイバー空間をめぐる情勢が重大な事態へと急速に発展していくリスクをはらんでいる[11]。

(4) 新型コロナウイルスの影響・経験

コロナ禍の影響による不連続な変化に直面し、様々な制約や社会的要請への対応を余儀なくされることを通じ、結果として、「ニューノーマル」とも呼ばれる新しい生活様式が Society5.0 の実現を部分的にも体現することとなった。具体的には、テレワークをはじめとする多様な働き方や教育における ICT 活用、遠隔診療などの取組が、コロナ禍以前と比べて大きく進展することとなった。

Mobile BroadBand)」、「超高信頼・低遅延通信（URLLC：Ultra Reliable and Low Latency Communications)」、「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications)」の 3 つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」、「1 ミリ秒程度の遅延」、「100 万台/㎢の接続機器数」が挙げられている。

[8] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）

[9] 2020 年 10 月に示された「我が国は、2050 年までに、温室効果ガスの排出を全体としてゼロにする、すなわち 2050 年カーボンニュートラル、脱炭素社会の実現を目指す」との方針。

[10] 「2050 年カーボンニュートラルに伴うグリーン成長戦略」（2021 年 6 月 18 日策定）

[11] 想定されるリスクについては、3.2 国際情勢からみたリスクに詳述している。

また、コロナ禍への対応の過程で、「パーソナルデータ」[12]を含む様々なデータを活用した新たなサービスの創出・活用も進展することとなった。

(5) 東京大会に向けた取組の活用

2021 年に開催された 2020 年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組は、コロナ禍という異例の環境下でも行われたことを含め、我が国にとって貴重な経験であると言えよう。こうした経験を、今後、2025 年日本国際博覧会（以下「大阪・関西万博」という。）等の大規模国際イベントを含め、我が国におけるサイバーセキュリティの向上に活用していくこととしている。また、これらの取組から得られた知見、ノウハウは、世界的にみても貴重なものであり、海外に発信・共有していくことで、国際連携への寄与も期待される。

1.2. 本戦略の位置付け

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。）に基づくサイバーセキュリティ戦略の策定は今回が 3 回目であり、基本法が制定された 2014 年から約 7 年が経過した。

本戦略は、中長期的視点から、先に述べた時代認識に立ち、2020 年代初めの今後 3 年間にとるべき諸施策の目標や実施方針を示すものである。同時に、未曽有のコロナ禍への対応から得られた教訓、デジタル改革、そして東京大会という大規模国際イベントでの対応を通じた経験を踏まえ、我が国としてのサイバーセキュリティに取り組む決意を、あらゆる主体、各国政府、そして攻撃者に対して発信するものである。

[12] 個人の属性情報、移動・行動・購買履歴、ウェアラブル機器から収集された個人情報及び特定の個人を識別できないように加工された人流情報、商品情報等を含む概念。

2. 本戦略における基本的な理念

我が国は、「基本法の目的」や過去 2 回のサイバーセキュリティ戦略で示してきた「確保すべきサイバー空間」に関する考え方、「基本原則」といった基本的な立場を堅持する。

2.1. 確保すべきサイバー空間

グローバルな拡張・発展を遂げたサイバー空間は、場所や時間にとらわれず、国境を越えて、質・量ともに多種多様な情報・データを自由に生成・共有・分析することが可能な場であり、流通する場である。こうした特徴を持つサイバー空間は、技術革新や新たなビジネスモデルなどの知的資産を生み出す場として、人々に豊かさや多様な価値実現の場をもたらし、今後の経済社会の持続的な発展の基盤となると同時に、自由主義、民主主義、文化発展を支える基盤でもある。

サイバー空間を「自由、公正かつ安全な空間」とすることにより、基本法に掲げた目的に資するべく、国は、これまで 2 度にわたり、我が国のサイバーセキュリティに関する施策についての基本的な計画として、サイバーセキュリティ戦略を策定してきた。

先に述べた時代認識を踏まえれば、その目的、そしてサイバー空間に対する考え方はいささかも変わるものではない。むしろ、その確保が危機に直面する中で、「自由、公正かつ安全なサイバー空間」を確保する必要性はこれまで以上に増しているとの認識が深められるべきである。

2.2. 基本原則

かかる認識の下、我が国は、サイバーセキュリティに関する施策の立案及び実施に当たって従うべき基本原則については、従来のサイバーセキュリティ戦略で掲げた 5 つの原則を堅持し、それに従うものとする。

(1) 情報の自由な流通の確保

サイバー空間が創意工夫の場として持続的に発展していくためには、発信した情報がその途中で不当に検閲されず、また、不正に改変されずに、意図した受信者へ届く世界（「信頼性のある自由なデータ流通」が確保される世界）が作られ、維持されるべきである[13]。なお、プライバシーへの配慮を含め、情報の自由な流通で他者の権利・利益をみだりに害することがないようにしなければならないことも明確にされるべきである。

(2) 法の支配

サイバー空間と実空間の一体化が進展する中、自由主義、民主主義等を支える基盤として発展してきたサイバー空間においても、実空間と同様に、法の支配が貫徹されるべきである。また、同様に、サイバー空間においては、国連憲章をはじめとした既存の国

[13] 基本法第 1 条において、「情報の自由な流通を確保しつつ」と規定されている。なお、例えば、「G7 首脳コミュニケ」（2021 年 6 月）において、信頼性のある自由なデータ流通（DFFT）ロードマップが承認されるなど、その重要性は国際的にも認識されている。

際法が適用されることを前提として、平和を脅かすような行為やそれらを支援する活動は許されるべきではないことも明確にされるべきである。

(3) 開放性

サイバー空間が新たな価値を生み出す空間として持続的に発展していくためには、多種多様なアイディアや知識が結びつく可能性を制限することなく、全ての主体に開かれたものであるべきである。サイバー空間が一部の主体に占有されることがあってはならないという立場を堅持していく。これには、全ての主体が平等な機会を与えられるという考え方も含まれる。

(4) 自律性

サイバー空間は多様な主体の自律的な取組により発展を遂げてきた。サイバー空間が秩序と創造性が共存する空間として持続的に発展していくためには、国家が秩序維持の役割を全て担うことは不適切であり、不可能である。サイバー空間の秩序維持に当たっては、様々な社会システムがそれぞれの任務・機能を自律的に実現することにより、社会全体としてのレジリエンスを高め、悪意ある主体の行動を抑止し対応することも重要であり、これを促進していく[14]。

(5) 多様な主体の連携

サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関及び個人などの多様な主体が活動することにより構築される多次元的な世界である。こうしたサイバー空間が持続的に発展していくためには、これら全ての主体が自覚的にそれぞれの役割や責務を果たすことが必要である。そのためには、個々の努力にとどまらず、連携・協働することが求められる。国は、連携・協働を促す役割を担うとともに、国際情勢の変化を踏まえ、価値観を共有する他国との連携や国際社会との協調をこれまで以上に推進していく[15]。

国民の自由な経済社会活動を保障し国民の権利や利便性の確保を図ること、また、適時適切な法執行・制度により悪意ある者の行動を抑制することによって国民を保護することこそ、国民から期待されるサイバーセキュリティ政策のあるべき姿である。我が国は、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段を選択肢として保持する点を、これまで以上に明確にする。

[14] 基本法第３条第２項において、「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す」と規定されている。

[15] 基本法第３条第１項において、「サイバーセキュリティに対する脅威に対して、（中略）多様な主体の連携により、積極的に対応することを旨として、行われなければならない。」と規定されている。

3. サイバー空間をとりまく課題認識

本戦略の策定に当たっては、サイバー空間がもたらす恩恵のみならず、この空間をとりまく変化やリスク（脅威、脆弱性いずれの観点も含む。）を的確に認識し、デジタル改革のビジョンである「一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」の実現に向けて、これら不確実性をできる限り制御していくアプローチが重要である。

サイバー空間そのものは、デジタルサービスが社会に定着していきサイバー空間に参画する層が増加をしていく過程で「量的」に拡大するとともに、取り扱えるデータ量の増大や IoT、AI 技術、モビリティ変革、AR/VR[16]技術をはじめとした最新技術の活用した新たなデジタルサービスの普及、「ニューノーマル」とも呼ばれる新しい生活様式の定着等を通じ、実現し得る価値の「質的」な多様化や、実空間との接点の「面的」な拡大が進んでいる。

これらが同時かつ相互影響的に進展する中で、サイバー空間が有する性質も変容しつつある。地域や老若男女問わず、全国民が参画し、自律的な社会経済活動が営まれる重要かつ公共性の高い場としての位置付け、すなわち、サイバー空間の「公共空間化」が進展するとともに、サイバー空間において提供される多様なサービスは、クラウドサービスの普及やサプライチェーン[17]の複雑化等に伴い、サイバー空間内やサイバーとフィジカルの垣根を越えた主体間の「相互連関・連鎖性」が一層深化していくことが想定される。

一方で、サイバー空間におけるデジタル技術の利用は、新たな課題も提示する。不適切に悪意をもって利用されれば、国家間における分断や危険を増大させ、人権を阻害し、不公平を拡大し得る[18]ことが指摘されている。サイバー空間の変容は、従来では想定し得なかったリスクも同様に拡大させることも想定され、さらに、コロナ禍等により不連続な形で起こる変化は、予期しない形でリスクを顕在化させるおそれがある。サイバー空間が公共空間へと変貌を遂げつつある一方で、このような状況により、国民がサイバー空間に対する不安感を完全に払拭できていないことも事実である[19]。

これらを念頭に、「自由、公正かつ安全なサイバー空間」を確保するためには、足元で起きている変化、又は近未来に起こり得る変化によって生じるリスクを適切に把握した上で、取り組むべき課題を明確化し、政策を推進していく必要がある。また、サイバー空間ではサービス提供の担い手は数年単位で入れ替わり、サイバーセキュリティの確保に大きな役割を果たす主体も変わり得ることから、中長期的にはその前提も大きく変わり得ることも同時に意識することが重要である。

以下では、経済社会をとりまく環境変化、国際情勢のそれぞれから、考慮すべきリスク要因を整理し、また、それらが具体的にどのように顕在化しているかについて示していく。

---

16 それぞれ、Augmented Reality（拡張現実）、Virtual Reality（仮想現実）の略。

17 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。

18 「国際連合創設 75 周年記念宣言」（2020 年 9 月 21 日）においても、新たな課題として提示されており、デジタルトラストとセキュリティの課題解決が優先事項とされている。

19 2020 年 9 月に警察庁が実施したアンケート調査によると、回答者の 75.3%がサイバー犯罪に不安を感じると回答。（出典：「令和 2 年度サイバーセキュリティ政策会議報告書」（2021 年 3 月 警察庁サイバーセキュリティ政策会議））

3.1. 環境変化からみたリスク

我が国経済社会をとりまく環境変化は、さまざまな恩恵をもたらし得る一方で、それに伴うリスクも表裏一体に拡大し得る。その動向について、脅威、そして経済社会が抱える脆弱性というそれぞれの観点に分けて示す。

(1) 脅威の観点

新たな技術の活用や、いわゆる「ニューノーマル」の定着等を通じ、新たなデジタルサービスが次々と生み出され、人々の生活に浸透していくということは、自らの生命、身体、財産に関わる情報を、量的にも質的にも、これまで以上にサイバー空間の場に委ねることを意味する。これらのデータが価値の源泉や利便性の向上に繋がることを通じて人々に対し恩恵を与えると同時に、そうしたデータは今後一層、攻撃者にとって、サイバー攻撃の対象となる誘引性が増すこととなり、結果としてサイバー攻撃の組織化・洗練化が、より計画的・大規模に行われる可能性がある。

また、このようにデジタルサービスが人々の生活に浸透していくことに伴い、デジタルサービス連携の間隙を突いたサイバー攻撃がみられるなど、攻撃手法も多様に変化・高度化していくことが考えられる。

加えて、技術革新の果実を攻撃側が活用することで脅威が増大する可能性も考えられる。例えば、AI 技術がサイバー攻撃に悪用されれば、人間の能力や技術的能力を超える速度と規模でサイバー攻撃が行われることもあり得、中長期的には、人間の制御によらない自律的攻撃の可能性も視野に入れなければならない。

(2) 経済社会が抱える脆弱性の観点

経済社会全体でみれば、デジタル化の進展により、これまでサイバー空間とは繋がりのなかった様々な業種・業態の企業や、若年層・高齢者を含めた個人までもが不可避的にサイバー空間に参画することとなる。サイバー空間がこれまで以上に誰もが安心して参画できる空間となることへの期待がより一層高まることとは裏腹に、サイバーセキュリティに関するリテラシーの差異や人材不足・偏在等が、攻撃者に狙われ得る弱点となる可能性がある。

また、企業組織や技術分野における人材不足は、サイバーセキュリティに係る製品・サービス、技術を、過度に海外に依存する状況を招き得る。リテラシー不足は、機器・サービスの誤用等を通じ、新たな脆弱性を経済社会に顕在化させる危険性もはらんでいる。

加えて、クラウドサービスの利用拡大や複雑かつグローバルなサプライチェーンを経由する製品・サービスの拡大・浸透、産業分野での IoT 機器の利用拡大（あらゆるモノがネットワークに接続されるようになること）や AI 技術の様々なシステムへの活用などにより、インシデントが発生した場合の経済社会活動への影響は、より広範に、多様な主体・場面に及ぶおそれがあり、それ故に解決に向けた困難性を増すと考えられる。

さらに、クラウドサービス利用の拡大は、テレワークの定着などとも相まって、従来の「境界型セキュリティ」の考え方[20]の限界も顕在化させつつある。

3.2. 国際情勢からみたリスク

サイバー空間は平素から、地政学的緊張を反映した国家間の競争の場の一部ともなっているが、サイバー攻撃が匿名性、非対称性、越境性という特性を有する中で、重要インフラの機能停止、国民情報や知的財産の窃取、民主プロセスへの干渉など国家の関与が疑われるものをはじめとする組織化・洗練化されたサイバー攻撃の脅威の増大がみられるなど、足元では、サイバー空間をめぐる情勢は、有事とは言えないまでも、最早純然たる平時とも言えない様相を呈している。

経済社会のデジタル化が広範かつ急速に進展する中、こうしたサイバー攻撃の増大等は、国民の安全・安心、国家や民主主義の根幹を揺るがすような重大な事態を生じさせ、国家安全保障上の課題へと発展していくリスクをはらんでいる。サイバー攻撃者の秘匿、偽装等が巧妙化しているが、特に国家の関与が疑われるサイバー活動として、中国は軍事関連企業、先端技術保有企業等の情報窃取のため、ロシアは軍事的及び政治的目的の達成に向けて影響力を行使するため、サイバー攻撃等を行っているとみられている。また、北朝鮮においても政治目標の達成や外貨獲得のため、サイバー攻撃等を行っているとみられている。さらに、中国・ロシア・北朝鮮において、軍をはじめとする各種機関のサイバー能力の構築が引き続き行われているとみられている[21]。

加えて、サイバー空間に関する基本的価値の相違や、国際ルール等をめぐる対立が顕在化する中、一部の国が主張するように、国家によるサイバー空間の管理・統制の強化が国際ルール等の潮流となれば、我が国の安全保障にも資する「自由、公正かつ安全なサイバー空間」や従うべき基本原則の確保が脅かされる。安全保障の裾野が経済・技術分野にも一層拡大する中で、技術覇権争いが顕在化し、また、国家によるデータ収集・管理・統制を強化する動きも見られる。

また、サイバー空間を構成するシステムのサプライチェーンの複雑化やグローバル化を通じ、サプライチェーンの過程で製品に不正機能等が埋め込まれるリスクや政治経済情勢による機器・サービスの供給途絶など、サイバー空間自体の信頼性や供給安定性に係るリスク（サプライチェーン・リスク）が顕在化している。

このように、サイバー攻撃の脅威に晒される対象の拡大とともに、その手段が組織化・洗練化され、サイバー空間の安定性が揺らぐ中で、個々の主体、あるいは一国のみで対応することが極めて困難な国際社会共通の切迫した課題となっており、まさに我が国が目指すべきグローバル規模での「自由、公正かつ安全なサイバー空間」の確保は危機に直面していると言えよう。

[20] 境界線（ペリメータ）で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。

[21] 具体的な動向は、4.3 国際社会の平和・安定及び我が国の安全保障への寄与の柱書きに詳述する。

3.3. 近年のサイバー空間における脅威の動向

以上で示したリスク要因は、近年のサイバー空間における脅威の動向をみても、明らかな傾向として表れている。

組織犯罪や国家の関与が疑われる攻撃が多く発生しており、海外では選挙に対する攻撃をはじめとする民主プロセスへの干渉や、サプライチェーンの弱点を悪用した大規模な攻撃、制御系システムを対象とした攻撃をはじめ広範な経済社会活動、ひいては国家安全保障に影響を与え得るインフラへの攻撃が猛威を奮っている。

また、テレワーク等の普及に伴い個々の端末経由又はVPN機器[22]の脆弱性を悪用しネットワークに侵入されるケースや、クラウドサービスが攻撃の標的とされるケースが増加しているほか、ワクチンに関するニュースに関連したビジネスメール詐欺やフィッシングなどのコロナ禍に乗じたサイバー攻撃や、比較的対策が行き届きづらい海外拠点を経由した攻撃、匿名性の高いインフラを通じて行われる攻撃など、足元の環境変化をタイムリーに捉えたサイバー攻撃も現にみられている。

これらに加えて、ばらまき型攻撃が2020年に入り急増するなど、標的型攻撃の被害は引き続き止んでいないほか、データ復元に加え窃取したデータを公開しない見返りの金銭要求も行ういわゆる「二重の脅迫」を行うランサムウェア[23]、匿名化技術や暗号技術の悪用による事後追跡の回避など、従来の脅威が複雑化・巧妙化している。背景として、マルウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、悪意のある者が高度な技術を持たなくても簡単に攻撃を行える状況が指摘されている。

こうしたサイバー攻撃により、生産活動の一時停止、サービス障害、金銭被害、個人情報窃取、機密情報窃取など、経済社会活動、ひいては国家安全保障に大きな影響が生じ得る状況となっている。

[22] Virtual Private Networkの略。インターネットや多人数が利用する閉域網を介して、暗号化やトラフィック制御技術により、プライベートネットワーク間が、あたかも専用線接続されているかのような状況を実現する技術又はそのための機器。

[23] 例えば、「G7首脳コミュニケ」（2021年6月）においては、「ランサムウェアの犯罪ネットワークによる脅威の高まり」について言及されている。

4. 目的達成のための施策　～Cybersecurity for All～

本項においては、基本法に掲げた目的を達成するため、前項までの課題認識を踏まえ、今後 3 年間にとるべき諸施策の目標や実施方針を示す。

サイバー空間は、これまで述べたように、空間そのものが量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来したと言えよう。今後、サイバー空間とは繋がりのなかった主体も含め、あらゆる主体がサイバー空間に参画することとなる中で、デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向けた取組を進める必要がある。この考え方の下、不確実性を増す環境において「自由、公正、かつ安全なサイバー空間」を確保するため、以下の 3 つの方向性に基づき、施策を推進する。

なお、これらは、主として、本項において示す「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に向けた取組にそれぞれ対応するものであるが、前項までの課題認識を踏まえれば、いずれの目的達成に向けた施策においても意識されるべきである。

＜3 つの方向性＞

(1) デジタル改革を踏まえたデジタルトランスフォーメーション[24]とサイバーセキュリティの同時推進

経済社会のデジタル化をめぐる状況をみれば、コロナ禍を通じて結果としていわゆる「ニューノーマル」の定着が進んだことに加え、デジタル社会の形成に向けた司令塔たるデジタル庁が 2021 年 9 月に設置されたことなど、今が、我が国が後れをとったデジタル化の時計の針を大きく進める絶好の機会であることは論をまたない。

一方で、サイバーセキュリティに対する意識や、サイバー空間を構成する技術基盤やデータ等に対する信頼が醸成されなければ、足元のデジタル化の潮流に対して積極的な参加・コミットメントを得られず、変革を伴わない表層的なデジタル化に留まるおそれがある。裏を返せば、デジタル化に応じたリスクの変容に適切に対処をすることで、サイバーセキュリティに対する意識や信頼の醸成にも繋がり得る。

また、経済社会全体のデジタル化だけではなく、個々の企業活動におけるデジタル化に視点を向けても、サイバーセキュリティ確保との強い関係性がみられる。デジタル化進展の中で、IT システムやデジタル化への対応能力が、業務、製品・サービス等の有する付加価値の源泉となっていくと想定される中で、サイバーセキュリティの確保は企業価値に直結する営為となると考えられる。加えて、迅速で柔軟な開発・対処の必要性が高まる中で、サイバーセキュリティを業務、製品・サービス等のシステムの企画・設計段階から確

[24] 「デジタルトランスフォーメーション」は、一般的に DX と略される。2018 年 9 月「DX レポート」（2018 年 9 月 経済産業省デジタルトランスフォーメーションに向けた研究会）においては、「企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第 3 のプラットフォーム（クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネス・モデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること」という定義が引用されている。

保する「セキュリティ・バイ・デザイン」の考え方は一層重要となり、デジタル投資とセキュリティ対策はより一層、一体性を増すと考えられる。

このように、ミクロ・マクロのいずれの視点においても、デジタル化の進展と併せてサイバーセキュリティ確保に向けた取組を同時に推進すること（以下「DX with Cybersecurity」という。）が重要であり、あらゆる主体においてこれが意識され、取組が推進されなければならない。足元のデジタル改革では、その基本法たるデジタル社会形成基本法（令和 3 年法律第 35 号）においてサイバーセキュリティの確保が明確に位置付けられるなど、デジタルトランスフォーメーションとサイバーセキュリティを同時に推進する素地が整えられたところであり、国として、その前提となる基盤づくりをはじめとして、デジタル化の動きを強力に後押しする。

(2) 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

2018 年に策定された従来のサイバーセキュリティ戦略では、サイバー空間の持続的な発展に向けて、サービス提供者の「任務保証」、「リスクマネジメント」、「参加・連携・協働」という 3 つの観点から官民の取組を進めることとしてきた。

サイバー空間の脅威の増大、経済社会が抱える脆弱性の顕在化、安全保障環境の変化等、不確実性を増す環境下で、サイバー空間においても、「公共空間」として実空間と変わらぬ安全・安心を確保していくため、攻撃者との非対称な状況を看過せず、それぞれの観点について深化・強化（①任務保証の深化、②「リスクマネジメント」に係る取組強化）し、その環境・原因の改善に正面から取り組んでいくことが求められている。

そうした社会的要請に伴い、サイバー空間に関わるあらゆる主体の役割が増している。自律的な取組（「自助」）や多様な主体の緊密連携（「共助」）の重要性は不変なるものであるが、それらの基盤となる「公助」の役割をはじめとして、各主体の役割や防御すべき対象を不断に検証し、多層的な取組を強化する。その際、自助共助では対応できないような事象に対して、国がインシデント対応とその後の再発防止や改善に向けた政策措置を一体的に推進するための総合的な調整を担う機能として、ナショナルサート（CSIRT/CERT）[25]の枠組みの強化を図りつつ、それが一層果たされるよう、検証による向上・充実強化を図る。

① 「任務保証」の深化（エンドユーザへのサービスの確実な提供を意識したサプライチェーン全体の信頼性確保）

従来の「任務保証」[26]の考え方は、サービス提供者が特に契約関係のあるサービスの直接的な利用者を中心に、遂行すべき業務を「任務」として着実に遂行するための考え方として位置付けられてきた。

---

[25] 一般的に、CSIRT は 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。CERT は Computer Emergency Response Team の略（サート）。コンピュータセキュリティインシデントに対応する活動を行う組織のこと。国際連携の下でサイバー攻撃に対処する際に、我が国においては、政府と民間の専門組織が連携して対応している。本戦略においては、ナショナルサートを、「深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能」と位置付けている（4.2.1(4)に詳述）。

[26] 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

近年、クラウドサービスの普及やサプライチェーンの複雑化等に伴い、サイバー空間を通じて提供されるサービスに対する様々な主体の関与や、クラウドサービス事業者等への依存度の増加により、サービス・業務の責任主体がエンドユーザから見えにくくなっている。また、インシデントが発生した際の影響も広範かつ複雑化し、その波及の予見や解決に向けた困難性も増している。クラウドサービスを例に挙げれば、あるクラウドサービスを利用する事業者のみならず、その利用事業者が提供するサービスを利用するエンドユーザにも影響が及び得る状況となっている。このような状況は、従来、サイバー空間への関与が少なく、デジタル化進展の過程で不可避的にサイバー空間に参加する者にとっては、なおさら深刻である。こうした認識に基づき、サイバー空間を活用して業務・サービスの提供に携わる者は、提供者と利用者間の一対一の関係だけではなく、サプライチェーン全体を俯瞰し、その信頼性を意識して責任ある行動をとることが求められる。

「任務保証」の考え方の重要性は今後も不変のものとして、さらにこれを深化させ、あらゆる組織が、サイバー空間を提供・構成する主体として、自らが遂行すべき業務や製品・サービスからエンドユーザに至るサプライチェーン全体の信頼性確保を「任務」と捉えることで、サイバー空間を構成する多様な製品やサービスについて、その安全性・信頼性が確保され、利用者が継続的に安心して利用できる環境をめざす。

② 「リスクマネジメント」に係る取組強化

組織化・洗練化されたサイバー攻撃の脅威の増大等がみられる中で、国として、各国政府・民間等様々なレベルで連携をしつつ、個々の主体による「リスクマネジメント」を補完し、一層実効的に取組を強化する。

具体的には、我が国として、サイバー攻撃に対して能動的かつ（自動化技術の活用等により）効率的に防御するとともに、脅威の趨勢を踏まえ、常に想定されるリスク等の見直しや事後追跡可能性（以下「トレーサビリティ」という。）の確保に努める。

また、国民の個人情報や国際競争力の源泉となる知的財産に関する情報、安全保障に係る情報の窃取のための一つの重要なチャネルとしてサイバー空間が利用されている現状を踏まえ、このようなサイバー攻撃への対処とともに、サイバー空間を構成する技術基盤自体の信頼性の確保に努める。

(3) 安全保障の観点からの取組強化

我が国の安全保障を巡る環境は厳しさを増し、サイバー空間が国家間の競争の場の一部ともなっている中で、サイバー空間における攻撃者との非対称な状況を看過してはならない。

各主体がその姿勢を明確化するとともに、防衛省・自衛隊をはじめとした政府機関等の能力強化により、国家の強靱性を確保するなどして防御力を強化し、攻撃者を特定し責任を負わせるためにサイバー攻撃を検知・調査・分析する能力を引き続き高め、抑止力を強化する。また、サイバー脅威に対しては、同盟国・同志国と連携をして、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。

全うするという考え方。

加えて、サイバー空間の健全な発展を妨げるような取組に対して、同盟国・同志国や民間団体と連携して対抗し、我が国の安全保障に資する形で、グローバルに「自由、公正かつ安全なサイバー空間」を確保するために、積極的な役割を果たす。

4.1.経済社会の活力の向上及び持続的発展　～DX with Cybersecurity の推進～

デジタル改革のビジョンである「デジタルの活用により、一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」の実現に向けて、我が国経済社会は、変革を伴うデジタルトランスフォーメーションを遂げることが必要である。

そして、その機会と影響が、あらゆる主体に例外なく及ぶ中で、「DX with Cybersecurity」があらゆる主体において意識され、取組があらゆる面で推進されなければならない。

経済社会のデジタル化を進めていく過程における、経営層の意識改革や、地域・中小企業に対する取組、デジタル時代において新たな価値創出を支えるサプライチェーン等の基盤づくり、経済社会全体でリテラシーを高める取組のいずれにおいても、サイバーセキュリティに関する視点が取り入れられ、施策が推進されることが重要である。

4.1.1 経営層の意識改革

新型コロナウイルスによりデジタル化は加速し、今後、企業において、より付加価値の高いデジタルサービス等を生み出す基盤を有しているかが重要な競争力の要素となっていくと想定される。経営層にとって、デジタル化とサイバーセキュリティ対策は、他人事ではなく、同時達成されるべき業務と収益の中核を支える基本的事項となり、両者を理解することが経営の基本的な素養・知識となると想定され、サイバー空間に関わるリスクの存在はデジタル化に取り組まない言い訳たり得なくなると考えられる。こうした認識に基づき、デジタル化と一体となったサイバーセキュリティの強化に向け、経営層の意識改革や企業の取組を推進していく必要がある。

デジタル経営の推進に向けては、自律的にデジタルトランスフォーメーションに取り組む企業へと、資金や人材、ビジネス機会が集まるような環境を整備していく観点から、経営者に求められる企業価値向上に向け実践すべき事柄をデジタル経営の指針としてまとめ、その実践を推進することとしている。

また、サイバーセキュリティの強化に向けては、これまで、経営層がリーダーシップを取ってセキュリティ対策を推進していくことの重要性を示したガイドラインの普及啓発を進めてきているところ、引き続き、その実践に向けた事例や手引き等の策定を通じて活用促進に取り組むとともに、必要に応じてその見直しを行っていくこととしている。

これらを踏まえつつ、デジタル化と一体となったサイバーセキュリティ強化に向けた取組状況が、サステナビリティを重視する投資家等のステークホルダーに可視化され、かつそうした取組に対しインセンティブが生まれるよう取り組む。これにより、企業の取組状況が、市場を含む企業内外から持続的な企業価値の向上に繋がるものとして評価され、更なる取組を促進する機運が形成されることが期待される。具体的には、デジタル経営に向けた行動指針やデジタル化に取り組む先進的な企業の選定・公表、デジタル関連投資への税制措置等のデジタル化促進施策においてサイバーセキュリティに係る取組を位置付けるとともに、取組状況を企業内外に可視化するためのツ

ールやガイドラインの活用促進等を推進する。これらを通じ、経営層によるサイバーセキュリティに係るリスク把握や企業情報開示といったプラクティスの普及促進も期待されるところ、企業の取組状況のフォローアップにも併せて取り組んでいく。

また、こうした一体的な推進策を通して、経営層がデジタル化と併せてサイバーセキュリティ対策に取り組む上で、自社の競争力の源泉たるデジタルサービス等に内在するリスクの所在を適切に把握できるようにするためには、企業内外の専門家とのコミュニケーションをとることが欠かせない営為となると想定される。このため、経営層に対し、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない場合にも、社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習得すべき知識（以下「『プラス・セキュリティ』知識」という。）を補充できる環境整備を推進する[27]。

4.1.2 地域・中小企業における DX with Cybersecurity の推進

コロナ禍への対応を余儀なくされること等を通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域・中小企業、そしてサイバー空間とは繋がりのなかった業種・業態の企業にも例外なく広がっていくと想定される。

一方で、中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たっては、セキュリティ専任の人材を配置できないなど、知見や人材等のリソース不足に直面しており、これらの課題への対処が必要である。

このため、「共助」の考え方に基づく、地域のコミュニティづくりにおいて、その機能を引き続き発展させ、専門家への相談に留まらず、ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など、リソース不足を踏まえた地域による課題解決・付加価値創出が行われる場の形成を促進するとともに、先進事例の共有を通じて全国への展開に取り組む。

また、中小企業においては、セキュリティに多額の予算を割くことが難しいという課題もあるところ、中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策の推進に取り組む。具体的には、中小企業を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムとも連携しつつ、一定の基準を満たすサービスに商標使用権を付与するための審査・登録、セキュリティ対策の自己宣言等の取組を推進するとともに、中小企業向け補助金における自己宣言等の要件化等を通じたインセンティブ付けに取り組む。これらの取組を通じ、サイバーセキュリティ強化に向けた取組状況が取引先等に対して可視化されることで、地域・中小企業に取組を広げる契機となることが期待される。

加えて、今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定される。その利用に当たっては、情報資産が企業外に置かれることに加え、設定の不備等により意図せず流出するリスクも一定程度伴うことから、クラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むと

[27] 経営層向けに限らない「プラス・セキュリティ」知識を補充できる環境整備に向けた具体施策については、4.4.2(1)①に詳述する。

ともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。

4.1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

サイバー空間と実空間が高度に融合する Society5.0 の実現に向けて、今後は、あらゆる主体が相互連関・連鎖を自由に形成することで新たな価値を創造することが期待される。一方で、その信頼性を確保する観点から、このように新たに形成される相互連関・連鎖の下で生じる課題に適切に対応していくことが必要となる。

こうした課題への適切な対応を目的として策定された、サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等も踏まえ、我が国において、新たな価値創出を支えるサプライチェーン等の信頼性確保の基盤となる、サイバーセキュリティ確保に向けた取組を推進する。

(1) サプライチェーンの信頼性確保

サプライチェーンの複雑化やデジタルサービスの連携が進む中、より柔軟で動的なサプライチェーンの構成が可能となる一方で、サイバーセキュリティに係る観点では、サイバー攻撃の起点となり得る箇所の拡大や実空間への影響の増大が懸念されるなど、サプライチェーン全体を見渡したリスク管理の重要性は増すと考えられる。

このような認識に立ち、上記フレームワーク等に基づく産業分野別及び産業横断的なガイドライン等の策定や活用促進を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

また、様々な産業分野の団体等が参加し、サプライチェーン全体でのサイバーセキュリティ対策強化を目的として意識喚起や取組の具体化を行うコンソーシアムの取組を支援する。加えて、この枠組みの下、一定の基準を満たす中小企業向けサービスの審査・登録や利用推奨、サイバーセキュリティ強化に向けた取組状況の可視化を行うことで、サプライチェーンを通じて地域・中小企業に取組を広げ、サプライチェーン全体の信頼性向上に繋がることが期待される。

(2) データ流通の信頼性確保

サイバー空間における多様な経済社会活動を進める上で、「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT)」[28]の実現に向けたデータガバナンス確保の観点を含め、その価値の源泉となるデータの真正性や流通基盤の信頼性を確保することが重要である。

主体間を流通する中でその属性が絶えず変化するデータの特性を踏まえ、リスクポイントの洗出しの観点から、データマネジメントに関する定義の明確化等を行い、リスクの洗い出しの手順やユースケースの検討等を含むフレームワークの整備を進めると

[28] 安倍内閣総理大臣（当時）による世界経済フォーラム年次総会演説 「『希望が生み出す経済』の新しい時代に向かって（仮訳)」（2019 年 1 月 23 日）

ともに、国境を越えて流通するデータを取り扱う各国等のルール間ギャップの把握等に活用する。

また、送信元のなりすましやデータの改ざん等を防止する仕組み（以下「トラストサービス」という。）については、その利活用に向けて実効的な仕組みとする必要がある。主体・意思、事実・情報、存在・時刻といった要素の真正性・完全性を確保・証明する各種トラストサービスの信頼性に関し、具備すべき要件等の整備・明確化や、その信頼度の評価・情報提供、国際的な連携（諸外国との相互運用性の確認）等の枠組みの整備に取り組む。

(3) セキュリティ製品・サービスの信頼性確保

サイバーセキュリティに向けた自律的な取組が広がりを見せるためには、市場において提供されるセキュリティ製品・サービスが信頼の置けるものであることが前提である。また、今後は、サプライチェーン・リスクへの懸念に加え、オープンAPI[29]やOSS[30]の活用が一般的となったことで開発者自身もシステム全体のリスクを把握する困難性が高まっている中で、自社製品等の信頼性を企業内外に示す観点から、第三者による客観的な検証・評価への需要が拡大し、そうした需要に応えるビジネスが産業として一層重要になっていくと考えられる。こうした観点から、信頼性確保の基盤づくりに取り組み、ひいては先端技術・イノベーションの社会実装に係る取組と相まって、他国に過度に依存しない日本発の製品・サービスの育成に取り組む。

具体的には、セキュリティ製品・サービスの有効性検証を行う基盤整備や実環境における試行検証を通じてビジネスマッチングを促進するほか、一定の基準を満たすセキュリティサービスを審査・登録しリスト化する取組や当該サービスの政府機関における利用促進に取り組む。また、検証ビジネスの市場形成に向け、国としても、検証事業者の信頼性を可視化する取組を検討する。

(4) 先端技術・イノベーションの社会実装

デジタル化が進展するにつれて、エビデンスが明確で組織内外への説明性の高い、又は自動化等を活用し効率的なセキュリティ対策が一層求められることとなる。こうした社会的要請に応える形で、産学連携が活発に行われるような産学官にわたるエコシステムの構築を推進し、オープンイノベーション活動を活性化していくことが急務である。

また、我が国におけるセキュリティ製品・サービスは海外に大きく依存している状態であり、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。

こうした状況を打破する取組の一環として、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し、安全保障の観点から情報管理に留意しつつ、産学官の結節点として、当該情報を産学官の様々な主体に効

[29] APIはApplication Programming Interfaceの略であり、あるソフトウェアが別のソフトウェアに対して公開する、入出力のための仕組みを指す。

[30] OSSはOpen Source Softwareの略であり、利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称を指す。

果的に共有する。この際、産学官が研究開発や製品開発等に利用しやすいものとなるよう、関係者との意見交換やコミュニティ形成を積極的に実施する。

このほか、IoT システム・サービス、サプライチェーン全体での活用に向けた基盤の開発・実証の取組について、様々な産業分野を念頭に置いた社会実装を促進する。

これら新技術の社会実装に向けた取組の一環として、政府機関における新技術の活用に向けた技術検討を促進する。さらに、国産セキュリティ製品・サービスのグローバル展開に向けて、国際標準化に向けた取組や海外展示会への出展支援等を引き続き推進する。

4.1.4 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

サイバー空間の基盤は人々のくらしにとっての基礎的なインフラとなりつつある中、「誰一人取り残さない、人に優しいデジタル化」[31]を進め、その恩恵を享受していくためには、国民一人ひとりが自らの判断で脅威から身を守れるよう、サイバーセキュリティに関する素養・基本的な知識・能力（いわゆるリテラシー）を身に付けていくことが必須である。

一方で、リテラシーは一朝一夕に身に付くものではない。行政のデジタル化、マイナンバーカードの普及や GIGA スクール構想[32]等が進み、様々なデジタルサービスに触れる機会が増えていく中、「まずは自分でやってみる」意識を持ち、リテラシーの向上と定着に向けて能動的に体験を積んでいくことが何よりも重要である。この際、情報教育が推進される中で、各種取組が進められるべきである。

国としても、デジタル活用の機会、またそれに応じたデジタル活用支援の取組と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。例えば、高齢者等向けには、携帯電話の販売代理店をはじめ様々な地域の担い手との連携、子供向けには、小中学校とサイバー防犯に係るボランティア等との連携も図りつつ、サイバーセキュリティに関する注意事項の啓発等に取り組む。GIGA スクール構想の推進に当たっては、教師の日常的な ICT 活用の支援等を行う支援員等の配置や教職課程における ICT 活用指導力の充実を図るとともに、児童生徒に対し、端末整備にあわせた啓発や、動画教材等を活用した情報モラルに関する教育を推進する。

また、インターネット上の偽情報の流布については、個人の意思決定や社会の合意形成に不適切な影響を与えるおそれがあることから、民間の自主的取組の 慫慂（しょうよう） を含め、幅広く周知啓発を行う。

[31] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）

[32] 全ての子供たちの可能性を引き出す個別最適な学びと協働的な学びを実現するため、児童生徒の１人１台端末と学校における高速大容量の通信ネットワークを一体的に整備する構想。

4.2. 国民が安全で安心して暮らせるデジタル社会の実現

サイバー空間の公共空間化とサイバー・フィジカルの垣根を越えた相互連関・連鎖の深化を踏まえ、あらゆるサービスの提供主体には、これまでの「任務保証」という考え方を深め、サイバー空間のこのような変容に適合したリスクマネジメントを講ずることが求められる。国は、サイバー空間の安全を確保することによって、サイバー空間に関わるあらゆる国民や主体が、安心してサイバー空間に参画できるよう、サイバー空間全体を俯瞰しつつ、関係主体との連携を通じて、自助・共助による自律的なリスクマネジメントが講じられる環境づくりに努める。また、国民の安全・安心の根幹に関わる経済社会基盤については、国は、防御すべき対象を不断に検証しつつ、関係主体と連携を図りながら、持ち得る全ての手段を活用して包括的なサイバー防御を講ずるとともに、先進的な取組の導入を率先して進めることで社会全体の実装を牽引（けん）し、サイバー空間の安全性・信頼性の確保を図る。

これらの取組を通じて、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって国全体のリスクの低減とレジリエンスの向上を図る。

4.2.1 国民・社会を守るためのサイバーセキュリティ環境の提供

サイバー空間の公共空間化を踏まえ、全ての主体が利便性と安心を感じられる社会を実現するため、国は、関係主体と連携しつつ、サイバー空間を構成する技術基盤やサービスの可視化とインシデント発生時のトレーサビリティの向上に取り組むことで、各主体がニーズに合った適切なリスクマネジメントを選択できるような環境を醸成するとともに、トレーサビリティの確保やサイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

また、このようなサイバー空間の変容を背景に、インシデントの影響が複雑かつ広範囲に伝播するリスクが顕在化している状況を踏まえ、各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は、関係主体と連携して環境づくりに取り組んでいく。

国民の安全・安心の根幹に関わる経済社会基盤の防護については、これを担う各主体が役割に応じた機密性、可用性、完全性を確実に保証することが基本であるが、前述のサイバー空間の変容に加え、近年の攻撃手法の組織化・洗練化などの脅威に晒されるなど厳しい環境下では、自助、共助の取組だけで対応することは益々困難となっていることから、国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講ずることによって、国全体のリスクの低減とレジリエンスの向上に精力的に取り組む。

また、国は特に防御すべき対象を不断に検証することも重要である。国家安全保障に関わる情報に加え、特に、国民の個人情報や国際競争力の源泉となる知的財産に関する

情報は、国として防護すべき重要な対象であり、サイバー攻撃を通じたこれらの不正な窃取は、国民の安全・安心や公正な経済取引を損なうものであることから、国は、経済安全保障の観点も含め、こうした情報の横断的な防護に向けた対策を強化する。

(1) 安全・安心なサイバー空間の利用環境の構築

国は、サイバー空間の公共空間化やそのサプライチェーンの深化を踏まえ、各主体の自助及び共助によるリスクマネジメントの向上に資するため、「セキュリティ・バイ・デザイン」の考え方に基づく基盤構築などの指針等を策定するとともに、サイバー空間のトレーサビリティや可視化の向上に官民が一体となって取り組む。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

① サイバーセキュリティを踏まえたサプライチェーン管理の構築

サプライチェーンに対してリスク管理等の必要な対策に取り組むべく、国は、サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別・産業横断的なガイドライン等の策定を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

また、国は、中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。

さらに、国は、機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼性の確保を図るための仕組みを構築するとともに、これら構成要素の信頼性が、サプライチェーン上において連続的に確保されるよう、トレーサビリティの確保と信頼性を毀損する攻撃に対する検知・防御の仕組みの構築を推進する。

② IoT や 5G 等の新たな技術やサービスの実装における安全・安心の確保

IoT が急速に普及する中、安全・安心な IoT 環境を実現していくため、国は、サイバー攻撃に悪用されるおそれのある機器を特定し注意喚起を進めていくとともに、「セキュリティ・バイ・デザイン」の考え方に基づいて、安全な IoT システムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施する。また、IoT 機器・システムの活用に当たっては、セーフティの観点からの対策とサイバーセキュリティ対策を組み合わせることが求められるところ、国は、そのようなセキュリティとセーフティの融合に対応したフレームワークの活用を推進する。

また、国は、全国及びローカル 5G のネットワークのサイバーセキュリティを確保するための仕組みの整備や、サイバーセキュリティを確保した 5G システムの開発供給・導入を促進する。

さらに、国は、自動運転、ドローン、工場の自動化、スマートシティ[33]、暗号資産[34]、宇宙産業等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通じて、安全・安心を確保する。

---

[33] ICT 等の新技術や官民各種のデータを活用した市民一人一人に寄り添ったサービスの提供や、各種分野におけるマネジメント(計画、整備、管理・運営等)の高度化等により、都市や地域が抱える諸課題の解決を行い、また新たな価値を創出し続ける、持続可能な都市や地域であり、Society 5.0 の先行的な実現の場。

[34] 法定通貨や法定通貨建ての資産ではなく、不特定の者に対する代価の弁済や不特定の者を相手方とした法定通貨との交換等に使用でき、電子的に記録され移転することが可能なもの。

③ 利用者保護の観点からの安全・安心の確保

利用者が安心して通信サービスを利用してサイバー空間において活動できるようにする観点から、必要に応じて関係法令に関する整理を行いながら、安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する。

また、多数の公的機関、企業及び国民が利用するサービスについては、その社会的基盤（プラットフォーム）としての役割に鑑み、国は、より一層のサプライチェーン管理を含めたサイバーセキュリティ対策を促進する。

(2) 新たなサイバーセキュリティの担い手との協調

サイバー空間が､日進月歩に変化する技術やサービスの実装により間断なく高度化し、サービス提供者の主体が変わりうる実態を踏まえ、国は、常にサイバー空間に登場する新たな技術やサービスを把握し、これらによるサイバー空間の各主体への相互影響度やその深刻度の分析を行い、それぞれの主体においてサイバーセキュリティへの確保に責任ある対応を果たせるような環境づくりを行う。

特に、クラウドサービスは、サイバー空間において欠かせないインフラとなっているが、例えば、サービスの設定不備等によって、利用者にとって意図しないインシデントが発生し、場合によっては当該インシデントを認識することも難しく、さらには自分の力だけでは正常化できないような事態も発生している。また、クラウドサービスは、これを利用する多数の間で同様のインシデントが同時多発的に発生するという問題もある。このため、利用者が安心してクラウドサービスに情報資産を委ねることができるよう、国は、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、政府機関や重要インフラ事業者等の利用者がクラウドサービスを用いた情報システムの設計及び開発の過程において考慮すべきサイバーセキュリティのルールを、当該利用者やクラウドサービス事業者、システム受託事業者等の関係者と連携しながら策定する。これによって、クラウドサービスの利用者側が、自らのリスクマネジメント指針に合致した適切なクラウドサービスを選択し、セキュリティに関するポリシーや責任分界を正しく理解することを可能とするほか、提供者との間で認識のずれが生じた場合にも適切に課題を処理できるような関係を構築していく。並行して、国は、政府情報システムのためのセキュリティ評価制度（ISMAP[35]）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。クラウドサービスは外国企業により提供されているものも多いことから、グローバルな連携も進める。

これらの対策を多層的に展開し、必要に応じてパッケージ化することも検討したうえで、中小企業や地方における利用者のサイバーセキュリティの確保も促し、日本社会全体における安全・安心なクラウドサービス利用環境を構築する。

(3) サイバー犯罪への対策

サイバー空間があらゆる主体が参画する公共空間へと進化していることを踏まえ、実

[35] Information system Security Management and Assessment Program の略。政府情報システムのためのセキュリティ評価制度（通称：ISMAP（イスマップ））。政府情報システムにおけるクラウドサービスのセキュリティ評価制度として 2020 年度に制度運用を開始。

空間と変わらぬ安全・安心を確保するため、国は、サイバー空間を悪用する犯罪者や、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

また、暗号資産、ダークウェブ、SNS 等を悪用した犯罪や、高度な情報通信技術を用いた犯罪に対処できるよう、捜査能力・技術力の向上に取り組むとともに、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化する。

さらに、犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働きかけ等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐほか、情報の共有・分析、被害の未然防止、人材育成等の観点から、官民が連携したサイバー犯罪対策を推進するとともに、国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯に係るボランティア等の関係機関・団体と連携し、広報啓発等を推進する。

あわせて、高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化することなど、情報技術の解析に関する態勢を強化する。

こうした取組に加え、攻撃者との非対称な状況を生んでいる環境・原因を改善するため、国は、諸外国における取組状況等を参考にしつつ、関連事業者との協力や国際連携等必要な取組を推進する。また、通信履歴等に関するログの保存の在り方については、関係のガイドラインを踏まえ、関係事業者における適切な取組を推進する。

これら取組を効果的に実施していくため、警察組織内にサイバー部門の司令塔を担う機能と、専門の実働部隊を創設することを検討するなど、対処能力の強化を図る。

(4) 包括的なサイバー防御の展開

重要インフラの機能停止、国民情報や知的財産の窃取、金銭窃取など国民の安全・安心の根幹を揺るがすような深刻なサイバー攻撃に対しては、サイバー空間の相互連関・連鎖の深化と相まって、個々の主体による自助・共助の取組だけでは対応に限界があり、また、その影響の全体像を把握することも困難となるなど、実効的な防御を講じることが難しい状況となっている。

このため、国は、このような深刻なサイバー攻撃に対して、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至るインシデント対応及びその後の再発防止や改善に向けたルールづくり等の政策措置の展開を一体的に推進する包括的なサイバー防御策について、関係主体との連携も図りつつ、持ち得る全ての能力と手段を活用して展開する。

① 包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化

国は、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（CSIRT/CERT）の枠組みを強化する。具体的には、対処官庁のリソース結集と連携強化を通じて対処能力の向上と対処に係る一体性・連動性を図るとともに、サイバー関連事業者との連携強化

によって組織・分野横断的に影響が波及し得る事案の情報収集や初動を含めた対処調整の迅速化を図る。また、サイバーセキュリティ協議会[36]やサイバーセキュリティ対処調整センター[37]、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間や海外関係機関との連携を一層推進することで、官民間・国際間での情報共有と対処調整の円滑化を図る。さらに、発生した事案等から得られた課題や気づきを踏まえ、国は、官民を含む関係者と総合的な調整を行い、適時に制度化など必要な政策の立案・措置を講じていく。

これらの取組により、官民を含む関係者からの適宜迅速な情報収集と被害の全体像の迅速な把握力を強化するとともに、国の防御に関する情報発信の訴求力と網羅性の向上、攻撃の特性や深刻度、個々の分野の事情に応じた系統的できめ細かい対応、防御の実効性向上に資する経営から現場レベルまでの様々なニーズに応じた適時な注意喚起や情報提供、サイバー攻撃の無害化等を模索するグローバルなオペレーションへの協力、さらに、円滑な総合調整による迅速な政策立案等の更なる推進を図り、国全体の包括的な防御力を向上する。

② 包括的なサイバー防御を着実に実施していくための環境整備

国は、深刻なサイバー攻撃への対処を実効たらしめる脆弱性対策等の「積極的サイバー防御」[38]に係る諸施策、IT システムやサービスの信頼性・安全性を確認するための技術検証体制の整備、情報共有・報告・被害公表の的確な推進、制御システムのインシデント原因究明機能の整備等について関係府省庁間で連携して検討する。

(5) サイバー空間の信頼性確保に向けた取組

現在認知されているサイバー攻撃の多くが国民の個人情報や国際競争力の源泉となる知的財産に関する情報を目的としていることを踏まえ、国は、経済安全保障の観点も含めた横断的な防護対策を講ずる。

また、我が国の国民生活や経済社会活動の根幹を支える基盤において実装されている IT システムに起因するインシデントが、それら基盤の機能停止に直結するリスクを踏まえ、国は、経済安全保障の観点から、任務及び機能の自律性の毀損に繋がるおそれのあるサイバー空間の脆弱性を把握し、その信頼性確保に向けた対応を検討する。

① 国民の個人情報や国際競争力の源泉となる知的財産に関する情報を保有する主体を支援する取組

国は、サイバー攻撃等から個人情報を保護する有効な安全管理措置について、適時適切に情報提供を行い、対策の徹底を図る。

また、国は、国民の個人情報や国際競争力の源泉となる知的財産に関する情報を保有または管理する主体である民間企業、大学等におけるセキュリティ対策に資する情報共有を促す取組を強化する。

---

[36] 2018 年 12 月に成立したサイバーセキュリティ基本法の一部を改正する法律（平成 30 年法律第 91 号）に基づき、2019 年 4 月 1 日に、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うために組織されたもの。本協議会は、官民又は業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を防ぎ、また、被害の拡大を防ぐことなどを目的としている。

[37] 東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織。2019 年 4 月 1 日に設置。2022 年 3 月末をもって閉鎖。

[38] サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じていく取組のこと。

② 経済安全保障の視点を踏まえたITシステム・サービスの信頼性確保

国は、我が国の国民生活や経済社会活動に大きな影響のある重要なインフラにおいて実装されるITシステム・サービスや、その業務提携や委託契約の態様について、サプライチェーン・リスクを含む様々なリスク・シナリオも勘案し、その安全性・信頼性を確保するための制度的検討を含む対策を推進する。また、それに必要となる新たな技術開発を推進する。

我が国と海外との通信の大部分を依存する国際海底ケーブル等のインフラについて、官民間・国際間で連携しつつ、安全性、信頼性及び冗長性の確保、防護を推進する。

また、国は、IT機器やサービスに係る国際標準の策定や、安全性・信頼性の可視化を促すための基準づくり・評価の取組についても国際連携も念頭に置きながら推進する。特に、政府情報システムの調達に係るサプライチェーンも含めた信頼性確保の取組強化やセキュリティ評価制度（ISMAP）の活用を進めるとともに、ITシステム・サービスの信頼性に関する技術面での検証能力の構築やそのための基準策定に着手することで制度面・技術面の双方から信頼性の底上げを図る。

4.2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

「誰一人取り残さない、人に優しいデジタル化」の実現のためには、国民目線に立った利便性向上の徹底とサイバーセキュリティの確保の両立が必要である。このため、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針（以下「整備方針」という。）において、サイバーセキュリティについても基本的な方針を示し、その実装を推進する。

また、デジタル庁は、データの安全・安心な利活用の観点から、マイナンバーや法人番号など個人・法人を一意に特定し識別するID制度や電子署名、商業登記電子証明書など情報とその発信者の真正性等を保証する制度の企画立案を関係府省庁と共管し、利用者視点で改革し、普及を推進する。

さらに、国は、クラウド・バイ・デフォルトの実現を支えるISMAP制度を運用し、運用状況等を踏まえて制度の継続的な見直しを行うとともに、民間における利用も推奨する。

4.2.3 経済社会基盤を支える各主体における取組①（政府機関等）

各政府機関においては、統一的な基準を踏まえたセキュリティ対策が講じられるとともに、当該基準に基づいた監査やCSIRT訓練・研修等、GSOC[39]による不正な通信の監視等の取組を通じて、政府機関全体としての対策の水準の向上を推進している。各政府機関は、社会全体のデジタル化と一体としてサイバーセキュリティ対策を進め、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく。

特に、各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は

[39] Government Security Operation Coordination teamの略（ジーソック）。政府関係機関情報セキュリティ横断監視・即応調整チーム。各機関に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各機関への助言、各機関の相互連携促進及び情報共有を行うためのGSOCシステムを運用する体制のこと。2008年4月から運用を開始した政府機関等に対する監視体制（第一GSOC）と、2017年4月から運用を開始した独立行政法人等に対する監視体制（第二GSOC）がある。

各府省庁と共同で整備・運用し、セキュリティも含めて安定的・継続的な稼働を確保する。

加えて、コロナ禍を契機としたテレワークやクラウドの浸透によって、新たなセキュリティリスクが顕在化していることから、国は、「新たな生活様式」を安全・安心に実現できる対策を講ずる。特に従来の「境界型セキュリティ」だけでは対処できないことも現実となりつつあることから、国は、こうした状況に対応したシステムの設計、運用・監視、インシデント対応、監査等やそれを担う体制・人材の在り方を検討する。

また、複雑化・巧妙化しているサイバー攻撃に鑑みれば、近年は、対策が手薄になりがちな海外拠点や中小企業等を含めた委託先を狙う等サプライチェーン全体を俯瞰したセキュリティ対策の必要性が増している。そのため、企業規模等に応じた実効性を見極めつつ、国は、このような新たな脅威に対し効果的なセキュリティ対策を進めていく。

具体的には、「クラウド・バイ・デフォルト原則」[40]に対応したセキュリティ対策として、国は、クラウドサービスの利用拡大を見据えた政府統一基準群[41]の改定と運用やクラウド監視に対応したGSOC機能強化の検討を実施する。

また、国は、第4期GSOC（2021年度～2024年度）を着実に運用するとともに、従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく。あわせて、GSOC等の在り方も検討する。

国は、行政分野におけるサプライチェーン・リスクやIoT機器・サービス（制御システムのIoT化も含む）への対応を強化する。

国は、情報システムの設計・開発段階から講じておくべきセキュリティ対策（認証機能、クラウドサービス等における初期設定、脆弱性対応等）を実施する。

国は、セキュリティ監査やCSIRT訓練・研修等を通じて政府機関等におけるサイバーセキュリティ対応水準を維持・向上する。

4.2.4 経済社会基盤を支える各主体における取組②（重要インフラ）

我が国の経済や社会は、様々な重要インフラサービスの継続的な提供に依存しているが、重要インフラ間の相互依存性の高まりやサプライチェーンの複雑化・グローバル化を踏まえると、安全で安心な社会の実現には、脅威が年々高まっている重要インフラのサイバーセキュリティを確保し、強靱性を高めることが不可欠である。

基本法では、重要インフラ事業者の責務を明確に定めるとともに、国は、重要インフラ事業者等のサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるよう規定されている。

こうしたことを踏まえ、重要インフラに関わる各主体がそれぞれの責務を認識し、官民が一体となって堅牢な重要インフラの実現に向けた取組を推進する。

---

[40] クラウドサービスの利用を第一候補とした、政府情報システムにおけるクラウド・バイ・デフォルトの基本的な考え方を整理したもの。

[41] 国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みであり、国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。

(1) 官民連携に基づく重要インフラ防護の推進

国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進する。

重要インフラをとりまく脅威は年々高度化・巧妙化しているが、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。このことを踏まえ、重要インフラ防護のよりどころとなる現行の「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」[42]を基本としつつ、重要インフラ分野が全体として今後の脅威の動向、システム、資産をとりまく環境変化に柔軟に対応できるようにするため、国は、行動計画を積極的に改定し、官民連携に基づく重要インフラ防護の一層の強化を図る。

重要インフラサービスの安全かつ持続的な提供において、デジタル技術は大きな役割を果たすものであり、サイバーセキュリティの確保は経営の根幹に関わるものである。この認識の下、ビジネスとセキュリティのバランスが取れ、先進的でセキュリティ対策が適切に講じられた重要インフラサービスの実現を確実なものとするため、国は、各組織が先行事例で得られた教訓を有効に生かせるよう、重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実を図るとともに、セキュリティ対策は組織一丸となって取り組むことが重要であることから、国は、経営層のリーダーシップが遺憾なく発揮できる体制の構築を図っていく。

(2) 地方公共団体に対する支援

地方公共団体は、個人情報等の多数の機微な情報を保有し、国民生活に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にセキュリティが確保されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。

「地方公共団体における情報セキュリティポリシーに関するガイドライン」[43]に基づくセキュリティ対策が着実に実施されるよう、国は、人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。

地方公共団体情報システムの標準化、行政手続のオンライン化、「クラウド・バイ・デフォルト原則」等を受けたクラウド化、働き方改革や業務継続のためのテレワークの導入等、新たな時代の要請に柔軟に対応できるよう、国は、同ガイドラインの継続的な見直し等、必要な諸制度の整備を推進する。

地方におけるデジタル改革（デジタル・ガバメントの実現）を促進するため、国は、「デジタル社会の実現に向けた改革の基本方針」[44]を踏まえ、整備方針において、地方

---

[42] 重要インフラ防護に係る基本的な枠組みとして、重要インフラ防護に責任を有する政府と自主的な取り組みを進める重要インフラ事業者等との共通の行動計画を策定し、これを推進してきた。昨今のサイバー攻撃による急速な脅威の高まりや、東京大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第 3 次行動計画を見直したもの。

[43] 2020 年 12 月に総務省において改定。各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。

[44] 2020 年 12 月 25 日閣議決定。「デジタル社会の将来像」、「IT 基本法の見直しの考え方」、「デジタル庁（仮称）設置の考え方」等について、デジタル・ガバメント閣僚会議の下で開催されたデジタル改革関連法案ワーキンググループにおける議論も踏まえ、政府としての方針を示すもの。

公共団体のセキュリティについての方針を規定する。

国民生活・国民の個人情報に密接に関わるマイナンバーについて、国は利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。

4.2.5 経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

大学・大学共同利用機関等（以下「大学等」という。）は、多様な構成員によって構成され、多岐にわたる情報資産や、多様なシステムを有するという実態を踏まえ、その自律的な対策はもちろん、連携協力体制の構築や情報共有等において、国の積極的な支援が重要である。

そのため、国は、大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する研修や訓練・演習の実施、事案発生時の初動対応への支援や、情報共有等の大学等の連携協力による取組を推進する。

また、先端的な技術情報等を保有する大学等については、国は、組織全体に共通して実施するセキュリティ対策のみならず、当該技術情報等を高度サイバー攻撃から保護するために必要な技術的対策や、サプライチェーン・リスクへの対策を強化できるよう取組を支援する。

4.2.6 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

サイバー空間におけるリスクの高まりを踏まえ、国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。

また、新たな攻撃にも国全体として網羅的な対処が可能となるよう、国は、ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は、東京大会での運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。

(1) 分野・課題ごとに応じた情報共有・連携の推進

サイバー空間における各主体の有機的な連携による多層的なサイバー防御体制の構築を図る観点から、各主体との緊密な連携の下、国は、セプターやISAC[45]を含む既存の情報共有における取組を充実・強化するほか、情報共有に関する新たな枠組みの構築・活性化を支援する。

(2) 包括的なサイバー防御に資する情報共有・連携体制の整備

サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサ

[45] Information Sharing and Analysis Center の略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。

ート（CSIRT/CERT）の枠組み整備の一環として、国は、サイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間の連携を進め、外部との連携や調整の在り方について具体的に検討する。

また、国は、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見やノウハウを、東京大会の運営を支える事業者等にとどまらず、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が国のサイバーセキュリティ全体の底上げを進める。

4.2.7 大規模サイバー攻撃事態等への対処態勢の強化

サイバー空間と実空間の一体化がますます進展し、インシデントの影響が広範囲に伝播するおそれやこれを考慮した被害予測等を踏まえ、国は、平時から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化する。

また、国は、分野や地域のコミュニティを活用してサイバー攻撃への対処態勢の強化に努めるとともに、官民連携により情報収集・分析・共有機能を強化する。

さらに、国及び各主体は官民連携の取組等を通じてセキュリティ人材を育成及び活用することで、大規模サイバー攻撃事態等への対処を強化する。

4.3.国際社会の平和・安定及び我が国の安全保障への寄与

我が国をとりまく安全保障環境は、厳しさを増しており、我が国が享受してきた既存の秩序についても、不確実性が急速に増している。政治・経済・軍事・技術を巡る国家間の競争の顕在化を含め、国際社会の変化の加速化・複雑化が進展している。

サイバー空間についても、地政学的緊張も反映しつつ、平素からこうした国家間の競争の場となっている。高度なサイバー能力を有する軍等が他国の重要インフラへのサイバー攻撃を行ったとされている事例も指摘される等、サイバー空間をめぐる情勢は有事とは言えないまでも、最早純然たる平時とも言えない様相を呈しており、社会のデジタル化が広範かつ急速に進展する中、重大な事態へと急速に発展していくリスクをはらんでいる。また、サイバー空間を利用した影響工作や、主体、被害等の把握が困難なサイバー攻撃等は、ときに軍事活動と複合的に組み合わされることにより、武力攻撃に至らない形での現状変更の試みに利用されうる。特に国家の関与が疑われるサイバー活動として、中国は軍事関連企業、先端技術保有企業等の情報窃取のため、ロシアは軍事的及び政治的目的の達成に向けて影響力を行使するため、サイバー攻撃等を行っているとみられている。また、北朝鮮においても政治目標の達成や外貨獲得のため、サイバー攻撃等を行っているとみられている[46]。加えて、中国・ロシア・北朝鮮において、軍をはじめとする各種機関のサイバー能力の構築・増強が引き続き行われているとみられている[47]。一方、同盟国である米国や基本的価値観を共有する同志国においても、サイバー脅威に対応するため、サイバー軍の能力構築が加速されるとともに、サイバー攻撃対処能力の強化が進められている[48]。

こうした中で、各国において同盟国・同志国との協力・連携を強化する重要性が認識されており、特に、国家の関与が疑われるサイバー事案やサイバー空間に関する国際ルール等をめぐる対立に対して同盟国・同志国等が連携して対抗している。2021 年 3 月に行われた日米安全保障協議委員会（以下「日米『2+2』」という。）、日米外相会談及び日米防衛相会談においては、この分野を一層強化していくことの重要性が確認された。加えて、近年、安全保障の裾野が経済・技術分野にも一層拡大している中で、技術基盤やデータをめぐる争いについても、同様に同盟国・同志国等と連携して対抗している。

このような中で、「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び我が国の安全保障に寄与することの重要性は一層高まっている。サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化する。

4.3.1 「自由、公正かつ安全なサイバー空間」の確保

グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、国際場裡

---

46 中国、ロシア及び北朝鮮によるサイバー攻撃等については「G7 首脳コミュニケ」（2021 年 6 月）、「G7 外相コミュニケ」（2021 年 5 月）、「国連安全保障理事会北朝鮮制裁委員会専門家パネルによる最終報告書」（2021 年 3 月）、米国国家サイバー戦略（2018 年 9 月）、米国国防総省サイバー戦略（2018 年 9 月）を参照。
なお、公安調査庁「サイバー空間における脅威の概況 2021」及び警察庁警備局「治安の回顧と展望」（2020 年 12 月）において、個別事案に係る米国等の発表に触れつつ、中国、ロシア及び北朝鮮の軍・情報機関等の関与が指摘されているとしている。また、中国に関しては、注釈 53 も参照。

47 防衛省「令和 3 年版防衛白書」（2021 年 7 月 13 日閣議報告）

48 防衛省「令和 3 年版防衛白書」（2021 年 7 月 13 日閣議報告）

において我が国の基本的な理念を発信していく。また、サイバー空間における法の支配の推進及びこのような我が国の基本的な理念に沿った国際ルール形成のため、引き続き、同盟国・同志国と連携し、積極的な役割を果たしていく。

(1) サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）

国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することが重要である。

グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、引き続き国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため積極的な役割を果たしていく。特に、コロナ禍において医療機関へのサイバー攻撃が多くの国で見られ、こうした攻撃を抑止し、また、重要インフラを防護するためにもサイバー空間において法の支配を推進することが一層の重要課題となっている。国連等においては、サイバー空間においても既存の国際法の適用を前提とし、サイバー空間における規範などの実践にも積極的に取り組んでいく立場から、国際法の適用に関する我が国の見解を積極的に発信し、「自由、公正かつ安全なサイバー空間」の確保のため同盟国・同志国と連携していく。そのような活動を通じ、我が国の安全保障及び日米同盟全体の抑止力向上の取組に資するよう、国内外における国際法の適用に関する議論・規範の実践の普及に取り組んでいく。

サイバー犯罪対策については、サイバー犯罪に関する条約等既存の国際的枠組み等を活用し、条約の普遍化及び内容の充実化を推進するとともに、国連における新条約策定に関する議論に十分関与することを通じ、サイバー空間における法の支配及び一層の国際連携を推進する。

(2) サイバー空間におけるルール形成

G20 大阪首脳宣言においてデジタル経済における「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT)」を促進する必要性が確認されたこと、「プラハ提案」[49]において 5G セキュリティにおけるトラストの重要性が言及されたこと等に見られるように同盟国・同志国等と連携した国際的な取組に向けた動きが進展している。また、我が国が目指す「自由、公正かつ安全なサイバー空間」の秩序形成に向けては、インターネット・ガバナンス・フォーラム等インターネット・ガバナンスに関するマルチステークホルダー・アプローチでの枠組みも発展してきている[50]。

他方、既存の秩序とは相容れないおそれのある提案が行われていること等も踏まえ、引き続き国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会のルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく。健全なサイバー空間の発展を妨げるような国際ルールの変更を目指す取組については、同盟国・同志国や民間団体等と連携して対抗する。

---

49 「プラハ提案」とは、プラハ 5G セキュリティ会議における議長声明（2019 年 5 月）を指す。

50 G7 伊勢志摩首脳宣言（2016 年 5 月 27 日）において「我々は、政府、民間部門、市民社会、技術コミュニティ及び国際機関による十分かつ積極的な参加を含むインターネット・ガバナンスに関するマルチステークホルダー・アプローチを促進することにコミットする」としている。

4.3.2 我が国の防御力・抑止力・状況把握力の強化

我が国をとりまく安全保障環境が厳しさを増している中、政府機関、重要インフラ事業者、先端技術を有する企業・学術機関等への攻撃や、民主主義の根幹を揺るがしかねない事例も発生している。さらに、それらの中には国家の関与が疑われる事案も存在する。

以上を踏まえ、サイバー攻撃から我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保し、サイバー攻撃から国家を防御する力（防御力）、サイバー攻撃を抑止する力（抑止力）、サイバー空間の状況を把握する力（状況把握力）をそれぞれ高めつつ、政府全体としてシームレスな対応を抜本的に強化していくことが重要である。

これら安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う府省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。

また、こうした政府全体の安全保障に係る取組の中で、防衛省・自衛隊は、「平成 31 年度以降に係る防衛計画の大綱」（2018 年 12 月 18 日閣議決定）に基づき、各種の取組を進め、サイバー防衛に関する能力を抜本的に強化する。

(1) サイバー攻撃に対する防御力の向上

① 任務保証

政府機関は、国民生活や経済社会を守り、支える任務を有しており、その機能停止は、安全保障上の重大な懸念事項である。政府機関の任務遂行は、重要インフラその他のシステムを担う事業者のサービスに依存している。また、これら事業者自身も、国民や社会に不可欠なサービスを提供するという重要な任務を有している。

任務保証の観点から政府機関及び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確保の推進が引き続き必要である。政府においては、安全保障上重要な情報を取り扱うネットワークについて、リスクの低減を含めた一層の防護を推進する。さらに、自衛隊及び米軍の活動が依拠する重要インフラ及びサービスの防護のため、自衛隊及び米軍による共同演習等を着実に実施していく。防衛省・自衛隊においては、サイバー関連部隊の体制強化等、サイバー防衛能力の抜本的強化を図る。

② 我が国の先端技術・防衛関連技術の防護

我が国の安全保障上重要な情報等が狙われている中で、宇宙関連技術、原子力関連技術、その他先端技術等我が国の安全保障に関連する技術等につき、リスク低減を含めた一層の防護が必要である。特に防衛産業については、新たな情報セキュリティ基準の策定や官民連携の一層の強化等によりセキュリティ確保の取組を進めていく。また、国の安全保障を支える重要インフラ事業者や先端技術・防衛関連技術産業、研究機関といった関係事業者と国の一層の情報や脅威認識の共有及び連携を図る。

③ サイバー空間を悪用したテロ組織の活動への対策

サイバー空間は、個人や団体が自由に情報をやり取りし、自らの考えを述べる場を提供するものであり、民主主義を支えているものの一つである。他方、テロ組織が、過激思想の伝播や示威行為、組織への勧誘活用、活動資金の獲得等の悪意ある目的でサイバー空間を利用することは防止しなければならない。このため、表現の自由を含む基本的人権を保障しつつ、サイバー空間を悪用したテロ組織の活動への対策に必要な措置を引き続き国際社会と連携して実施する。

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応

国際連合憲章を始めとする国際法は、サイバー空間において適用される[51]。サイバー空間における国家による国際違法行為は当該国家の国家責任を伴い、被害者である国家は、一定の場合には、当該責任を有する国家に対して均衡性のある対抗措置及びその他合法的な対応をとることが可能である。また、一定の場合には、サイバー攻撃が国際法上の武力の行使又は武力攻撃となり得る[52]。

これらを踏まえ、我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。この点に関し、2019 年の日米「2+2」において、一定の場合には、サイバー攻撃が日米安全保障条約第 5 条の規定の適用上武力攻撃を構成し得ることを確認したところである。また、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用していくとともに、サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含め、然るべく対応していく。この点に関し、外交的手段の例としては、2021 年 7 月、中国政府を背景に持つ可能性が高いサイバー攻撃グループによるサイバー攻撃や、中国人民解放軍を背景に持つサイバー攻撃グループが関与した可能性が高いサイバー攻撃[53]について、断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話の発出[54]等が挙げられる[55]。また、刑事訴追等の例としては、2021 年 4 月に警察において書類送致した事件への捜査[53]等が挙げられる。この捜査等を通じ、国内企業等への攻撃を実行したサイバー攻撃集団の背景組織として、中国人民解放軍が関与している可能性が高いと評価するに至ったところであり、今後も警察組織内に設置される実働部隊をはじめとした捜査機関による厳正な取締りを進めていく。

---

[51] 2015 年国連第 4 会期政府専門家会合報告書において、サイバー空間に対する国連憲章全体を含む既存の国際法が適用されることが確認され、2021 年国連オープンエンド作業部会報告書においても同趣旨を再確認した。

[52] G7 伊勢志摩サミット　サイバーに関する G7 の原則と行動（2016 年 5 月）

[53] 2021 年 4 月に警視庁が中国共産党員の男を被疑者として、東京地方検察庁に書類送致した事件。本件に関し、2021 年 4 月 20 日の内閣官房長官記者会見では、「本件捜査を通じて、契約された日本のレンタルサーバーが、JAXA 等に対するサイバー攻撃に悪用されたこと、またその攻撃には中国人民解放軍 61419 部隊を背景に持つ「Tick」と呼ばれるサイバー攻撃集団が関与した可能性が高いことが判明したとも承知をしております。」としている。

[54] 中国政府を背景に持つ可能性が高い APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について断固非難する旨の外務報道官談話を発出している（2021 年 7 月 19 日）。

[55] この他、これまで同盟国・同志国と連携して、2017 年にも「ワナクライ」事案の背後に、北朝鮮の関与があったことを非難する外務報道官談話を発出し、2018 年には中国を拠点とする APT10 といわれるグループによるサイバー攻撃について非難する旨の外務報道官談話を発出している。[56] 情報通信技術を用いた外国の諜報活動に対抗する情報防衛活動

また、サイバー攻撃は、重大な事態へと急速に発展していくリスクをはらんでいることから、平時・大規模サイバー攻撃事態・武力攻撃という事態のエスカレーションにもシームレスに移行することで、迅速に事態に対処するとともに、2021年3月の日米「2+2」の成果を踏まえ、引き続き日米同盟の抑止力を維持・強化していく。

② 信頼醸成措置

サイバー攻撃を発端とした不測の事態の発生や悪化を防止するため、国家間の信頼を醸成する。サイバー空間は匿名性、隠密性が高く、意図せず国家間の緊張が高まり、事態が悪化するリスクがある。このように、偶発的又は不必要な衝突を防ぐため、国境を越える事案が発生した場合に備え、信頼醸成措置として国際的な連絡体制を平素から構築することが重要である。

また、二国間・多国間の協議における情報交換、政策対話等を積極的に行うことを通じ、透明性を高め、国家間の信頼を醸成する必要がある。各国と協力し、サイバー空間の問題を調整するメカニズムを活用する。

(3) サイバー空間の状況把握力の強化

① 関係機関の能力向上

状況把握力は、防御力ひいては抑止力の基盤である。深刻化するサイバー攻撃やサイバー空間を利用した影響工作の脅威を抑止していくためには、対応力の強化に加え、攻撃者を特定し、責任を負わせるために、サイバー攻撃等を検知・調査・分析する十分な能力が求められる。このため、関係機関におけるこうした能力を質的・量的に引き続き向上させ、関係機関の全国的なネットワーク・技術部隊・人的情報も駆使しながらサイバー攻撃等の更なる実態解明を推進する。

加えて、高度な分析能力を有する人材の育成・確保、サイバー攻撃等を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンス[56]に係る取組を進める。

② 脅威情報連携

国家の関与が疑われるサイバー攻撃、非政府組織による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係府省庁及び同盟国・同志国との情報共有を推進する。また、内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

4.3.3 国際協力・連携

サイバー空間においては事象の影響が容易に国境を越え、他国で生じたサイバー事案は我が国にも容易に影響を及ぼす可能性があることから、各国政府・民間等様々なレベルで重層的に協力・連携することが重要である。このため、知見の共有・政策調整、サイバー事案等に係る国際連携及び能力構築支援を推進する。

(1) 知見の共有・政策調整

国際ルールや技術基盤をめぐる争いが顕在化する中、米国その他同志国等とのサイバー協議に見られるハイレベルでの府省庁横断的な二国間協議及び多国間協議のほか、内

[56] 情報通信技術を用いた外国の諜報活動に対抗する情報防衛活動

閣官房や各府省庁のそれぞれのカウンターパートにおいて平素から実務的な国際連携を実施する重層的な枠組みを強化し、同盟国・同志国との連携を強化する。「自由で開かれたインド太平洋（Free and Open Indo-Pacific: FOIP）」の実現に向けた、サイバーセキュリティ分野における米豪印やASEAN[57]等との協力についても積極的に推進する。

また、民間における情報共有に係る国際連携も拡大するとともに、国際場裡で我が国の立場を主張できる官民の人材を確保し、他国への人材派遣や国際会議への参加等を通じて育成する。加えて、我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。

(2) サイバー事案等に係る国際連携の強化

サイバー事案への迅速な対応や被害の拡大防止のため、サイバー攻撃関連情報（脆弱性情報やIoC[58]情報など）に関する平素からの国際的な情報共有を引き続き強化し、他国と共同した情報発信を検討する。CERT 間連携や国際サイバー演習への参加のみならず、我が国が国際サイバー演習等を主導して連携対処のための信頼関係を構築するとともに、情報のハブとなり、サイバーコミュニティにおける国際的なプレゼンスの向上を図る。

(3) 能力構築支援

国際的な相互依存関係が進む現在、我が国の平和と安全は我が国一国のみでは確保できない。我が国の安全保障の確保に寄与するためには、全世界的に連携してサイバーセキュリティ上の脆弱性を低減し、撲滅を目指していくことが重要である。このような観点から、世界各国におけるサイバーセキュリティの能力構築を支援することは、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の安全の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資する。

能力構築支援については、他国においても様々な支援が実施されている中、我が国の基本的な理念の下、産学官連携や外交・安全保障を含めた取組の強化を示す能力構築支援の基本方針に基づき、求められる支援を、同志国、世界銀行等の国際機関、産学といった多様な主体と連携して重層的に、かつオールジャパンで戦略的・効率的な支援を実施していく。

このようなサイバーセキュリティの確保により SDGs の達成を促進するほか、サイバーハイジーンの確保に繋げていく。また、人材育成やサイバー演習のみならず、国際法理の理解・実践、政策形成、技術基準策定や5G、IoT といった次世代のサイバー環境を形成する分野においても、能力構築支援を実施していく。加えて、海外へのサイバーセキュリティに係るビジネス展開を後押ししていく[59]。

こうした取組に加え、特にASEANを含むインド太平洋地域については、能力構築支援を中心としたこれまでの成果と経験、また、その地政学的な重要性を踏まえ、サイバー分野における外交・安全保障を含めた連携の抜本的な強化を図る。

---

[57] 東南アジア諸国連合（Association of South‐East Asian Nations）
[58] IoC (Indicator of Compromise)。サイバー攻撃の痕跡を表す情報
[59] 「インフラシステム海外展開戦略 2025」（2021 年 6 月 17 日経協インフラ戦略会議決定）

4.4.横断的施策

「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」の 3 つの政策目標を達成するためには、その基盤として、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組んでいくことが重要である。

なお、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」、「安全保障の観点からの取組強化」という 3 つの方向性を意識して、取組推進を図る。

4.4.1 研究開発の推進

サイバーセキュリティ研究分野は、脅威に関する情報やユーザ等のニーズを踏まえ、実践的な研究開発を進めることが非常に重要な分野である。一方で、実践的な研究開発を有効に進めるためには、我が国においてその基盤となる研究開発の国際競争力が確保されていることや産学官エコシステムが築かれていることが大前提である。こうした基盤づくりに向けた中長期的観点からの取組と、それを基礎とした実践的な取組の双方の視点をあわせ持って取組を進めていく。

また、研究開発の推進に当たってはデジタル技術の進展に応じた観点も重要であり、中長期的な技術トレンドを視野に入れた対応を行う。

(1) 研究開発の国際競争力の強化と産学官エコシステムの構築

サイバーセキュリティ研究分野は、様々な分野から研究者が流入すること等により、世界的に論文投稿数が急成長するとともに、国際共著・産学官連携論文などコラボレーションが活発である。今後、デジタル活用とサイバーセキュリティ対策の一体性が深くなる中、デジタル技術分野と相まって、重要な研究分野である。

我が国でもサイバーセキュリティ研究者が増えている一方、経済社会のデジタル化とそれに応じたサイバーセキュリティ対策及び技術に対する社会的要請が高まっていることから、その充実・発展・自給に向けて、中長期的観点から研究及び産学官連携を振興し、研究開発の国際競争力の強化と産学官にわたるエコシステムの構築に取り組んでいく。

具体的には、関係府省が提供する、科学的理解やイノベーションの源泉となるような研究及び産学官連携の振興施策の活用を促進し、研究コミュニティの自主的な発展努力と相まった、重点的な研究・産学官連携の強化を図る。これとあわせ、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。

産学官にわたるエコシステム構築が図られるためには、それぞれの主体の自主的な発展努力が必要不可欠であり、これらの取組状況についてフォローアップを行いながら、取組を推進していく。

(2) 実践的な研究開発の推進

サプライチェーン・リスクの増大やサイバーセキュリティ自給、AI や IoT 等の進展による新たな脅威の発生可能性など、安全保障の観点を含め我が国をとりまく現下の課題認識に基づき、我が国において、以下の方向性で、サイバーセキュリティに係る実践的な研究開発を推進していく。

① サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備

不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化を推進する。具体的には、IoT 機器等の信頼性を高度に検証するハイレベルな検証サービスの実証等を通じた包括的な検証基盤の構築や、5G に係る各構成要素におけるセキュリティを総合的かつ継続的に担保する仕組みの整備、チップの設計回路の解析や各種システム・サービスの挙動・動作の観測を通じた悪性機能を検出する技術や、セキュアな Society 5.0 の実現に向けた検証技術の研究開発及びその社会実装等を推進する。

また、これらの取組を踏まえ、国産技術の確保・育成のための取組や、政府調達における活用も視野に入れつつ、サプライチェーン全体の信頼性確保に向けた、ICT 機器・サービスのセキュリティの技術検証を行うための推進体制を、政府一体となって整備する。

② 国内産業の育成・発展に向けた支援策の推進

サイバーセキュリティ産業の育成・発展を目指し、製品・サービスを安心して利用するための有効性検証基盤や、中小企業のニーズに対応したビジネス創出など国内産業のビジネス環境を整備するとともに、シーズとニーズに係るビジネスマッチングを実施し、市場展開を促進する。

③ 攻撃把握・分析・共有基盤の強化

サイバー攻撃の巧妙化・複雑化・多様化や、IoT 機器の普及に伴う脆弱性拡大等のサイバー攻撃の脅威動向に適切に対処するため、AI 等の先端技術も活用しつつ、サイバー攻撃の観測・把握・分析技術や情報共有基盤を強化する。

具体的には、巧妙かつ複雑化したサイバー攻撃や今後本格普及する IoT 等への未知の脅威に対応するため、広域ダークネットや攻撃種別に柔軟に対応するハニーポット技術等を用いたサイバー攻撃観測技術の高度化や、AI 技術による攻撃挙動解析の自動化技術に係る研究開発を実施する。また、標的型攻撃の攻撃挙動の把握・解析やそのための迅速な対応を進めるために、サイバー攻撃誘引基盤の高度化、及びその活用の拡大を図り、標的型攻撃の具体的な挙動収集や未知の標的型攻撃等を迅速に検知・解析する技術等の研究開発を行う。加えて、脆弱な IoT 機器の確度の高い把握、及びそのセキュリティ対策のため、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンのための研究開発を行う。このほか、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築・共有する取組を推進する。

④ 暗号等の研究の推進

実用的で大規模な量子コンピュータが実現することによる既存の暗号技術の危殆化を想定しつつ、耐量子計算機暗号や量子暗号等に関する先進的な研究を推進し、安全性

を確保するための基盤を確立する。また、IoT 等のリソースの限られたデバイスにおいても、安全な通信が可能となるよう、軽量な暗号技術を確立する。

具体的には、実用的で大規模な量子コンピュータの実現や IoT 等の普及、新たな暗号技術の動向等を踏まえ、暗号技術の安全性・信頼性確保や普及促進等に関する検討を継続的に実施するとともに、耐量子計算機暗号、軽量暗号等に関するガイドラインの作成に向けた検討を行う。また、盗聴や改ざんが極めて困難な量子暗号等を活用した量子情報通信ネットワーク技術や、量子暗号通信を超小型衛星に活用するための技術の確立に向けた研究開発を推進する。

本戦略の計画期間において、これら関係府省の取組を推進するとともに、研究及び産学官連携の振興に係る関係府省の取組を含め取組状況をフォローアップし、取組のマッピング等による点検と必要な再整理を行う。あわせて、研究開発の成果の普及や社会実装を推進するとともに、その一環として政府機関における我が国発の新技術の活用に向けて、関係府省による情報交換等を促進する。

(3) 中長期的な技術トレンドを視野に入れた対応

Beyond 5G[60]をはじめとするネットワーク技術の高度化など、デジタル技術の進展に応じ、中長期的な視点から技術トレンドを捉え研究開発を推進していくことが重要である。特に、AI 技術・量子技術をはじめとする先端技術の進展を見据えた対応が求められるところ、それぞれの技術進展に関し、以下のような状況認識に基づいて、取組を推進していく。

① AI 技術の進展を見据えた対応

AI 技術は、近年、加速度的に発展しており、世界の至るところでその応用が進むことにより、広範な産業領域や社会インフラなどに大きな影響を与えている。サイバーセキュリティとの関係では、AI を活用したサイバーセキュリティ対策、AI を使ったサイバー攻撃、AI そのものを守るセキュリティの 3 つの観点があると考えられる。

まず、AI を活用したサイバーセキュリティ対策（AI for Security）に関しては、実際に AI を活用したセキュリティ製品やサービスの商用化が進んでいる。国は、AI 技術に関する総合的な戦略等に基づき、AI を活用した民間のサイバー対策を引き続き後押しするとともに、予防、検知、対処の各フェーズにおいて AI を活用した高効率かつ精緻な対策技術の確立を推進していく。

また、AI を使ったサイバー攻撃に対処する観点から、攻撃者の防御側に対する非対称性をさらに拡げないためにも、「AI for Security」の取組は重要となる。その際、攻撃の視点から知見を得て、先手を打ってセキュリティ対策を高度化するプロアクティブな研究のアプローチが重要であると考えられる。

さらに、AI そのものを守るセキュリティ（Security for AI）では、AI のセキュリティ面での脆弱性[61]がどのようなものかまだ十分に理解されていないと考えられるところ、学術面では、例えば、機械学習の誤認識を誘発し得る敵対的サンプルの生成を試

[60] 5G の特徴的機能の更なる高度化、持続可能で新たな価値の創造に資する機能の付加を指す。
[61] 脅威としては、例えば、データポイズニング攻撃（汚染された学習データを与えることにより、判断を誤らせる攻撃）などが考えられる。

みる研究や、一方でその防御に関する研究も海外では多くなっている。我が国においても基礎的な研究を振興するとともに、5～10 年先に実現を目指す長期的取組として、引き続き技術課題の検討を進めていく。

② 量子技術の進展を見据えた対応

量子コンピュータの進展により、現代のインターネットセキュリティを支える公開鍵暗号技術が解読される可能性が生じ、国際的に耐量子計算機暗号に関する検討が進められている。我が国においても、耐量子計算機暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立することとしている。

一方、耐量子計算機暗号においても危殆化のリスクがあるため、各国が安全保障にも関わる重大脅威との認識の下、原理的に安全性が確保される量子通信・暗号に関する研究開発を急速に進めている。我が国としても、量子技術に関する総合的な戦略に基づき、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要な情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発や、その事業化・標準化等に取り組んでいく。

以上のほか、Beyond 5G をはじめとした様々な技術トレンドを中長期的な視点から捉え、国として推進すべき技術課題の検討を不断に行っていく。

4.4.2 人材の確保、育成、活躍促進

サイバー攻撃が複雑化・巧妙化する中、企業が事業継続を確固なものとしつつ、新たな価値を創出していくためには、サイバーセキュリティ確保に向けた人材の育成・確保が不可欠である。我が国におけるサイバーセキュリティ人材の不足が指摘されて久しいが、一方で、実務者層・技術者層の育成に向けては、資格・試験や演習、学び直しの促進等の官民の取組も進展している。こうした現状認識やデジタル化に向けた取組の広がりを踏まえれば、「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要である。

また、デジタル化がそれに応じた脅威への対処と併せて推進されていくためには、サイバーセキュリティに係る人材が、男女等を問わず多様な視点や優れた発想で幅広く活躍できる環境をつくり、次代を担う優秀な人材を引きつけられる好循環を生むことが重要である。このため、環境変化に対応して以下の政策目的に適った取組の重点化を図るとともに、優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境整備に取り組んでいく。

(1) 「DX with Cybersecurity」に必要な人材に係る環境整備

デジタル化の進展と併せてサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が社会全体で実現されるためには、企業・組織内でのデジタル化進展に伴い新たに必要となるセキュリティを含む人材・仕事の需要の増加と、若年層や社会的要請に応じた人材流入や適切なマッチング等による人材・仕事の供給の増加が、双方とも連関して好循環を形成することが重要である。

実務者層・技術者層向けの人材育成プログラムの「質」・「量」の確保はもちろん、企業・組織内での機能構築、人材の流動性・マッチングの観点から、セキュリティ人材が活躍できるような環境整備が図られなければ、悪循環に陥り、経済社会のデジタル化推進は不確実性をはらむものとなり得る。

加えて、そのためには、経営層はもちろん、企業・組織内でデジタルトランスフォーメーションを推進したり関与したりする様々な者において、デジタル化とサイバーセキュリティ対策は他人事ではなく、同時達成されるべき、業務と収益の中核を支える基本的事項として認識されることがその前提となる。経営層の意識改革に取り組みつつ、必要な素養や基本的知識が補充できる環境整備が重要となる。

① 「プラス・セキュリティ」知識を補充できる環境整備

経営層や、特に企業・組織内で DX を推進するマネジメントに関わる人材層をはじめとして、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要である。同時に、経営層の方針を踏まえた対策を立案し実務者・技術者を指導できる人材の確保に向けた取組も重要であり、これらの取組により「戦略マネジメント層」の充実を図る。

しかしながら、IT リテラシーや「プラス・セキュリティ」知識に係る研修・セミナー等の人材育成プログラムは、社会的に必ずしも普及していないと考えられる。このため、環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指していく。

需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内において、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む）が、今後デジタル化に様々に関わるために IT リテラシーや「プラス・セキュリティ」知識を補充しなければならない必要性は増しており、潜在的な大きな需要が存在すると考えられる。このため、様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行われることや、職員研修等の機会が提供されることが重要であり、こうした需要の顕在化に繋がる取組を企業・組織等に促す普及啓発を、国や関係機関・団体が先導して行う。

また、国や人材育成プログラム等を提供する関係機関・企業・教育機関等が、先導的・基盤的なプログラム提供を図ることに加え、趣旨に適うプログラムを一覧化したポータルサイト等を通じて官民の取組の積極的な発信を行うなど、企業・組織の需要者からみて供給側の一定の質が確保・期待される仕組みの構築を図る。これとあわせ、対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。

② 企業・組織内での機能構築、人材の流動性・マッチングに関する取組

今後、業務等のデジタル化、製品等のネットワーク接続、デジタルサービスの開発や他のサービスとの連携などが増加する中で、迅速で柔軟な開発・対処、新たなリスクに対応した監視・対処のプラクティスが必要となる。特に、前者の実践に当たっては「セキュリティ・バイ・デザイン」の考え方の重要性も一層増し、企画部門や開発運

用部門と企業・組織内のセキュリティ機能との連携・協働が一層重要となると考えられる。一方で、こうした機能の構築や普及に向けては、必ずしも参照できる導入事例や人材の蓄積が十分とは言えないのも事実である。

また、人材の活躍の場という観点では、コロナ禍への対応の結果として雇用環境の変化や労働時間管理のあり方の明確化等を踏まえ、兼業・副業といった柔軟な雇用形態の活用の機会が今後増していくと考えられる。また、デジタル改革の動きを踏まえ、国の機関のみならず、地方自治体を含め、行政分野における業務改革を含むデジタル化関連業務における人材需要が今後増していくと考えられる。社会全体で「DX with Cybersecurity」を推進していくためには、働き方や雇用形態の多様化、デジタル改革の推進を機会としてIT・セキュリティ人材の流動性・マッチング機会の促進が図られるための環境整備が必要である。

したがって、これらの動向や人材の偏在等を考慮しつつ、企業・組織内での機能構築やIT・セキュリティ人材の確保・育成に関するプラクティス実践の促進に向け、人材ニーズに係る実態把握とあわせ、実際のインシデントを踏まえた普及啓発や、参考となる手引き資料の活用促進、企業・組織内での機能構築や人材の活躍等の先進事例の収集・整備、ポータルサイト等を通じた積極的な発信、学び直しの機会の提供に取り組む。

また、特に地域・中小企業においてセキュリティ人材の不足が顕著であるところ、地域における「共助」の取組や、産業界と教育機関との連携促進・エコシステム構築を通じ、プラクティスの実践に当たって参考となるノウハウやネットワークの提供を行う。

(2) 巧妙化・複雑化する脅威への対処

巧妙化・複雑化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大、制御系システムを対象とする攻撃等もみられる中で、実践的な対処能力を持つ人材育成の重要性は一層増している。

実務者層・技術者層の育成に向けては、資格制度の整備・改善、若年層向けのプログラムや制御系システムに携わる実務者を対象とするプログラムの実施、演習環境の提供、学び直しの促進など、官民で取組の推進が行われてきているところ、近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく。

また、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう、講師の質の担保等に留意しつつ、産学に開放する。

なお、こうした人材の活躍促進やマッチング促進の観点から、多様な人材の活躍等の先進事例の発信、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にも併せて取り組む。

(3) 政府機関における取組

IT・セキュリティ人材の活躍促進の観点からも、優秀な人材が、各府省庁、地方公共団体、民間企業、独立行政法人を行き来しながらキャリアを積める環境の整備が重要である[62]。この考え方を踏まえ、外部の高度専門人材を活用する仕組みの強化や、新たに創設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向けた方針に基づき、政府機関全体で取組を強化していく。

また、当該方針に基づき各府省庁において人材確保・育成計画を作成し、「サイバーセキュリティ・情報化審議官」等による司令塔機能の下、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保についても着実に取り組むとともに、毎年度計画のフォローアップを行い、一層の取組の強化を図る。

特に、高度なサイバー犯罪や安全保障への対応等を行うため、外部の高度専門人材を活用するだけでなく、政府機関等内部においても独自に高度専門人材を育成・確保する。

4.4.3 全員参加による協働、普及啓発

サイバー空間と実空間の一体化の進展、サイバー攻撃の巧妙化・複雑化の中で、実空間における防犯対策や交通安全対策と同様に、サイバー空間における公衆衛生活動として、国民一人ひとりがサイバーセキュリティに対する意識・理解を醸成し、基本的な取組を平時から行い、様々なリスクに対処できることが不可欠である。リテラシーを身に付け、自らの判断で脅威から身を守れるよう、官民が一体となって行動強化に繋げるための普及啓発・情報発信に取り組むことが重要である。

また、様々な関係者がお互いの役割分担の下で連携・協働することが何より重要である。国は、地域、企業、学校など様々なコミュニティの自主的な活動を尊重しつつ、各々の関係者が、お互いの役割分担の下で、連携・協働をできるような仕組みを構築し、その仕組みを下支えしていく役割を担う。

こうした認識の下で、普及啓発に向け産学官民の関係者が円滑かつ効果的に活動できるよう、「全員参加による協働」に向けた具体的なアクションプランを策定し、地域・中小・若年層を重点対象として、取組推進を行ってきた。本戦略では「Cybersecurity for All」という考え方を示しているが、これは「全員」が自らの役割を主体的に自覚しサイバーセキュリティに取り組む、という考え方を含んでいる。今後、デジタル改革の推進により、サイバー空間に参加する層が広がることが予想される中で、当該アクションプランを着実に推進することはもちろん、取組状況をフォローアップし、継続的な改善に取り組んでいくことが求められる。また、高齢者への対応を含め、当該アクションプランの見直しを検討する。

加えて、特に、テレワークの増加やクラウドサービスの普及等の近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料等の整備が進められている。これらも含め、情報発信・普及啓発のあり方（コンテンツ）についても、必要な対応を実施する。

---

[62] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）にも示されている。

5. 推進体制

本戦略においては、政府において進められているデジタル改革と一体となったサイバーセキュリティの確保が求められている[63]。また、サイバーセキュリティの確保を通じて、我が国の安全保障を万全のものとする[64]ことは、従来からの我が国政府の方針である。

我が国のサイバーセキュリティ政策により、「自由、公正かつ安全なサイバー空間」を確保するためには、政府一体となった推進体制が必要である。サイバーセキュリティ戦略本部（以下「本部」という。）は、本戦略に基づく取組が、デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを有効活用しつつその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。その中で、内閣サイバーセキュリティセンターは、本部の事務局として、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。

本部は、新たに設置されたデジタル庁と、整備基本方針作成等における緊密連携を図る[65]。また、危機管理対応についても一層の強化を図ることが必要である。本部は、必要に応じて、重大テロ対策本部など危機管理体制と情報共有・連携する。さらに、安全保障に関わる問題については、国家安全保障会議との緊密な連携により対応し、内閣官房国家安全保障局による全体取りまとめの下、関係府省庁が連携して対応する。

本部は、変化するサイバーセキュリティリスクに対応して各主体に期待される具体的な対策に繋がるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、各府省庁と連携して、本戦略を国内外の関係者に積極的に発信する。

また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が着実かつ効果的に実施されるよう、経費の見積り方針を定め、政府としての必要な予算の確保と執行を図る。さらに、情報収集・分析機能に加え、サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能の強化のため、所要の体制について検討する。本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。

今後、本部は、本戦略を的確に実施するため、3年間の計画期間内において、各年度の年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映する。年次計画と年次報告は一体的に検討を行い、本戦略に基づく前年度の取組実績、評価及び次年度の取組を、本戦略の事項に沿って、報告と計画について一連の流れを示すように整理する。

63 「デジタル社会の実現に向けた重点計画」（2021年6月18日閣議決定）

64 「国家安全保障戦略」（2013年12月17日国家安全保障会議決定・閣議決定）は、「情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠」としている。

65 デジタル庁設置法（令和3年法律第36号）附則第43条により、サイバーセキュリティ戦略本部員にデジタル大臣が加えられた。

別紙

担当府省庁一覧

項目	担当府省庁 （◎：主担当、○：関係府省庁）
4.1. 経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity の推進～	
4.1.1 経営層の意識改革	◎：NISC[66]、総務省、経済産業省 ○：金融庁
4.1.2 地域・中小企業における DX with Cybersecurity の推進	◎：NISC、総務省、経済産業省
4.1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	
(1) サプライチェーンの信頼性確保	◎：総務省、経済産業省 ○：その他の府省庁
(2) データ流通の信頼性確保	◎：デジタル庁、総務省、経済産業省 ○：法務省
(3) セキュリティ製品・サービスの信頼性確保	◎：経済産業省 ○：NISC、総務省
(4) 先端技術・イノベーションの社会実装	◎：NISC、内閣府、総務省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
4.1.4 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	◎：NISC、総務省、文部科学省 ○：デジタル庁、経済産業省
4.2. 国民が安全で安心して暮らせるデジタル社会の実現	
4.2.1 国民・社会を守るためのサイバーセキュリティ環境の提供	◎：内閣官房、警察庁、総務省、経済産業省 ○：外務省、財務省、防衛省、その他の府省庁 ※内閣官房：国家安全保障局
(1) 安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、金融庁、消費者庁、デジタル庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、内閣府、宮内庁、警察庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：小型無人機等対策推進室、 ※内閣府（◎）：政策統括官（科学技術・イノベーション担当） ※内閣官房（○）：内閣官房副長官補（事態対処・危機管理担当）、内閣総務官室、内閣情報調査室、成長戦略会議事務局 ※内閣府（○）：地方創生推進事務局
(2) 新たなサイバーセキュリティの担い手との協調	◎：NISC、デジタル庁、総務省、経済産業省
(3) サイバー犯罪への対策	◎：内閣府、警察庁、総務省、法務省、経済産業省 ※内閣府：個人情報保護委員会

[66] National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015 年 1 月 9 日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。

(4) 包括的なサイバー防御の展開	◎：NISC、内閣官房、警察庁、総務省、外務省、経済産業省、防衛省 ※内閣官房：国家安全保障局、内閣情報調査室
(5) サイバー空間の信頼性確保に向けた取組	◎：NISC、内閣官房、内閣府、金融庁、総務省、文部科学省、厚生労働省、経済産業省、国土交通省 ※内閣官房：国家安全保障局 ※内閣府：個人情報保護委員会
4.2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	◎：NISC、内閣府、デジタル庁、総務省、厚生労働省、経済産業省 ※内閣府：番号制度担当室
4.2.3 経済社会基盤を支える各主体における取組①（政府機関等）	◎：NISC、デジタル庁、総務省、厚生労働省、経済産業省 ○：人事院、内閣府、消費者庁、外務省、財務省、文部科学省、農林水産省、国土交通省、環境省、防衛省
4.2.4 経済社会基盤を支える各主体における取組②（重要インフラ）	
(1) 官民連携に基づく重要インフラ防護の推進	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：警察庁
(2) 地方公共団体に対する支援	◎：NISC、内閣府、総務省 ○：デジタル庁厚生労働省 ※内閣府：個人情報保護委員会、番号制度担当室
4.2.5 経済社会基盤を支える各主体における取組③（大学・教育研究機関等）	◎：文部科学省 ○：NISC
4.2.6 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	◎：NISC、内閣官房、警察庁、法務省 ※内閣官房：東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局
(1) 分野・課題ごとに応じた情報共有・連携の推進	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省
(2) 包括的なサイバー防御に資する情報共有・連携体制の整備	◎：NISC、内閣官房、警察庁、総務省、外務省、経済産業省、防衛省 ※内閣官房：国家安全保障局、内閣情報調査室
4.2.7 大規模サイバー攻撃事態等への対処態勢の強化	◎：NISC、内閣官房、内閣府、警察庁、金融庁、経済産業省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当） ※内閣府：個人情報保護委員会
4.3. 国際社会の平和・安定及び我が国の安全保障への寄与	
4.3.1 「自由、公正かつ安全なサイバー空間」の確保	
(1) サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省
(2) サイバー空間におけるルール形成	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省
4.3.2 我が国の防御力・抑止力・状況把握力の強化	◎：内閣官房、防衛省 ○：警察庁、外務省、財務省、経済産業省 ※内閣官房：国家安全保障局
(1) サイバー攻撃に対する防御力の向上	◎：NISC、内閣官房、警察庁、法務省、外務省、文部科学省、防衛省 ○：内閣府、総務省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省 ※内閣官房：内閣情報調査室

(2) サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省、その他の府省庁 ※内閣官房：国家安全保障局
(3) サイバー空間の状況把握の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：総務省、外務省※内閣官房：内閣情報調査室
4.3.3 国際協力・連携	
(1) 知見の共有・政策調整	◎：NISC、警察庁、総務省、法務省、外務省、経済産業省、防衛省 ○：その他の府省庁
(2) サイバー事案等に係る国際連携の強化	◎：NISC、経済産業省、防衛省 ○：警察庁、外務省
(3) 能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省 ○：法務省
4.4. 横断的施策	
4.4.1 研究開発の推進	
(1) 研究開発の国際競争力の強化と産学官エコシステムの構築	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(2) 実践的な研究開発の推進	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ○：その他の府省庁 ※内閣府：政策統括官（科学技術・イノベーション担当）
(3) 中長期的な技術トレンドを視野に入れた対応	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
4.4.2 人材の確保・育成・活躍促進	◎：警察庁、文部科学省、厚生労働省
(1) 「DX with Cybersecurity」に必要な人材に係る環境整備	◎：NISC、総務省、経済産業省 ○：厚生労働省、文部科学省
(2) 巧妙化・複雑化する脅威への対処	◎：NISC、総務省、文部科学省、経済産業省 ○：その他の府省庁
(3) 政府機関における取組	◎：NISC、警察庁、総務省、防衛省 ○：その他の府省庁
4.4.3 全員参加による協働、普及啓発	◎：NISC、総務省、経済産業省 ○：その他の府省庁
5.推進体制	◎：NISC、内閣官房 ○：警察庁、金融庁、総務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、国土交通省、防衛省、その他の府省庁 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、国家安全保障局

サイバーセキュリティ戦略の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurity の推進

3．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

4．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

国民が安全で安心して暮らせるデジタル社会の実現

1．国民・社会を守るためのサイバーセキュリティ環境の提供

2．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

3・4・5．経済社会基盤を支える各主体における取組
①(政府機関等)
②(重要インフラ)
③(大学・教育研究機関等)

6．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

7．大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

1．「自由、公正かつ安全なサイバー空間」の確保

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　人材の確保・育成・活躍促進　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

３　根拠法令等

サイバーセキュリティ基本法

（平成二十六年十一月十二日法律第百四号）
最終改正：令和四年六月一七日法律第六十八号

目次

第一章　総則

（目的）

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法（令和三年法律第三十五号）第二条に規定する情報通信技術（以下「情報通信技術」という。）の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

（定義）

第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（基本理念）

第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、

重要社会基盤事業者（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に関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

2　サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。

3　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨として、行われなければならない。

4　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。

5　サイバーセキュリティに関する施策の推進は、デジタル社会形成基本法の基本理念に配慮して行われなければならない。

6　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。

（国の責務）

第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。

（地方公共団体の責務）

第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

（重要社会基盤事業者の責務）

第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（サイバー関連事業者その他の事業者の責務）

第七条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（教育研究機関の責務）

第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリ

ティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（国民の努力）

第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

（法制上の措置等）

第十条　政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない。

（行政組織の整備等）

第十一条　国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。

第二章　サイバーセキュリティ戦略

第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。

２　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。

一　サイバーセキュリティに関する施策についての基本的な方針

二　国の行政機関等におけるサイバーセキュリティの確保に関する事項

三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項

３　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。

４　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。

５　前二項の規定は、サイバーセキュリティ戦略の変更について準用する。

６　政府は、サイバーセキュリティ戦略について、その実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない。

第三章　基本的施策

（国の行政機関等におけるサイバーセキュリティの確保）

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、

かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十三条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

（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促進）

第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

（民間事業者及び教育研究機関等の自発的な取組の促進）

第十五条　国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

２　国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

（多様な主体の連携等）

第十六条　国は、関係行政機関相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする。

（サイバーセキュリティ協議会）

第十七条　第二十八条第一項に規定するサイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣（次項において「本部長等」という。）は、サイバーセキュリティに関する施策の推進に関し必要な協議を行うため、サイバーセキュリティ協議会（以下この条において「協議会」という。）を組織するものとする。

２　本部長等は、必要と認めるときは、協議して、協議会に、次に掲げる者を構成員として加えることができる。

一　国の関係行政機関の長（本部長等を除く。）

二　地方公共団体又はその組織する団体

三　重要社会基盤事業者又はその組織する団体
四　サイバー関連事業者又はその組織する団体
五　大学その他の教育研究機関又はその組織する団体
六　その他本部長等が必要と認める者

3　協議会は、第一項の協議を行うため必要があると認めるときは、その構成員に対し、サイバーセキュリティに関する施策の推進に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない。

4　協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない。

5　協議会の庶務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。

6　前各項に定めるもののほか、協議会の組織及び運営に関し必要な事項は、協議会が定める。

（犯罪の取締り及び被害の拡大の防止）

第十八条　国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする。

（我が国の安全に重大な影響を及ぼすおそれのある事象への対応）

第十九条　国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする。

（産業の振興及び国際競争力の強化）

第二十条　国は、サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため、サイバーセキュリティに関し、先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化及び新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。

（研究開発の推進等）

第二十一条　国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。

（人材の確保等）

第二十二条　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講

ずるものとする。
2　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。

（教育及び学習の振興、普及啓発等）
第二十三条　国は、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるものとする。
2　国は、前項の施策の推進に資するよう、サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策を講ずるものとする。

（国際協力の推進等）
第二十四条　国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し、国際的な規範の策定への主体的な参画、国際間における信頼関係の構築及び情報の共有の推進、開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力、犯罪の取締りその他の国際協力を推進するとともに、我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策を講ずるものとする。

第四章　サイバーセキュリティ戦略本部

（設置）
第二十五条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。

（所掌事務等）
第二十六条　本部は、次に掲げる事務をつかさどる。
一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。
二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）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。
三　国の行政機関、独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること。
四　サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整に関すること。
五　前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。
2　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、国家安全保障会議の意見を聴かなければならない。
3　本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国

家安全保障会議との緊密な連携を図るものとする。

（組織）

第二十七条　本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

（サイバーセキュリティ戦略本部長）

第二十八条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。

２　本部長は、本部の事務を総括し、所部の職員を指揮監督する。

３　本部長は、第二十六条第一項第二号、第三号及び第五号に規定する評価又は第三十二条若しくは第三十三条の規定により提供された資料、情報等に基づき、必要があると認めるときは、関係行政機関の長に対し、勧告することができる。

４　本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、その勧告に基づいてとった措置について報告を求めることができる。

５　本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、内閣総理大臣に対し、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう意見を具申することができる。

（サイバーセキュリティ戦略副本部長）

第二十九条　本部に、サイバーセキュリティ戦略副本部長（以下「副本部長」という。）を置き、国務大臣をもって充てる。

２　副本部長は、本部長の職務を助ける。

（サイバーセキュリティ戦略本部員）

第三十条　本部に、サイバーセキュリティ戦略本部員（次項において「本部員」という。）を置く。

２　本部員は、次に掲げる者（第一号から第六号までに掲げる者にあっては、副本部長に充てられたものを除く。）をもって充てる。

一　国家公安委員会委員長

二　デジタル大臣

三　総務大臣

四　外務大臣

五　経済産業大臣

六　防衛大臣

七　前各号に掲げる者のほか、本部長及び副本部長以外の国務大臣のうちから、本部の所掌事務を遂行するために特に必要があると認める者として内閣総理大臣が指定する者

八　サイバーセキュリティに関し優れた識見を有する者のうちから、内閣総理大臣が任命する者

（事務の委託）

第三十一条　本部は、次の各号に掲げる事務の区分に応じて、当該事務の一部を当該各号に定める者に委託することができる。

一　第二十六条第一項第二号に掲げる事務（独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準に基づく監査に係るものに限る。）又は同項第三号

に掲げる事務（独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象の原因究明のための調査に係るものに限る。）　独立行政法人情報処理推進機構その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人

二　第二十六条第一項第四号に掲げる事務　サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人

2　前項の規定により事務の委託を受けた法人の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない。

3　第一項の規定により事務の委託を受けた法人の役員又は職員であって当該委託に係る事務に従事するものは、刑法（明治四十年法律第四十五号）その他の罰則の適用については、法令により公務に従事する職員とみなす。

（資料提供等）

第三十二条　関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない。

2　前項に定めるもののほか、関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。

（資料の提出その他の協力）

第三十三条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長又は理事長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の理事長、特殊法人及び認可法人であって本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該求めを受けた者は、正当な理由がある場合を除き、その求めに応じなければならない。

2　本部は、その所掌事務を遂行するため特に必要があると認めるときは、前項に規定する者以外の者に対しても、同項の協力を依頼することができる。

（地方公共団体への協力）

第三十四条　地方公共団体は、第五条に規定する施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を求めることができる。

2　本部は、前項の規定による協力を求められたときは、その求めに応じるよう努めるものとする。

（事務）
第三十五条　本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。

（主任の大臣）
第三十六条　本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣とする。

（政令への委任）
第三十七条　この法律に定めるもののほか、本部に関し必要な事項は、政令で定める。

第五章　罰則

第三十八条　第十七条第四項又は第三十一条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

附　則

（施行期日）
第一条　この法律は、公布の日から施行する。ただし、第二章及び第四章の規定並びに附則第四条の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

（検討）
第二条　政府は、武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（平成十五年法律第七十九号）第二十一条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、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等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする。

附　則　（平成二七年九月一一日法律第六六号）　抄

（施行期日）
第一条　この法律は、平成二十八年四月一日から施行する。

附　則　（平成二七年九月三〇日法律第七六号）　抄

（施行期日）
第一条　この法律は、公布の日から起算して六月を超えない範囲内において政令で定める日から施行する。

附　則　（平成二八年四月二二日法律第三一号）　抄

（施行期日）
第一条　この法律は、公布の日から起算して六月を超えない範囲内において政令で定める日から施行する。ただし、次条並びに附則第三条、第五条及び第六条の規定は、公布の日から施行する。

（政令への委任）

第六条　附則第二条から前条までに定めるもののほか、この法律の施行に関して必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

附　則　（平成三〇年一二月一二日法律第九一号）　抄

（施行期日）

１　この法律は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

附　則　（令和元年五月二四日法律第一一号）　抄

（施行期日）

第一条　この法律は、平成三十二年四月一日から施行する。ただし、第二条中国立大学法人法附則に一条を加える改正規定、第四条中独立行政法人大学改革支援・学位授与機構法第三条の改正規定及び同法第十六条第一項の改正規定並びに次条並びに附則第四条第三項及び第四項、第九条、第十一条並びに第十二条の規定は、公布の日から施行する。

附　則　（令和三年五月一九日法律第三五号）　抄

（施行期日）

第一条　この法律は、令和三年九月一日から施行する。

附　則　（令和三年五月一九日法律第三六号）　抄

（施行期日）

第一条　この法律は、令和三年九月一日から施行する。ただし、附則第六十条の規定は、公布の日から施行する。

第五十七条　この法律の施行前にこの法律による改正前のそれぞれの法律（これに基づく命令を含む。以下この条及び次条において「旧法令」という。）の規定により従前の国の機関がした認定等の処分その他の行為は、法令に別段の定めがあるもののほか、この法律の施行後は、この法律による改正後のそれぞれの法律（これに基づく命令を含む。以下この条及び次条において「新法令」という。）の相当規定により相当の国の機関がした認定等の処分その他の行為とみなす。

２　この法律の施行の際現に旧法令の規定により従前の国の機関に対してされている申請、届出その他の行為は、法令に別段の定めがあるもののほか、この法律の施行後は、新法令の相当規定により相当の国の機関に対してされた申請、届出その他の行為とみなす。

３　この法律の施行前に旧法令の規定により従前の国の機関に対して申請、届出その他の手続をしなければならない事項で、この法律の施行の日前に従前の国の機関に対してその手続がされていないものについては、法令に別段の定めがあるもののほか、この法律の施行後は、これを、新法令の相当規定により相当の国の機関に対してその手続がされていないものとみなして、新法令の規定を適用する。

（命令の効力に関する経過措置）

第五十八条　旧法令の規定により発せられた内閣府設置法第七条第三項の内閣府令又は国家行政組織法第十二条第一項の省令は、法令に別段の定めがあるもののほか、この法律の施行後は、新法令の相当規定に基づいて発せられた相当の第七条第三項のデジタル庁令又は国家行政組織法第十二条第一項の省令としての効力を有するものとする。

（罰則の適用に関する経過措置）

第五十九条　この法律の施行前にした行為に対する罰則の適用については、なお従前の例による。

（政令への委任）

第六十条　附則第十五条、第十六条、第五十一条及び前三条に定めるもののほか、この法律の施行に関し必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

附　則　（令和四年六月一七日法律第六八号）　抄

（施行期日）

1　この法律は、刑法等一部改正法施行日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　第五百九条の規定　公布の日

サイバーセキュリティ基本法施行令

（平成二十六年十二月十九日政令第四百号）
最終改正：令和三年七月二日政令第一九五号

内閣は、サイバーセキュリティ基本法（平成二十六年法律第百四号）第三十五条の規定に基づき、この政令を制定する。

（国務大臣以外の本部員の定数等）

第一条　サイバーセキュリティ戦略本部員（以下「本部員」という。）のうち、サイバーセキュリティ基本法（第五条において「法」という。）第三十条第二項第八号に掲げる本部員の定数は、十人以内とする。

２　前項の本部員の任期は、二年とする。ただし、補欠の本部員の任期は、前任者の残任期間とする。

３　第一項の本部員は、再任されることができる。

４　第一項の本部員は、非常勤とする。

（専門調査会）

第二条　サイバーセキュリティ戦略本部（第四条において「本部」という。）は、専門の事項を調査させるため必要があるときは、その議決により、専門調査会を置くことができる。

２　専門調査会の委員は、当該専門の事項に関し学識経験を有する者のうちから、内閣総理大臣が任命する。

３　専門調査会の委員は、非常勤とする。

４　専門調査会は、その設置に係る調査が終了したときは、廃止されるものとする。

（専門調査会に属する本部員）

第三条　サイバーセキュリティ戦略本部長（次条において「本部長」という。）は、必要があると認める場合は、専門調査会に属すべき者として本部員を指名することができる。

（本部の運営）

第四条　この政令に定めるもののほか、本部の運営に関し必要な事項は、本部長が本部に諮って定める。

（法第三十一条第一項第二号の政令で定める法人）

第五条　法第三十一条第一項第二号の政令で定める法人は、一般社団法人ＪＰＣＥＲＴコーディネーションセンター（平成十五年三月十八日に有限責任中間法人ＪＰＣＥＲＴコーディネーションセンターという名称で設立された法人をいう。）とする。

附　則

この政令は、サイバーセキュリティ基本法附則第一条ただし書に規定する規定の施行の日（平成二十七年一月九日）から施行する。

附　則　（平成三一年三月一三日政令第三七号）

この政令は、サイバーセキュリティ基本法の一部を改正する法律の施行の日（平成三十一年四月一日）から施行する。

附　則　（令和三年七月二日政令第一九五号）　抄

（施行期日）

第一条　この政令は、令和三年九月一日から施行する。

重要インフラ専門調査会の設置について

（平成２７年２月１０日
サイバーセキュリティ戦略本部決定）
平成３１年４月１日
一部改定

１．サイバーセキュリティ基本法施行令（平成26年政令第400号）第２条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。

２．専門調査会の委員は、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について優れた見識を有する者のうちから、内閣総理大臣が任命する者（当該委員がサイバーセキュリティ戦略本部員の場合にあっては、サイバーセキュリティ戦略本部長が指名する者）とする。

３．専門調査会の会長は、その委員の互選により決する。

４．専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して意見を述べることを求めることができる。

５．専門調査会の会長は、必要があると認めるときは、専門調査会の下にワーキンググループを置くことができる。

６．専門調査会の委員の任期は、任命又は指名の日から２年以内とする。ただし、再任又は再指名を妨げない。

７．専門調査会の庶務は、関係省庁の協力を得て、内閣官房において処理する。

８．前各項に掲げるもののほか、専門調査会の運営に関する事項その他必要な事項は会長が定める。

９．「重要インフラ専門委員会」（平成17年９月15日情報セキュリティ政策会議決定）が決定した事項及び検討した事項等については、専門調査会に引き継がれるものとする。

サイバーセキュリティ戦略本部資料提供等規則

（平成２７年２月１０日
サイバーセキュリティ戦略本部決定）

平成２８年１０月１２日
一部改定
平成３１年４月１日
一部改定

サイバーセキュリティ基本法（平成26年法律第104号。以下「法」という。）第32条及び第33条の規定に基づき、並びに当該規定による事務を適切に遂行するため、当該事務等について、次のとおり定める。

（提供しなければならない資料等）

第１条　法第32条第１項の規定に基づき関係行政機関の長がサイバーセキュリティ戦略本部（以下「本部」という。）に対して提供しなければならない資料又は情報は、次に掲げる事項に関するものとする。

一　当該行政機関又は当該行政機関が所管する独立行政法人若しくは法第13条に規定する指定法人において発生したサイバーセキュリティに関する事象に関する事項のうち、サイバーセキュリティ戦略本部重大事象施策評価規則（平成27年２月10日サイバーセキュリティ戦略本部決定）第１条に規定する特定重大事象に該当する事象に関する重要なものその他我が国のサイバーセキュリティの向上に資するもの

二　当該行政機関が所管する法第12条第2項第3号に規定する重要社会基盤事業者等において発生したサイバーセキュリティに関する事象に関する事項のうち、重要社会基盤事業者等のサービスの安定的かつ適切な提供に著しい支障を及ぼし、又は及ぼすおそれがある事象に関する重要なものその他我が国のサイバーセキュリティの向上に資するもの

三　二に掲げるもののほか、サイバーセキュリティに関する事項であって、本部の所掌事務の遂行に資すると当該行政機関の長が認めるもの

２　前項各号に掲げる事項の詳細その他法第32条第１項の規定の実施に必要な細目的事項については、内閣サイバーセキュリティセンターが関係行政機関に通知するものとする。

（特殊法人等の指定）

第２条　法第33条第１項の本部が指定する特殊法人及び認可法人は、別表のとおりとする。

（関係事務の処理等）

第３条　法第32条及び第33条の規定による事務は、内閣サイバーセキュリティセンターに行わせるものとする。

２　法第32条又は第33条の規定により提供された資料、情報等に基づき法第28条第３項の規定による勧告を行う場合において、当該勧告及び同条第４項の規定による報告の求めに関する事務は、内閣サイバーセキュリティセンターに行わせるものとする。

別表

沖縄振興開発金融公庫
沖縄科学技術大学院大学学園
株式会社地域経済活性化支援機構
原子力損害賠償・廃炉等支援機構
銀行等保有株式取得機構
預金保険機構
株式会社東日本大震災事業者再生支援機構
地方公共団体情報システム機構
地方公務員共済組合連合会
地方職員共済組合
都職員共済組合
全国市町村職員共済組合連合会
日本放送協会
日本電信電話株式会社
東日本電信電話株式会社
西日本電信電話株式会社
日本郵政株式会社
日本郵便株式会社
日本たばこ産業株式会社
株式会社日本政策金融公庫
株式会社日本政策投資銀行
輸出入・港湾関連情報処理センター株式会社
株式会社国際協力銀行
日本銀行
国家公務員共済組合連合会
公立学校共済組合
日本私立学校振興・共済事業団
放送大学学園
日本年金機構
日本赤十字社
健康保険組合連合会
全国健康保険協会
国民年金基金連合会
日本中央競馬会
農水産業協同組合貯金保険機構
株式会社商工組合中央金庫

日本アルコール産業株式会社
株式会社産業革新機構
株式会社海外需要開拓支援機構
北海道旅客鉄道株式会社
四国旅客鉄道株式会社
日本貨物鉄道株式会社
東京地下鉄株式会社
成田国際空港株式会社
東日本高速道路株式会社
中日本高速道路株式会社
西日本高速道路株式会社
首都高速道路株式会社
阪神高速道路株式会社
本州四国連絡高速道路株式会社
新関西国際空港株式会社
中間貯蔵・環境安全事業株式会社

サイバーセキュリティ協議会規約

平成 31 年 4 月 1 日制定
令和元年 9 月 6 日一部改正
令和 2 年 3 月 6 日一部改正
令和 3 年 9 月 1 日一部改正
令和 4 年 1 月 20 日一部改正
令和 4 年 3 月 22 日一部改正
令和 5 年 4 月 28 日一部改正

第 1 章　総論

第 1 条　サイバーセキュリティ基本法（平成 26 年法律第 104 号、以下「法」という。）第 17 条第 1 項の規定に基づき、サイバーセキュリティ協議会を組織する。

（定義）
第 2 条　本規約において使用される用語の定義は、次のとおりとする。
一　協議会　法第 17 条第 1 項に規定するサイバーセキュリティ協議会
二　本部長等　法第 28 条第 1 項に規定するサイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣
三　加入構成員　法第 17 条第 2 項及び本規約第 6 条の規定に基づき加えられた構成員
四　構成員　本部長等たる構成員及び加入構成員
四の二　非構成員　構成員、事務局、NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）並びにその受託者（再受託者を含む。以下同じ。）以外の者
五　協議会事務従事者　法第 17 条第 4 項にいう協議会の事務に従事する者（従事する可能性がある者を含む。）
五の二　登録事務従事者　協議会事務従事者のうち、第 6 条第 7 項若しくは第 9 項（第 13 条に基づき準用する場合を含む。）又は第 22 条第 2 項若しくは第 24 条第 5 項の規定による登録を受ける者
六　NISC　内閣官房内閣サイバーセキュリティセンター
七　JPCERT/CC　一般社団法人 JPCERT コーディネーションセンター
八　重要社会基盤事業者　法第 3 条第 1 項に規定する重要社会基盤事業者（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に関する事業を行う者）
九　サイバー関連事業者　法第 7 条に規定するサイバー関連事業者（インターネットそ

の他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者）

十　政令指定法人 JPCERT/CC　法第 31 条第 1 項第 2 号及びサイバーセキュリティ基本法施行令（平成 26 年政令第 400 号）第 5 条に基づき事務の委託を受けた法人としての JPCERT/CC

十一　GSOC　国の関係行政機関等におけるサイバーセキュリティ対策について政府横断的な立場から推進するため、NISC に設置された国の関係行政機関等に対する政府関係機関情報セキュリティ横断監視・即応調整チーム（以下「第一 GSOC」という。）及び、NISC の監督の下、独立行政法人情報処理推進機構（以下「IPA」という。）に設置された独立行政法人及び法第 13 条に規定する指定法人に対する情報セキュリティ横断監視・即応調整チーム（以下「第二 GSOC」という。）の双方を併せたもの

十二　GSOC 連携構成員　構成員のうち、国の関係行政機関の長（当該国の関係行政機関の長が内閣総理大臣又は本部長等の場合にあっては、担当する部局の長を含む。第 6 条第 11 項第 1 号及び第 21 条第 1 号において同じ。）その他これに準ずる者であって NISC（第一 GSOC 担当）と連携する者及び独立行政法人又は法第 13 条に規定する指定法人であって、IPA（第二 GSOC 担当）と連携する者

十二の二　JISP（Japan cyber security Information Sharing Partnership）　我が国のサイバーセキュリティ全体の底上げを進めるため、民間団体、地方公共団体、情報セキュリティ関係機関、政府関係組織等の間でサイバーセキュリティに係る脅威・インシデント情報の共有、事案対処に対する関係組織間での協力連携の調整、参加者の能力向上に資する演習等の取組を推進する情報共有体制で、NISC が中心となって運用するもの

十二の三　JISP 参加構成員　JISP に参加する者で、第 6 条第 6 項の規定によるみなし承認を受けた構成員

十三　協議会システム（情報共有活動用）　協議会における情報共有を行うために用いられる情報システムとして政令指定法人 JPCERT/CC が指定するもの

十三の二　システム登録者　協議会事務従事者のうち、第 14 条第 1 項の規定に基づき協議会システム（情報共有活動用）への登録を受けている者

十四　早期警戒情報提供サービス　JPCERT/CC が協議会システム（情報共有活動用）と互換性がある情報システムを用いて協議会とは別の事業として行う早期警戒情報の提供サービスであって、政令指定法人 JPCERT/CC が指定するもの

十五　　協議会システム（JISP 参加構成員用）　協議会における第 8 章の 2 の活動を行うために用いられる情報システムとして NISC が指定するもの

（目的）

第 3 条　協議会は、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等のうち、我が国のサイバーセキュリティに対する脅威に積極的に

対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うことを目的とする。

（活動）

第４条　協議会は、前条の目的を達成するため、次の各号に掲げる活動を行う。

一　サイバーセキュリティに関する脅威情報等の共有及び分析

二　前号の共有及び分析に基づき我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有

三　前各号の活動に資する関係者間の連携の促進

四　前３号に掲げるもののほか、前条の目的を達成するために必要な活動

２　協議会は、前項に規定する活動を行うにあたって、次の各号に掲げる情報その他のサイバーセキュリティの確保に資する情報を取り扱うものとする。

一　サイバー攻撃による被害発生の動向等に関する情報

二　サイバー攻撃の攻撃手法等に関する情報

３　協議会は、特に、協議会事務従事者には法第 17 条第４項及び法第 38 条に基づき罰則により担保された守秘義務が適用されるという協議会の特徴を最大限に活かし、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等の多様な主体が、サイバーセキュリティに関する事象発生の疑いがある段階においても、協議会に対し、これに関する連絡、相談等を気兼ねなく安心して行うことができるよう、運用において特に配慮するものとする。

第２章　構成員の加入等

（協議会の構成員）

第５条　協議会は、構成員をもって構成する。

２　構成員になろうとする者は、本規約に同意の上、運営委員会が定めるところにより、運営委員会に対して加入申込書を提出して入会の申込みを行い、運営委員会の承認を得たときに構成員となるものとする。何人も、自らの意に反して、入会の申込みを行うことを強要されることはない。

（構成員の加入等）

第６条　協議会への入会申込みについては、運営委員会が定めるところにより、運営委員会が定める募集期間において協議会への入会申込みの募集を実施することとし、構成員になろうとする者は、当該期間中において、入会の申込みを行うものとする。この場合において、運営委員会は、当該期間を、あらかじめ運営委員会が定めるところにより公表しなければならない。

2　前項の申込みを行うことができる者は、次の各号のいずれかに該当する者等であって、第３条に規定する協議会の目的及び第４条第１項に規定する活動内容に賛同する者とする。

一　法第 17 条第２項第１号から第５号までに掲げる者（国の行政機関に関しては、府省に限るものではなく、庁、委員会等も含む。次号において同じ。）

二　前号に定める者に準ずる者として協議会へ加入する必要性が認められる法人その他の団体

3　運営委員会は、第５条第２項の申込みを行った者が前項に規定する申込みの基準に適合しないと認める場合、第８条第１項各号に掲げる事由に該当する場合又は第３条に規定する協議会の目的の達成若しくは第４条第１項に規定する協議会の活動に支障を生じさせるおそれがあると認める場合は、その者の入会を承認しない場合がある。この場合において、承認をしなかった理由等を開示することが我が国のサイバーセキュリティ確保に支障を生じるおそれがあると認められる場合等には、理由等を開示しないことがある。

4　次のいずれかに該当する加入構成員は、第 24 条に規定する 24 条タスクフォースに参加することができない。ただし、我が国におけるサイバーセキュリティの確保にとって特に重要な貢献をなす意欲及び能力並びに長年の我が国におけるサイバーセキュリティに関する官民の様々な公益的取組みへの積極的な協力の実績を有するものであり、かつ、協議会の事務に関して知り得た秘密に該当する情報を日本国内で管理するとともに、秘密の保持について高度の信頼をおくことができるものとして運営委員会が特別に承認したものについては、この限りでない。

一　日本の国籍を有しない人

二　外国政府又はその代表者

三　外国の法人又は団体

四　法人又は団体であって、前各号に掲げる者（以下この号において「外国法人等」という。）がその議決権の過半数を有するものその他これに準ずる事情があると認められるもの（当該外国法人等が当該加入構成員の経営等を支配しているとは明らかに認められないものを除く。）

5　GSOC 連携構成員になろうとする者は、本規約に同意の上、運営委員会が定めるところにより、事務局を経由して運営委員会に対して入会通知書（GSOC 連携構成員用）を提出して入会の通知を行い、運営委員会が当該通知を受領したときに、第５条第２項に基づき運営委員会から承認されたものとみなす。

6　JISP 参加構成員になろうとする者は、JISP に参加し、本規約に同意の上、運営委員会が定めるところにより、事務局を経由して運営委員会に対して入会通知書（JISP 参加構成員用）を提出して入会の通知を行い、運営委員会が当該通知を受領したときに、第５条第２項に基づき運営委員会から承認されたものとみなす。なお、JISP 参加構成員になろうとして入会通知書（JISP 参加構成員用）を提出した時点で既に構成員であった者は、

本項の規定により JISP 参加構成員としての入会を承認されたものとみなされた場合、以後、JISP 参加構成員として取り扱うものとする。

7　加入構成員（JISP 参加構成員を除く。以下この項から第 10 項までにおいて同じ）は、協議会への入会にあたって、運営委員会が定めるところにより、事務局に対し、当該加入構成員に係る協議会事務従事者のうち、当該加入構成員及びその受託者に所属する派遣労働者を含む役職員（当該加入構成員又は受託者が一の組織における一部局である場合は、当該一の組織の役職員を含む。）であって、協議会の情報（法第 17 条第 4 項に基づく守秘義務の対象となる秘密を含む情報に限る。）を取り扱う者（取り扱う可能性がある者を含む。）を全て登録しなければならない。

8　加入構成員は、当該加入構成員に係る協議会事務従事者に対し、必要性及び緊急性が生じた場合において当該協議会事務従事者の判断で協議会に対して情報提供及び相談を迅速に行う権限をあらかじめ付与するよう努めるものとする。

9　加入構成員は、当該加入構成員に係る登録事務従事者を変更しようとするときは、あらかじめ事務局に対しその旨を登録するものとする。ただし、あらかじめ登録することが困難である特別の理由がある場合は、変更後速やかに事務局に対しその旨を登録するものとする。

10　加入構成員は、第 5 条第 2 項の加入申込書の記載事項に変更がある場合は、速やかに事務局に対して届け出るものとする。GSOC 連携構成員は、第 5 項の入会通知書の記載事項に変更がある場合は、速やかに事務局に対してその旨通知するものとする。

11　GSOC 連携構成員（GSOC 連携構成員になろうとする者を含む。以下本項において同じ。）が第 5 項若しくは第 10 項の通知、第 7 項若しくは第 9 項の登録又は第 7 条の退会の届出を行おうとするときは、次の各号に掲げる区分に応じて、当該各号に定める者を経由してこれを行うものとする。

一　GSOC 連携構成員のうち、国の関係行政機関の長その他これに準ずる者として NISC（第一 GSOC 担当）と連携する者　NISC（第一 GSOC 担当）

二　GSOC 連携構成員のうち、独立行政法人及び法第 13 条に規定する指定法人　IPA（第二 GSOC 担当）

12　第 1 項に定める外、運営委員会が必要かつ相当と認める者については、募集期間を定めることなく、第 5 条第 2 項にいう入会の申込みを受け付けることができる。この場合においても、何人も、自らの意思に反して、入会の申込みを行うことを強要されることはない。

13　JISP 参加構成員のうち、運営委員会が相当と認める者については、前項の申込みを受け付けることができる。

第３章　構成員の脱退等

（協議会からの脱退）

第７条　加入構成員は、運営委員会が定めるところにより、事務局に対し退会の届出を行うことで、協議会を脱退することができる。

（加入構成員の除名等）

第８条　運営委員会は、加入構成員に関して次の各号に掲げるいずれかの事由に該当すると認めるときは、運営委員全員の同意を得て、当該加入構成員を除名することができる。

一　当該加入構成員、当該加入構成員の受託者、当該加入構成員に係る協議会事務従事者、当該加入構成員を介して情報提供を受けた非構成員、当該非構成員の受託者及び当該非構成員に係る協議会事務従事者が協議会の事務遂行上取得した情報を漏えいしたとき

二　当該加入構成員及び当該加入構成員に所属する協議会事務従事者（以下本項において「当該加入構成員等」という。）が法又は本規約その他協議会が定める規則等に違反したとき

三　当該加入構成員等が協議会もしくは構成員の名誉を傷つけ、または協議会の目的に反する行為をしたとき

四　当該加入構成員等が法令又は公序良俗に違反したとき

五　当該加入構成員等が反社会的勢力や団体又はその関係者であると認められるとき

六　当該加入構成員等が協議会の目的と協調しがたい事業等に関与したと認められるとき

七　その他当該加入構成員を除名すべき特別の理由があると認められるとき

２　運営委員会は、構成員に関して次の各号に掲げるいずれかの事由に該当すると認めるときは、直ちに、運営委員会が定めるところにより、運営委員の４分の３以上の賛成をもって、当該構成員に対する情報共有等を制限することができる。

一　当該構成員、当該構成員の受託者、当該構成員に係る協議会事務従事者、当該構成員を介して情報提供を受けた非構成員、当該非構成員の受託者及び当該非構成員に係る協議会事務従事者が協議会の事務遂行上取得した情報を漏えいした疑いがあると認められるとき

二　当該構成員及び当該構成員に所属する協議会事務従事者が前項第２号から第６号までのいずれか（このとき、前項第２号の「当該加入構成員及び当該加入構成員に所属する協議会事務従事者」は「当該構成員及び当該構成員に所属する協議会事務従事者」と、前項各号の「当該加入構成員等」は「当該構成員等」と読み替えるものとする。）に該当する疑いがあると認められるとき

三　その他当該構成員に対する情報共有等を制限すべき相当の理由があると認められるとき

（構成員たる資格の喪失）

第９条　前条の場合のほか、加入構成員は、死亡し若しくは失踪宣告を受け又は解散したときは、その資格を喪失する。

第４章　協議会の運営等

（総会）

第 10 条　協議会は、原則として毎年、構成員(JISP 参加構成員を除く。以下この条において同じ。)による定時総会を開催するものとする。また、運営委員会が必要と認めるときは、臨時総会を開催することができる（以下、定時総会及び臨時総会をあわせて「総会」という。）。

２　総会においては、以下の事項を実施する。

一　本規約（別表１を除く。）又は第 18 条第６項に基づき規定する情報管理規程の改正の決議

二　本協議会の活動・運営に関する報告

三　運営委員会において総会に付議すべきものと決議した事項

３　総会の招集及び議事進行は、運営委員長が行う。総会を招集する場合には、総会の開催方法、日時、議決が必要な事項その他の必要な事項を定めた上で、構成員に対して総会の開催通知を発しなければならない。

４　総会における議決権は、構成員１者につき１個とする。

５　総会は、すべての構成員の議決権の過半数を有する構成員の出席もしくは委任状の提出をもって成立する。

６　第２項のうち、議決が必要な事項については、総会に出席した構成員の過半数の賛成をもって成立するものとする。ただし、運営委員全員が反対した場合はこの限りではない。

７　総会は、必要に応じて、電子的手段により開催することができる。

８　構成員は、各総会における第３項の開催通知に係る議決が必要な事項に対して賛否を表明するにあたって効率化の観点から必要と認める場合にあっては、運営委員会が定めるところにより、事務局に対し、当該事項に関して異議がある場合その他当該総会に出席する必要があると認める場合にのみ、当該総会に出席し、当該事項について賛否を表明することとする旨の届出を行うことができる。当該届出を行った当該構成員が当該総会に出席しなかった場合又は当該事項について異議を述べなかった場合、運営委員長は、当該構成員が当該総会に出席し、当該事項について包括的に賛成したものとみなす。

（運営委員会）

第 11 条　協議会に運営委員会を置く。

２　運営委員会は、本部長等が法第 17 条第１項及び同条第２項に基づき、協議会を組織すること及び構成員を加えることができることに鑑み、別表１に掲げる本部長等を運営委

員として構成する。なお、運営委員である国の関係行政機関の長において、当該行政機関自身のサイバーセキュリティの確保を担当する部局が第６条の規定に基づき協議会への入会を別に行うことは妨げない。

３　運営委員会は、協議会の運営上必要な事項として次に掲げる事項に関する業務を行う。ただし、政令指定法人 JPCERT/CC が行う構成員間の連絡調整に関すること（第 14 条第３項に関することを除く。）及び第 24 条に規定する 24 条タスクフォースの業務に関すること（第６条第４項に関することを除く。）を除く。

一　加入構成員の入会の承認及び退会申込みの受付に関すること

二　加入構成員の除名及び加入構成員たる資格の喪失に関すること

三　構成員に対する情報共有等の制限に関すること

四　第 23 条に基づく情報提供等協力の求めに関すること

五　本規約（別表１に限る。）の改正に関すること

六　前各号に定めるもののほか、協議会の組織及び運営に関すること

４　運営委員会は、前項の業務を行うにあたって必要があると認めるときは、政令指定法人 JPCERT/CC その他当該業務に関して十分な知識又は経験を有する者等の意見を聴くことができる。

５　運営委員会に、運営委員長を置き、サイバーセキュリティ戦略本部長をもって充てる。

６　運営委員会の定足数は運営委員の過半数とし、決議は、出席した運営委員の過半数をもって行うこととする。運営委員は、各１個の議決権を有するが、議決について特別の利害関係を有するときは、議決権を有しないものとする。

７　運営委員会は、必要に応じて、電子的手段により開催することができる。

８　運営委員長は、運営委員会の業務を総理し、運営委員会を招集する。

９　運営委員長は、協議会の目的及び活動に照らし必要があると認めるときは、第６項に基づく運営委員会の議決を拒否することができる。

10　前各項に定めるもののほか、運営委員会の運営及び手続に関し必要な事項は、運営委員会において定める。

（事務局）

第 12 条　協議会に事務局を置く。

２　事務局は、NISC 及び政令指定法人 JPCERT/CC が務める。

３　NISC が第６条の規定に基づき協議会への入会を行うことは妨げない。

４　政令指定法人 JPCERT/CC は、第４条第１項第１号に基づく情報共有等を行うため、構成員を含む関係者間の連絡調整を行うものとする。

（準用）

第 13 条　第６条第７項から第９項までの規定については、本部長等たる構成員、事務局、

NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）に対して準用する。

第５章　情報共有システム（情報共有活動用）の利用

（情報共有システムについて）

第 14 条　構成員（GSOC 連携構成員及び JISP 参加構成員を除く。以下この章において同じ。）は、協議会における情報共有について協議会システム（情報共有活動用）を利用することとし、当該システムの利用にあたり、当該システムに適用される利用規約を遵守しなければならない。構成員は、次のいずれかに該当する協議会事務従事者を、当該システムに登録することができる。

一　当該構成員に係る協議会事務従事者のうち、当該構成員に所属する派遣労働者を含む役職員（当該構成員が一の組織における一部局である場合は、当該一の組織の役職員を含む。）

二　当該構成員に係る協議会事務従事者のうち、当該構成員の受託者に所属する派遣労働者を含む役職員（当該受託者が一の組織における一部局である場合は、当該一の組織の役職員を含む。）であって、当該構成員に係る登録事務従事者である者

２　協議会システム（情報共有活動用）の管理権限は、政令指定法人 JPCERT/CC が有する。管理権限を有する政令指定法人 JPCERT/CC に限り、第 17 条第１項及び同条第２項の規定にかかわらず、協議会システム（情報共有活動用）における全ての投稿にアクセスすることができる。

３　NISC（協議会庶務担当）は、第 17 条第１項及び同条第２項の規定にかかわらず、協議会システム（情報共有活動用）の利用者間で発生した紛争等を裁定する必要がある場合、又は、協議会の庶務を処理する上で必要な場合に、当該目的を達成するために当該システムにおける必要最小限度の投稿にアクセスすることができる。この場合において、NISC（協議会庶務担当）は、運営委員会に付議すべき案件があると思料するときは、運営委員会に対し、必要最小限度の情報を提供することができる。

４　協議会における情報共有に当たって、本規約と第１項の利用規約との間に矛盾・抵触する規定がある場合は、本規約の規定が優先するものとする。

（早期警戒情報提供サービスについて）

第 15 条　構成員は、構成員となったときに、併せて、早期警戒情報提供サービスの登録を受けたものとみなし、JPCERT/CC から早期警戒情報の提供を受けるものとする。ただし、当該構成員が構成員となるにあたって、運営委員会が定めるところにより別段の意思表示を行った場合はこの限りではない。

２　協議会において作出された情報のうち、当該情報の内容、機微性、脅威度等を総合的に勘案し、第 17 条第４項第４号の TLP:GREEN 又は第５号の TLP:CLEAR を付与するこ

とが相当と認められるものは、より幅広い主体に共有されることが望ましいと考えられることから、特別の事情がある場合を除き、早期警戒情報提供サービスを経由して提供するものとする。この場合、構成員の多くが既に早期警戒情報の提供を受けており、提供される情報の重複を避ける必要があることに鑑み、特別の事情がある場合を除き、構成員への当該情報の提供については、協議会システム（情報共有活動用）は利用しない。

第５章の２　JISP 参加構成員における情報システムの利用

（協議会システム（JISP 参加構成員用））

第 15 条の２　JISP 参加構成員は、第８章の２にいう活動について協議会システム（JISP 参加構成員用）を利用することとし、当該システムの利用にあたり、当該システムに適用される利用規約を遵守しなければならない。

２　JISP 参加構成員でない構成員が、協議会システム（情報共有活動用）の利用と併せて、協議会システム（JISP 参加構成員用）の利用も希望する場合には、それを妨げない。この場合において、当該構成員は、当該システムに適用される利用規約を遵守しなければならない 。

第６章　情報共有活動

（事務局と構成員との情報共有）

第 16 条　事務局は、JPCERT/CC から提供される情報、構成員（JISP 参加構成員を除く。以下この章及び第７章において同じ。）から直接提供される情報、非構成員から直接提供される情報を取り扱うこととする。

２　事務局は、構成員に対し、サイバーセキュリティの確保に資する情報を随時提供するものとする。

３　構成員は、事務局に対し、サイバーセキュリティの確保に資する情報を任意に提供することができる。構成員は、第４条第３項の規定の趣旨に鑑み、自組織内において収集・分析した情報のみでは情報システムの被害の内容・範囲を検知または認知するに至っておらず、平常時に比して直感的な違和感があるといった程度にとどまる早期・初動の時点においても、国内外における類似関連情報その他の有益な助言や情報を、専門的知見を有する政令指定法人 JPCERT/CC や他の構成員から得ることを目的として、事務局に対する相談に伴い、情報を提供することができる。

（情報の共有範囲の指定）

第 17 条　構成員は、事務局に対し任意に情報を提供するに際し、当該情報の共有範囲を指定することができる。事務局を含め、何人も、当該構成員の同意を得ることなく、当該共

有範囲を超えて情報の共有を行ってはならない。

2　事務局は、構成員に対し情報を提供するに際し、当該情報の共有範囲を指定することができる。何人も、事務局の同意を得ることなく、当該共有範囲を超えて情報の共有を行ってはならない。

3　事務局は、前条第２項の規定に基づき提供する情報の中に、同条第３項の規定に基づき任意に提供された情報が含まれるときは、当該情報を提供した構成員の同意を得ることなく、第１項の規定に基づき当該構成員が指定した共有範囲を超えて、前項に規定する情報の共有範囲を指定してはならない。

4　事務局は、構成員（GSOC 連携構成員を除く。以下この項において同じ。）に対し情報を提供するに際し、第２項に規定する情報の共有範囲の指定の有無及び内容に応じて、当該情報に以下に掲げる TLP（Traffic Light Protocol）のいずれかを付与するものとする。

一　TLP:RED　情報の共有範囲が、構成員に所属する協議会事務従事者（当該構成員に係る登録事務従事者を含む。）に限られる場合

二　TLP:AMBER+STRICT　情報の共有範囲が、構成員に係る協議会事務従事者に限られる場合

三　TLP:AMBER　情報の共有範囲が、前号に掲げる者及び第 19 条第３項第２号又は同項第３号の規定に基づき当該構成員を介して非構成員のサイバーセキュリティを確保する必要がある場合における当該非構成員に係る協議会事務従事者に限られる場合

四　TLP:GREEN　前号に規定する範囲よりも広い範囲での共有が認められるが、一般に公開することは認められない場合

五　TLP:CLEAR　一般に公開することが認められる場合

（秘密の管理）

第 18 条　構成員は、事務局に対し任意に情報を提供するに際し、法第 17 条第４項に規定する秘密の有無を明示することとする。

2　事務局は、構成員に対し情報を提供するに際し、法第 17 条第４項に規定する秘密の範囲を明示することとする。

3　事務局は、法第 17 条第４項に規定する秘密を含む情報については、前条の規定に基づき指定する当該情報の共有範囲に、構成員、事務局、NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）（以下本条において「構成員等」という。）に係る登録事務従事者以外の者を含めてはならない。

4　構成員等は、法第 17 条第４項に規定する秘密を含む情報を、当該構成員等に係る登録事務従事者以外の者に取り扱わせてはならない。

5　構成員は、法第 17 条第４項に規定する秘密の受領を希望しない場合にあっては、運営委員会が定めるところにより、事務局に対し秘密の受領を拒否する旨届け出ることができる。

6　構成員等は、前各項に定めるもののほか、別途協議会が定める情報管理規程に基づき法第 17 条第４項に規定する秘密を取り扱うものとする。

（情報の利用の目的）

第 19 条　事務局、NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）は、協議会の事務を通じて知り得た情報を、第４条第１項に規定する協議会の活動目的以外の目的で利用してはならない。政令指定法人 JPCERT/CC、NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）は、協議会の事務を通じて知り得た情報を、協議会とは別の事業（早期警戒情報提供サービス及び GSOC としての活動を除く。）の活動目的で利用してはならない。

2　構成員は、協議会の事務を通じて知り得た情報を、自らのサイバーセキュリティを確保する目的以外の目的で利用してはならない。第 16 条第３項の規定に基づき情報を提供する構成員は、自ら任意に提供する情報が自ら又は情報の原提供者に対する犯罪捜査、行政処分、行政調査又は行政指導のために用いられるおそれがあると思料するときは、該当する捜査機関、監督官庁等を、第 17 条第１項の規定に基づき指定する情報の共有範囲からあらかじめ除外することができる。

3　構成員は、前項の規定にかかわらず、次の各号に掲げる場合には、当該各号に定める目的で、協議会の事務を通じて知り得た情報を利用することができる。

一　当該情報に第 17 条に規定する情報の共有範囲が指定されていない場合　普及啓発目的

二　当該構成員が複数の組織間の共助等を目的とする非営利の法人その他の団体である場合　当該法人その他の団体が共助等の対象とする組織（法第 17 条第２項第１号、第２号、第３号又は第５号に該当する者に限る。）のサイバーセキュリティを確保する目的

三　前２号に定めるほか、事務局が個別に認める場合　事務局が個別に認める目的

4　構成員は、前項の規定に基づき協議会の事務を通じて知り得た情報を利用するに際し、当該規定があることのみをもって、以下の義務を免れるものと解してはならない。

一　法第 17 条第４項に規定する守秘義務及び前条第４項に規定する情報の取扱い範囲の遵守義務

二　本規約第 17 条第１項及び第２項に規定する情報の共有範囲の遵守義務

（事務局を介さない情報共有）

第 20 条　構成員が協議会の事務の一環として他の構成員との間で情報の共有を行おうとするときは、事務局を通じて行うこととし、構成員の間における直接の情報共有は、特別の理由がある場合に限って行うこととする。この場合において、第 16 条第３項、第 17 条第１項、第 18 条第１項及び同条第４項から第６項まで並びに第 19 条第２項から第４項

までの規定は、構成員の間における直接の情報共有について準用する。

（GSOC 連携構成員との情報共有）

第 21 条　事務局若しくは構成員が協議会の事務の一環として GSOC 連携構成員に対して情報提供を行おうとするとき又は GSOC 連携構成員が協議会の事務の一環として事務局若しくは他の構成員に対して情報提供を行おうとするときは、次の各号に掲げる区分に応じて、当該各号に定める者を経由してこれを行うものとする。ただし、第 24 条に規定する 24 条タスクフォースの活動として情報の共有を行おうとする場合等を除く。

一　GSOC 連携構成員のうち、国の関係行政機関の長その他これに準ずる者として NISC（第一 GSOC 担当）と連携する者　NISC（第一 GSOC 担当）

二　GSOC 連携構成員のうち、独立行政法人及び法第 13 条に規定する指定法人　IPA（第二 GSOC 担当）

（非構成員との情報共有）

第 22 条　第 16 条第３項の規定は、非構成員について準用する。この場合において、第 17 条から第 19 条までの規定は、非構成員から事務局に対し任意に提供された情報の取り扱いについて準用する。なお、事務局は、複数の構成員及び非構成員から同時に相談に伴う情報提供を受ける等して業務が逼迫している場合、非構成員への対応より構成員への対応を優先することとする。

２　事務局は、第 19 条第３項第２号の規定に基づき非構成員のサイバーセキュリティを確保する必要がある場合その他構成員を介して非構成員に対して情報を提供する必要があると認める場合であり、かつ、当該非構成員に対し法第 17 条第４項に規定する秘密を含む情報を提供する緊急の必要があると認めるときは、第 18 条第３項の規定にかかわらず、第 17 条第２項に規定する情報の共有範囲に、当該非構成員を追加することができ、この場合において、当該構成員は、第 18 条第４項の規定にかかわらず、当該情報を当該非構成員に提供することができる。なお、当該情報の提供を受けた当該非構成員は、当該非構成員に係る協議会事務従事者のうち、当該非構成員及びその受託者に所属する派遣労働者を含む役職員（当該非構成員又は受託者が一の組織における一部局である場合は、当該一の組織の役職員を含む。）であって、当該情報を取り扱った者を、当該構成員を介して全て事務局に事後すみやかに登録するものとし、登録事務従事者以外の者に当該情報を取り扱わせてはならない。事務局は、当該非構成員に当該情報を提供するにあたって、当該登録が必要となる旨を当該構成員を介してあらかじめ通知するものとする。

３　第 17 条第３項（第１項の規定により準用する場合を含む。）の規定は、前項の規定に基づき事務局が情報の共有範囲の追加を行う場合における当該情報の中に第 17 条第１項（第１項の規定により準用する場合を含む。）の規定に基づき任意に提供された情報が含まれる場合について準用する。

４　第 17 条第２項、第 18 条第６項並びに第 19 条第２項及び第３項の規定は、第２項の規定により秘密を含む情報の提供を受けた非構成員について準用する。

第７章　情報提供等協力の求め

（協議会からの協力の求め）

第 23 条　協議会は、次の各号に掲げる場合に限り、構成員に対して、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

一　大規模なサイバー攻撃が発生するなど、情報提供等の協力を求める特別の必要性が認められる場合又はこれに準ずる状況であると認められる場合

二　構成員にとって協議会による求めがなければ提供することができない情報を提供する場合であって、当該構成員が協議会による協力の求めを受けることについて同意している場合

２　協議会は、前項の規定に基づき情報提供等の協力の求めを行うにあたっては、必要に応じて、当該協力の求めの目的及び当該求めに基づき取得した情報の共有範囲を明示するものとする。

第８章　タスクフォースに関する特則

（タスクフォース）

第 24 条　協議会に、24 条タスクフォース（以下「タスクフォース」という。）を置く。

２　タスクフォースは、政令指定法人 JPCERT/CC 及び次項に基づき追加された者をもって構成する。

３　タスクフォースは、第４条第１項第１号及び同項第２号に規定する活動に積極的に貢献する意欲と能力を有する者として承認した者をタスクフォースに加えることができる。何人も、自らの意に反して、当該承認の申込みを行うことを強要されることはない。

４　タスクフォースを構成する者（タスクフォースが定める要件に該当する者に限る。）は、第 19 条第１項及び同条第２項の規定にかかわらず、タスクフォースが定めるところにより、タスクフォースの事務の遂行上取得した情報について、第三者のサイバーセキュリティ確保のために用いることができる。この場合において、第 19 条第４項の規定は、当該タスクフォースを構成する者について準用する。

５　タスクフォースを構成する者（タスクフォースが定める要件に該当する者に限る。以下この項において「タスクフォース情報提供者」という。）は、タスクフォースへの提供を前提として第三者（以下この項において「原提供者」という。）から取得した情報を含む情報をタスクフォースへ提供し、当該情報に対し他のタスクフォースを構成する者から秘密を含むフィードバック情報を得られた場合であって、原提供者その他の第三者のサ

イバーセキュリティ確保のため当該情報を原提供者に提供する必要があると認めるときは、当該他のタスクフォースを構成する者の同意を得た場合に限り、第18条第４項の規定にかかわらず、当該情報を原提供者に提供することができる。この場合において、当該情報の提供を受けた原提供者は、当該原提供者に係る協議会事務従事者のうち、当該原提供者及びその受託者に所属する派遣労働者を含む役職員（当該原提供者又は受託者が一の組織における一部局である場合は、当該一の組織の役職員を含む。）であって、当該情報を取り扱う者（取り扱う可能性がある者を含む。）を、当該情報に係るタスクフォース情報提供者を介して事務局に対してあらかじめ全て登録するものとし、登録事務従事者以外の者に当該情報を取り扱わせてはならない。第22条第３項及び第４項の規定は、この規定により秘密を含む情報の提供を受けた原提供者について準用する。

６　タスクフォースの組織及び運営に関することは、タスクフォースにおいて定める。タスクフォースは、タスクフォースを構成する者に対してのみ適用されるものに限り、本規約の特則を設けることができる。当該特則は、タスクフォースを構成する者以外の構成員に対しては効力を生じない。

第８章の２　JISP参加構成員の活動

（JISP参加構成員の活動）

第24条の２　事務局（政令指定法人JPCERT/CCを除く。）は、第４条第１項第４号の活動として、JISP参加構成員の対処能力強化等に資する取組を行う。具体的な運用方法等は、第15条の２の利用規約のほか、必要に応じて運営委員会が定めるところによる。

２　JISP参加構成員は、前項の取組に積極的に参加するよう努めるものとする。

第９章　雑則

（構成員の公表等）

第25条　協議会は、運営委員会が定めるところにより、本規約及び構成員の名簿を公表するものとする。この場合において、協議会は、公表を望まない加入構成員の名称等を、当該公表する名簿に記載してはならない。

２　前項に基づき公表される名簿の中には、協議会事務従事者の氏名を記載してはならない。

３　構成員は、第１項の規定に基づき名簿の公表を望まない構成員を含む全ての構成員の名称を知ることができる。また、事務局は、協議会の事務遂行上必要な範囲で、構成員が他の構成員に係る協議会事務従事者の所属・氏名を知りうる状態に置くことができる。

４　事務局は、名簿の公表を望まない構成員の名称及び各構成員に係る協議会事務従事者に係る情報を第三者に漏らしてはならない。

５　構成員は、第３項の規定に基づき知ることとなった名簿の公表を望まない構成員の名称及び他の構成員に係る協議会事務従事者の所属・氏名を第三者に漏らしてはならない。

（サイバーセキュリティ戦略本部との連携）

第 26 条　協議会は、必要があると認めるときは、我が国のサイバーセキュリティ確保に関する事項について、サイバーセキュリティ戦略本部との連携を図るものとする。

（協議会における議事等について）

第 27 条　総会、運営委員会及びタスクフォースの議事は原則非公開とする。

２　構成員の間で共有される情報のうち、情報共有の範囲が指定されているものについては、非公開とする。

（免責）

第 28 条　協議会及び構成員は、協議会の活動として提供した情報の正確性を保証しないものとする。

２　協議会及び構成員は、協議会の活動として提供した情報に基づき、情報提供者以外の者に損害が発生したとしても、当該損害について一切の法的責任を負わないものとする。ただし、故意又は重過失による場合はこの限りではない。

３　政令指定法人 JPCERT/CC は、協議会システム（情報共有活動用）の利用又は協議会システム（情報共有活動用）の利用の停止、休止、中断、制限若しくは通信回線の障害等によりシステムを利用した構成員又は他の第三者が被った損害について一切の法的責任を負わないものとする。

（違反に関する連絡）

第 29 条　構成員、政令指定法人 JPCERT/CC、NISC（第一 GSOC 担当）及び IPA（第二 GSOC 担当）は、協議会において取り扱われる情報の漏えい、共有範囲の逸脱、目的外利用をはじめとする法令、本規約その他関係規則の違反があると思料するときは、NISC（協議会庶務担当）に対してその旨連絡することができる。

（個人情報の取扱い）

第 30 条　協議会の庶務を処理するにあたって NISC が取得する個人情報（個人情報の保護に関する法律第２条第１項に規定する個人情報をいう。）の取扱いに関しては、別途 NISC が定めるプライバシーポリシーに従うものとする。

附　則

この規約は、平成 31 年４月１日から施行する。

附　則（令和元年９月６日改正）

この規約改正は、令和元年９月６日から施行する。

附　則（令和２年３月６日改正）

この規約改正は、令和２年３月６日から施行する。

附　則（令和３年９月１日改正）

この規約改正は、令和３年９月１日から施行する。

附　則（令和４年３月 22 日改正）

この規約改正は、令和４年３月 22 日から施行する。ただし、第 30 条の改正については、令和４年４月１日から施行する。

附　則（令和５年４月 28 日改正）

この規約改正は、令和５年４月 28 日から施行する。

別表１　運営委員一覧

サイバーセキュリティ戦略本部長（内閣官房長官）
サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
国家公安委員会委員長
デジタル大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
経済安全保障担当大臣

24 条タスクフォース規則

平成 31 年４月１日　24 条タスクフォース決定
令和元年９月 11 日　一部改正
令和２年３月６日　一部改正
令和４年４月１日　一部改正

（タスクフォース参加者の区分）

第１条　24 条タスクフォース（以下「タスクフォース」という。）に参加する者は、政令指定法人 JPCERT/CC のほか、第一類構成員及び第二類構成員の２つの区分により構成する。

一　第一類構成員　構成員のうち、他の情報共有体制に参加又は運営する主体であって、サイバーセキュリティ協議会規約（以下「規約」という。）第４条第１項第１号及び同項第２号に定める活動に積極的に貢献する能力と意欲を有する者として、サイバーセキュリティの確保に資する情報を積極的に提供することができる者

二　第二類構成員　構成員のうち、第一類構成員等（政令指定法人 JPCERT/CC 及び第一類構成員をいう。以下同じ。）から提供される情報に対し一定の応答を行うことができる能力と意欲を有する者

（タスクフォースの業務）

第２条　タスクフォースは、規約第４条第１項第１号及び同項第２号に掲げる協議会の活動として、サイバーセキュリティに関する脅威情報等の積極的な共有及び分析を行い、我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有を積極的に行うものとする。

２　タスクフォースは、タスクフォースとして決定すべき事項がある等必要と認めるときは、タスクフォース会合を開催することができる。

３　タスクフォース会合は、タスクフォース参加者全員の出席をもって成立し、タスクフォースとしての決定は、原則としてタスクフォース参加者全員の賛成をもって行うこととする。

４　タスクフォース会合は、必要に応じて、電子的手段により開催することができる。

５　タスクフォースとして決定すべき事項のうち、タスクフォースの運営への影響が軽微な事項については、第２項及び第３項の規定にかかわらず、事務局において定めることができる。事務局が当該定めをタスクフォース参加者に対して通知した日から２週間以内にタスクフォース参加者のいずれからも異議が出なかった場合に、当該定めは効力を生じるものとする。

６　前各項に規定するもののほか、タスクフォースの運営に関する事項は、別途タスクフォ

ースにおいて定める。

（地位の取得）

第３条　第一類構成員又は第二類構成員になろうとする構成員は、別途タスクフォースが定めるところにより、タスクフォースに対して申込みを行い、タスクフォースの承認を得たときに第一類構成員又は第二類構成員となるものとする。

（情報提供等の協力の求め）

第４条　協議会は、規約第 23 条第１項の規定にかかわらず、第一類構成員又は第二類構成員に対して情報提供等の協力を求める必要があると認められる場合には、別途タスクフォースが定めるところにより、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

（情報提供の範囲に関する留意事項）

第５条　タスクフォース参加者は、タスクフォースが高度な信頼関係に基づき機微性の高い情報をタスクフォースの中で共有することに鑑み、タスクフォース参加者以外の構成員にとって不要な情報を当該構成員に対し提供しないよう留意しなければならない。

（第一類グループ）

第６条　タスクフォースに、第一類グループを置く。

２　第一類グループは、第一類構成員等をもって構成する。

３　第一類グループは、第一類グループとして決定すべき事項がある等必要と認めるときは、第一類グループ会合を開催することができる。

４　第一類グループ会合は、第一類構成員等全員の出席をもって成立し、第一類グループとしての決定は、原則として第一類構成員等全員の賛成をもって行うこととする。

５　第一類グループ会合は、必要に応じて、電子的手段により開催することができる。

６　第一類グループとして決定すべき事項のうち、第一類グループの運営への影響が軽微な事項については、第３項及び第４項の規定にかかわらず、事務局において定めることができる。ただし、事務局が当該定めを第一類構成員等に対して通知した日から２週間以内に第一類構成員等のいずれからも異議が出なかった場合に、当該定めは効力を生じるものとする。

７　前各項に規定するもののほか、第一類グループによる情報の提供に関することその他第一類グループの運営に関することは、第一類グループにおいて定める。

（情報提供等の協力の求め）

第７条　協議会は、規約第 23 条第１項の規定にかかわらず、第一類構成員に対して情報提

供等の協力を求める必要があると認められる場合には、別途第一類グループが定めるところにより、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

（規約第 24 条に基づきタスクフォースが定める要件）

第８条　規約第 24 条第４項に規定するタスクフォースが定める要件は、第一類構成員等であることとする。

２　規約第 24 条第５項に規定するタスクフォースが定める要件は、第一類構成員等であることとする。

（タスクフォース等の庶務）

第９条　タスクフォース及び第一類グループの庶務は、NISC（協議会庶務担当）が務める。この場合において、NISC（協議会庶務担当）は、規約第 12 条第３項及び規約第 14 条第３項の規定の適用を除外されるものではない。

内閣法

（昭和二十二年一月十六日法律第五号）
最終改正：令和五年九月一日法律第十四号

第一条　内閣は、国民主権の理念にのつとり、日本国憲法第七十三条その他日本国憲法に定める職権を行う。
２　内閣は、行政権の行使について、全国民を代表する議員からなる国会に対し連帯して責任を負う。

第二条　内閣は、国会の指名に基づいて任命された首長たる内閣総理大臣及び内閣総理大臣により任命された国務大臣をもつて、これを組織する。
２　前項の国務大臣の数は、十四人以内とする。ただし、特別に必要がある場合においては、三人を限度にその数を増加し、十七人以内とすることができる。

第三条　各大臣は、別に法律の定めるところにより、主任の大臣として、行政事務を分担管理する。
２　前項の規定は、行政事務を分担管理しない大臣の存することを妨げるものではない。

第四条　内閣がその職権を行うのは、閣議によるものとする。
２　閣議は、内閣総理大臣がこれを主宰する。この場合において、内閣総理大臣は、内閣の重要政策に関する基本的な方針その他の案件を発議することができる。
３　各大臣は、案件の如何を問わず、内閣総理大臣に提出して、閣議を求めることができる。

第五条　内閣総理大臣は、内閣を代表して内閣提出の法律案、予算その他の議案を国会に提出し、一般国務及び外交関係について国会に報告する。

第六条　内閣総理大臣は、閣議にかけて決定した方針に基いて、行政各部を指揮監督する。

第七条　主任の大臣の間における権限についての疑義は、内閣総理大臣が、閣議にかけて、これを裁定する。

第八条　内閣総理大臣は、行政各部の処分又は命令を中止せしめ、内閣の処置を待つことができる。

第九条　内閣総理大臣に事故のあるとき、又は内閣総理大臣が欠けたときは、その予め指定する国務大臣が、臨時に、内閣総理大臣の職務を行う。

第十条　主任の国務大臣に事故のあるとき、又は主任の国務大臣が欠けたときは、内閣総理大臣又はその指定する国務大臣が、臨時に、その主任の国務大臣の職務を行う。

第十一条　政令には、法律の委任がなければ、義務を課し、又は権利を制限する規定を設けることができない。

第十二条　内閣に、内閣官房を置く。
２　内閣官房は、次に掲げる事務をつかさどる。
一　閣議事項の整理その他内閣の庶務
二　内閣の重要政策に関する基本的な方針に関する企画及び立案並びに総合調整に関する事務
三　閣議に係る重要事項に関する企画及び立案並びに総合調整に関する事務
四　行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務
五　前三号に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務
六　内閣の重要政策に関する情報の収集調査に関する事務
七　国家公務員に関する制度の企画及び立案に関する事務
八　国家公務員法（昭和二十二年法律第百二十号）第十八条の二（独立行政法人通則法（平成十一年法律第百三号）第五十四条第一項において準用する場合を含む。）に規定する事務に関する事務
九　国家公務員の退職手当制度に関する事務
十　特別職の国家公務員の給与制度に関する事務
十一　国家公務員の総人件費の基本方針及び人件費予算の配分の方針の企画及び立案並びに調整に関する事務
十二　第七号から前号までに掲げるもののほか、国家公務員の人事行政に関する事務（他の行政機関の所掌に属するものを除く。）
十三　行政機関の機構及び定員に関する企画及び立案並びに調整に関する事務
十四　各行政機関の機構の新設、改正及び廃止並びに定員の設置、増減及び廃止に関する審査を行う事務
十五　前各号に掲げるもののほか、法律（法律に基づく命令を含む。）に基づき、内閣官房に属させられた事務
３　前項の外、内閣官房は、政令の定めるところにより、内閣の事務を助ける。
４　内閣官房の外、内閣に、別に法律の定めるところにより、必要な機関を置き、内閣の事務を助けしめることができる。

第十三条　内閣官房に内閣官房長官一人を置く。
２　内閣官房長官は、国務大臣をもつて充てる。
３　内閣官房長官は、内閣官房の事務を統轄し、所部の職員の服務につき、これを統督する。

第十四条　内閣官房に、内閣官房副長官三人を置く。
２　内閣官房副長官の任免は、天皇がこれを認証する。
３　内閣官房副長官は、内閣官房長官の職務を助け、命を受けて内閣官房の事務（内閣感染症危機管理統括庁及び内閣人事局の所掌に属するものを除く。）をつかさどり、及びあらかじめ内閣官房長官の定めるところにより内閣官房長官不在の場合その職務を代行する。

第十五条　内閣官房に、内閣危機管理監一人を置く。
２　内閣危機管理監は、内閣官房長官及び内閣官房副長官を助け、命を受けて第十二条第二項第一号から第六号までに掲げる事務のうち危機管理（国民の生命、身体又は財産に重大な被害が生じ、又は生じるおそれがある緊急の事態への対処及び当該事態の発生の防止

をいう。次項、第十六条第二項第一号及び第十七条第三項において同じ。）に関するもの（国の防衛に関するもの及び内閣感染症危機管理統括庁の所掌に属するものを除く。）を統理する。

3　前項に定めるもののほか、内閣危機管理監は、臨時に命を受け、感染症に係る危機管理に関する事務について、内閣感染症危機管理統括庁の事務の処理に協力する。

4　内閣危機管理監の任免は、内閣総理大臣の申出により、内閣において行う。

5　国家公務員法第九十六条第一項、第九十八条第一項、第九十九条並びに第百条第一項及び第二項の規定は、内閣危機管理監の服務について準用する。

6　内閣危機管理監は、在任中、内閣総理大臣の許可がある場合を除き、報酬を得て他の職務に従事し、又は営利事業を営み、その他金銭上の利益を目的とする業務を行つてはならない。

第十五条の二　内閣官房に、内閣感染症危機管理統括庁を置く。

2　内閣感染症危機管理統括庁は、次に掲げる事務をつかさどる。

一　新型インフルエンザ等対策特別措置法（平成二十四年法律第三十一号）第六条第一項に規定する政府行動計画の策定及び推進に関する事務

二　新型インフルエンザ等対策特別措置法第十七条第二項の規定により内閣感染症危機管理統括庁が処理することとされた新型インフルエンザ等対策本部に関する事務

三　新型インフルエンザ等対策特別措置法第七十条の七の規定により内閣感染症危機管理統括庁が処理することとされた新型インフルエンザ等対策推進会議に関する事務

四　前三号に掲げるもののほか、第十二条第二項第二号から第五号まで及び第十五号に掲げる事務のうち感染症の発生及びまん延の防止に関するもの（国家安全保障局、内閣広報官及び内閣情報官の所掌に属するものを除く。）

3　内閣感染症危機管理統括庁に、内閣感染症危機管理監一人を置く。

4　内閣感染症危機管理監は、内閣官房長官を助け、命を受けて庁務を掌理するものとし、内閣総理大臣が内閣官房副長官の中から指名する者をもつて充てる。

5　内閣感染症危機管理統括庁に、内閣感染症危機管理監補一人を置く。

6　内閣感染症危機管理監補は、内閣感染症危機管理監を助け、庁務を整理するものとし、内閣総理大臣が内閣官房副長官補の中から指名する者をもつて充てる。

7　内閣感染症危機管理統括庁に、内閣感染症危機管理対策官一人を置く。

8　内閣感染症危機管理対策官は、内閣感染症危機管理監及び内閣感染症危機管理監補を助け、命を受けて、内閣感染症危機管理統括庁の所掌事務に係る重要な政策に関する事務を総括整理し、及びその所掌事務のうち重要事項に係るものに参画するものとし、厚生労働省の医務技監をもつて充てる。

第十六条　内閣官房に、国家安全保障局を置く。

2　国家安全保障局は、次に掲げる事務をつかさどる。

一　第十二条第二項第二号から第五号までに掲げる事務のうち我が国の安全保障（第二十一条第三項において「国家安全保障」という。）に関する外交政策、防衛政策及び経済政策の基本方針並びにこれらの政策に関する重要事項に関するもの（危機管理に関するもの並びに内閣広報官及び内閣情報官の所掌に属するものを除く。）

二　国家安全保障会議設置法（昭和六十一年法律第七十一号）第十二条の規定により国家安全保障局が処理することとされた国家安全保障会議の事務

三　国家安全保障会議設置法第六条の規定により国家安全保障会議に提供された資料又は情報その他の前二号に掲げる事務に係る資料又は情報を総合して整理する事務

3　国家安全保障局に、国家安全保障局長を置く。
4　国家安全保障局長は、内閣官房長官及び内閣官房副長官を助け、命を受けて局務を掌理する。
5　第十五条第四項から第六項までの規定は、国家安全保障局長について準用する。
6　国家安全保障局に、国家安全保障局次長二人を置く。
7　国家安全保障局次長は、国家安全保障局長を助け、局務を整理するものとし、内閣総理大臣が内閣官房副長官補の中から指名する者をもつて充てる。

第十七条　内閣官房に、内閣官房副長官補三人を置く。
2　内閣官房副長官補は、内閣官房長官、内閣官房副長官及び内閣危機管理監を助け、命を受けて内閣官房の事務（第十二条第二項第一号に掲げるもの並びに内閣感染症危機管理統括庁、国家安全保障局、内閣広報官、内閣情報官及び内閣人事局の所掌に属するものを除く。）を掌理する。
3　前項に定めるもののほか、内閣官房副長官補（第十五条の二第六項の規定により内閣総理大臣が指名した者を除く。）は、臨時に命を受け、感染症に係る危機管理に関する事務について、内閣感染症危機管理統括庁の事務の処理に協力する。
4　第十五条第四項から第六項までの規定は、内閣官房副長官補について準用する。

第十八条　内閣官房に、内閣広報官一人を置く。
2　内閣広報官は、内閣官房長官、内閣官房副長官及び内閣危機管理監を助け、第十二条第二項第二号から第五号までに掲げる事務について必要な広報に関することを処理するほか、同項第二号から第五号までに掲げる事務のうち広報に関するものを掌理する。
3　第十五条第四項から第六項までの規定は、内閣広報官について準用する。

第十九条　内閣官房に、内閣情報官一人を置く。
2　内閣情報官は、内閣官房長官、内閣官房副長官及び内閣危機管理監を助け、第十二条第二項第二号から第五号までに掲げる事務のうち特定秘密（特定秘密の保護に関する法律（平成二十五年法律第百八号）第三条第一項に規定する特定秘密をいう。）の保護に関するもの（内閣広報官の所掌に属するものを除く。）及び第十二条第二項第六号に掲げる事務を掌理する。
3　第十五条第四項から第六項までの規定は、内閣情報官について準用する。

第二十条　内閣官房に、内閣人事局を置く。
2　内閣人事局は、第十二条第二項第七号から第十四号までに掲げる事務をつかさどる。
3　内閣人事局に、内閣人事局長を置く。
4　内閣人事局長は、内閣官房長官を助け、命を受けて局務を掌理するものとし、内閣総理大臣が内閣官房副長官の中から指名する者をもつて充てる。

第二十一条　内閣官房に、内閣総理大臣補佐官五人以内を置く。
2　内閣総理大臣補佐官は、内閣総理大臣の命を受け、国家として戦略的に推進すべき基本的な施策その他の内閣の重要政策のうち特定のものに係る内閣総理大臣の行う企画及び立案について、内閣総理大臣を補佐する。
3　内閣総理大臣は、内閣総理大臣補佐官の中から、国家安全保障に関する重要政策を担当する者を指定するものとする。
4　内閣総理大臣補佐官は、非常勤とすることができる。

５　第十五条第四項及び第五項の規定は内閣総理大臣補佐官について、同条第六項の規定は常勤の内閣総理大臣補佐官について準用する。

第二十二条　内閣官房に、内閣総理大臣に附属する秘書官並びに内閣総理大臣及び各省大臣以外の各国務大臣に附属する秘書官を置く。
２　前項の秘書官の定数は、政令で定める。
３　第一項の秘書官で、内閣総理大臣に附属する秘書官は、内閣総理大臣の、国務大臣に附属する秘書官は、国務大臣の命を受け、機密に関する事務をつかさどり、又は臨時に命を受け内閣官房その他関係各部局の事務を助ける。

第二十三条　内閣官房に、内閣事務官その他所要の職員を置く。
２　内閣事務官は、命を受けて内閣官房の事務を整理する。

第二十四条　この法律に定めるもののほか、内閣官房の所掌事務を遂行するため必要な内部組織については、政令で定める。

第二十五条　内閣官房に係る事項については、この法律にいう主任の大臣は、内閣総理大臣とする。
２　内閣総理大臣は、内閣官房に係る主任の行政事務について、法律又は政令の制定、改正又は廃止を必要と認めるときは、案をそなえて、閣議を求めなければならない。
３　内閣総理大臣は、内閣官房に係る主任の行政事務について、法律若しくは政令を施行するため、又は法律若しくは政令の特別の委任に基づいて、内閣官房の命令として内閣官房令を発することができる。
４　内閣官房令には、法律の委任がなければ、罰則を設け、又は義務を課し、若しくは国民の権利を制限する規定を設けることができない。
５　内閣総理大臣は、内閣官房の所掌事務について、公示を必要とする場合においては、告示を発することができる。
６　内閣総理大臣は、内閣官房の所掌事務について、命令又は示達をするため、所管の諸機関及び職員に対し、訓令又は通達を発することができる。

第二十六条　内閣総理大臣は、管区行政評価局及び沖縄行政評価事務所に、内閣官房の所掌事務のうち、第十二条第二項第十三号及び第十四号に掲げる事務に関する調査並びに資料の収集及び整理に関する事務を分掌させることができる。

附　則

１　この法律は、日本国憲法施行の日から、これを施行する。
２　復興庁が廃止されるまでの間における第二条第二項の規定の適用については、同項中「十四人」とあるのは「十五人」と、同項ただし書中「十七人」とあるのは「十八人」とする。
３　国際博覧会推進本部が置かれている間における第二条第二項の規定の適用については、前項の規定にかかわらず、同条第二項中「十四人」とあるのは「十六人」と、同項ただし書中「十七人」とあるのは「十九人」とする。
４　東京オリンピック競技大会・東京パラリンピック競技大会推進本部が置かれている間における第二条第二項の規定の適用については、前二項の規定にかかわらず、同条第二

項中「十四人」とあるのは「十七人」と、同項ただし書中「十七人」とあるのは「二十人」とする。

5　内閣人事局は、第二十条第二項に規定する事務のほか、当分の間、国家公務員制度改革基本法（平成二十年法律第六十八号）第二章に定める基本方針に基づいて行う国家公務員制度改革の推進に関する企画及び立案並びに当該国家公務員制度改革に関する施策の実施の推進に関する事務をつかさどる。

内閣官房組織令

（昭和三十二年七月三十一日政令第二百十九号）
最終改正：令和六年七月一日政令第二百三十一号

内閣は、内閣法（昭和二十二年法律第五号）第十六条第二項及び第十七条の規定に基き、この政令を制定する。

（内部組織）
第一条　内閣官房に、次の三室及び内閣サイバーセキュリティセンターを置く。
内閣総務官室
内閣広報室
内閣情報調査室

（内閣総務官室）
第二条　内閣総務官室においては、次の事務をつかさどる。
一　閣議事項の整理に関すること。
二　機密に関すること。
三　内閣の主管に属する人事に関すること。
四　内閣総理大臣、内閣官房長官及び内閣官房副長官の官印その他の公印の保管に関すること。
五　公文書類の接受、発送及び保存に関すること。
六　職員の厚生及び教養訓練に関すること。
七　予算、決算及び会計に関すること。
八　総理大臣官邸の管理運営に関すること。
九　前各号に掲げるもの以外の内閣の庶務
２　内閣総務官室に、内閣総務官一人を置く。
３　内閣総務官は、内閣総務官室の事務を掌理する。

（内閣広報室）
第三条　内閣広報室においては、次の事務をつかさどる。
一　内閣の重要政策に関する基本的な方針に関する企画及び立案並びに総合調整に関する事務のうち広報に関するもの
二　閣議に係る重要事項に関する企画及び立案並びに総合調整に関する事務のうち広報に関するもの
三　行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務のうち広報に関するもの
四　前三号に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうち広報に関するもの
２　前項に定めるもののほか、内閣広報室は、内閣広報官が内閣法第十八条第二項に規定する広報に関することを処理することについて、これを補佐する。
３　内閣広報官は、内閣広報室の事務を掌理する。

（内閣情報調査室）

第四条　内閣情報調査室においては、次の事務をつかさどる。

一　内閣の重要政策に関する情報の収集及び分析その他の調査に関する事務（各行政機関の行う情報の収集及び分析その他の調査であつて内閣の重要政策に係るものの連絡調整に関する事務を含む。）

二　次に掲げる事務のうち特定秘密（特定秘密の保護に関する法律（平成二十五年法律第百八号）第三条第一項に規定する特定秘密をいう。）の保護に関するもの（内閣広報室においてつかさどるものを除く。）

イ　内閣の重要政策に関する基本的な方針に関する企画及び立案並びに総合調整に関する事務

ロ　閣議に係る重要事項に関する企画及び立案並びに総合調整に関する事務

ハ　行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務

ニ　イからハまでに掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務

２　内閣情報官は、内閣情報調査室の事務を掌理する。

（内閣サイバーセキュリティセンター）

第四条の二　内閣サイバーセキュリティセンターにおいては、次の事務をつかさどる。

一　情報通信ネットワーク又は電磁的記録媒体（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものに係る記録媒体をいう。）を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること。

二　行政各部におけるサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下この項において同じ。）の確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること（内閣情報調査室においてつかさどるものを除く。）。

三　行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関すること。

四　行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。

五　前各号に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの（国家安全保障局、内閣広報室及び内閣情報調査室においてつかさどるものを除く。）

２　内閣サイバーセキュリティセンターに、内閣サイバーセキュリティセンター長一人を置く。

３　内閣サイバーセキュリティセンター長は、内閣官房長官、内閣官房副長官及び内閣危機管理監を助け、内閣サイバーセキュリティセンターの事務を掌理するものとし、内閣総理大臣が内閣官房副長官補の中から指名する者をもつて充てる。

（内閣衛星情報センター）

第四条の三　内閣情報調査室に、内閣衛星情報センターを置く。

２　内閣衛星情報センターにおいては、内閣情報調査室の事務のうち次に掲げるものをつかさどる。

一　我が国の安全の確保、大規模災害への対応その他の内閣の重要政策に関する画像情報の収集を目的とする人工衛星（以下「情報収集衛星」という。）に関すること。

二　情報収集衛星により得られる画像情報の分析その他の調査に関すること。
三　情報収集衛星以外の人工衛星の利用その他の手段により得られる画像情報の収集及び分析その他の調査に関すること。
3　内閣衛星情報センターに、所長一人を置く。
4　所長は、内閣情報官を助け、内閣衛星情報センターの事務を掌理する。

（公文書監理官）
第四条の四　内閣総務官室に、公文書監理官一人（関係のある他の職を占める者をもつて充てられるものとする。）を置く。
2　公文書監理官は、命を受けて、内閣官房の所掌事務に関する公文書類の管理並びにこれに関連する情報の公開及び個人情報の保護の適正な実施の確保に係る重要事項についての事務並びに関係事務を総括整理する。

（総理大臣官邸事務所長）
第五条　内閣総務官室に、総理大臣官邸事務所長一人を置く。
2　総理大臣官邸事務所長は、内閣総務官室の事務のうち総理大臣官邸の管理運営に関すること及び特に命ぜられた機密に関することをつかさどる。

（人事政策統括官）
第五条の二　内閣人事局に、人事政策統括官三人（うち一人は、関係のある他の職を占める者をもつて充てられるものとする。）を置く。
2　人事政策統括官は、命を受けて内閣人事局の事務の一部をつかさどる。

（内閣審議官）
第六条　内閣官房に、内閣審議官を置く。
2　内閣審議官は、命を受けて、内閣官房の事務のうち重要事項に係るものに参画し、及びその事務の一部を総括整理し、又は人事政策統括官のつかさどる職務のうち重要事項に係るものを助ける。
3　内閣審議官の定数は、併任の者を除き、七十八人とする。ただし、そのうち四十六人は、内閣総理大臣が特に必要と認める場合に置かれるものとする。

第七条　内閣総務官室、国家安全保障局、内閣広報室、内閣情報調査室若しくは内閣サイバーセキュリティセンター（以下「内閣総務官室等」という。）又は内閣人事局に属しない内閣審議官は、内閣官房副長官補を助け、命を受けて、内閣官房副長官補の掌理する事務（内閣サイバーセキュリティセンターにおいてつかさどるものを除く。以下同じ。）のうち重要事項に係るものに参画し、及びその事務の一部を総括整理する。
2　内閣総務官室等に属する内閣審議官は、命を受けて、その属する内閣総務官室等の事務のうち重要事項に係るものに参画し、及びその属する内閣総務官室等の事務の一部を総括整理する。
3　内閣人事局に属する内閣審議官は、命を受けて、人事政策統括官のつかさどる職務のうち重要事項に係るものを助ける。
4　内閣総務官室等又は内閣人事局に属する内閣審議官は、前二項に定める職務を行うほか、命を受けて、内閣官房副長官補を助け、内閣官房副長官補の掌理する事務のうち重要事項に係るものに参画し、及びその事務の一部を総括整理する。

（内閣参事官）
第八条　内閣官房に、内閣参事官を置く。
２　内閣参事官は、命を受けて、内閣官房の事務の一部をつかさどり、又は人事政策統括官のつかさどる職務を助ける。
３　内閣参事官の定数は、併任の者を除き、百十二人とする。ただし、そのうち三十二人は、内閣総理大臣が特に必要と認める場合に置かれるものとする。

第九条　内閣総務官室等又は内閣人事局に属しない内閣参事官は、内閣官房副長官補を助け、命を受けて内閣官房副長官補の掌理する事務の一部をつかさどる。
２　内閣総務官室等に属する内閣参事官は、命を受けてその属する内閣総務官室等の事務（内閣総務官室については、総理大臣官邸事務所長のつかさどるものを除く。）の一部をつかさどる。
３　内閣人事局に属する内閣参事官は、命を受けて、人事政策統括官のつかさどる職務を助ける。
４　内閣総務官室等又は内閣人事局に属する内閣参事官は、前二項に定める職務を行うほか、命を受けて、内閣官房副長官補を助け、内閣官房副長官補の掌理する事務の一部をつかさどる。

（内閣危機管理監の事務の整理）
第十条　内閣総理大臣の指定する内閣官房副長官補は、内閣危機管理監の事務の整理を掌理する。

（内閣総理大臣等に附属する秘書官の定数）
第十一条　内閣総理大臣に附属する秘書官の定数は五人とし、内閣総理大臣及び各省大臣以外の各国務大臣に附属する秘書官の定数はそれぞれ一人とする。

（組織の細目）
第十二条　この政令に定めるもののほか、内閣官房の内部組織に関し必要な細目は、内閣総理大臣が定める。

附　則
１　この政令は、昭和三十二年八月一日から施行する。
２　第六条の内閣審議官（同条第三項ただし書の規定により置かれるものを除く。）のうち、四人は令和七年三月三十一日まで、他の一人は令和八年三月三十一日まで置かれるものとする。
３　第六条の内閣審議官（同条第三項ただし書の規定により置かれるもの及び前項に規定するものを除く。）のうち一人は、郵政民営化法（平成十七年法律第九十七号）第八条に規定する移行期間の末日まで置かれるものとする。
４　第八条の内閣参事官（同条第三項ただし書の規定により置かれるものを除く。）のうち四人は、令和七年三月三十一日まで置かれるものとする。
５　当分の間、第八条第三項の規定の適用については、同項中「百十二人」とあるのは「百十一人」と、同項ただし書中「三十二人」とあるのは「三十一人」とし、第十一条の規定の適用については、同条中「五人」とあるのは、「八人」とする。