# 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

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<br>○ 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<br>○ 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<br>○ 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<br>○ 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<br>○ 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<br>○ ISAC 連携等による分野間・官民連携の枠組みの整備の検討<br>○ 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<br>○ 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<br>○ 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<br>○ 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<br>○ 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。

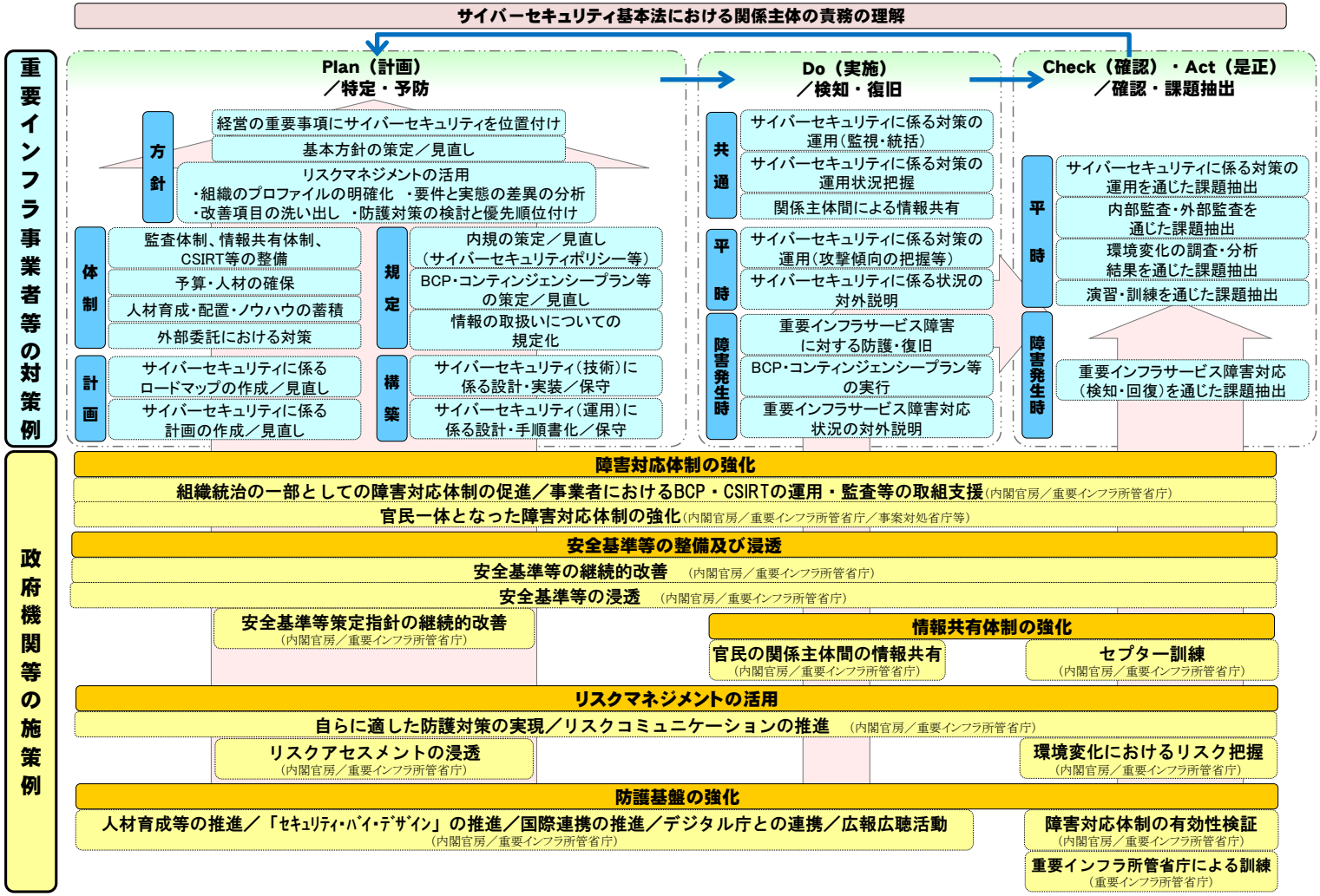



図 1 「重要インフラ事業者等の対策例」と「政府機関等の施策例」

# 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」及び「石油」の14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。

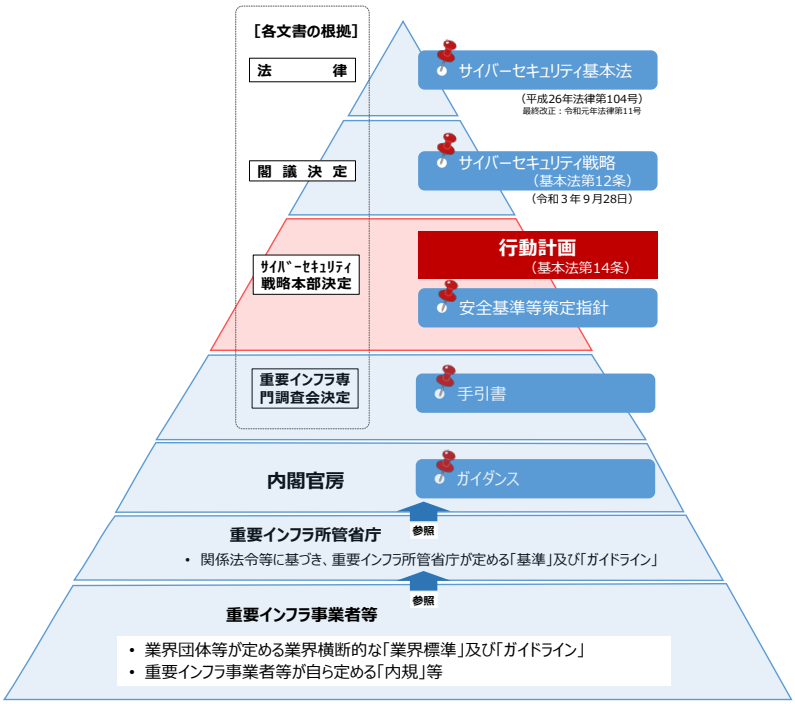



**図 2 重要インフラ防護に関する安全基準等に係る体系**

### 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。

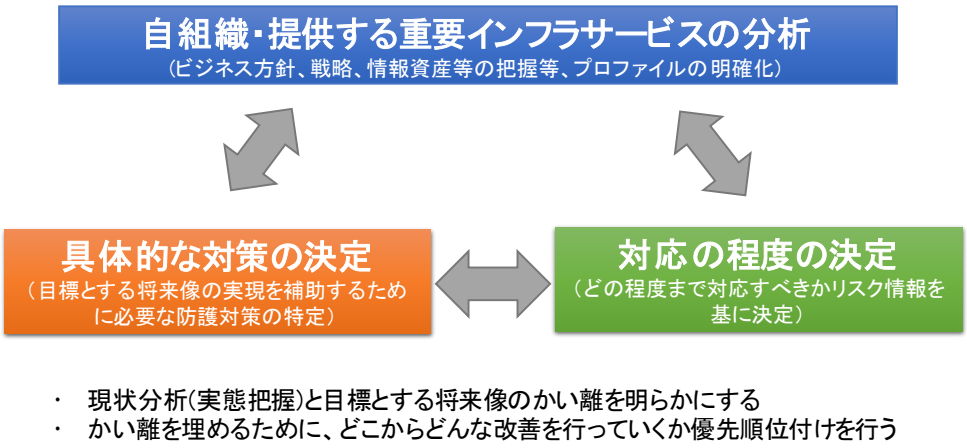



**図 3 自組織に適した防護対策の実現（概念図）**

**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。

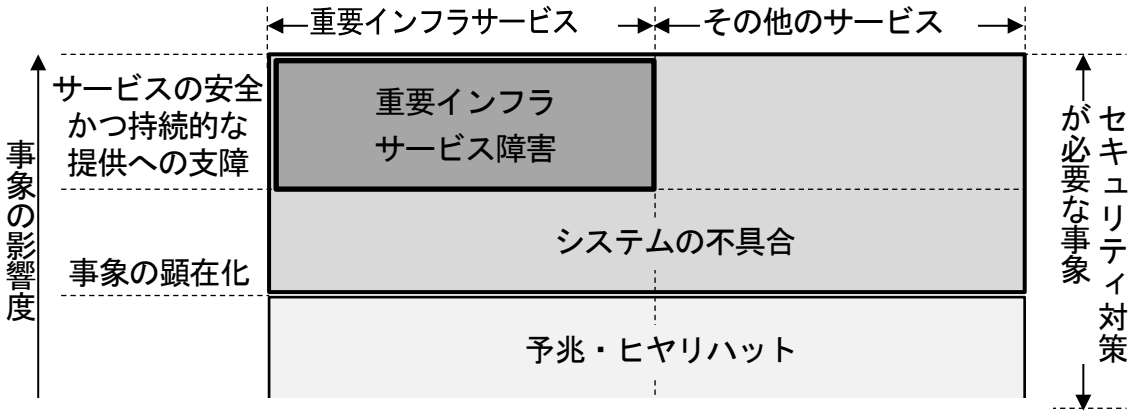



**図　情報共有の対象範囲**

[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<br>・主要な地上基幹放送事業者<br>・主要なケーブルテレビ事業者 | ・ネットワークシステム<br>・オペレーションサポートシステム<br>・編成・運行システム |
| 金融　銀行等<br>生命保険<br>損害保険<br>証券<br>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<br>・資金清算機関<br>・電子債権記録機関<br>・生命保険<br>・損害保険<br>・証券会社<br>・金融商品取引所<br>・振替機関<br>・金融商品取引清算機関<br>・主要な資金移動業者<br>・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<br>・資金証券系システム<br>・国際系システム<br>・対外接続系システム<br>・金融機関相互ネットワークシステム<br>・電子債権記録機関システム<br>・保険業務システム<br>・証券取引システム<br>・取引所システム<br>・振替システム<br>・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<br>・予約・搭乗システム<br>・整備システム<br>・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<br>・フライトインフォメーションシステム<br>・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<br>・電力管理システム<br>・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<br>・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<br>・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<br>（ただし、小規模なものを除く。） | ・診療録等管理システム<br>・診療業務支援システム<br>・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<br>（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<br>・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<br>・貨物追跡システム<br>・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<br>・主要な決済代行業者<br>・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<br>・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<br>・生産管理システム<br>・生産出荷システム |

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<br>・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<br>・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<br><br>【サービス維持レベル】<br>・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<br>・放送法施行規則（報告を要する重大な事故）第125条<br><br>【サービス維持レベル】<br>・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<br>・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<br>・放送法施行規則（報告を要する重大な事故）第157条<br><br>【サービス維持レベル】<br>・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<br>・貸付<br>・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）<br>・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）<br>・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<br>・融資業務の遅延・停止<br>・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<br>・中小・地域金融機関向けの総合的な監督指針<br>・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）<br>・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）<br>・保険金等の支払審査（保険業法第97条第1項）<br>・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）<br>・損害調査等（保険業法第97条第1項）<br>・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<br>・有価証券の売買等の取引の媒介、取次ぎ又は代理<br>・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）<br>・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）<br>・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<br>・一般振替機関の監督に関する命令（事故）第17条<br>・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<br>・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<br>・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<br>・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<br>・予約、発券、搭乗・搭載手続<br>・運航整備<br>・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）<br>・航空旅客の予約、航空貨物の予約<br>・航空券の発券、料金徴収<br>・航空旅客のチェックイン・搭乗、航空貨物の搭載<br>・航空機の点検・整備<br>・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<br>・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<br>・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<br>・空港利用者等への正確・迅速な情報提供<br>・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<br>・情報提供等に支障が発生することによる利便性の低下<br>・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<br>・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）<br>・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<br>・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<br>・鉄道事故等報告規則（鉄道運転事故等の報告）第5条<br>・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<br>・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）<br>・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<br>・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<br><br>【サービス維持レベル】<br>・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<br><br>・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）<br>・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<br>・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<br><br>【サービス維持レベル】<br>・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<br>・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<br>・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<br>・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）<br>・水道分野における情報セキュリティガイドライン |

| 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) | | |
| 物流 | ・貨物自動車運送事業<br>・船舶運航事業<br>・港湾運送事業<br>・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)<br>・船舶により物の運送をする事業(海上運送法第２条)<br>・他人の需要に応じ、港湾においてする船舶への貨物の積込又は船舶からの貨物の取卸の行為等を行う事業(港湾運送事業法第２条)<br>・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<br>・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 |
| 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<br>・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)<br>・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<br>・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<br>・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<br>・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 |

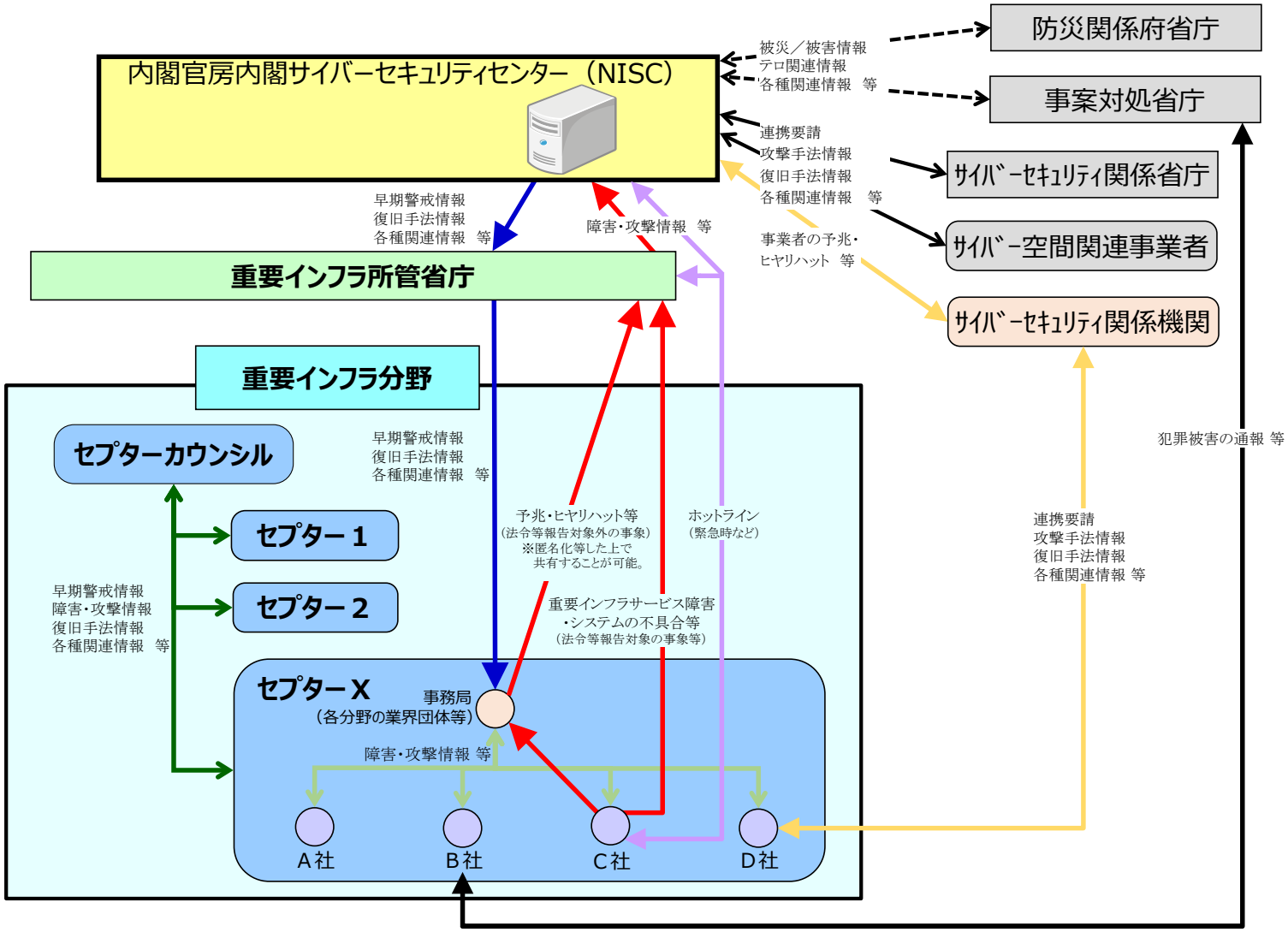
注１　ITを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。

## 別紙３　情報連絡における事象と原因の類型

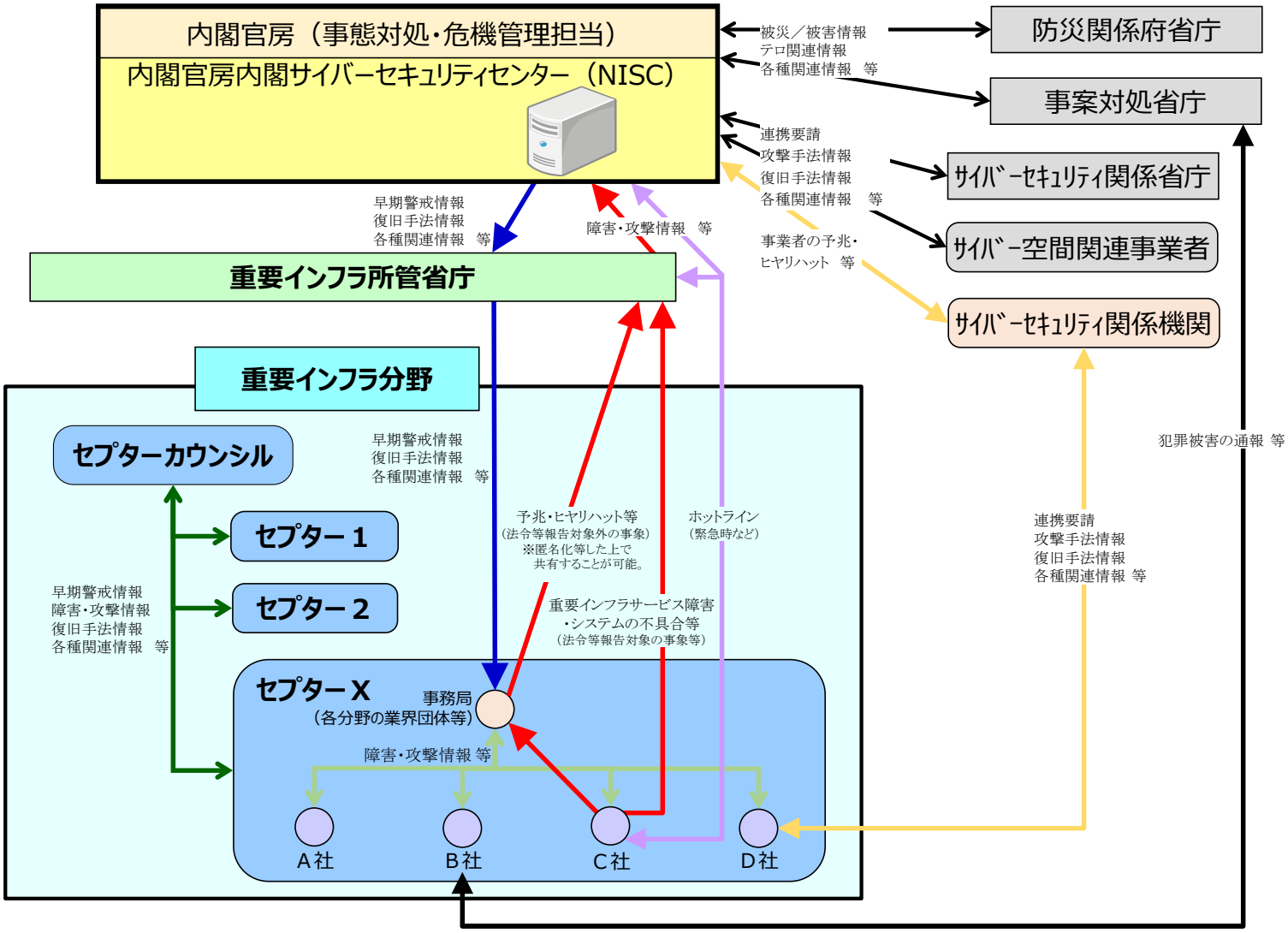
| 事象の類型 | | 事象の例 | 説明 |
|---|---|---|---|
| 未発生の事象 | | 予兆・ヒヤリハット | サイバー攻撃の予告などの予兆や、事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信などによるヒヤリハットの発生 |
| 発生した事象 | 機密性を脅かす事象 | 情報の漏えい | 組織の機密情報等の流出など、機密性が脅かされる事象の発生 |
| | 完全性を脅かす事象 | 情報の破壊 | Webサイト等の改ざんや組織の機密情報等の破壊など、完全性が脅かされる事象の発生 |
| | 可用性を脅かす事象 | システム等の利用困難 | 制御システム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<br>（事態対処・危機管理担当） | 重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。 | 通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。 |
| ○ 内閣官房<br>（ＮＩＳＣ） | 重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。 | 内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。 |
| ○ 重要インフラ所管省庁 | 所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣから受領したシステムの不具合等に関する情報を該当するセプターに提供する。 | 通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。 |
| ○ セプターカウンシル | セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。<br>主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。 | 通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。 |
| ○ セプター事務局 | 重要インフラ所管省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。 | 通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。 |
| ○ 重要インフラ事業者等 | システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、「別添：情報連絡・情報提供について」に基づき重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。 | 通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。 |

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

# 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。<br>※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」及び「石油」の 14 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。 |