参考資料３

重要インフラの情報セキュリティ対策に係る
第３次行動計画

平 成 ２ ６ 年 ５ 月 １ ９ 日

情 報 セ キ ュ リ テ ィ 政 策 会 議

（本ページは白紙です。）

目次

Ⅰ．総論

1. 行動計画策定に当たっての認識

重要インフラに係る行動計画は、重要インフラ防護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であり、内閣官房情報セキュリティセンター（NISC）設立以前から「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月情報セキュリティ対策推進会議決定）」が策定される等、我が国の重要インフラの情報セキュリティ対策に関する施策の根幹を成すものとして策定してきた。

NISC設立後の行動計画については、2005年に情報セキュリティ政策会議が提示した、ＩＴ障害から重要インフラを防護し、重要インフラ事業者等の事業継続性を確保するために取るべき対策についての基本的方向性を踏まえ、同年に「重要インフラの情報セキュリティ対策に係る行動計画」（以下「第１次行動計画」という。）を決定した。この第１次行動計画に基づき、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し、政府及び重要インフラ10分野等からなる関係主体による取組が開始された。

さらに、第１次行動計画において構築された重要インフラの基本的な情報セキュリティ対策や官民の情報共有の枠組みを基礎とし、国として取り組むべき施策を示した「重要インフラの情報セキュリティ対策に係る第２次行動計画」（以下「第２次行動計画」という。）を2009年に決定した。第２次行動計画では、第１次行動計画における主な施策である「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析[1]」、「分野横断的演習」を引き続き実施しつつも、刻々と変化する社会環境や技術環境に的確に対応するため、新たに「環境変化への対応」についての施策を追加した。

このように、我が国の重要インフラ防護は、特別行動計画から見て13年間、現行の形態となった行動計画でも８年間の実績を有しており、確固たる情報共有体制の構築を始め、５つの施策に基づく対策が着実に進展したものと評価できる。

したがって、本行動計画策定においては、「サイバーセキュリティ戦略（2013年６月情報セキュリティ政策会議決定）」を踏まえつつ、第２次行動計画における施策群の評価によって得られた良好事例、要改善事例等の知見を的確に反映した。

また、東日本大震災発災時のシステム障害、データ滅失等への対応において得られた知見等の活用に加え、刻々と変化する社会環境・技術環境、近年の複雑化・巧妙化するサイバー攻撃の趨勢への適切な対応を反映した。

[1] 第１次行動計画では、「相互依存性解析」という施策名である。

2. 重要インフラ防護の目的の明確化

本行動計画の実施の前提として、重要インフラ防護の目的を明確化し、関係者間で認識を共有することが必要である。

サイバーセキュリティ戦略については、「情報の自由な流通の確保」、「深刻化するリスクへの新たな対応」、「リスクベースによる対応の強化」及び「社会的責務を踏まえた行動と共助」を基本的な考え方において示しており、第２次行動計画の目的はサイバーセキュリティ戦略と整合している。

したがって、第２次行動計画における目的を継承しつつも、「重要インフラにおけるサービスの持続的な提供のために行う」ことを追加し、重要インフラ防護の目的を更に明確化した。

○「重要インフラ防護」の目的

・ 重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する。

○基本的な考え方

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

・ 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。

・ 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。

・ 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

3. 第２次行動計画の施策の成果と課題

第２次行動計画は、次の５つの施策から構成されている。

［1］安全基準等の整備及び浸透
［2］情報共有体制の強化
［3］共通脅威分析
［4］分野横断的演習
［5］環境変化への対応

以下に、各施策の成果と課題の概要を示す。

3.1 成果

今回、これら施策群の評価を行うに際し、第２次行動計画は2009年時点での重要インフラを取り巻く最新知見を踏まえて策定されたものであることを考慮し、５つの施策に対して第２次行動計画における評価指標に照らして効果について評価を行った。その結果、所期の目標については、以下に示すとおり一定の成果を挙げたと評価できるものであった。

安全基準等の整備及び浸透については、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指した結果、指針と安全基準等の一体的・安定的な見直しサイクルを確立し、情報セキュリティ対策の推進等を強化した。

情報共有体制の強化については、刻々と変化する重要インフラの情報セキュリティを取り巻く社会環境や技術環境及び複雑・巧妙化するサイバー攻撃等に対応することを目的に、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター内・各セプター間における情報共有体制の整備及び重要インフラ事業者等における必要情報の享受・活用を実現した。

共通脅威分析については、重要インフラ全体の防護能力の維持・向上に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った結果、重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映した。

分野横断的演習については、ＩＴ障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じて相互の連絡・連携における仕組みの検証機会の提供に取り組んだ結果、演習参加組織数・人数は増加傾向にあり、演習で得られた知見に基づく重要インフラ事業者等のＩＴ障害時の早期復旧手順及び事業継続計画等の検証を通じた情報セキュリティ対策に貢献した。

環境変化への対応のうち広報公聴活動については、重要インフラの情報セキュリテ

ィ施策の結果資料、重要インフラ専門委員会の会議資料等を内閣官房のWebサイトに掲載し、公表するとともに、情報セキュリティ政策に係る講演等を行った。リスクコミュニケーションの充実については、情報セキュリティに係る関係機関との意見交換会の開催、セプターカウンシルにおける相互理解ＷＧの開催を行った。国際連携の推進については、Meridian[2]、Cyber Storm演習[3]への参加等を通じて諸外国との連携を行った。こうした取組を通じて、環境変化に伴う脅威の察知能力の向上に努めた。

3.2 課題

各施策の実施を通じて、社会・技術面での環境変化を踏まえた改善・補強を要する課題も抽出された。各施策の主たる課題を以下に記載する。

安全基準等の整備及び浸透においては、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・向上にも効力が及ぶこと、重要インフラ事業者等から対策の実情に基づいて優先順位付けされた指針の提示要望があること等から、重要インフラ事業者等における情報セキュリティ対策のPDCAサイクルに沿った継続的改善の取組との整合に基づく見直しを課題とする。

情報共有体制の強化においては、実効性のある情報共有体制の構築を目的に、分野間における情報共有頻度の格差の解消、「脅威の類型」の細分化、平時の体制の延長線上として位置付けられる大規模ＩＴ障害対応時の情報共有体制の構築、新たな関係主体との連携の在り方の整理等を課題とする。

共通脅威分析においては、共通脅威分析の対象・位置付けや実施頻度の見直しに向けて、調査対象を全分野の共通脅威に限定せず、全分野に及ばずとも影響が大きな脅威を調査対象に加える運営に係る検討や、効果を高めるため、時間経過や環境変化の顕在化に応じた脅威等の詳細分析等を課題とする。

分野横断的演習においては、各組織のＩＴ利用形態や情報管理態勢がそれぞれ異なっていることから演習環境の設定に限界があり、大幅な参加者拡大が望めない。このため、重要インフラ事業者等における情報セキュリティ対策の課題抽出機会の提供を目的に、演習成果の更なる普及・浸透を、参加者拡大のみに依存せず、重要インフラ分野全体に図ることを課題とする。また、演習評価に基づく運営の質的改善、重要インフラのＩＴ障害発生時の対応を踏まえた関係主体の在り方の検討、並びに重要インフラ所管省庁及び防災関係府省庁が主催する演習・訓練との連携についての検討を課題とする。

環境変化への対応のうち広報公聴活動においては、次期行動計画における本施策と

[2] 各国の重要情報インフラ防護政策担当者が集まり、重要情報インフラ防護に特化して議論を行う国際的なフォーラム。
[3] 米国政府が主催する大規模な演習。サイバー空間の脆弱性・脅威・攻撃に対応する国際的な取組を促進する場であるIWWN(International Watch and Warning Network)の一員として参加している。

他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しを課題とする。リスクコミュニケーションの充実においては、国際標準と整合したリスクマネジメントの定義、機微情報の秘匿と情報の有用性のバランスを念頭に置いた情報共有の見直し、及び中長期的に実現・利用され脅威の影響の大きさが予想される新たなＩＴ技術等を対象にした環境変化のテーマに係る中長期的な継続調査・検討を課題とする。国際連携の推進においては、国境を越えて形成されたサイバー空間において深刻化・グローバル化するリスクへの迅速な対応に向けて、諸外国との連携推進を継続するとともに、ASEAN等のアジア太平洋地域や欧米等の二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化を課題とする。

4. 考慮すべき課題

前節における課題やサイバーセキュリティ戦略において検討を求められた課題をまとめるとともに、これらの課題を踏まえた本行動計画策定の方向性について、以下のとおり検討を行った。

課題１　重要インフラ防護が体制としての成熟度を高めている一方、基本的な考え方に示した「情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施する」ことに関して、その実行や実行に当たっての意識が不十分な重要インフラ事業者等が見受けられる。このような重要インフラ事業者等の実効的かつ自主的な取組をどのように促進することが適当なのか。

＜方向性＞

○重要インフラ事業者等にとって実現が困難な理想論を記載するのではなく、現実を見据え、身の丈に合った「実行可能」なものとする。例えば、「安心があたりまえ」「100%の完璧を期する」といった表現は避けるようにする。

○重要インフラ事業者等における情報セキュリティ対策の鍵を握る経営層が十分にその必要性を把握できるよう、基本的な項目を行動計画に記載する。

○「専門家」ではない可能性のある関係者が含まれることを念頭に、各々の関係主体に何が求められているか、読んで理解できるものとする。

○重要インフラ防護能力の維持・向上、とりわけ対策途上や中小規模の重要インフラ事業者等による実効的かつ自主的な取組に資するPDCAサイクルを明確化する。

○環境変化に対して柔軟に対応できるよう、重要インフラ事業者等におけるリスクマネジメントの重要性と導入の必要性に関して具体的に記載する。

○重要インフラ事業者等が把握すべき階層化された規程類をパッケージ化し、異動の激しい関係者間でも引き継ぎが容易になる構造・内容とする。

○行動計画策定後も、刻々と変化する環境に適切に対応し、適切な情報収集・提供を継続的に行うことを可能とするための広報公聴活動を一層充実させる。

課題２　刻々と変化する社会環境や技術環境、年々深刻化している脅威に関して、適切かつ迅速に対応できる方策が十分に講じられていない懸念があるが、これらの環境変化や脅威に適切に対応するためにどのような取組が官民双方に必要になるのか。また、関係主体として追加すべき者の有無を検証すべきではないか。

＜方向性＞

○サイバー空間関連事業者のうち必要な者も関係主体に加え、情報共有を更に充実させる。

○サイバー空間での重要インフラ事業者等の活動が、標的にされたり、踏み台とされたりする可能性があることを認識し、こうした弱点について相応の責任が生じ得ることに関して一層の自覚を促す。

○個々の重要インフラ分野、更には重要インフラ事業者等における脅威や脆弱性がそれぞれ異なること、また、社会環境や技術環境が刻々と変化することを認識し、複数の分野に及ぶ優先度の高いリスク源[4]についての調査や新しい技術・システム等の中長期的な変化の継続的な調査を実施する。

課題３　ＩＴ障害発生時の対応については、関係主体において様々な取組が開始されている一方、重大なＩＴ障害等が発生した際の対処及びその体制（官民間、官官間）が十分整理されていない懸念があるが、このような重大なＩＴ障害発生時の官民各機関における、共有・連絡すべき情報の整理、各々の対応の明示及び各機関間の連携体制の強化が必要ではないか。

＜方向性＞

○関係主体が実施する演習・訓練間の連携を通じて、当該演習・訓練等の効果を高めていく。

○大規模ＩＴ障害対応時、当該事態が重要インフラ事業者等にとって特別な警戒を要するものであると認知するメカニズムを構築するとともに、平時（大規模ＩＴ障害対応時以外の状態）における対応体制に誰がどう追加されるのかを可能な限り明確化する（なお、事態発生時に全く新しい体制を立ち上げることは現実的ではない。）。

[4] 「JIS Q 31000:2010」によれば、「それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素。」と定義されている。

5. 重要インフラの範囲の見直しについて

本行動計画の策定に当たっては、第２次行動計画において10分野と規定されている重要インフラの範囲の妥当性について検証し、新たな分野の追加について検討を行った。

なお、サイバーセキュリティ戦略[5]において検討することとされている重要インフラの範囲等については、環境変化に応じて、関係者との調整を踏まえつつ、引き続き見直しを行っていく。

5.1 検討結果

第２次行動計画において重要インフラと位置付けられていないが、既存の重要インフラ分野と同等にＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼし得る分野の位置付け等、第２次行動計画における重要インフラの範囲の妥当性に関して、東日本大震災発災時における対応等これまでの知見を踏まえた検証を行い、図表１に示すとおり新たに重要インフラとして追加する必要があると認められる分野を特定した。

図表１　重要インフラの範囲に関する検討結果

区分	視点・必要性	分野
当該分野が有する情報システムが障害に至った場合の影響を考慮して追加する分野	処理するサービス提供の価値及び規模	クレジット
	制御が困難な状態において生じ得るリスクの大きさ	化学、石油
既存の重要インフラ分野における情報システムに与える影響を考慮して追加する分野	既存の重要インフラ分野との間での相互依存性	石油 （再掲）

これにより、本行動計画における重要インフラ分野は、「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）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の13分野となった。

なお、追加分野が重要インフラに参加するに当たっては、当該追加分野がなぜ重要インフラに指定されるのか、参加に見合うメリットがあるのか、といった観点での疑問を払しょくし、自らが活動することの必要性に関する理解を醸成することが重要である。

追加分野を所管している省庁及び情報共有体制の要となるセプター事務局候補と想定される業界団体に対しては、上記観点についての説明を行い、重要インフラへの参画について合意を得ており、当該業界団体においては、対象となる重要システムやサービス維持レベルの特定、セプター設立の準備等を行っている。

[5] ２．基本的な方針（3)各主体の役割 ②重要インフラ事業者等の役割（P.20）を参照。

5.2 既存の重要インフラ分野と追加分野との関係

情報共有体制は、2007年度の構築から７年が経過しており、既存の各セプターは、情報セキュリティ対策の経験値を有するほか、業務性質等から独自色を有している。

こうした中で、追加分野が新規セプターとして加入した場合、取組が進んでいる既存セプターの活動に委縮してしまう懸念があることから、内閣官房は、重要インフラ分野内の他重要インフラ事業者等や、他重要インフラ分野の重要インフラ事業者等との連携の充実が重要であることを念頭に置いて追加分野への助言を行うことが必要である。また、セプターカウンシルにおいても、相互扶助の精神で追加分野のセプターに助言を行い、重要インフラ全体の防護能力の維持・向上を図ることが期待される。

6. 本行動計画策定に当たっての検討結果

前節までに抽出した課題及び整理した方向性を踏まえ、本行動計画策定に当たっては、サイバーセキュリティ戦略と整合する第２次行動計画の基本的骨格を維持するが、個別の施策やその実施体制を見直し、必要な補強・改善を行った上で、図表２に示す施策群の構成とすることとした。

図表２　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２次行動計画の施策群との対応	第２次行動計画からの補強・改善の方向性
１．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	○他施策の結果を指針本編・対策編に反映するプロセスの明示 ○指針による成長モデル等の訴求及び対策の実情の調査
２．情報共有体制の強化	「[2] 情報共有体制の強化」を基本的に踏襲	○新たな関係主体を含めた情報共有体制における各関係主体の位置付けの見直し及び関係主体間の関係の再整理 ○サイバー攻撃関係情報の増加を踏まえた共有すべき情報（脅威の類型等）の見直し ○平時における対応を念頭に置いた大規模ＩＴ障害対応時の事案対処体制の明確化
３．障害対応体制の強化	「[4] 分野横断的演習」を整理	○重要インフラ関係の演習・訓練の全体像を把握した上でＩＴ障害対応体制の総合的な強化 ○新たな関係主体との連携を念頭に置いた分野横断的演習の質的改善
４．リスクマネジメント	「[3] 共通脅威分析」を「[5] 環境変化への対応」の一部と統合した上で整理	○環境変化等に応じて生じる複数分野において大きな影響を生じ得るリスク源、将来的に多大な影響が予想される環境変化についての中長期的な調査の実施 ○重要インフラ事業者等が自らの状況を正しく認識し、活動目標を主体的に定めるに当たって必要となるリスクマネジネントの訴求
５．防護基盤の強化	「[5] 環境変化への対応」を「[3] 共通脅威分析」と統合される部分を除いた上で整理	○広報公聴、国際連携に加え、関連する国際標準・規格、参照すべき規程類の整理、活用方法の提示を追加

なお、行動計画策定後に環境が大きく変化した場合でも適切に対応できるようにするため、環境変化を継続的に監視して得られる情報から脅威を特定し、柔軟に対応できる体制を構築する必要がある。さらに、従来重点が置かれていた未然防止のみならず、障害対応体制の強化に係る取組を充実するとともに、平時から大規模ＩＴ障害対応時へシームレスに移行できるものとすることが重要である。

Ⅱ．本行動計画の要点

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基本的な考え方、③重要インフラ事業者等・政府機関・情報セキュリティ関係機関等の関係主体の在り方、その中でも④重要インフラ事業者等の経営層に期待する在り方を以下に示す。

①「重要インフラ防護」の目的

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する。

②基本的な考え方

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

－重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。

－政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。

－取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

③関係主体の在り方

－自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。

－ＩＴ障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、ＩＴ障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

④重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

－上記の目的達成に当たっての情報セキュリティを中心とするリスク源の認識。

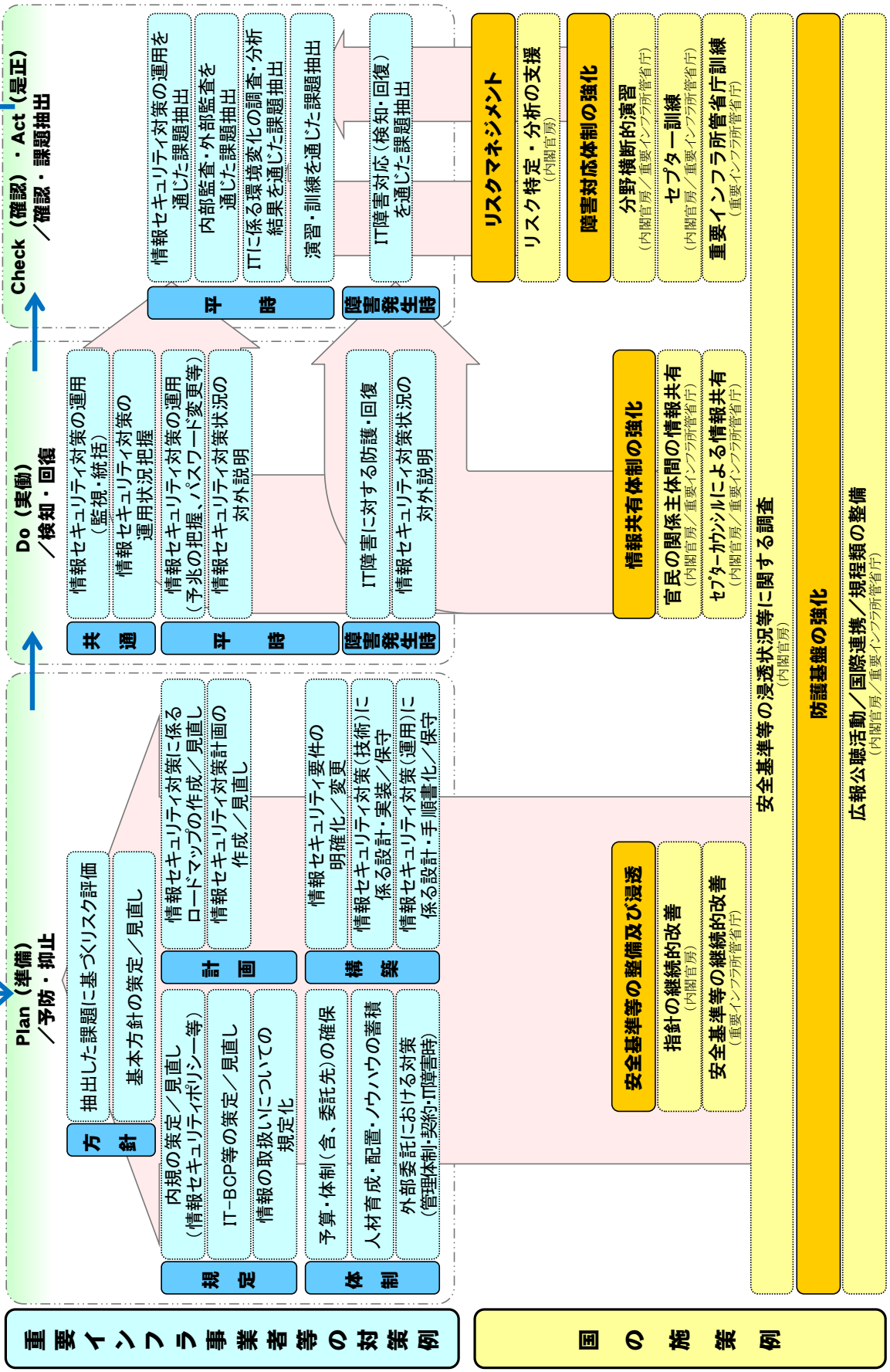
－上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。

－システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営資源の継続的な確保。

－システムの運用状況の把握等を通じた当該方針の実行の有無の検証。

－演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の検証及び改善策の有無の検証。

図表３　「重要インフラ事業者等の対策例」と各対策に関連する「国の施策例」



Ⅲ．計画期間内に取り組む情報セキュリティ対策

1．安全基準等の整備及び浸透

本行動計画期間においては、内閣官房は、重要インフラ防護能力の維持・向上を目的に、重要インフラ事業者等のPDCAサイクルとの整合及び他施策との連携を強化した指針改定及び調査運営の見直しを行う。

また、重要インフラ事業者等は、情報セキュリティ対策の重要性に鑑み、その対応においてはPDCAサイクルに沿った継続的かつ着実な実施に取り組む。

1.1 指針の継続的改善

重要インフラ防護能力の維持・向上、とりわけ対策途上や中小規模の重要インフラ事業者等による実効的かつ自主的な取組に資することを目的に、内閣官房は、指針本編・対策編の見直しを2014年度に行う。

具体的には、重要インフラ事業者等のPDCAサイクルに沿った情報セキュリティ対策の項目を整理するとともに、本行動計画の他施策から得た知見等を追加項目として採録する。

また、重要インフラ事業者等が情報セキュリティ対策を実施する際の優先順位付け、対策の段階的な追加及び予防的対策と事後的対策のバランスに係る考え方を成長モデルとして例示する。

さらに、重要インフラ事業者等における段階的・継続的な対策の強化に不可欠な方針化、規定化、計画化、体制化・人材育成及びシステム構築に係る重要インフラ事業者等の経営層の在り方の重要性を訴求する。

なお、2015年度以降、年度ごとに社会動向の変化及び新たに得た知見を必要に応じて公表し、また、指針本編・対策編の改定は３年に１度又は必要に応じて実施する。

1.2 安全基準等の継続的改善

各重要インフラ事業者等の対策を通じ、当該重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・向上を目的に、重要インフラ所管省庁及び重要インフラ事業者等は、対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。

具体的には、情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及びＩＴ障害対応から課題を抽出し、リスク評価を経て、安全基準等の継続的改善に取り組む。

なお、安全基準等の検証に際しては、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。

1.3 安全基準等の浸透

重要インフラ事業者等における安全基準等の浸透状況の把握を目的に、内閣官房は、重要インフラ事業者等の対策状況を調査する。加えて重要インフラ事業者等による実効的かつ自主的な取組に資することを目的に、本調査への回答が自ずと対策状況のセルフチェックにつながるよう調査運営を見直す。

調査に係る具体的な取組としては、より具体的な対策状況を確認し得る調査項目を追加するとともに、調査対象の拡張の下、浸透状況が良好な重要インフラ事業者等を対象とした経年調査を通じて対策状況の退化を検知し得る項目を追加する。

調査運営の見直しに係る具体的な取組としては、調査票の構成を重要インフラ事業者等の対策プロセスに沿って整理し、重要インフラ事業者等にとって強化対象の対策及びプロセスが明示的になるように取り組む。

加えて、アンケート方式による本調査の補完を目的に、内閣官房は、重要インフラ事業者等へ往訪調査を行う。

往訪調査に係る具体的な取組については、往訪による面会にてアンケート方式の調査項目を掘り下げたヒアリングを通じて、具体的な対策状況に係る課題抽出及び良好事例の収集を行う。

なお、アンケート及び往訪調査にて得た調査結果については、原則、年度ごとに公表するとともに、得た改善課題については本行動計画の各施策に連携する。

また、調査項目については、経年調査を損なわない程度に柔軟な変更を行うことを可能とする。

2. 情報共有体制の強化

重要インフラを取り巻く社会環境や技術環境は刻々と変化する中、重要インフラの情報セキュリティ対策の有効性を保ち続けるには、これらの環境変化を的確に捉えた上で情報セキュリティ対策への反映が必要である。また、サイバー攻撃の複雑・巧妙化に伴い、情報セキュリティ対策の水準の向上、サイバー攻撃への対応能力の向上はますます重要になっている。

「I.2. 重要インフラ防護の目的の明確化」における基本的な考え方で述べたとおり、情報セキュリティ対策は一義的に重要インフラ事業者等が自らの責任において実施するものではあるが、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは、多様な脅威への対応が十分であることを確認することは難しい。このため、分野内、分野間あるいは官民間の情報共有を行うことで連携して、必要な情報セキュリティ対策に取り組むことが重要である。

これらの状況を踏まえ、本行動計画期間において、内閣官房は、追加された分野、関係主体を含む情報共有体制を運用し、情報共有を更に促進するとともに、重要インフラ事業者等による情報共有活動の更なる活性化を図る。

2.1 本行動計画期間における情報共有体制

本行動計画策定に際し、大規模ＩＴ障害対応時における情報共有体制の強化に向けて、防災の観点から防災関係府省庁を追加するとともに、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設計・構築・運用・保守に携わるシステムベンダー、情報セキュリティ対策を提供するセキュリティベンダー及び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からなるサイバー空間関連事業者を追加した。追加後の体制については「別紙４－１　情報共有体制（平時)」及びその延長線上にある「別紙４－２　情報共有体制（大規模ＩＴ障害対応時)」に表した。

また、追加した新たな分野を含め、重要インフラ分野の重要システム及びサービス維持レベルを見直した。その結果については「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」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」に表した。

本行動計画期間中、関係主体は、各々の位置付け・役割に基づき情報共有体制を運用する。なお、サイバー空間関連事業者においては、脆弱性情報の共有やサイバー攻撃等に起因するＩＴ障害発生時における被害拡大の防止等、情報セキュリティの確保に必要に応じて取り組むことが期待される。

2.2 情報共有の更なる促進

共有すべき情報の整理については、「ＩＴ障害の未然防止」、「ＩＴ障害の拡大防止・迅速な復旧」、「ＩＴ障害の原因等の分析・検証による再発防止」の３つの側面から、政府機関や重要インフラ事業者等の各関係主体に応じて共有すべき情報の抽出と整理を行うことが重要である。

本行動計画策定に際し、内閣官房は、これら３つの側面を踏まえ、ＩＴ障害の未然防止を含む重要インフラ防護に資することを目的に、平時及び大規模ＩＴ障害対応時の情報共有体制にて用いる情報連絡・情報提供について、「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」の見直しを行った。

具体的には、「別紙３　情報連絡における事象と原因の類型」においては、ＩＴ障害の迅速かつ正確な状況把握を目的に、情報セキュリティのＣ・Ｉ・Ａ[6]の観点に基づく事象[7]項目の見直し及び新たな脅威等を踏まえた原因項目の詳細化を行った。「別添：情報連絡・情報提供について」においては、分野間における情報共有頻度の格差解消を目的に、ＩＴ障害の予兆情報の取扱い等、情報連絡の対象の明確化を行った。

関係主体間でＩＴ障害の事象や原因等に関する情報共有を行うことで、重要インフラ事業者等における運用や対策等の確認に活かされ、ＩＴ障害の未然防止につながることが期待されることから、本行動計画期間においては、内閣官房は、見直しを行った情報共有体制の下、関係主体との間で別添に従って情報連絡・情報提供を行い、情報共有の連携、促進を図る。また環境変化等が生じた場合には、適宜その見直しを図る。

2.3 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活動に取り組むとともに、CSIRT[8]等のＩＴ障害対応体制を構築・強化することが期待される。また、セプターにおいては、第２次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

[6] 機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability）を指す。

[7] 情報セキュリティ事象（Information Security Event）とは、「ISO/IEC 27000:2013」によれば、「システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているものをいう。」と定義されている。

[8] Computer Security Incident Response Team。情報システムに情報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、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。

（PoC[9]）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ＩＴ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。

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[10]。

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。

2.4 情報共有体制における各関係主体の役割

情報共有体制については、平時の情報共有体制の延長線上に大規模ＩＴ障害対応時の情報共有体制を構築しており、大規模ＩＴ障害対応時における各関係主体の役割も平時の役割の延長線上にある。

平時と大規模ＩＴ障害対応時における情報共有の全体像については、「別紙４－１　情報共有体制（平時）」及び「別紙４－２　情報共有体制（大規模ＩＴ障害対応時）」に示すとおりであり、各関係主体の役割は以下のとおりである。

2.4.1 平時の情報共有体制における各関係主体の役割

平時の情報共有体制における関係主体が行う情報共有は次のとおり。

(1) 重要インフラ事業者等

ＩＴ障害やサイバー攻撃に係る情報共有は所属するセプターにおいて行うことを基本とする。また、必要に応じてＩＴ障害やサイバー攻撃に係る情報連絡を重要インフラ所管省庁に行う。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に通報を行う。

(2) セプター

セプターカウンシルや重要インフラ所管省庁、情報セキュリティ関係機関と連携し、相互にＩＴ障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の共有を行う。

---

[9] PoC：Point of Contact。

[10] 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。

(3) 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はなく、独立した会議体である。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。

(4) 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ＩＴ障害やサイバー攻撃に係る情報連絡を内閣官房（NISC）に行う。また必要に応じて所管するセプターに行う。内閣官房（NISC）から受領したＩＴ障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の情報提供を所管するセプターに行う。

(5) 内閣官房（NISC）

重要インフラ所管省庁、情報セキュリティ関係省庁、あらかじめ連携を要請した情報セキュリティ関係機関及びサイバー空間関連事業者と相互にＩＴ障害やサイバー攻撃に係る情報、復旧手法等に関する情報共有を行う。

2.4.2　大規模ＩＴ障害対応時の情報共有体制における各関係主体の役割

災害やテロ等に起因する大規模ＩＴ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ものとされている。事態が悪化し、大規模ＩＴ障害対応に移行した際、事案対処省庁、防災関係府省庁及び内閣官房における情報の一元化が重要であることから、次のような情報共有体制を敷く。

(1) 内閣官房（事態対処・危機管理担当）

内閣官房（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、内閣官房（NISC）と相互に情報共有を行う。

(2) 内閣官房（NISC）

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、情報セキュリティ関係省庁、あらかじめ連携を要請した情報セキュリティ関係機関及びサイバー空間関連事業者と相互に各種関連情報、復旧手順方法等に関する情報共有を行う。

(3) 重要インフラ所管省庁

平時の役割に加え、必要に応じて大規模ＩＴ障害対応時の体制に協力する。

(4) 重要インフラ事業者等

平時の役割に加え、各重要インフラ事業者等が定める大規模ＩＴ障害対応時の体制を構築する。

⑸ セプター

平時の役割に加え、各セプターが定める大規模ＩＴ障害対応時の体制を構築する。

⑹ セプターカウンシル

平時の役割に加え、セプターカウンシルが定める大規模ＩＴ障害対応時の体制を構築する。

3. 障害対応体制の強化

本行動計画期間においては、第２次行動計画における分野横断的演習に加え、ＩＴ障害対応に関する能力向上及び検証を目的とする各種演習・訓練をＩＴ障害対応体制の強化策の一環に位置付け、これらの演習・訓練の相互の関係を把握し、連携を行うことで、重要インフラ全体の防護能力の維持・向上を図る。

その中で、分野横断的演習については、これまでの実績を踏まえ、引き続き重要インフラ分野のＩＴ障害対応体制を強化する中核的な取組としての位置付けの充実を図る。具体的には、分野横断的演習がセプター訓練及び重要インフラ所管省庁が実施する他の演習・訓練と相互に連携・補完し、相乗効果を発揮できるよう、各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の体制を強化する。

また、被害の拡大防止の観点から迅速な事案対処等も必要となることから、関係主体は重要インフラ事業者等のＩＴ障害対応能力を高めるための対策又は支援策について、関係主体間の連携強化と役割分担の明確化を図りつつ必要に応じて実施する。

3.1 分野横断的演習の改善

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への分野横断的演習成果の浸透を通じた重要インフラ防護能力の維持・向上に資することを目的に、我が国唯一の取組である分野横断的演習を改善しつつ引き続き実施する。

その際、第２次行動計画で掲げた３つの目標である「分野横断的な脅威に対する共通認識の醸成」、「他分野の対応状況把握による自分野の対応力強化」及び「官民の情報共有をより効果的に運用するための方策の獲得」を踏襲し、障害対応体制の強化に資するよう、蓄積した運営手法や成果を用いて分野横断的演習の充実を図る。

3.1.1 分野横断的演習の企画立案に係る質的改善

本行動計画期間において、内閣官房は、分野横断的演習の改善を継続的に図ることを目的として、演習運営を通じて得た知見・課題、他施策から得られた課題及びＩＴ障害を引き起こす要因であるリスク源に係る最新動向を演習に取り込むことに加え、重要インフラ事業者等が保有するＩＴシステムの維持に密接に関連する関係主体の参画も視野に入れた演習の企画立案を検討する。

また、内閣官房は、演習成果が重要インフラ事業者等の情報セキュリティ対策並びにＩＴ障害時の早期復旧手順及びIT-BCP等に係る検証の更なる強化に資することを目的に、演習結果の評価プロセスの改善に向けた検討を行う。

加えて、演習を通じて得た知見・課題を基礎資料として本行動計画の他施策に提供する。

3.1.2　重要インフラ全体への分野横断的演習の成果の浸透

第２次行動計画期間中、演習参加者数は着実に増加し、演習を有意義と評価する参加者が８割を超えており、演習未経験者への新規参加を促すことで、重要インフラ分野における演習成果の浸透を目指す。一方、参加者拡大には一定の限界があることから、更なる重要インフラ全体への演習成果の普及・浸透を行うためには、新規参加の促進に加え、演習に参加していない重要インフラ事業者等を対象とした取組も必要である。

そのため、内閣官房は、経営層の理解増進にも寄与し得る演習のメリットについての説明資料の作成・公表及び重要インフラ分野全体への訴求を通じて、各重要インフラ分野・重要インフラ事業者等内での演習実施を促進する。

また、個別の重要インフラ事業者等による演習実施の支援に資することを目的に、これまでの演習において蓄積してきた実施・評価・助言手法の整備及びその共有化の実現に向けた検討を進める。

3.1.3　物理的な要因によるＩＴ障害への対応

現実のＩＴ障害対応には、物理的な要因によるＩＴ障害も想定され、その状況によっては、各府省庁や各重要インフラ事業者等の情報セキュリティ部門だけではなく、防災・危機管理部門との情報共有を要する可能性がある。

今後、内閣官房は、分野横断的演習において当該ＩＴ障害への対応も検証対象とする場合、シナリオ作成等において必要に応じ、防災関係府省庁等の知見の活用及び重要インフラ所管省庁や重要インフラ事業者等の防災・危機管理担当者の協力の在り方について検討する。

3.1.4　重要インフラ所管省庁との連携

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・訓練は、内閣官房が実施する分野横断的演習と期待する効果が異なるが、分野横断的演習と相互に連携・補完しつつ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。

このことから、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の対応能力の向上を目的に、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について検討する。

なお、検討項目の一例として、分野横断的演習では重要インフラ事業者等間やセプター、重要インフラ所管省庁、内閣官房等との情報共有・連携対応を主な検証対象とし、重要インフラ所管省庁の演習では重要インフラ事業者等における実機システムを用いたＩＴ障害対応手順や各分野の連絡体制を確認・検証対象とすることが考えられる。

3.2 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。

実施に際しては、セプターからの要望も取り込みながら訓練内容を充実しつつ、ＩＴ障害対応を念頭においたより実態に即した情報共有訓練の実現を目指す。

また、セプター訓練は多くの重要インフラ事業者等の参加が期待できることから、分野横断的演習における検証内容を踏まえた状況設定を行う等、必要に応じてセプター訓練と分野横断的演習との連携を検討する。

4. リスクマネジメント

重要インフラ事業者等は、国民に対する重要インフラサービスの安定的供給や事業継続等といった事業目的の達成に向け、情報セキュリティの確保に係る目的を確立し、組織内へと展開する必要がある。

一方、重要インフラを取り巻く社会環境や技術環境等が刻々と変化する中、重要インフラにおいて守るべき情報システム及びその中で利活用されるデータのサイバー空間への依存度が一層高まっている。

このような状況の下、サイバー空間に潜む脅威や脆弱性等といったリスク源に起因するＩＴの不具合による影響は甚大化しており、ひとたびＩＴの不具合が発生すれば、重要インフラサービスの提供が困難となる可能性がある。

このことから、重要インフラ事業者等においては、個別の対策等に代表されるＩＴの不具合への対症療法のみならず、事業目的の達成に向け、情報セキュリティに係るリスク源から導き出されるリスクに対する包括的なマネジメントを行う必要性が高まってきている。なお、本行動計画において、リスクとは、目的に対する不確かさの影響を指すものとする。

このため、重要インフラ事業者等におけるリスク評価手法等に基づく情報セキュリティ対策の重点化を目的に、第２次行動計画の「共通脅威分析」及び「リスクコミュニケーションの充実」(「環境変化への対応」の一施策）を包括的に捉え直し、各重要インフラ事業者等が主体的に行うリスクマネジメントに係る施策を新たに実施する。

4.1 リスクマネジメントの標準的な考え方

リスクマネジメントは各重要インフラ事業者等がそれぞれにおいて主体的に実施するものである。一方で、各関係主体間において共通的なリスクマネジメントの考え方や用語による情報共有及び議論がされない状態では、本行動計画における各種取組が、各重要インフラ事業者等のリスクマネジメントにおいて効果的に活かされない可能性がある。

このことから、本行動計画期間においては、各関係主体は、国際的にも標準的なリスクマネジメントの考え方やそこで利用される情報セキュリティに関わる用語の定義等を利活用することが望ましい。

具体的には、内閣官房は、内閣官房が実施する施策や各種関連資料において、以下の図表４に示す枠組み[11]を軸とした考え方や枠組みの中で利用される用語の定義等を可能な限り適用する。

[11] 「JIS Q 31000:2010」やENISA(欧州 ネットワーク情報セキュリティ庁)が公表している「Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools」を参照。

図表４　標準的なリスクマネジメントのプロセス（例）

<table>
<tr><td rowspan="8">リスクマネジメント</td><td colspan="2">組織の状況の確定</td></tr>
<tr><td colspan="2">リスクアセスメント</td></tr>
<tr><td></td><td>リスク特定</td></tr>
<tr><td></td><td>リスク分析</td></tr>
<tr><td></td><td>リスク評価</td></tr>
<tr><td colspan="2">リスク対応</td></tr>
<tr><td colspan="2">リスクの受容</td></tr>
<tr><td colspan="2">リスクコミュニケーション及び協議</td></tr>
<tr><td colspan="2">モニタリング及びレビュー</td></tr>
</table>

また、重要インフラ事業者等は、内閣官房が作成する手引書等[12]を自組織のリスクマネジメントにおいて利活用することが期待される。

なお、本施策は、各関係主体に国際標準への準拠を求めるものではなく、本施策において内閣官房が適用する考え方や用語の定義等を参照することで、重要インフラ事業者等が既に自組織において実施しているリスクマネジメントの更なる最適化及び情報セキュリティ対策の水準の向上に資することを目的としている。

4.2　リスクマネジメントの支援

リスクマネジメントは、基本的に各重要インフラ事業者等が自組織に最適化して取り組むものである。一方、各重要インフラ事業者等によるリスクマネジメントのうち、特にリスクアセスメント[13]やリスクコミュニケーション及び協議[14]においては、重要インフラ分野横断的な調査・分析及び意見交換等といった自組織だけでの取組が容易ではないものも存在する。

このため、内閣官房は、こうした分野横断的なものについて以下のとおり取組を行い、その調査・分析結果の共有や意見交換の機会の提供等により、重要インフラ事業者等のリスクマネジメントの支援を行う。

4.2.1　リスクアセスメント

内閣官房は、重要インフラ分野を取り巻くＩＴに係る環境の変化について、情報セキュリティの視点から主な設備・技術等の実態・動向調査及び主な設備・技術等に内在するリスク源やそこから導き出される新たなリスク（以下「新たなリスク源・リスク」という。）の分析を行う。

また、重要インフラ分野において生じたＩＴ障害等の影響波及に係る解析を継続し

[12] 「5.3.3 国際基準等を重要インフラ防護に適用する場合の手引書等の整備」において、国際標準等を読み替えた手引書等を必要に応じて取りまとめることとしている。

[13] 「JIS Q 31000:2010」によれば、「リスク特定、リスク分析及びリスク評価のプロセス全体。」と定義されている。

[14] 定義は「4.2.2 リスクコミュニケーション及び協議」を参照。

て行う。

具体的には、各調査・分析の効率、他施策との相互反映等の観点も踏まえ、以下のとおりとし、その調査・分析結果については重要インフラ事業者等に提供する。

(1) 環境変化調査

第２次行動計画中に実施した環境変化調査においては、クラウド、スマートフォン・タブレット端末及びリモートメンテナンスは重要インフラ分野において導入率が高いことが明らかになり、BYOD[15]やビッグデータは今後の導入拡大が想定される結果となった。

本行動計画において、内閣官房は、これら変化に加え、M2M、スマートコミュニティ等、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・システムも環境変化調査の対象とした実態調査及び新たなリスク源・リスクの分析を行う。また、その実施に際しては、時間経過や環境変化の顕在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、年度をまたいで継続的に行う。また、例えば制御系、勘定系、情報系等一定の分野に共通するもので全分野に及ばずとも影響が大きい新たなリスク源・リスクについても当該分析の対象とする。

なお、本調査にて新たなリスク源・リスクが明らかになった場合及び新たな重要インフラ分野が追加となった場合、必要に応じて、それらの分野共通性の分析を詳細調査と位置付けて行う。

(2) 相互依存性解析

各重要インフラ分野におけるＩＴ利用が進展し、分野間の相互依存関係が増大する中、重要インフラ分野における相互依存性の把握は、ＩＴ障害等が生じた際の効率的な復旧対策において重要である。

このことから本行動計画において、内閣官房は、環境変化に伴う相互依存性の変化及び新たな重要インフラ分野の追加が生じた場合、第１次行動計画及び第２次行動計画における解析結果をもとに再調査・解析を行うことを含め、相互依存性解析を継続的に行う。

また、各重要インフラ分野におけるＩＴ依存度は相互依存性解析に密接に関連することから、ＩＴ依存度についても詳細調査として定期的に調査を行う。

なお、新たな重要インフラ分野が追加となった場合、相互依存性解析に合わせてＩＴ依存度の調査を行う。

4.2.2　リスクコミュニケーション及び協議

リスクコミュニケーション及び協議とは、「リスクの運用管理について、情報の提供、共有又は取得、及びステークホルダとの対話を行うために、組織が継続的に及び

[15] Bring Your Own Device。企業等において、従業員が私用で使っているスマートフォン等の情報端末から企業等の情報システムにアクセスし、必要な情報を閲覧・入力する等、私物の情報端末を業務で利用すること。

繰り返し行うプロセス。」と定義[16]されている。

内閣官房は、関係主体間による分野横断的な情報や意見の交換の充実に資することを目的に、重要インフラ防護に関連する者によるリスクコミュニケーション及び協議の支援を行う。

具体的には、セプターカウンシル及び分野横断的演習を利活用し、各関係主体と協力しつつ、情報や意見の交換の機会を提供する。

また、これにより、本施策における調査・分析に必要となる情報の収集を図る。

4.3 本施策と他施策による結果の相互反映プロセスの確立

内閣官房は、本行動計画の他施策に資することを目的に、本施策における調査・分析結果を基礎資料として他施策に提供する。

また、他施策の実施結果から顕在化した分野横断的な対策を要する新たなリスク源・リスクを本施策の調査・分析の対象とし、必要な調査・分析を行う。

[16] 「JIS Q 31000:2010」を参照。

5. 防護基盤の強化

重要インフラを取り巻く社会環境や技術環境等が刻々と変化する中、情報セキュリティ対策の有効性の確保に向けては、図表３で示した通り、基本方針の策定、人材育成・配置、情報セキュリティ対策状況の対外説明、ＩＴに係る環境変化に伴うリスク源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、第２次行動計画に引き続き、他の関係主体と協力しつつ広報公聴活動及び国際連携を行うことに加え、関係主体が適時に適切な関連規程類を参照し得るよう、重要インフラ防護に係る関連規程類、情報セキュリティ対策に関する国際基準等についての手引書等を整備する。

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 広報公聴活動

ＩＴ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情報セキュリティ対策の水準の向上のみならず、国民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、各関係主体は、国民による冷静な対応に資することを目的に、行動計画に基づく取組の広報を通じて、引き続き国民への説明責任を果たすよう努める。

また、重要インフラ事業者等による情報セキュリティ対策の水準の向上には、本行動計画に基づく取組への広範な協力・支援を得ることも重要である。

内閣官房は、Webサイトやニュースレターを通じた広報及び講演等を通じた公聴活動を、引き続き行う。その際、広報の構成については、本行動計画の取組を広く認識・理解し得るように努める。

5.2 国際連携

サイバー空間を取り巻くリスクは、ボーダレスに進行しており、国境のないグローバルなリスクへの一層の対応が求められるとともに、我が国だけではなく国際的な情報セキュリティ対策の水準の向上のため、キャパシティビルディング（能力向上）への積極的な寄与が求められている。

このため、内閣官房は、重要インフラ所管省庁及び情報セキュリティ関係機関と連携して、引き続き、欧米・ASEANやMeridian等の二国間・地域間・多国間の枠組みの積極的な活用を通じて国際連携の強化を行う。その際、国際連携にて得た事例、ベス

トプラクティス等を国内の関係主体に積極的に提供するよう努める。

加えて、重要インフラ事業者等においても、情報セキュリティ対策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・多面的な国際連携に取り組むことが期待される。

5.3 規格・標準及び参照すべき規程類の整備

重要インフラの情報セキュリティ対策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等は重要である。この規程類の整備等についての内閣官房の取組は、以下のとおりである。

5.3.1 重要インフラ防護に係る関連規程集の発行

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に、関係主体が共通に参照するサイバーセキュリティ戦略、本行動計画等の各関連文書を合本し、「重要インフラ防護に係る規程集」として発行する。

5.3.2 重要インフラ防護に係る関連規格の体系的な可視化

内閣官房は、重要インフラ防護に係る関連規格について、適切な版を必要なときに参照できるようにするため、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を整理し、その結果を明示する。

5.3.3 国際基準等を重要インフラ防護に適用する場合の手引書等の整備

重要インフラを取り巻く社会環境や技術環境等が刻々と変化する中、その変化に迅速かつ柔軟に対応するためには、「5.3.2 重要インフラ防護に係る関連規格の体系的な可視化」にて整理した結果から抽出した適切な関連規格、特に国際基準等の利活用が効果的な場合がある。

一方、上記の整理した結果に基づき一般論を記載する国際基準等を利活用しようとする場合、そのまま適用することが困難なものについては読み替え等を行うことが必要である。

内閣官房は、当該国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、他の関係主体との協力の下、必要に応じて、手引書等を取りまとめる。

なお、重要インフラ防護に係る国際的な手引書等が現存しないことを踏まえ、本施策で取りまとめた手引書等をASEAN各国及びISO等の国際規格に提案することによる国際貢献についても併せて検討する。

5.3.4 情報セキュリティに関する評価・認証制度の拡充

内閣官房は、検討が進む制御系機器・システム等の調達及び運用に係る国際標準に

則した評価・認証の導入の在り方について、他の関係主体との協力の下、制御系機器・システムの第三者認証制度の拡充を支援[17]する。

[17] 制御系機器・システムの第三者認証制度の導入に取り組んでいる、技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）とも協力して実施。

Ⅳ．関係主体において取り組むべき事項

本行動計画に示した情報セキュリティ対策の施策群は、重要インフラ事業者等が取り組むことが望ましい自主的な対策と、内閣官房を中心とした政府機関等において実施することが望ましい施策によって支えられる。各関係主体はそれぞれ以下の取組を基本として、情報セキュリティ対策を推進することが期待される。

1．内閣官房の施策

(1)「安全基準等の整備及び浸透」に関する施策

① 本行動計画の初年度及び必要に応じた指針の改定に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表。

② 必要に応じて社会動向の変化及び新たに得た知見に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表。

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を状況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の協力を得つつ、毎年、安全基準等の浸透状況等の調査を実施し、結果を公表。

(2)「情報共有体制の強化」に関する施策

① 平時及び大規模ＩＴ障害対応時の情報共有体制の運営を通じた更なる促進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 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。

④ 先進的なセプターの機能や活動の紹介。

⑤ セプターカウンシルに参加するセプターと連携しつつ、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。

⑥ 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。

⑦ 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、ＩＴ障害発生時に適時適切な情報提供を実施。

(3)「障害対応体制の強化」に関する施策

① 他省庁のＩＴ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。

② 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。

③ 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。

④ 分野横断的演習の改善策検討。

⑤ 分野横断的演習の機会を活用して、リスク分析の成果の検証並びに重要インフラ事業者等が任意に行うＩＴ障害発生時の早期復旧手順及びIT-BCP等の検討の状況把握等を実施し、その成果を演習参加者等に提供。

⑥ 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供。

⑦ 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。

(4) 「リスクマネジメント」に関する施策

① リスクマネジメントの標準的な考え方や定義等の利活用や国際標準等を読み替えた手引書等の提示による関係主体間の共通認識の醸成。

② 本施策における調査・分析による重要インフラ事業者等におけるリスクマネジメントの支援。

③ 本施策における調査・分析の結果を安全基準等に反映する基礎資料として提供。

④ セプターカウンシル及び分野横断的演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議を支援。

(5) 「防護基盤の強化」に関する施策

① Webサイトやニュースレターを通じた広報を実施。

② 講演等を通じた公聴活動を実施。

③ 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

④ 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

⑤ 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に、関係主体が共通に参照する関連文書を合本し、規程集を発行。

⑥ 関連規格を整理、可視化。

⑦ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、必要に応じて、手引書等を整備。

⑧ 制御系機器・システムの第三者認証制度の拡充を支援。

2. 重要インフラ所管省庁の施策

(1) 「安全基準等の整備及び浸透」に関する施策

① 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安全基準等の浸透状況等の調査に協力。

(2) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、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。

③ 重要インフラ事業者等からのＩＴ障害に係る報告の内閣官房への情報連絡。

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。

(3) 「障害対応体制の強化」に関する施策

① 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。

② 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。

③ 分野横断的演習への参加。

④ 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。

⑤ 分野横断的演習の改善策検討への協力。

⑥ 必要に応じて、分野横断的演習成果を施策へ活用。

⑦ 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。

(4) 「リスクマネジメント」に関する施策

① 本施策における調査・分析を必要とする対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供。

② 本施策における調査・分析の施策へ活用。

③ 重要インフラ事業者等のリスクコミュニケーション及び協議を支援。

(5) 「防護基盤の強化」に関する施策

① 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

② 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

③ 内閣官房と協力し、関連規格を整理、可視化。

④ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備。

⑤ 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援。

3. 情報セキュリティ関係省庁の施策

(1) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、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. 事案対処省庁の施策

(1) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、大規模ＩＴ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。

(2) 「障害対応体制の強化」に関する施策

① 重要インフラ事業者等からの要望があった場合、ＩＴ障害対応能力を高めるための支援策を実施。

5. 重要インフラ事業者等の自主的な対策として期待する事項

(1)「安全基準等の整備及び浸透」に関する対策

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、情報セキュリティ対策の実施や対策を実装するための環境整備を検討。

④ 情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及びＩＴ障害対応から課題を抽出し、リスク評価を経た安全基準等の継続的改善。

⑤ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。

(2)「情報共有体制の強化」に関する対策

① セプターカウンシル、セプター及び重要インフラ所管省庁と連携しつつ、情報共有体制の運用。

② ＩＴ障害発生時等に必要に応じて情報連絡を実施。

③ 攻撃手法及び復旧手法に関する情報等の収集。

④ 情報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。

(3)「障害対応体制の強化」に関する対策

① 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。

② 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。

③ 分野横断的演習への参加。

④ 分野横断的演習の改善策検討への協力。

⑤ 必要に応じて、自らのＩＴ障害発生時の早期復旧手順及びIT-BCP等への取組に対し、分野横断的演習成果を活用。

(4)「リスクマネジメント」に関する対策

① 自組織におけるリスクマネジメントを推進、強化。

② 本施策における調査・分析の結果として提供される基礎情報について自組織のリスクアセスメントへの活用。

③ 重要インフラサービスの情報セキュリティ対策に直接関係する関係主体間でのリスクコミュニケーション及び協議の充実。

④ 自らが単独で分析することが困難で、調査・分析する価値のある環境変化やリスク源を本施策における調査・分析の取組対象として提案。

⑤ 本施策における調査・分析の議論・検討に参画。

(5) 「防護基盤の強化」に関する対策

① 情報セキュリティ対策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。

② 内閣官房と協力し、関連規格を整理、可視化。

③ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備。

④ 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援。

6. セプターの自主的な対策として期待する事項

(1) 「情報共有体制の強化」に関する対策

① セプターカウンシル、重要インフラ事業者等及び重要インフラ所管省庁と連携しつつ、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則って重要インフラ事業者等への情報提供を実施。

③ 情報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。

④ セプターの機能強化・充実。

⑤ 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。

⑥ セプターカウンシルへの参加。

(2) 「障害対応体制の強化」に関する対策

① 情報疎通機能の定期的な確認。

② 重要インフラ事業者等の分野横断的演習への参加及び成果展開を支援。

③ 分野横断的演習への参加。

(3) 「リスクマネジメント」に関する対策

① 自セプターを構成する重要インフラ事業者等の自主的な取組を支援。

7. セプターカウンシルの自主的な対策として期待する事項

(1)「情報共有体制の強化」に関する対策

① 各セプターと連携しつつ、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)「障害対応体制の強化」に関する対策

① 必要に応じて分野横断的演習への参加。

8. 情報セキュリティ関係機関の自主的な取組として期待する事項

(1)「情報共有体制の強化」に関する対策

① 内閣官房と連携しつつ、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 情報共有を行う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の実施。

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)「障害対応体制の強化」に関する対策

① 分野横断的演習に必要となるＩＴ障害の事例等に関する情報を内閣官房に提供。

(3)「防護基盤の強化」に関する対策

① 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

② 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

9. サイバー空間関連事業者の自主的な対策として期待する事項

(1)「情報共有体制の強化」に関する対策

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、ＩＴ障害発生時に必要に応じて、積極的な情報連絡の実施。

Ⅴ．評価・検証と見直し

本行動計画の評価については、個々の取組がどのような結果をもたらしたのかという「結果（アウトプット）を測る視点」からの各年度における進捗状況の確認と、本行動計画における取組により社会が実際にどの程度理想とする将来像に近づいたのかという「成果（アウトカム）を測る視点」からの行動計画期間中における成果の確認といった２つの視点で取り組む。この際、進捗状況の確認は、可能な限り客観的な指標を用いることとし、また成果の確認は、本行動計画の目標、すなわち理想とする将来像に照らして行う。

なお、本行動計画における「検証」とは、指標を用いて各々の取組についてその進捗状況に係る客観的事実を確認することとする。

1．本行動計画期間の目標（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は、以下のようなものである。

○各関係主体の自覚に基づく自主的な取組はそれぞれの行動規範として浸透しており、その行動様式が情報セキュリティ文化を形成するようになっている。

○各関係主体間において、ＩＴ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るとともに、ＩＴ障害が発生した場合には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。

○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。また、多様な主体間でのコミュニケーションが充実し、ＩＴ障害の発生時に冷静に対処できるようになっている。

○こうした取組が行動計画として公表され、定期的に評価されるとともに必要に応じて適切に見直されている。

○これら各関係主体の取組が社会の持続的な発展を支えるものとして確実に定着している。

以降、具体化した将来像を記載する。

1.1 関係主体共通

関係主体共通の具体化した将来像は以下のようなものである。

○自らの置かれている状況を正しく認識し、自らの活動目標を主体的に定めている。

○各々必要な取組を進めており、これについて定期的に自らの対策・施策の進捗状況の確認を行っている。また、他の関係主体の活動状況を把握し、相互に自主的な協力をすることができる。

○ＩＴ障害発生時の対応において、ＩＴ障害の規模に応じて、誰がどのような情報

を集積しているか、誰とどのような情報を共有すべきか、また自らは何をなすべきかを理解している。

○自主的な対応に加えて、必要に応じて他の関係主体と連携を図り統制の取れた対応をとることができる。

1.2 重要インフラ事業者等

重要インフラ事業者等における具体化した将来像は以下のようなものである。

○「情報セキュリティガバナンス」に関する以下の事項が十分に浸透している。

－情報セキュリティ対策は単に情報システムの構築・運用の観点のみならず、企業経営の観点からも検討していること。

－システムの構築・運用と企業経営のそれぞれの責任者が適切に関与する体制を有すること。

－守るべき重要インフラサービスとサービス維持レベルを踏まえて、自らがなすべき必要な対策を理解していること。

－情報セキュリティ対策の対外的な説明に努めていること。

－情報セキュリティ対策の水準の向上のためには可能な限り情報共有を行うという姿勢が積極的に評価される価値観が醸成されていること。

－事業におけるＩＴ障害の発生は隠すべきものではなく、重要インフラ事業者等内の対策に取り組む関係者間で共有すべきものであるという認識を有していること。

○「課題抽出」、「リスク評価」及び「対策の改善」に関する以下の事項が十分に浸透している。

－本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、自らの対策の程度及び残存するリスクを認識していること。

－各種対策の進展や環境変化によるリスク源やＩＴ障害に係るリスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっていること。

－ＩＴ障害が発生した場合でも適切な対策を講じることが可能になっており、その結果として、ＩＴ障害が国民生活や社会経済活動に重大な影響を与えるリスクは可能な限り低減させることができていること。

－これらの取組が対策の継続的な改善の原動力のひとつとなっていること。

○「情報共有」に関する以下の事項が十分に浸透している。

－ＩＴ障害の発生状況等の情報を把握できており、必要に応じて当該情報を分野ごとのセプターやセプターカウンシルを通じて外部の関係主体と共有し、公式又は非公式の連携を行っていること。

1.3 内閣官房

内閣官房における具体化した将来像は以下のようなものである。

○より効果的な対策を進めるための総合調整機能を発揮している。本行動計画の施策群を通じて、情報セキュリティ対策に資する多様な情報が寄せられるようになっており、当該情報を踏まえて関係主体との連携を図っている。

○特に、重大なリスク源やＩＴ障害に係るリスクについての認識が得られ、その対処が重要インフラ事業者等だけでは困難な場合は、解決策の検討とその実現に向けた有機的連携及び調整を速やかに実施している。

2. 各年度における進捗状況の確認・検証を通じた対策・施策の継続的改善

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、本行動計画の進捗状況についての確認・検証を行う。継続的な改善においては、各関係主体がそれぞれの取組を通じて得た経験を関係主体全体で共有し、相互に取組の改善に活かせるようにすることを重視する。ＩＴ障害は回避すべきものであるが、ＩＴ障害を防いだ経験やＩＴ障害が発生した際に影響範囲を限定した経験は、それ自体を将来の糧として活かすべきものであることを認識することが重要である。

当然ながら、ＩＴ障害を発生させた当事者はその原因と責任の所在を把握し、自らの取組を改善するよう努めるべきものである。しかし、本行動計画の評価・検証においては、原因と責任を追及することに主眼を置くのではなく、むしろ様々な経験から将来の取組の改善に活かせる教訓を抽出し、これを各関係主体のそれぞれの取組の改善に役立てるようにすることを主眼とする。

3. 各年度における進捗状況の確認・検証の実施方法

各年度で行う「結果（アウトプット）を測る視点」からの確認・検証は、本行動計画に基づく個別の情報セキュリティ対策の施策に着目して行う。本行動計画に基づく情報セキュリティ対策の施策群は、いずれも複数の関係主体による多層構造をなしているため検証に用いる指標も多様なものが考え得るが、大別して重要インフラ事業者等による対策の総合的な確認・検証に用いる指標と、政府機関等による施策の確認・検証に用いる指標を設定する。この際、情報セキュリティ対策の施策群ごとの指標については、その数値自体の多寡、増減にとらわれるのではなく、その数値の意味するところを適切に解釈することが重要である。

これらの確認・検証は、情報セキュリティ政策会議が主管の下、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、重要インフラ専門委員会での審議を経て、情報セキュリティ政策会議に付議する。

また、個別の重要インフラ事業者等による自身の対策の確認・検証については、それが自主的なものであることに鑑み、基本的には重要インフラ事業者等自らが、各年度に行うことが望ましい。

3.1 重要インフラ事業者等による対策の総合的な確認・検証に用いる指標

重要インフラ事業者等は重要インフラサービスの安定的供給に一義的な責任を負うものとして、日々情報セキュリティ対策に取り組んでいる。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、情報セキュリティ対策の成果を客観的に検証することが重要である。

対策の総合的な確認・検証は、本行動計画の目標である「ＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を踏まえ、重要インフラ分野ごとのＩＴ障害の発生状況を確認・検証することとする。対象とする重要インフラサービスとサービス維持レベルは「別紙２　重要インフラサービスとサービス維持レベル」に示すとおりとする。具体的な指標は、内閣官房が認知したＩＴ障害事例の分野全体での数とする。

なお、個別の重要インフラ事業者等の対策が各々の経営判断に基づく自主的な対策を含むものである以上、重要インフラ事業者等ごと又は分野ごとのＩＴ障害の発生状況を比較して対策を評価することは不適当である。そのため、対策の評価は重要インフラ事業者等による自己評価によるものとし、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、可能であれば自己評価の実施状況を明らかにすることが望ましい。

3.2 政府機関等による施策の確認・検証に用いる指標

本行動計画の施策は「Ⅲ．計画期間内に取り組む情報セキュリティ対策」に示したとおりであるが、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである。本行動計画期間においては第２次行動計画にて用いた指標を踏襲しつつ、各施策の効果の検証方法を見直した。

施策の確認・検証は、それぞれの情報セキュリティ対策の施策ごとに、重要インフラ事業者等による情報セキュリティ対策への寄与を検証することとし、具体的な指標は以下のとおりとする。

3.2.1 安全基準等の整備及び浸透

「安全基準等の整備及び浸透」に期待される成果は、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことの実現に向けた、重要インフラ事業者等における各種対策の更なる充実と、その着実な実践である。そのため、指針と安全基準等の項目の充実と、重要インフラ事業者等の安全基準等に基づいた取組の確実な実施に着目した指標を設定する。

＜具体的な指標＞

○指針に採録した対策項目数

○安全基準等の浸透状況等の調査にて把握した安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の割合

○重要インフラ事業者等による指針への意見・要望

3.2.2 情報共有体制の強化

「情報共有体制の強化」に期待される成果は、最新の情報共有体制及び情報連絡・情報提供に基づく情報共有、並びに各セプター及びセプターカウンシルの自主的な活動の充実強化を通じて、重要インフラ事業者等が必要な情報を享受し活用できることである。そのため、整備された情報共有体制と共有された情報の充実に着目した指標を設定する。

＜具体的な指標＞

○内閣官房による情報連絡・情報提供の件数

○セプターカウンシルや分野横断的演習等の関係主体間の情報交換の開催回数

○セプターカウンシルにおける情報共有の件数

3.2.3 障害対応体制の強化

「障害対応体制の強化」に期待される成果は、分野横断的演習を中心とする演習・訓練への参加を通じて、重要インフラ事業者等のＩＴ障害発生時の早期復旧手順及びIT-BCP等の検証、そのために必要な関係主体間における情報共有・連絡の有効性の検証や技術面での対処能力の向上等に対する貢献をすることである。そのため、演習成

果の浸透、現実に即した演習環境の構築、分野横断的演習に加えて参加した演習・訓練及び演習・訓練で得られた知見による重要インフラ事業者等の取組への貢献状況に着目した指標を設定する。

＜具体的な指標＞

○分野横断的演習の参加者数

○演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した参加者の割合

○分野横断的演習を含め組織内外で実施する演習・訓練への参加状況

3.2.4　リスクマネジメント

「リスクマネジメント」に期待される成果は、重要インフラ事業者等が実施するリスクマネジメントの推進、強化である。そのため、重要インフラ事業者等が実施するリスクマネジメントプロセスのうち、内閣官房が支援するリスクアセスメントとリスクコミュニケーション及び協議に着目した指標を設定する。

＜具体的な指標＞

○内閣官房が実施した環境変化調査や相互依存性解析の件数

○セプターカウンシルや分野横断的演習等の関係主体間が情報交換できる機会の開催回数

3.2.5　防護基盤の強化

「防護基盤の強化」に期待される成果は、「広報公聴活動」については、行動計画の枠組みついて広く国民の理解を得ることと及び本行動計画への協力者を関係主体以外にも拡大することであり、「国際連携」については、二国間・地域間・多国間の枠組み等を通じた各国との情報交換の機会や支援・啓発であり、「規格・標準及び参照すべき規程類の整備」については、整備した規程類についての重要インフラ事業者等における利活用である。そのため、本行動計画の周知機会及び国際連携機会の充実並びに規程類の整備状況に着目した指標を設定する。

＜具体的な指標＞

○ニュースレター等による情報の発信回数

○行動計画に関連した講演等の回数

○二国間・地域間・多国間による意見交換等の回数

○重要インフラ防護に資する手引書等の整備状況

○制御系機器・システムの第三者認証制度の拡充状況

4. 行動計画期間の成果の評価に基づく行動計画の見直し

「成果（アウトカム）を測る視点」からの評価は、本行動計画の目標、すなわち理想とする将来像に照らして行う。この際、行動計画に基づく様々な取組が相互に関連して結果・成果を成すものであることに鑑み、個別の取組に対して評価を行うのではなく、重要インフラ防護能力の維持・向上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かつ分析的に行う。

本行動計画の枠組みの評価を行う際には、施策群の個別の結果・成果だけでは把握しきれない状況も適切に把握して評価を行うことが重要である。そのため、評価に必要となる補完的な情報を収集するために、補完調査を原則として毎年度実施する。

また、評価運営については、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、原則として３年に１度、情報セキュリティ政策会議で実施することとし、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委員会で行う。

このことから、成果の評価を踏まえた行動計画の見直しについても原則として３年に１度、情報セキュリティ政策会議での実施とし、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委員会で行う。

なお、社会動向の大きな変化等、本行動計画が想定しえなかった事象が発生した場合は、３年に１度はその限りとしない。

別添：情報連絡・情報提供について

1. ＩＴの不具合等に関する情報

ＩＴ障害を含むＩＴの不具合や予兆・ヒヤリハットに関する情報（以下「ＩＴの不具合等に関する情報」という。）には、①ＩＴ障害の未然防止、②ＩＴ障害の拡大防止・迅速な復旧、③ＩＴ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。

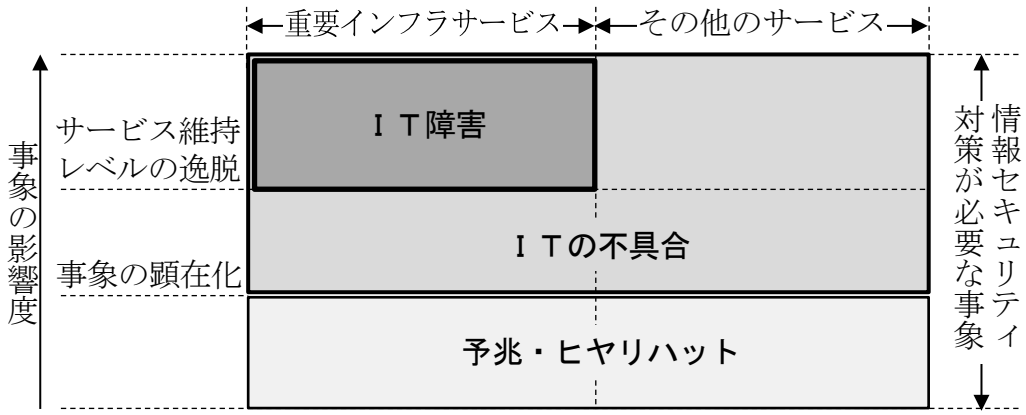
ＩＴの不具合等に関する情報の各側面としては以下のようなものが含まれる。

①未然防止　　ＩＴの不具合等の原因に係る情報（防護方策等を含む）
②拡大防止・復旧　ＩＴ障害発生後の影響伝搬予測及び復旧に資する情報
③再発防止　　事後分析に資する情報の共同収集及び分析・検証の結果

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ＩＴ障害に至ることも考えられることから、ＩＴの不具合と同様に、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、図表５に示すものとする。

図表５　情報共有の対象範囲



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

情報連絡が必要となる場合は、ＩＴ障害を含むＩＴの不具合や予兆・ヒヤリハットを確認した場合であって、法令等で報告が義務付けられている場合又は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である。

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 情報連絡の内容

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する。この際、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。

なお、重要インフラ所管省庁から内閣官房に情報連絡を行う際に必要なＩＴの不具合等に関する共通の分類及びカテゴリの設定等は、各重要インフラ事業者等の運用性等も勘案して行うこととする。

2.3 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５　ＩＴ障害発生時における連絡体制等」に示す連絡体制等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への併任者（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。

2.4 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、原則として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（任意提供情報）として取り扱う。なお、当該情報が同号ただし書に規定する情報に該当する場合には、公開されることがある。

3. 重要インフラ事業者等への情報提供

3.1 情報提供の対象とする重要インフラ事業者等の範囲

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提供元との間で調整を行うことができる。

3.2 情報提供の内容

情報提供は、重要インフラ所管省庁、情報セキュリティ関係省庁、情報セキュリティ関係機関及びサイバー空間関連事業者から提供される幅広い情報について、集約、分析等を行い、重要インフラ事業者等の情報セキュリティ対策に有効と考えられるものについて行う。

また、重要インフラ事業者等からの情報連絡が次に掲げる①又は②に該当する場合、情報連絡を行った重要インフラ事業者等が不利益を被らないよう、情報連絡をした重要インフラ事業者等が特定されないよう情報を加工する等適切な措置を講じた上で情報提供を行う。

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問題が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。

3.3 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。

3.4 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、情報セキュリティ関係省庁、情報セキュリティ関係機関、サイバー空間関連事業者等と以下のとおり連携する。

① 情報セキュリティ関係省庁及び情報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、ＩＴ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、情報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ＩＴ障害に関する情報については、平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。

3.5 情報の質の向上（分析情報、影響度等）

提供する情報については、以下の点を考慮しつつ、その質の向上を図る。

① 情報を突き合わせることによる精度の向上。

② ①に基づく重要度・優先度の判断。

③ 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ＩＴ障害や各分野間に共通するリスク源により発生したＩＴ障害に関する他の重要インフラ分野への影響予測。

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(注1)		対象となる重要インフラ事業者等(注2)	対象となる重要システム例(注3)	ＩＴ障害やその影響の例
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	・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等 ・放送サービスの停止
金融	銀行等 生命保険 損害保険 証券	・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　　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　　等	・預金の払い出し、振込等資金移動、融資業務の停止 ・資金清算の停止 ・電子記録、資金決済に関する情報提供の停止 ・保険金の支払い停止 ・有価証券売買の停止 ・社債・株式等の振替の停止 ・金融商品取引の清算の停止　　等
航空		・主たる定期航空運送事業者 ・国土交通省（航空管制・気象）	・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 ・航空管制システム ・気象情報システム	・運航の遅延、欠航 ・航空機の安全運航に対する支障等
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	・列車運行の遅延、運休 ・列車の安全安定輸送に対する支障等
電力		・一般電気事業者、日本原子力発電(株)及び電源開発(株)	・制御システム ・運転監視システム	・電力供給の停止 ・電力プラントの安全運用に対する支障等
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	・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等
政府・行政サービス		・各府省庁 ・地方公共団体	・各府省庁及び地方公共団体の情報システム（電子政府・電子自治体への対応）	・政府・行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん
医療		・医療機関 （ただし、小規模なものを除く。）	・診療録等の管理システム等（電子カルテシステム、遠隔画像診断システム等、医用電気機器等）	・診療支援部門における業務への支障等
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等	・水道による水の供給の停止 ・不適当な水質の水の供給　　等
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	・輸送の遅延・停止 ・貨物の所在追跡困難

注１　本行動計画において新たに追加された重要インフラ分野（化学、クレジット及び石油の各分野）に係る対象となる重要インフラ事業者等と重要システム例については、別途整理を行う。
注２　ここに掲げている者は、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、対象とする者の見直しを行う。
注３　対象となる重要システムの詳細については、ＩＴ障害やその影響の例を踏まえ、重要インフラ事業者等において定める。

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(注1)		重要インフラサービス（手続きを含む）(注2)		サービス維持レベル	
		呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
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	・電気通信事業法施行規則第58条による
		・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）	・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	・放送法施行規則第125条第１項から第３項までによる
		・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）	・ケーブルテレビ設備の故障により、放送の停止が、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	・放送法施行規則第157条による
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）	・ＩＴの不具合により、預金の払戻しの遅延・停止が生じないこと ・ＩＴの不具合により、融資承諾をした貸付の実行の遅延・停止が生じないこと ・ＩＴの不具合により、為替（銀行振込）の遅延・停止が生じないこと	・「主要行等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合（例えば、一部のATMが停止した場合であっても同一店舗又は近隣店舗の他のATMや窓口において対応が可能な場合等）を除く
		・資金清算	・資金清算（資金決済に関する法律第２条第５項）	・ＩＴの不具合により、資金清算の遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
		・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）	・ＩＴの不具合により、電子記録及び資金決済に関する情報提供の遅延・停止が生じないこと	・「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）」を参照
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付 ・保険金等の支払審査 ・保険金等の支払い	・ＩＴの不具合により、保険金等の支払いに遅延・停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
	損害保険	・保険金等の支払い	・事故受付 ・損害調査等 ・保険金等の支払い	・ＩＴの不具合により、保険金等の支払いに遅延・停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く

重要インフラ分野(注1)		重要インフラサービス（手続きを含む）(注2)		サービス維持レベル	
		呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
	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）	・ＩＴの不具合により、預り有価証券等の売却、解約代金の払い出し等に遅延・停止が生じないこと	・「金融商品取引業者等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合（例えば、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く
		・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）	・ＩＴの不具合により、有価証券の売買又は市場デリバティブ取引等に遅延・停止が生じないこと	・金融商品取引所等に関する内閣府令第112条第７項を参照
		・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）	・ＩＴの不具合により、社債・株式等の振替等に遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
		・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）	・ＩＴの不具合により、金融商品取引の清算等に遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
航空		・旅客、貨物の航空輸送サービス ・航空交通管制業務 ・気象情報配信 ・予約、発券、搭乗・搭載手続き ・運航整備	・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） ・空域の適正な利用及び安全かつ円滑な航空交通の確保（航空法第95条の２） ・航空機の利用に適合する予報・警報等の配信（気象業務法第14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	・ＩＴの不具合により、貨客の運送に支障を及ぼす定期便の欠航が生じないこと	・「航空分野におけるCEPTOAR」に係る申し合わせにおいて対応

重要インフラ分野(注1)	重要インフラサービス（手続きを含む）(注2)		サービス維持レベル	
	呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
	・飛行計画作成	・飛行計画の作成、航空局への提出		
鉄道	・旅客輸送サービス ・発券、入出場手続き	・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	・ＩＴの不具合により、旅客の輸送に支障を及ぼす列車の運休が生じないこと	・鉄道事故等報告規則第５条（鉄道運転事故等の報告）による
電力	・一般電気事業	・一般の需要に応じ電気を供給する事業（電気事業法第２条及び第18条）	・ＩＴ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	・電気関係報告規則第３条による
ガス	・一般ガス事業	・一般の需要に応じ導管によりガスを供給する事業（ガス事業法第２条）	・ＩＴ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	・ガス事業法施行規則第112条による
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）	・ＩＴの不具合により、住民等の権利利益の保護に支障が生じないこと ・住民等の安全・安心を確保できる時間内にシステムの復旧を行うこと	
医療	・診療	・診察や治療等の行為	・医療機器の誤作動の招来等により、人の生命に危険が及ばないこと。 ・ＩＴの不具合により、診療の継続に支障が生じないこと。	・ＩＴの依存度によらず、診療や治療等の行為の水準の維持に努めること。
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）	・ＩＴの不具合により、断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと	・重大なシステム障害とは、システム停止に伴う給水への影響が大きい制御システム（浄水場の監視制御システム、ポンプ場の運転システム、水運用システム等）の障害を想定 ・「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）の「6.(2)水道における情報システム障害等が発生した場合」による
物流	・物流	・貨物の運送及び保管	・ＩＴの不具合により、貨物運送の停止や貨物の紛失が生じないこと	・「物流分野における情報共有・分析機能(CEPTOAR)に係る申し合わせ」において対応

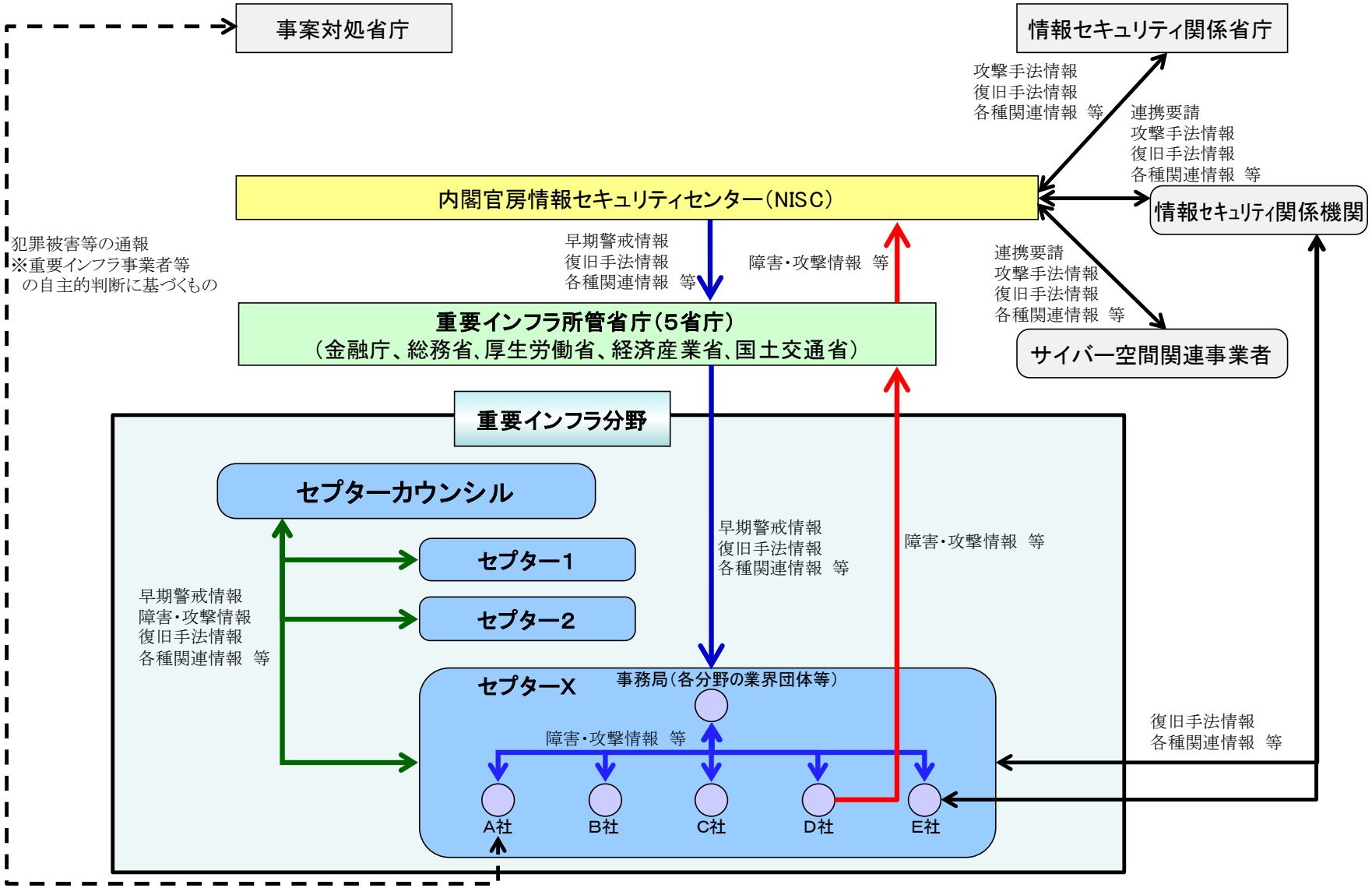
注１　本行動計画において新たに追加された重要インフラ分野（化学、クレジット及び石油の各分野）に係る重要インフラサービスとサービス維持レベルについては、別途整理を行う。
注２　ＩＴを全く利用していないサービスについては対象外。

別紙３　情報連絡における事象と原因の類型

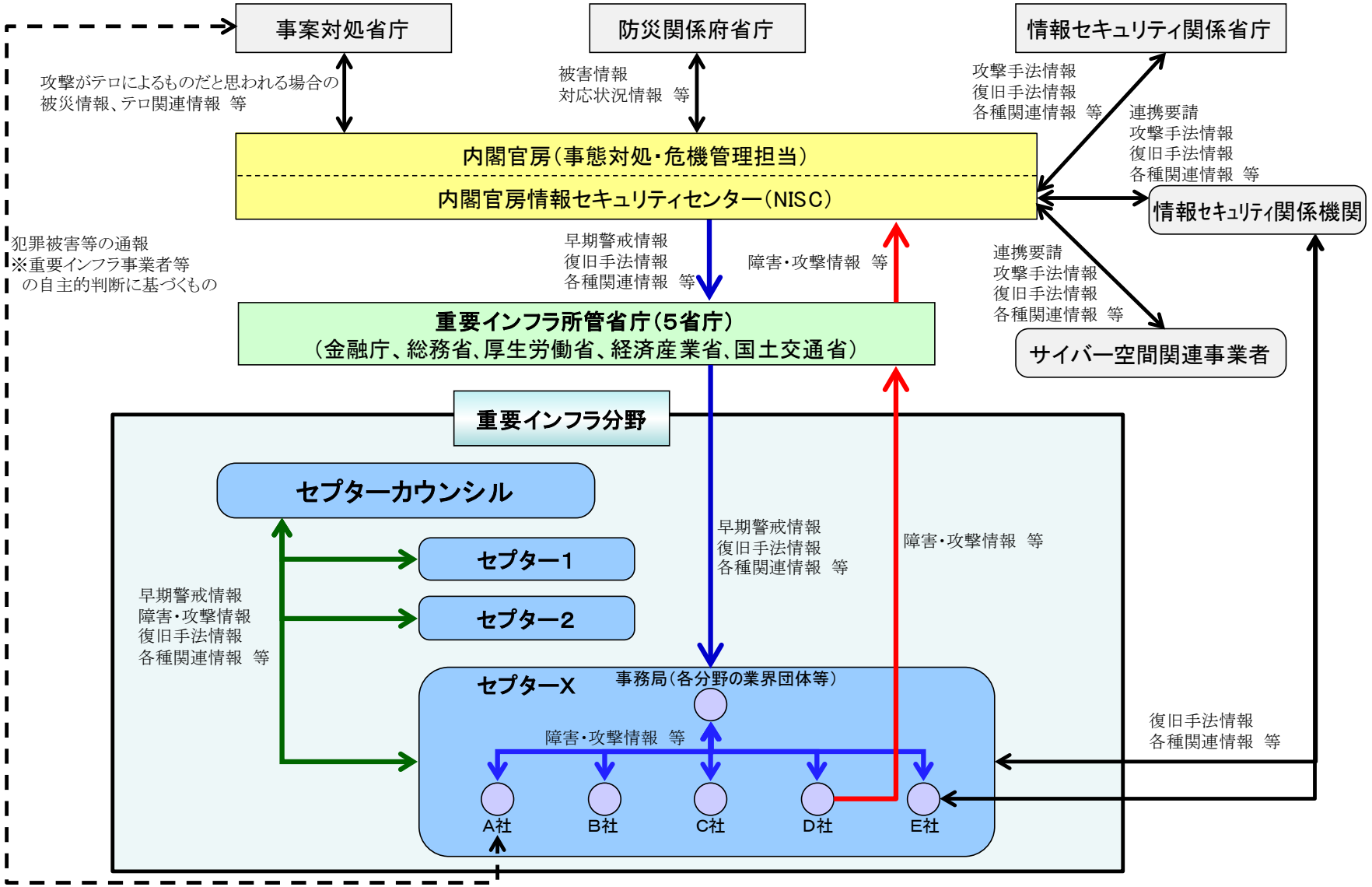
事象の類型		事象の例	説明
未発生の事象		予兆・ヒヤリハット	サイバー攻撃の予告などの予兆や、事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信などによるヒヤリハットの発生
発生した事象	機密性を脅かす事象	情報の漏えい	組織の機密情報等の流出など、機密性が脅かされる事象の発生
	完全性を脅かす事象	情報の破壊	Webサイト等の改ざんや組織の機密情報等の破壊など、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やWebサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記につながる事象	マルウェア等の感染	マ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、DoS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など
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など
環境的な原因	災害や疾病など
その他の原因	上記以外の脅威や脆弱性、原因不明など

別紙４－１　情報共有体制（平時）



別紙４－２　情報共有体制（大規模ＩＴ障害対応時）



別紙５　ＩＴ障害発生時における連絡体制等

重要インフラ分野(注)		既存の連絡体制	ＩＴ障害発生時における緊急時の連絡体制
情報通信		(1) 重要インフラ事業者等→政府 ・電気通信事業法に基づく、業務の停止等の総務大臣への報告 ・放送中止事故、重要無線通信妨害等の総務省への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ウィルス発生等緊急情報を業界内及び総務省との間で通報・共有	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・T-CEPTOAR、放送CEPTOAR及びケーブルテレビCEPTOARの連絡体制を活用して実施 ・既存の連絡体制を活用して実施
金融	銀行等 生命保険 損害保険 証券	(1) 重要インフラ事業者等→政府 ・業法に基づく、サービス遅延・停止等の内閣総理大臣（金融庁）への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・銀行等CEPTOARの連絡体制を活用して実施 ・証券CEPTOARの連絡体制を活用して実施 ・生命保険CEPTOARの連絡体制を活用して実施 ・損害保険CEPTOARの連絡体制を活用して実施 ・その他事業者団体等を通じて実施
航空		(1) 重要インフラ事業者等→政府 ・航空法に基づく、航空機の事故等に関する国土交通大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ＩＴ障害に関する連絡窓口を設置 ・航空保安体制の不具合に関する情報を関係する機関で共有（空港単位）	(1) 重要インフラ事業者等→政府 ・事故時は既存の事故報告体制により実施。 ・事故に至らないＩＴ障害に関しては、航空分野におけるCEPTOARの連絡体制を活用して実施。 (2) 政府→重要インフラ事業者等 ・航空分野におけるCEPTOARの連絡体制を活用して実施 ・連絡窓口を通じて重要インフラ事業者等へ直接連絡
鉄道		(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通大臣への報告 ・ＩＴ障害に関する連絡体制を整備 (2) 重要インフラ事業者等間 ・特になし	(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・事故時は既存の事故報告体制により実施。 ・鉄道CEPTOARの連絡体制を活用して実施
電力		(1) 重要インフラ事業者等→政府 ・電気関係報告規則に基づく、供給支障事故等に関する経済産業大臣への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ＩＴ障害に関する窓口を設置	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・電力におけるＩＴ障害に係る情報共有・分析機能の連絡体制を活用して実施 ・連絡窓口を通じて重要インフラ事業者等へ直接連絡

重要インフラ分野(注)	既存の連絡体制	ＩＴ障害発生時における緊急時の連絡体制
ガス	(1) 重要インフラ事業者等→政府 ・ガス事業法施行規則に基づく、一定規模のガス供給支障等の経済産業大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・災害によりガス供給支障が発生した場合等における、ガス協会「救援措置要綱」に基づく業界内連絡	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・ガスCEPTOARの連絡体制を活用して実施 ・事業者団体を通じて実施
政府・行政サービス	(1) 各府省庁→内閣官房 ・「政府機関の情報システムに関する緊急時の連絡等について（平成12年４月17日）」に基づく連絡 (2) 内閣官房→各府省庁 ・「政府機関の情報システムに関する緊急時の連絡等について（平成12年４月17日）」に基づく情報提供 (3) 地方公共団体→政府 ・「情報セキュリティインシデント発生時における対応及び報告並びに緊急時連絡体制の整備等について（通知）」に基づく情報提供 (4) 政府→地方公共団体 ・「情報セキュリティインシデント発生時における対応及び報告並びに緊急時連絡体制の整備等について（通知）」に基づく情報提供	(1) 各府省庁→内閣官房、内閣官房→各府省庁 ・政府部内連絡体制で実施 (2) 地方公共団体→政府、政府→地方公共団体 ・自治体CEPTOARの連絡体制を活用して実施 ・既存の連絡体制を活用して実施
医療	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等 ・医療CEPTOARの連絡体制を活用して実施
水道	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等 ・水道CEPTOARにおけるＩＴ障害情報の取扱いに関するガイドラインの連絡体制を活用して実施
物流	(1) 重要インフラ事業者等→政府 ・各事業法等に基づく、事故等の国土交通大臣への報告 (2) 政府→重要インフラ事業者等 ・内閣府　災害対策基本法に定める指定公共機関	(1) 重要インフラ事業者等→政府 ・事故等は既存の事故報告体制により実施 ・事故に至らないＩＴ障害に関しては、物流CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・物流CEPTOARの連絡体制を活用して実施

注　本行動計画において新たに追加された重要インフラ分野（化学、クレジット及び石油の各分野）に係る連絡体制については、別途整理を行う。

別紙６　定義・用語集

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。
ＩＴ障害	ＩＴの不具合のうち、重要インフラサービスの提供水準が「別紙２　重要インフラサービスとサービス維持レベル」における「サービス維持レベル」を下回るもの。
ＩＴ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。
安全基準等	業法に基づき国が定める「強制基準」、業法に準じて国が定める「推奨基準」及び「ガイドライン」、業法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」、業法や国民・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、指針は含まない。
関係主体	内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、重要インフラ事業者等、セプター、セプターカウンシル、情報セキュリティ関係機関及びサイバー空間関連事業者。
サイバー空間関連事業者	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に関係する、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情報セキュリティ対策を提供するセキュリティベンダー及びハードウェア・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。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
指針	安全基準等の策定・改訂に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先進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。本編は情報セキュリティ政策会議決定による。対策編は対策項目のチェックリストとして具体例を記載したもの。
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、わ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、重要インフラ分野として指定する分野。
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きのうち、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「別紙２　重要インフラサービスとサービス維持レベル」に定めるもの。
重要インフラ事業者等	重要インフラ分野に属する事業を営む者等のうち「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」における「対象となる重要インフラ事業者等」に指定された事業者等及び当該事業者等から構成される団体。
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	「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）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
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。「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」に例を示す。
情報共有	見聞や知識・ノウハウ等の情報を、仲間に伝達したり、組織・メンバー間で伝達合ったりして共有すること。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。
情報セキュリティ関係機関	警察庁サイバーフォース、独立行政法人情報通信研究機構（NICT）、独立行政法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般財団法人日本データ通信協会テレコム・アイザック推進会議（Telecom-ISAC Japan）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）。
情報セキュリティ関係省庁	警察庁、総務省、外務省、経済産業省及び防衛省。

情報セキュリティ対策	ＩＴ障害が国民生活や社会経済活動に影響を与えないようにするための幅広い取組。
情報提供	情報セキュリティ対策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ＩＴの不具合等に関する情報（ＩＴ障害を含むＩＴ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ＩＴ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等の政府として集中的な対応が必要となる規模のＩＴ障害。
ヒヤリハット	想定外又は予期しない事象によって、ＩＴの不具合に至らなかったものの、ＩＴの不具合に直結するおそれのあった事象。
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項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。