資料６

重要インフラの情報セキュリティ対策に係る
次期行動計画
（草案）

平 成 ２５ 年 １１ 月 ２９ 日

重要インフラ専門委員会事務局

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かかる特別行動計画(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。）を策定した。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年に策定した。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、本行動計画策定に当たっては、「サイバーセキュリティ戦略」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するものとする。

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するものとする。

[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

本行動計画の策定に当たり、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」を基本的考え方において示しており、第２次行動計画における目的は「サイバーセキュリティ戦略」と整合していることを確認した。

その上で、目的を更に明確化するため、「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、第２次行動計画における目的を継承することとする。

○「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、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。

・ 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、重要インフラ事業者等の単独のものだけでなく、分野内の他重要インフラ事業者等や他分野の重要インフラ事業者等のものとの連携をも充実させる。
（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万全であることを確認することは難しいため。）

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つの施策群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記載する。

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た。第２次行動計画における所期の目標については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啓発推進等を強化した。

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・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・強化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、メリディアン会合、サイバーストーム演習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・強化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を踏まえた段階的な（優先順位付けされた）指針の提示要望があること等から、各重要インフラ事業者等の情報セキュリティ対策に資することを目的に、重要インフラ事業者等のPDCAサイクル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、大規模ＩＴ障害対応時の情報共有体制について、平時の体制の延長線上への構築、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、時間的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、区々である各組織のＩＴ利用形態や情報管理態勢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。このことから、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、多国間、地域的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次期行動計画策定に当たっての方向性の検討を以下のとおり行った。

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「一義的には重要インフラ事業者等の責任で対策を行う」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・強化、とりわけ対策途上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。

○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。

○インターネット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つい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[2]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　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る。

○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（通常状態又は通常のＩＴ障害発生時）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。）。

[2] JIS Q 31000:2010 によれば、「それ自体又はほかの組み合わせによって、リスクを生じさせる本来潜在的にもっている要素。」と定義されている。

5. 重要インフラの定義及び範囲の見直し結果について

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、関係主体の追加等の是非を検討した。

現在、重要インフラとは位置付けられていないが、現行10分野と同等にその機能障害が国民生活及び社会経済活動に多大な影響を及ぼし得る分野におけるシステム、サービスの位置付けを踏まえた重要インフラの範囲の見直し等を図った。具体的には、現在、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、必要があると認められたものについては、新たに分野の追加、関係主体の追加等を実施した。

図表１　重要インフラの定義及び範囲の見直しの考え方

検討対象	視点
情報システムの場合	情報サービス提供価値、情報システムが処理するサービスの提供規模
制御システムの場合	制御が困難な状態において生じ得るリスクの大きさ
共通	既存分野における重要システムに与える影響 既存分野との間で認め得る相互依存性
既存分野での補強・拡大	既存分野で活動に至っていないものの追加

5.1 追加候補分野の絞り込みについて

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、新たに重要インフラとなり得る分野の候補を数分野に特定した。

候補となる分野・関係主体の中から検討を行い、今回追加するに至った重要インフラ分野及び追加する必要性の視点を図表２に示す。

なお、当該分野が重要インフラに参加するに当たり、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の理解を醸成することが重要な課題である。

図表２　重要インフラへの追加検討結果

重要インフラへの追加区分	追加する必要性の視点		分野数
当該分野が有する情報システムや制御システムが障害に至った場合の社会・経済に与える影響	情報システム	情報サービス提供価値、情報システムが処理するサービス提供の規模	１分野
	制御システム	制御が困難な状態において生じ得るリスクの大きさ	２分野
既存の重要インフラ分野における重要システムに与える影響	既存重要インフラ分野との間で認め得る相互依存性		１分野
既存の重要インフラ分野での補強・拡大	既存重要インフラ分野において、現時点で活動に至っていないものの追加		１分野

5.2 追加候補分野の活動開始の準備

追加候補となる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、重要インフラへの参加を打診した。参加が見込まれる状況に至った時点で、業界団体の位置付け、第２次行動計画の施策群への整合をどのように図っていくかを確認するとともに、セプターの設立について働きかけを行った。

5.3 新規追加分野との関係の整理

情報共有体制は、2007年度の構築から６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しており、また、業務性質等から独自色を有している。

こうした中で、新規にセプターが加入した場合、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、分野内の他重要インフラ事業者等や他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新規追加分野の助言を行うこととする。また、セプターカウンシルにおいても、相互扶助の精神で新規参入セプターに助言を行い、全体の底上げを図ることが必要である。

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、以下の施策群の構成とすることとした。

図表３　本行動計画における施策群と補強・改善の方向性

第２次行動計画	本行動計画における施策群	補強・改善の方向性
①安全基準等の整備及び浸透	第２次行動計画を基本的に踏襲	○他施策の結果を指針・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	第２次行動計画を基本的に踏襲	○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共通脅威分析	「⑤環境変化への対応」の一部と統合し、「リスクマネジメント」として整理	○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持ち得るリスク源、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
④分野横断的演習	「障害対応体制の強化」として整理	○重要インフラ関係の演習・訓練の全体像を把握した上での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横断的演習の質的改善
⑤環境変化への対応	「リスクマネジメント」に統合される部分を除き、「防護基盤の強化」として整理	○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

本行動計画における施策群をまとめると、次の５つから構成される。

１．安全基準等の整備及び浸透
２．情報共有体制の強化
３．障害対応体制の強化
４．リスクマネジメント
５．防護基盤の強化

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、「重要インフラ防護」の目的、基本的な考え方及び関係主体、その中でも重要インフラ事業者等の経営層に期待する在り方は以下のとおりである。

○「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、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。

－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、重要インフラ事業者等の単独のものだけでなく、分野内の他重要インフラ事業者等や他分野の重要インフラ事業者等のものとの連携をも充実させる。（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万全であることを確認することは難しいため。）

○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。また、他の関係主体の活動状況を把握し、互いに自主的に協力。

－ＩＴ障害の規模に応じて、情報の５Ｗ１Ｈを理解しており、ＩＴ障害の発生時に冷静に対処が可能。多様な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可能。

－以上のような、重要インフラ防護への連携した取組を広く国民に周知し、国民の安心感を醸成。

○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。

－上記目的を達成するに当たっての情報セキュリティ対策を含むリスク源の認識。

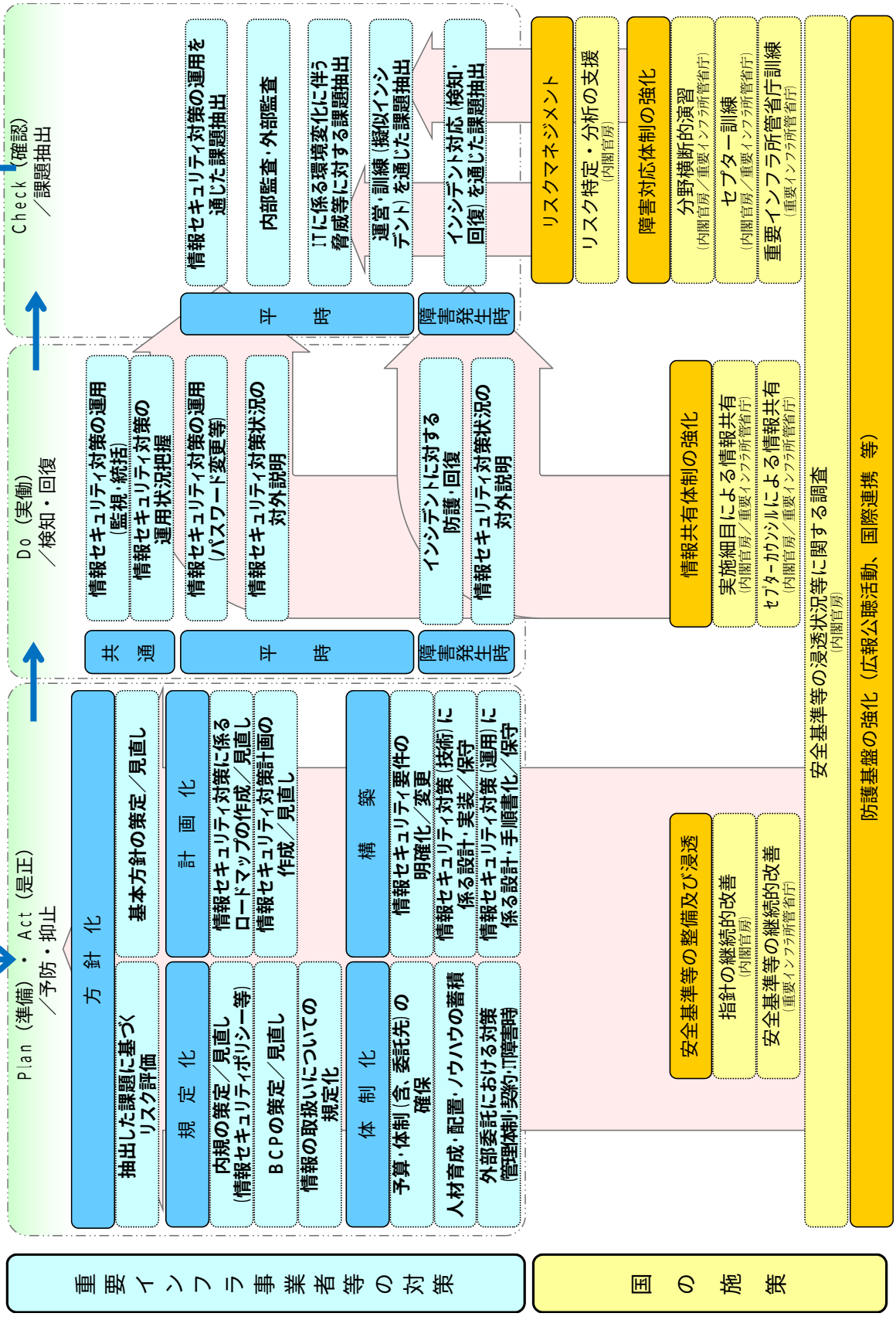
－上記のリスク源の評価及びそれに対する方針の策定。

－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及び経営資源の継続的な確保。

－システムの運用状況の把握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４　「重要インフラ事業者等の対策」と各対策に関連する「国の施策」



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ける本項の内閣官房の取組については、重要インフラ防護能力の維持・強化を目的に、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、本行動計画期間における本項の重要インフラ事業者等の取組については、対策の重要性に鑑み、情報セキュリティ対策に係るガバナンスに基づいた実装・運用の下、PDCAサイクルに沿った対策の着実な維持・向上に取り組む。

1.1 指針の継続的改善

重要インフラ防護能力の維持・強化、とりわけ対策途上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サイクルに沿った各対策項目の整理を行うとともに、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ガバナンスの重要性を訴求する。

なお、2015年度以降の取組においては、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するとともに、その改定は３年に１度の実施を原則とする。ただし、改定の必要を認められた場合はその限りとしない。

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・強化を目的に、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、対策における検知・回復に係る取組、関係性を有する主体間での情報共有、環境変化に伴い生じた脅威の分析、擬似インシデントを契機とした訓練・演習

及び内部・外部監査等から課題を抽出し、リスク評価を経て、安全基準等を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[3]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可能とする。

[3] 往訪調査にて得た課題・事例が公表できない場合は、直接、重要インフラ所管省庁又はセプター等への情報提供にて代替することとする。

2. 情報共有体制の強化

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は刻々と変化しており、重要インフラの情報セキュリティ対策に有効性を保ち続けるには、そ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に反映させていく必要がある。また、サイバー攻撃等をはじめとしたＩＴ障害についての手法も、複雑・巧妙化してきており、情報セキュリティ水準の向上、サイバー攻撃等に対する対処能力の向上は、ますます重要視されている。

このような状況下の中、本行動計画の策定にあたり、これまで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、関係主体の追加を行った。内閣官房は、情報共有体制を更に強化するために、これまでの関係主体間で共有する情報についての再整理を行い、新たな関係主体との位置付け、範囲の整理を行う。その結果を踏まえ、各関係主体との情報共有に関する事務手順を定めた実施細目に従い、本行動計画期間における確実な情報共有を構築し、維持する。

2.1 情報共有体制の見直し

大規模ＩＴ障害対応時における情報共有を強化するためには、これまでの各関係主体だけでなく、防災も含めた新たな連携を図るための取組を行うことが必要である。本行動計画の策定にあたり、サイバー空間関連事業者の中でも、重要インフラシステムの保守・運用に関与しているシステムベンダー、標的型攻撃等含むＩＴ障害に対して、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、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に対しての位置付け、役割を明確にした上で、「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）」に組み入れている。また、新たな分野の追加、関係主体の追加を行っており、これらの新たな重要インフラ分野に対しての位置付け、範囲及び役割を明確にし、「別紙１　対象となる重要インフラと重要システム」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」の見直しを行っている。

本行動計画においては、内閣官房は、これまでの各関係主体の位置付け、役割、情報の整理を行うとともに、新たな関係主体との整理も行うこととする。新たな関係主体として参加することとなる、サイバー空間に係る製品、サービスや技術等を提供するサイバー空間関連事業者においては、サイバー攻撃等の事案発生時に、被害の拡大を防止する等、情報セキュリティの確保に取り組むことが期待される。

なお、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という基本的考え方を踏まえつつ、重要インフラ事業者等の単独のものだけでなく、分野内の他重要インフラ事業者等や他分野の重要インフラ事業者等のものとの連携をも充実させる観点から、情報共有体制の円滑な運用は、情報セキュリ

ティ対策の基本であることを付言する。

2.2 情報共有機能の強化に向けた共有すべき情報の見直し

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、関係機関、重要インフラ所管省庁、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。

内閣官房は、これら３つの側面を踏まえた上で、ＩＴ障害発生時の連絡体制については、更なる発展、向上を図るための取組を行う。具体的には、これまでの各関係主体との整理に加え、本行動計画では防災関係、サイバー空間関連事業者を含めた新たな連携の見直しを図ることとしている。見直しを行った情報共有体制をもとに、平常時及び大規模ＩＴ障害対応時における、関係主体との連携を再整理し、情報共有体制を強化する。情報の整理を行う上で、情報連絡体制における認識の相違懸念等があることから、認識の統一を含めた見直しを行う。また、再整理した内容をもとに、情報連絡・情報提供に関する実施細目の見直しを行う。

また、重要インフラ事業者等において、情報を共有することは、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観点からも重要である。ＩＴ障害が発生した際に迅速かつ正確にＩＴ障害を把握するために、発生時に連絡すべき情報を現在の原因中心の情報の整理に加えて、事象[4]に関する情報共有の項目を、情報セキュリティのＣ・Ｉ・Ａ[5]の観点から再整理を行った。また、ＩＴ障害の原因についても、新たな脅威等を踏まえ、原因の項目を再検討した。

これらＩＴ障害の事象や原因に関する情報共有を行うことで、他の重要インフラ事業者等においても、自らの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。未然防止の観点から、実際に発生した事象だけでなく、予兆等を含む事象についても、情報共有の対象となるよう整理を行った。

こうした検討を行った結果を「別紙３　ＩＴ障害の事例と原因の例」として取りまとめた。内閣官房は、重要インフラ所管省庁との間で情報共有を行う際の具体的な事務取扱手順を実施細目として定め、これに従い情報連絡・提供を行うものとする。

[4] 情報セキュリティ事象（Information Security Event）とは、「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（ISO/IEC 27000:2013 参照）。

[5] 機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）のことを指す。

2.3 重要インフラ事業者等の自主的な活動の促進

重要インフラ事業者等が、自主的な活動を行うにあたり、セプターを整備する必要があるが、セプターに具備すべき要件として、以下の２点の要件については、引き続きこれを継続し、内閣官房から提供する情報の共有を図ることとする。

①内閣官房が提供する情報の取扱いに関する取決め、機密保持及び外部への情報提供に関し、構成員間で合意されたルールが存在すること。

②緊急時に各構成員及び外部との連絡が可能な窓口（PoC[6]）が設定されていること。

各セプターは、引き続き積極的なセプター間における情報共有を充実させるとともに、分野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や、ＩＴ障害に至らない事例や現行情報連絡の対象とならないＩＴ障害の事例についての情報共有の機能、セプター間やセプターカウンシル等との情報共有等に必要な機能の充実について、重要インフラ事業者等の自主的な取組の中で図られることが望まれる。

また、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。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・復旧能力の向上に向けた自発的な幅広い取組が行われることが期待される。

本行動計画では、引き続きセプターカウンシルにおいて、セプター間の情報共有の一層の充実を図るために、共有すべき情報や連携の更なる強化を図ることが期待される。

2.4 情報共有体制の全体像

各関係主体は、大規模ＩＴ障害が発生した際、平常時の情報連絡・提供体制を維持しつつ、政府全体の対処態勢と連携をとることで必要な情報共有を図ることとする。

具体的には、「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、平時及び大規模ＩＴ障害対応時に分けて、情報共有体制を敷くこととする。

2.4.1　平時の情報共有体制

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

所属するセプターにおいてＩＴ障害・攻撃情報等を共有することを基本とする。攻撃、ＩＴ障害情報等は、重要インフラ所管省庁を通じて内閣官房（NISC）へ提供する。犯罪被害にあった際、自主的な判断により、事案対処省庁に対して通報を行う。

[6] POC：Point of Contact

(2) 各セプター

セプターカウンシルや重要インフラ所管省庁、関係機関と連携し、相互にＩＴ障害・攻撃情報、各種関連情報、復旧手法情報、早期警戒情報等に関する情報共有を行う。

(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。

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・復旧能力の向上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提供されたＩＴ障害・攻撃情報等を内閣官房（NISC）及び必要に応じて所管するセプターに提供する。

内閣官房（NISC）から提供される各種関連情報、復旧手法情報、早期警戒情報等を所管するセプターに情報提供する。

(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、あらかじめ連携要請した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。

2.4.2　大規模ＩＴ障害対応時の情報共有体制

災害やテロ等の大規模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。事象が進展し、サイバー攻撃や自然災害などによる大規模ＩＴ障害対応に移行した際、事案対処省庁、防災関係省庁、情報セキュリティ関係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（安全保障・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省庁から提供される被害情報、対応状況情報等を集約し、相互に情報共有を行う。

(2) 内閣官房（NISC）

内閣官房（安全保障・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、あらかじめ連携要請した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

平時に加え、必要に応じ、事案対処体制に協力する。

(4) 重要インフラ事業者等

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講じる他は、平時に同じ。

(5) 各セプター

各セプターが定める大規模ＩＴ障害対応時の体制を講じる他は、平時に同じ。

(6) セプターカウンシル

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講じる他は、平時に同じ。

3. 障害対応体制の強化

本行動計画期間においては、ＩＴ障害対応に関する能力向上や検証を目的とする各種演習・訓練について、相互の関係を把握しつつ、重要インフラ防護対策の向上のためにＩＴ障害対応体制の強化策の一環に位置付ける。

また、分野横断的演習は、これまでの実績を踏まえ、引き続き重要インフラ分野の障害対応体制を強化する中核的な取組として位置付け充実を図るとともに、セプター訓練や重要インフラ所管省庁が実施する他の演習・訓練と各分野内の「縦」方向と分野間の「横」方向の体制強化に向け、互いに連携・補完し相乗効果を発揮できるよう実施していく。

3.1 分野横断的演習の改善

第１次行動計画から引き継がれた「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」、「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」の３つの目標の下継続して演習が実施され、参加者からはおおむね高い評価を得てきており、その運営手法や成果の蓄積がされてきている。

本行動計画期間も引き続き、内閣官房は、ＩＴ障害を引き起こす要因である脅威に関する最新動向を把握しつつ、我が国唯一の取組である分野横断的演習の継続的な実施により、演習の課題の抽出及び演習実施のための知見の整備を行い、演習の分野全体への浸透を通じて、分野横断的な重要インフラ防護対策の強化を推進する。また、障害対応体制の強化に資する分野横断的演習自身の充実として、これまで蓄積した運営ノウハウ・成果の展開、重要インフラ事業者等のＩＴシステム維持に密接にかかわる主体の参画も視野に入れた取組の検討を行う。

3.1.1 演習成果の分野全体への浸透

過去４年間で演習参加者は着実に増加し、演習を有意義と感じる参加者割合も８割を超え、その運営手法や成果の蓄積がされてきている一方で、毎年の参加組織のうち約６割が固定化しており、新たな参加組織は必ずしも多くない。繰り返し演習に参加することで組織としての知見を継承し深化させていくことも大切だが、演習未経験の組織が新たに演習に参加する、演習成果を効果的に展開する等、重要インフラ全体への演習成果の普及・浸透についても取り組む必要がある。

そのため、内閣官房は、演習成果（参加のメリット）をわかりやすく説明する資料の作成・公表を通じ、重要インフラ分野全体への周知及び経営者層への理解増進の取組等を進め、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、そうした個別の重要インフラ事業者等での演習実施を支援するために、これまでの演習で蓄積した実施・評価・助言手法をとりまとめ共有化できるよう検討を進め

る。さらに、演習成果の次年度活動への反映や他の重要インフラ防護施策への展開を進めるとともに、継続的に重要インフラ事業者等が演習成果を自身の情報セキュリティ対策や事業継続計画等に結び付け反映できるよう、内閣官房による演習結果の評価プロセスについて改善を検討する。

3.1.2　防災関係省庁との連携

現実のＩＴ障害対応時には、物理的ＩＴ障害が発生する状況も想定され、その状況次第で、各省庁や各企業等の情報セキュリティ部門だけでなく防災・危機管理部門との情報共有が生じる可能性は否定できない。

今後、分野横断的演習において、物理的ＩＴ障害への対応も検証課題として取り扱う場合には、必要に応じシナリオ作成等に防災関係省庁や内閣官房の知見の活用、及び各省や各企業等の防災・危機管理関係者の協力の在り方を検討する。

3.1.3　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演習・訓練は内閣官房が実施している分野横断的演習と期待される効果が異なっているものの、分野横断的演習と相互に連携・補完し合いながら実施することにより、相互に効率的かつ効果的に重要インフラの防護能力の向上を図っていくことが期待される。

したがって、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・連携対処を主に検証し、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使用したＩＴ障害対応手順の検証、又は分野ごとの連絡体制について確認・検証する等、重要インフラ所管省庁と内閣官房との連携により重要インフラ事業者等の対処能力の向上を図ることを目指す方向性とし、主な対象者、検証目的の明確化及び相互の連携の在り方について検討する。

3.2　セプター訓練

内閣官房は、「実施細目」に基づくセプター及び重要インフラ所管省庁との各分野の「縦の情報共有」体制の維持・向上を目的として、セプター訓練を継続して実施する。実施に当たっては、ＩＴ障害対応を念頭においたより具体的な情報連絡訓練を目指し、重要インフラ防護対策の向上のために、セプターの要望を取り入れながら内容の充実を図る。

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、分野横断的演習で検証した内容を踏まえて状況設定を行うなど、必要に応じて連携を検討する。

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継続的な事業継続等の事業目的の達成にむけ、情報セキュリティの確保に関する目的も確立し、組織内へと展開する必要がある。

一方で、重要インフラを取り巻く社会環境や技術環境等は刻々と変化しており、またその環境変化のなかで、重要インフラにおいて守るべき情報や情報システムのサイバー空間への依存が一層高まっている。このような状況のもと、サイバー空間に潜む脅威や脆弱性等のリスク源[7]により引き起こされるＩＴ障害による影響は甚大化しており、ひとたびＩＴ障害が発生すれば、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。そこで、重要インフラ事業者等においては、ＩＴ障害への対処療法のみではなく、事業目的の達成に向け、情報セキュリティに関するリスク源から導き出されるリスクをどのようにマネジメントしていくかが求められている。

そこで本行動計画においては、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図るため、第２次行動計画で実施してきた環境変化への対応や共通脅威分析の施策をリスクマネジメントのなかで包括的にとらえ直し、各重要インフラ事業者等において実施される情報セキュリティのリスクマネジメントの推進、強化に向けた取組として実施する。

4.1 リスクマネジメントの実施主体と標準的な考え方や定義等の利活用

リスクマネジメントは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。つまり、各重要インフラ事業者等がおこなってきた環境変化への対応や共通脅威分析は、各重要インフラ事業者等におけるリスクマネジメントプロセスの一部として位置付けられ、政府が行ってきたこれらの施策はその支援である。

このとき、重要インフラ事業者等をはじめとした関係主体におけるリスクマネジメントの考え方や関連する言葉の定義に統一性が欠けると適切な情報共有や議論がなされず、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。そこで、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のなかで利用される情報セキュリティに関わる言葉の定義などを利活用する。

具体的には図表５に示すとおり、組織の状況の確定にはじまり、リスクアセスメント、リスク対応、リスクの受容、リスクコミュニケーション及び協議、モニタリング及びレビューといった標準的なリスクマネジメントプロセスの枠組み[8]や、そのなかで

[7] 「ISO 31000:2009」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。

[8] 「ISO/IEC 27005:2011」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 -

利用される言葉の定義などを内閣官房が実施する施策や作成する各種ドキュメントにおいて適切に用いることとし、それらの成果を重要インフラ事業者等が利活用するものとする。これによって、各関係主体間における共通認識の醸成や各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過不足の再認識等を図り、結果として重要インフラ分野の情報セキュリティレベルが底上げされることを期待する。

なお、重要インフラ事業者等における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においては、必ずしも国際標準等に準拠するものではない。関係主体は、これらを参照した上で、自らの組織において最適な理解が得られる考え方や定義等への再整理をすることが望ましい。

図表５　標準的なリスクマネジメントの例

<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 rowspan="3"></td><td>リスク特定</td></tr>
<tr><td>リスク分析</td></tr>
<tr><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>

4.2　リスクマネジメントの支援

各重要インフラ事業者等が自組織のリスクマネジメントにおけるリスクアセスメント[9]プロセスを実施する際、各重要インフラ分野に共通の環境変化に起因する脅威等の把握やこれら脅威等により引き起こされたＩＴ障害がもたらす影響の重要インフラ分野間における相互依存性の分析等が必要となる。しかし、これらの分野横断的な調査・分析を、重要インフラ事業者等が各々で実施することは難しい。

また、重要インフラ分野間での相互依存性が高まるなか、上記の調査・分析の実施や結果の共有においては、重要インフラ事業者等が分野を横断して情報や意見の交換を行うことが重要である。この分野横断的な情報や意見交換等は、重要インフラ事業者等のリスクマネジメントにおけるリスクコミュニケーション及び協議[10]プロセスの一部である。しかし、重要インフラ事業者等が個別に分野横断的な情報や意見交換の

Principles and Inventories for Risk Management / Risk Assessment methods and tools」を参照。

[9] 「ISO/IEC 27000:2013」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。」と定義されており、特に、リスクを発見、認識及び記述するプロセスとされているリスク特定は、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれる、とされている。

[10] 「ISO/IEC 27000:2013」では「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繰り返し行うプロセス。」と定義されている。また、米National Research Councilにおいてリスクコミュニケーションは、「個人とグループ、そして組織の間で情報や意見を交換する相互作用的過程。」と定義されている（1989年）。

機会や場を設けることは難しい。

そのため、内閣官房は、これらの調査・分析等の実施や情報や意見交換の場の提供を引き続き行うこととする。

4.2.1 リスクアセスメント

内閣官房は、以下の調査を引き続き行う。

○重要インフラ分野をとりまく環境の変化に伴うリスク源やそれから導き出されるリスクの分析である環境変化調査

○重要インフラ分野に共通に起こりうるリスク源が何であるかを把握する共通脅威分析

○ある重要インフラ分野にＩＴ障害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解析　等

ただし、継続にあたっては、これら取組の関係性を、各調査・分析の効率化、分析結果の他施策との相互反映プロセスの確立という観点なども踏まえ、以下のとおり整理する。

(1) 環境変化調査

重要インフラにおける情報セキュリティに係る主な設備・技術等についての実態を調査するとともに、それに伴って発生する新たなリスク源やそれから導き出されるリスクについて分析をおこなう。第２次行動計画の期間内に実施した環境変化調査によれば、クラウドやスマートフォン・タブレット端末、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く、BYOD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は、これら変化に伴い発生する新たなリスク源やそれから導き出されるリスクについて分析を進めるとともに、M2Mやスマートコミュニティなど中長期的に重要インフラ分野への浸透が予想される新しい技術・システムについても環境変化調査の対象とし、これら中長期的な変化に対する調査や分析は年度をまたいで継続的に実施する。

なお、環境変化調査によって新たなリスク源やそれから導き出されるリスクが明らかとなった場合や新たな重要インフラ分野が加わった場合に、必要に応じ、詳細調査としてそれらの分野共通性を分析する。なお、分析の対象とするリスク源やそれから導き出されるリスクについては全重要インフラ分野に共通するものだけではなく、例えば制御系、勘定系、情報系など一定の分野に共通するものも対象とする。

(2) 相互依存性解析

各重要インフラ分野におけるＩＴ利用の進展にともない、重要インフラ分野相互の依存関係が増大しており、我が国全体としての各重要インフラ分野における情報セキュリティ対策を向上させていくためには、分野横断的な状況の把握・解析が不可欠で

ある。特に重要インフラ分野にＩＴ障害が生じた場合の相互依存性の把握は、効率的な復旧対策のために重要となる。このことから、本行動計画においても相互依存性解析を継続的に取り組むものとする。

実施にあたっては、環境変化に伴う相互依存性の変化や新たな重要インフラ分野が加わった場合等に、第１次、第２次行動計画において実施された結果をもとに、再調査・解析をおこなうこととする。

また、各重要インフラ分野においてどこまでＩＴ利用が進んでいるかというＩＴ依存度は相互依存性解析に影響を与えるため、詳細調査としてＩＴ依存度についても定期的に調査する。なお、新たな重要インフラ分野が加わった場合には、相互依存性解析に合わせてＩＴ依存度についても調査する。

4.2.2　リスクコミュニケーション及び協議

内閣官房は、分野を横断する関係主体を対象とした情報や意見の交換の充実に継続して取り組む。これにより、内閣官房が調査・分析する際に重要インフラ事業者等からの情報収集を図り、内閣官房からの一方的な情報提供に留まらない相互の協力体制を充実させていくとともに、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支援を行う。

具体的には、情報共有体制のセプターカウンシルに係る会議体やＩＴ障害対応体制の取組の一つである分野横断的演習の検討会等を利用した参加事業者の協力の元で情報や意見の交換を行う。

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、本施策の取組における調査・分析結果について、重要インフラ事業者等が行うリスクマネジメントの支援に際してこれらを活用するとともに、本行動計画における他施策にとっての基礎資料として、安全基準等の整備及び浸透、情報共有体制の強化、ＩＴ障害対応体制の強化等への反映に図るものとする。

また、内閣官房は、各重要インフラ分野における直近の安全基準等の策定・変更状況の把握・評価等の他施策から顕在化した分野横断的に対策を講じることが望ましいリスク源やそれから導き出されるリスクに基づき、必要な調査を行う。さらに、本行動計画では、この相互反映プロセスを明確化し、各施策の適正な遂行を図る。

5. 防護基盤の強化

社会環境や技術環境等の状況は刻々と変化するため、情報セキュリティ対策の有効性を確保するためには、これまでに述べた各施策に加え、その共通基盤的な取組を強化することも必要になってくる。

具体的には、第２次行動計画に引き続き、内閣官房は、他の関係主体と協力しつつ、広報公聴活動と国際連携を行うとともに、本行動計画やその関連規程が参照することとなる情報セキュリティに関する規格・標準の体系的な整理や、整理された規程類の重要インフラ分野への展開を推進する。

5.1 広報公聴活動

ＩＴ障害が発生した際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強化のみならず、国民が状況を踏まえ冷静に対応できるようになることもまた重要である。

そのため、関係主体は、行動計画に基づき実施した取組を広報することによって、国民に対しての説明責任を果たすとともに、国民が冷静な対応をとる上で必要な情報が得られるように努める。また、広報公聴活動を通じて本行動計画に関心をもつ主体を増やすことが、広く協力、支援を得るためにも重要である。

具体的には、内閣官房は、Webサイトやニュースレターを通じた広報や、講演等を通じた公聴活動を引き続き積極的に行っていく。

また、内閣官房は、より多くの人々が本行動計画の内容を認識・理解できるような広報の構成に努める。

5.2 国際連携

内閣官房は、重要インフラ所管省庁と連携して、世界的な枠組みに加え、日米等の二国間や日ASEAN等の多国間での連携等、引き続き国際連携を積極的に推進していく。

国際連携を通じて得られた事例やベストプラクティス等について、国内の関係主体への情報発信を強化していくよう努める。

また、サイバー攻撃は容易に国境を越えることや、サイバー攻撃に関するインシデントの国際的な動向把握が重要であることから、政府機関における取組に加え、重要インフラ事業者等においても、取組を海外の同業他社に展開したり、海外の動向把握を行ったり等、多角的・多面的な国際連携を可能な限り促進する。

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を十全に講じていくためには、必要な規格・基準及び参照すべき規程類の整備が不可欠である。

5.3.1 重要インフラ防護業務規程集の発行

重要インフラ防護に関係する者が共通に参照する、「情報セキュリティ戦略」、「重要インフラの情報セキュリティ対策にかかる行動計画」、「重要インフラの情報セキュリティ対策にかかる行動計画の実施細目」等、情報セキュリティ戦略を頂点とする関連文書について、内閣官房は、これらを合本した「重要インフラ防護業務規程集」を発行し、ナレッジベースの平準化を図る。

5.3.2 重要インフラ防護に関連する関連規格の可視化

重要インフラ防護に関して、国内外で関連規格が策定されてきている。

こうした状況を踏まえ、内閣官房は、他の関係主体と協力して、関連規格を整理し、可視化することによって、必要な時に必要な関連規格が参照できるようにする。

5.3.3 情報セキュリティに関する評価・認証制度の導入

制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討が進められていることを踏まえ、内閣官房は、他の関係主体と協力して、制御系機器・システムの第三者認証制度の拡充を支援する。

5.3.4 重要インフラ防護に適用するセクター規格の策定

重要インフラ防護は、今後一層の国際的な取組を展開していく必要がある。このため、重要インフラ防護に対する考え方、対策などについて、国際整合性を図っていく必要がある。

しかしながら、国際的に用いられている一般的な情報セキュリティ関連規格をそのままの形で我が国の重要インフラ防護に適用できるものは現在存在していない。

このため、内閣官房は、他の関係主体を協力して、国際基準を参考としながら、重要インフラ防護への適用のための指針や、セクター規格の策定について検討していく。

重要インフラ防護の国際的な基準がないことを踏まえると、我が国で重要インフラ防護に対する基準類を策定し、ASEAN各国に提案することや、ISOなどの国際規格に提案することも検討する。

Ⅳ．関係主体において取り組むべき事項

1．行動計画の推進体制

第２次行動計画に示した情報セキュリティ対策の柱は、重要インフラ事業者等を始めとした民間事業者等がとる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関係機関等において実施する事が望ましい施策によって支えられる。関係主体はそれぞれ以下の役割を基本として、情報セキュリティ対策を推進する事が期待される。

内閣官房は、関係主体の協力を得て、各重要インフラ分野に共通の分野横断的に実施すべき施策に取り組む。また、関係主体の協力を得て、重要インフラ防護に資する官民の体系的な情報共有体制の整備を推進する。また、各関係主体の防護能力の向上を支援する。

重要インフラ所管省庁は、我が国全体として重要インフラを防護するために、内閣官房が行う施策と連動した施策に取り組む。また、重要インフラ事業者等の情報セキュリティに関する活動の把握に努めるとともに、重要インフラ事業者等への情報提供、助言、指導等に取り組む。

情報セキュリティ関係省庁は、内閣官房を中心とした我が国全体としての重要インフラ防護に資する施策に取り組む。

事案対処省庁は、内閣官房を中心とした我が国全体としての重要インフラ防護体制に資する施策に取り組む。

関係機関は、我が国全体の重要インフラ防護体制の強化のための施策及び対策に取り組むことが期待される。

重要インフラ事業者等は、内閣官房で行う施策と連動した対策に取組、官民連携の実効性を高めるよう努めることが期待される。また、セプター及びセプターカウンシルの活動に協力することが期待される。

セプターは、重要インフラ防護に資する自分野内の情報共有の充実に努めることが期待される。また、内閣官房及び重要インフラ所管省庁との情報共有の充実に努めるとともに、セプターカウンシルに参加し、分野横断的な情報共有の推進に努めることが期待される。

セプターカウンシルは、セプター間の分野横断的な情報の共有の推進を図ることが期待される。

2. 各関係主体の取組

2.1 内閣官房の施策

2.1.1 「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並びに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。

⑥ 「情報共有体制の強化」に関する施策

(1) 各関係主体の位置付けの見直し

① 各関係主体の協力を得つつ、各関係主体との位置付け、役割を明確にした上で、情報の整理を実施。

② 新たな分野や関係主体と、既存分野との連携を視野にいれた情報の整理を実施

③ 整理された情報をもとに、実施細目の見直しを実施。

④ 見直した実施細目に対して、重要インフラ所管省庁の協力を得つつ、必要に応じ、セプターや重要インフラ事業者等に周知。

⑤ 実施細目及び参考資料について、関係主体の協力を得つつ、適宜見直しを実施。

(2) 情報共有機能の強化に向けた共有すべき情報の見直し

① 各関係主体の協力を得つつ、共有対象とする情報及びその共有方法の整理を実施。

② ＩＴ障害が発生した際に連絡すべき情報を、新たな脅威等を踏まえた上で、整理を実施。

③ 整理された情報をもとに、情報連絡を頂く際のＩＴ障害情報の見直しを実施。

④ 見直したＩＴ障害情報に対して、重要インフラ所管省庁の協力を得つつ、必要に応じ、セプターや重要インフラ事業者等に周知。

⑤ 見直したＩＴ障害情報に対して、情報共有を行うことで、他の重要インフラ事業者等において、自らの運用や対策等の確認に活かされているかどうかの確認。

⑥ ＩＴ障害情報について、関係主体の協力を得つつ、適宜見直しを実施。

(3) セプターの強化

⑥ 重要インフラ所管省庁の協力を得つつ、定期的に各セプターの機能や活動状況を把握するための調査・ヒアリング等を実施。

⑦ 先進的なセプターの機能や活動の紹介。

(4) セプターカウンシル

① セプターカウンシルに参加するセプターと連携しつつ、運営及び活動に対する支援を実施。

② 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を実施。

(5) 大規模ＩＴ障害対応時の情報共有体制の整理

① 各関係主体の協力を得つつ、大規模ＩＴ障害等を想定した上で、各関係主体との情報の整理を実施。

② これまでの情報連絡・情報提供の枠組みを拡大し、防災関係省庁との位置付け、役割を明確にした上で、情報の整理を実施。

③ 平時と大規模ＩＴ障害対応時における情報連絡・情報提供の連携の整理を実施。

④ 整理された情報をもとに、実施細目の見直しを実施。

⑤ 各関係主体の協力を得つつ、適宜見直しを実施。

2.1.2 「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 分野横断的演習の機会を活用して、リスク分析の結果の検証及び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・事業継続計画等の検討の状況把握等を実施し、その結果を演習参加者等に提供。

⑤ 分野横断的演習の改善策検討。

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。

2.1.3 「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による関係主体間の共通認識の醸成。

② 環境変化や相互依存性についての継続的調査・分析。

③外部の研究機関等に広く協力を求め、同研究機関との協業により調査・分析内容の質を向上。
④当該研究機関等と重要インフラ事業者等との円滑な情報交換、意思疎通を推進。
⑤調査・分析の報告書を取りまとめ、重要インフラ事業者等におけるリスク分析等の基礎資料として、また安全基準等に反映する基礎資料として提供。
⑥重要インフラ事業者等のリスクコミュニケーションを支援。

2.1.4 「防護基盤の強化」に関する施策

(1) 広報公聴活動

①Web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。

(2) 国際連携

①世界的な枠組みに加え、日米等の二国間や日ASEAN等の多国間での連携等を推進。
②国際連携を通じて得られた事例やベストプラクティス等について、国内の関係主体への情報発信。

(3) 規格・標準及び参照すべき規程類の整備

①重要インフラ防護に関係する者が共通に参照する、関連文書を規程集と発行し、ナレッジベースの平準化を図る。
②関連規格を整理、可視化。
③制御系機器・システムの第三者認証制度の拡充を支援。
④国際基準を参考としながら、重要インフラ防護への適用のための指針や、セクター規格の策定について検討。

2.2 重要インフラ所管省庁の施策

2.2.1 「安全基準等の整備及び浸透」に関する施策

①安全基準等として新たに位置付けることが可能な基準及びガイドライン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自らが安全基準等の策定主体でない場合は、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。

2.2.2 「情報共有体制の強化」に関する施策

(1) 各関係主体の位置付けの見直し

① 情報の適切な収集・提供・共有を行う体制強化のための、内閣官房との連携。

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 情報提供、情報連絡の充実、運用改善のために内閣官房が行う実施細目の見直し、並びにこれらをセプター及び重要インフラ事業者等へ周知する際の協力。

④ 重要インフラ事業者等からのＩＴ障害に係る報告について、実施細目及び重要インフラ事業者等との間の情報共有ルールに則って内閣官房への情報連絡を実施。

⑤ 内閣官房からの情報提供について、実施細目及びセプターとの間の情報共有ルールに則ってセプターへの情報提供を実施。

(2) 情報共有機能の強化に向けた共有すべき情報の見直し

① 情報提供、情報連絡の充実、運用改善のために内閣官房が行うＩＴ障害情報の見直し、並びにこれらをセプター及び重要インフラ事業者等へ周知する際の協力。

② 重要インフラ事業者等からのＩＴ障害に係る報告について、ＩＴ障害情報の見直し結果に基づいた記載に則って内閣官房への情報連絡を実施。

(3) セプターの強化

① 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。

② セプターの機能充実への支援。

(4) セプターカウンシル

① セプターカウンシルへの支援。

② セプターカウンシルからの要望があった場合、意見交換等を実施。

2.2.3 「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、分野横断的演習結果の施策への活用に努める。

2.2.4 「リスクマネジメント」に関する施策

① 重要インフラ事業者等と内閣官房が円滑な協力体制を構築できるよう重要インフラ事業者等と調整。

② 環境変化調査や相互依存性解析を必要とする取組対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供。

③ 環境変化調査や相互依存性解析の結果として提供される基礎資料の評価。

④ 環境変化調査や相互依存性解析の結果として提供される基礎資料の施策へ活用。

⑤ 重要インフラ事業者等のリスクコミュニケーションを支援。

2.2.5 「防護基盤の強化」に関する施策

(1) 国際連携

① 世界的な枠組みに加え、日米等の二国間や日ASEAN等の多国間での連携等を推進。

② 国際連携を通じて得られた事例やベストプラクティス等について、国内の関係主体への情報発信。

(2) 規格・標準及び参照すべき規程類の整備

① 内閣官房と協力し、関連規格を整理、可視化。

② 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 内閣官房と協力し、国際基準を参考としながら、重要インフラ防護への適用のための指針や、セクター規格の策定について検討。

2.3 情報セキュリティ関係省庁の施策

2.3.1 「情報共有体制の強化」に関する施策

① 保有する能力・機能に応じ、テロ関連情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等の収集

② 情報の収集、提供、共有を行う体制強化のための内閣官房との連携を推進し、内閣官房に対する積極的な情報提供を実施

③ 情報提供、情報連絡の充実及び運用改善のために内閣官房が行う実施細目の見直しへの協力

④ セプターカウンシルからの要望があった場合、意見交換等を実施

2.4 事案対処省庁の施策

2.4.1 「情報共有体制の強化」に関する施策

① 保有する能力・機能に応じ、テロ関連情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等の収集

② 情報の収集、提供、共有を行う体制強化のための内閣官房との連携を推進し、内閣官房に対する情報提供を実施

③ 情報提供、情報連絡の充実及び運用改善のために内閣官房が行う実施細目の見直しへの協力

④ セプターカウンシルからの要望があった場合、意見交換等を実施

2.5 関係機関の自主的な取組として期待する事項

2.5.1 「情報共有体制の強化」に関する施策及び対策

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 情報提供、情報連絡の充実、運用改善のために内閣官房が行う実施細目の見直しに対する協力

③ 内閣官房に対して、積極的な情報提供の実施

④ 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

⑤ 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

⑥ 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

2.6 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

2.6.1 「安全基準等の整備及び浸透」に関する施策

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における検知・回復に係る取組、関係性を有する主体間での情報共有、環境変化に伴い生じた脅威、擬似インシデントを契機とした訓練・演習及び内部・外部監査等から課題を抽出し、リスク見積りに基づく評価

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

2.6.2 「情報共有体制の強化」に関する施策

① セプター内の情報取扱いルールの内容を適切に運用するとともに、セプター構成員としての活動を実施

② 情報共有体制を維持し、ＩＴ障害発生時に必要に応じて情報連絡を実施

③ 保有する能力・機能に応じた、重要インフラ事業者等に提供すべき情報（テロ関係情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等）の収集

④ 関係機関との合意に基づく補完的な情報共有の実施

⑤ セプターカウンシルからの要望に応じての活動の実施

2.6.3 「障害対応体制の強化」に関する施策

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の維持・向上に努める

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、事業継続計画等への取組に対し、分野横断的演習結果の活用に努める

2.6.4 「リスクマネジメント」に関する施策

① 自組織における情報セキュリティのリスクマネジメントを推進、強化

② 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脅威等を環境変化調査や相互依存性解析の取組対象として提案

③ 内閣官房、及び、環境変化調査や相互依存性解析で協業対象となる外部研究機関との円滑な情報交換、意思疎通の実現

④ 環境変化調査や相互依存性解析に必要な実際的な情報を、積極的に内閣官房に提供

⑤ 環境変化調査や相互依存性解析の議論・検討に参画

⑥ 環境変化調査や相互依存性解析の成果として提供される基礎資料の評価

⑦ 環境変化調査や相互依存性解析の結果として提供される基礎情報を自組織のリスク分析等への活用

⑧ 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主体間でリスク

コミュニケーションの充実に努める

2.6.5 「防護基盤の強化」に関する施策

(1) 国際連携

① 取組を海外の同業他社に展開したり、海外の動向把握を行ったり等、多角的・多面的な国際連携を促進。

(2) 規格・標準及び参照すべき規程類の整備

① 内閣官房と協力し、関連規格を整理、可視化。

② 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 内閣官房と協力し、国際基準を参考としながら、重要インフラ防護への適用のための指針や、セクター規格の策定について検討。

2.7 セプターの自主的な対策として期待する事項

2.7.1 「情報共有体制の強化」に関する対策

① 重要インフラ所管省庁等と連携し、セプター内で共有する情報及びセプター内での共有方法の整理を実施するとともに、必要により実態に即した見直しを実施

② 整理した情報及び情報提供の共有方法に基づいたセプター内及び他セプターとの間での情報提供・情報共有の実施

③ 情報提供、情報連絡の充実及び運用改善のために内閣官房が行う実施細目の見直しへの協力

④ 情報疎通機能の定期的な確認

⑤ 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

⑥ 関係機関との合意に基づく補完的な情報共有の実施

⑦ セプターの機能強化・充実

⑧ 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

⑨ セプターカウンシルへの参加

2.7.2 「リスクマネジメント」に関する施策

① 環境変化調査や相互依存性解析に関する重要インフラ事業者等の自主的な取組に参加

2.7.3 「障害対応体制の強化」に関する施策

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

2.8 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

2.8.1 「情報共有体制の強化」に関する対策

① 共有対象とする情報及びその共有方法の整理の実施

② 内閣官房が実施する実施細目の見直し、参考資料の作成時等における改善の提案、内閣官房から重要インフラ事業者等への情報を提供する体制の改善に係る提案を行うこと等についての検討を実施

③ 整理した共有対象とする情報及びその共有方法を踏まえた、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 政府機関等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

2.9 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

2.9.1 「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、積極的な情報提供の実施

2.9.2 「障害対応体制の強化」に関する施策

① 必要に応じて分野横断的演習への参加

Ⅴ．評価・検証と見直し

1．評価の基本的考え方

本行動計画については、個々の情報セキュリティ対策・施策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情報セキュリティ対策・施策により、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の成果の確認の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こととする。

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。

1.1 本行動計画期間の目標（理想とする社会像）

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（個別の重要インフラ事業者等、重要インフラ分野、政府の各層）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、万が一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。

○この枠組みは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情報セキュリティ対策・施策に関する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、各関係主体別に具体化した将来像を記載する。

1.1.1 各関係主体共通

各関係主体別における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、互い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。

○関係主体が連携して重要インフラ防護に取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。

1.1.2　個別の重要インフラ事業者等

個別の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」における以下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。

－社会基盤の情報セキュリティ対策の強化のためには可能な限り情報共有する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」における以下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、脅威や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」における以下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うようになっていること。

1.1.3　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。この実現に向け以下が十分に浸透している。

－本行動計画に基づく諸施策、関係主体間のリスクコミュニケーション、国際連携等を通じて、情報セキュリティ対策に資する多様な情報が内閣官房に寄せられるようになっていること

－これを踏まえて関係主体との連携を図っていること

○特に、特異重大な脅威やＩＴ障害に係るリスクについての認識が得られ、これへの対処が重要インフラ事業者等だけでは困難な場合は、関係主体間の有機的な連携によって、解決策の検討とその実現に向けた調整が速やかに実施されるようになっている。

1.2　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、そ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、関係主体がそれぞれの取組を通じて得た経験を、行動計画の関係主体の全体で共有し、それぞれがそれぞれの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着目するのではなく、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。

1.3　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。行動計画に基づく様々な情報セキュリティ対策・施策が相互に関連して結果をなすものであることに鑑み、個別の情報セキュリティ対

策・施策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・強化に資する情報セキュリティ対策・施策の全体、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こととする。

この際、行動計画の枠組みの評価を行う際には、情報セキュリティ対策の施策群ごとの個別の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、補完調査を実施することとする。

また、行動計画に基づく取組の成果の評価は、そ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、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。

1.4　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群に着目して行う。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ととする。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事が重要である。

これらの確認・検証、補完調査は、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、情報セキュリティ会議に付議する。なお、そのために必要な調査検討は、重要インフラ専門委員会が主管の下、重要インフラ所管省庁の協力を得て内閣官房が行う。

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事に鑑み、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。

1.4.1　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、互いが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、重要インフラの分野ごとの重要インフラサービスについて、サービス維持レベルを超えた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、サービス維持レベルを超えたＩＴ障害事例のうち内閣官房が認知したものの分野全体での総数とする。

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事が適当である。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。

1.4.2　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Ⅱ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。

施策の成果検証では、それぞれの情報セキュリティ対策の施策群ごとに、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する。具体的な指標は以下のとおりとする。

(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を目指し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。

具体的な指標は、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率、重要インフラ事業者等による指針への評価とする。

(2) 情報共有体制の強化

「情報共有体制の強化」により期待される成果は、関係主体間で共有する情報についての整理がなされ、情報提供、情報連絡等に必要な環境整備等が進展し、各セプタ

ー、セプターカウンシルの自主的な活動が充実強化された結果として、重要インフラ事業者等が必要な情報を享受し、活用できるようになっていることである。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。具体的な指標は、内閣官房が発信した情報件数、セプター等で共有された情報件数、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コミュニケーションの機会の開催回数、共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数とする。

「情報共有体制の強化」により期待される成果は、関係主体間で共有する情報についての整理がなされ、情報提供、情報連絡等に必要な環境整備等が進展し、各セプター、セプターカウンシルの自主的な活動が充実強化された結果として、重要インフラ事業者等が必要な情報を享受し、活用できるようになっていることである。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。具体的な指標は、内閣官房が発信した情報件数、セプター等で共有された情報件数、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コミュニケーションの機会の開催回数、共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数とする。

(3) 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、リスク分析とリスクコミュニケーションに対する支援に着目した指標を設定する。具体的な指標は、リスク分析の支援として、実施した環境変化調査や共通脅威分析等の件数とリスクコミュニケーションとして、セプターカウンシルや分野横断的演習等における関係主体間が情報交換できる機会の開催回数に加え、これら施策に対する重要インフラ事業者等による評価とする。

(4) 障害対応体制

「障害対応体制」に期待される成果は、分野横断的演習を中心とする演習・訓練への参加を通して、重要インフラ事業者等のＩＴ障害発生時の早期復旧手順、事業継続計画等の検証、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などに対する貢献である。各演習・訓練で得られた知見を現実のＩＴ障害発生時の事業継続、早期復旧活動に効果的に活用できるものとするためには、より現実の状況を模擬し、参加者の求める目的や効果に応じた多様な各種演習・訓練の実施が望ましい。そのため、演習参加組織の拡充、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・訓練と、演習・訓練で得られた知見が、重要インフラ事業者等の取組に貢献したかどうかに着目した指標を設定する。具体的な指標は、分野横断的演習の参加組織数、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の他、分野横断的演習を含

め組織内外で実施する演習・訓練への参加状況とする。

(5) 防護基盤の強化

「防護基盤の強化」に挙げた施策のうち、「広報公聴活動」に期待される成果は、行動計画の枠組みついて広く国民の理解を得ることと、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る。そのため、本行動計画の周知機会の充実に着目した指標を設定する。具体的な指標は、Webサイトのコンテンツの充実度、行動計画を紹介したセミナー等の回数とする。

また、国際連携の強化で期待される成果は、二国間、多国間交流を通じた各国関係機関との情報交換の機会や支援・啓発である。具体的な指標は、二国間、多国間による意見交換の回数、今後重要インフラ防護に力を入れようとする国への啓発・支援の回数とする。

(6) 調査活動の充実

これらの施策が重要インフラ事業者等の対策にどう活かされたかを把握することは重要である。内閣官房は関係主体が自主的にまとめている統計情報の収集を進めるとともに、自らの調査活動の充実を図ることとする。この際、施策の対策への効果をより高めるために、内閣官房は重要インフラ事業者等のサービスレベルの設定状況を可能な範囲で把握することとする。なお、この際、重要インフラ事業者等に過度の負担をかけないよう配慮する事が必要である。

別添：情報提供・情報連絡について

1. ＩＴ障害に関する情報

「ＩＴ障害に関する情報」とは、ＩＴ障害、ＩＴの機能不全等に関する情報セキュリティ対策に資する幅広い情報である。

ＩＴ障害に関する情報には、①ＩＴ障害の未然防止、②ＩＴ障害の拡大防止・迅速な復旧、③ＩＴ障害の要因等の分析・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並びに相互依存性のある重要インフラ分野間においてはこれら情報を共有する体制を強化することが必要である。

ＩＴ障害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障害発生の脅威に係る情報（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

2. 重要インフラ事業者等への情報提供

2.1 （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なうことができる。

2.2 情報提供の内容

情報提供は、情報セキュリティ関係省庁、事案対処省庁、関係機関等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ものとする。

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ものとする。

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。

2.3 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において所管分野ごとに選任されたリエゾン（内閣官房併任）を通じて行う。その際、情報の参照者にとっての当該情報の活用を容易化することを目的に、その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、識別方法の改善を図ることとする。

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の間で情報共有を図る。

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、（３）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の手順に準ずるものとする。

なお、早期警戒情報等については、その取扱いに注意を要することから、情報提供先と内閣官房との間で情報の取扱いに関する取り決めが合意されていることを条件とする。

2.4 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あたり、情報セキュリティ関係省庁、事案対処省庁、関係機関と連携する。

① 情報セキュリティ関係省庁、事案対処省庁、関係機関から提供される幅広い情報の集約。
② 攻撃がテロによるものと思われる場合における被災情報等の事案対処省庁への提供及び攻撃手法情報等の情報セキュリティ関係省庁への提供。
③ 情報の集約・分析においては、必要に応じ、関係機関に連携等を要請。
④ 災害に関する情報については、内閣官房、内閣府及び関係省庁間の既存の情報共有体制の下で情報を集約及び共有。

2.5 情報の質の強化（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、その質の強化を図る。

① 情報を突き合わせることによる精度の向上
② これに基づく重要度・優先度の判断
③ 第１次行動計画で実施された相互依存性解析及び今後実施される共通脅威分析に基づく影響予測
④ 他の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脅威により発生したＩＴ障害について、その内容、規模により、統計的な発生状況を把握

3. 重要インフラ事業者等からの情報連絡

3.1 情報連絡を行う場合と連絡する情報

情報連絡が必要となる場合は、以下に掲げる場合であって、法令等で報告が義務付けられている場合、及び重要インフラ事業者等が特異重大なものとして連絡を要すると判断した場合である。

①サイバー攻撃をはじめとする意図的要因による次の場合

－ＩＴ障害が発生した場合

－サイバー攻撃を検知した場合又は攻撃の予告があった場合

－サイバー攻撃による被害を検知した場合

－ＩＴの機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合

②非意図的要因による次の場合

－ＩＴ障害が発生した場合

－ＩＴの機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合

③災害や疾病による次の場合

－ＩＴ障害が発生した場合

－２次被害によりＩＴ障害が発生すると考えられる場合

－ＩＴの機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合

④他分野の障害からの波及による次の場合

－ＩＴ障害が発生した場合

－ＩＴの機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合

なお、上記に該当しない場合においても、各重要インフラ事業者等のＩＴ障害が他の重要インフラ事業者等のＩＴ障害に波及あるいは影響を及ぼすおそれがある場合など、ＩＴ障害の未然防止、被害の拡大防止等に資すると考えられる場合や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。

3.2 情報連絡の内容

情報連絡の内容は、ＩＴ障害発生時における利用可能な連絡手段、連絡担当者等の連絡を確保するための情報を必須とするほかは、その時点で判明している情報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

も差し支えないものとする。

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障害に関する共通の分類及びカテゴリの設定等は別に定める「実施細目」によるものとする。なお、「実施細目」については、各重要インフラ事業者等の運用性等も勘案し、必要に応じて見直しを行う。

3.3 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」に示された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 重要インフラ事業者等から受けた連絡については、重要インフラ所管省庁の当該分野担当のリエゾンから、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識別管理し、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ものとする。

3.4 連絡された情報の取扱いに関する考え方

本連絡・連携体制において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）として取り扱うものとする。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。

別紙１　対象となる重要インフラと重要システム

重要インフラ分野	ＩＴ障害やその影響の例	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	・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	・主要な電気通信事業者 ・主要な地上基幹放送事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融　銀行等 生命保険 損害保険 証券	・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・株式等の振替えの停止 ・金融商品取引の清算の停止　　等	・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
航空	・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・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
鉄道	・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	・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・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	・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
ガス	・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	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・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	・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）
医療	・診療支援部門における業務への支障等	・医療機関	・診療録等の管理システム （電子カルテシステム、遠隔画像診断システム等）
水道	・水道による水の供給の停止 ・不適当な水質の水の供給　　等	・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
物流	・輸送の遅延・停止 ・貨物の所在追跡困難	・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

注１　ここに掲げている対象事業者等は、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、対象とする事業者等の見直しを行うこととする。

注２　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		重要インフラサービス（手続きを含む）（注）		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無線通信の送信（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
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の機能不全により、預金の払戻しの遅延、停止が生じないこと ・ＩＴの機能不全により、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の機能不全により、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（資金決済法第２条第５項）	・ＩＴの機能不全により、資金清算の遅延、停止が生じないこと	・資金決済法第72条を参照
		・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の機能不全により、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の機能不全により、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の機能不全により、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		重要インフラサービス（手続きを含む）（注）		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の機能不全により、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の機能不全により、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（振替法第８条）	・ＩＴの機能不全により、社債・株式等の振替え等に遅延、停止が生じないこと	・一般振替機関の監督に関する命令第17条を参照
		・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の機能不全により、金融商品取引の清算等に遅延、停止が生じないこと	・金融商品取引清算機関等に関する内閣府令第48条第４項及び第５項を参照
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 ・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） ・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 ・飛行計画の作成、航空局への提出	・ＩＴの機能不全により、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
鉄道		・旅客輸送サービス	・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）	・ＩＴの機能不全により、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

重要インフラ分野	重要インフラサービス（手続きを含む）（注）		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
	・発券、入出場手続き	・座席の予約、乗車券の販売、入出場の際の乗車券等の確認		
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の機能不全により、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の機能不全により、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の機能不全により、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 ・診療録及び診療諸記録類等の記録・保存	・ＩＴの機能不全により、診療録等の保存に支障が生じないこと	・ＩＴの依存度によらず、診察や治療等の行為は継続可能である ・保存に関しては、即時を求めるものではなく、医師法第24条第２項による
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の機能不全により、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 ・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19年６月19日事務連絡）の「5.(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の機能不全により、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

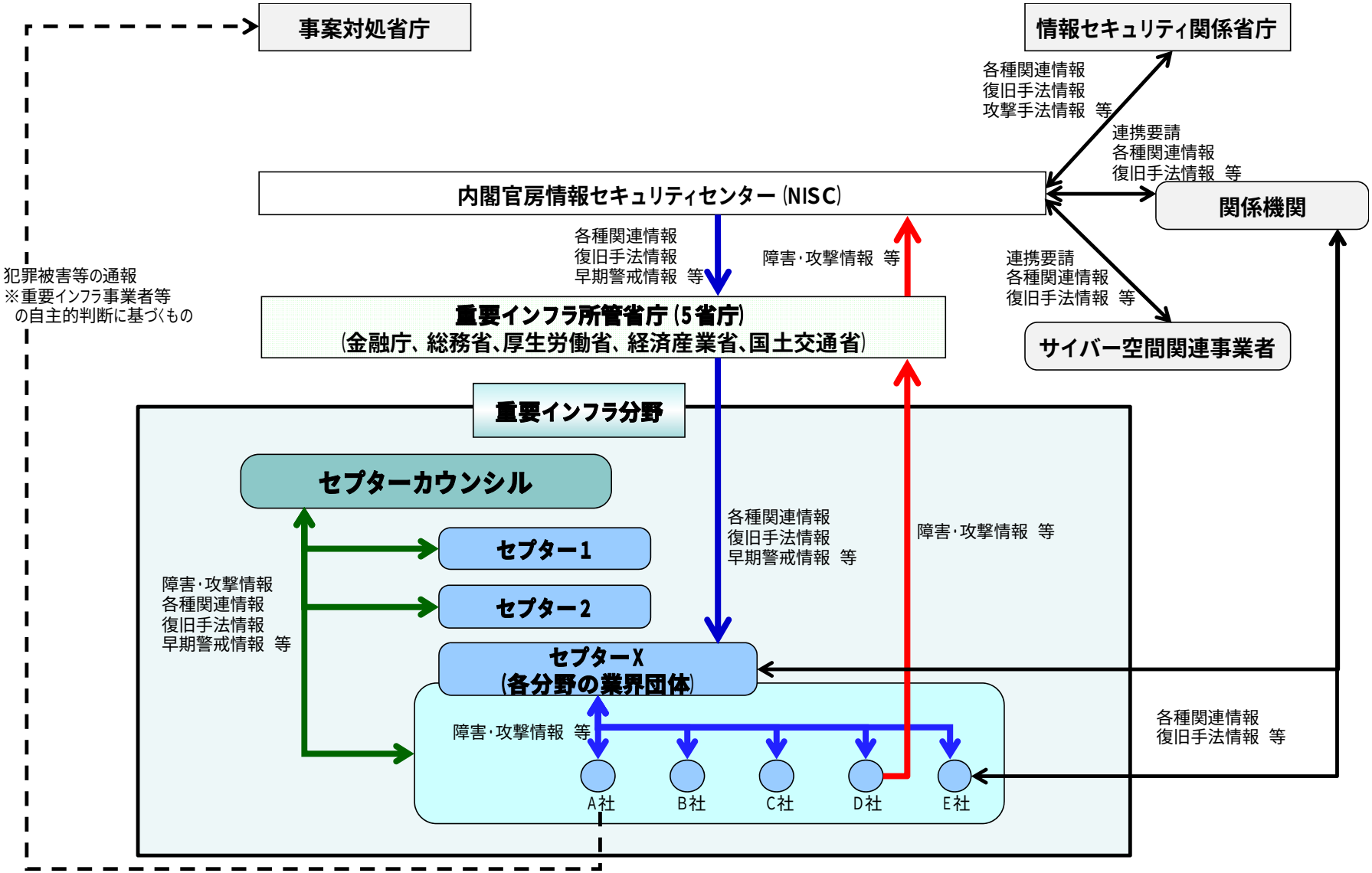
注　本行動計画の目標から、ＩＴを全く利用していないサービスについては対象外。

別紙３　ＩＴ障害の事例と原因の例

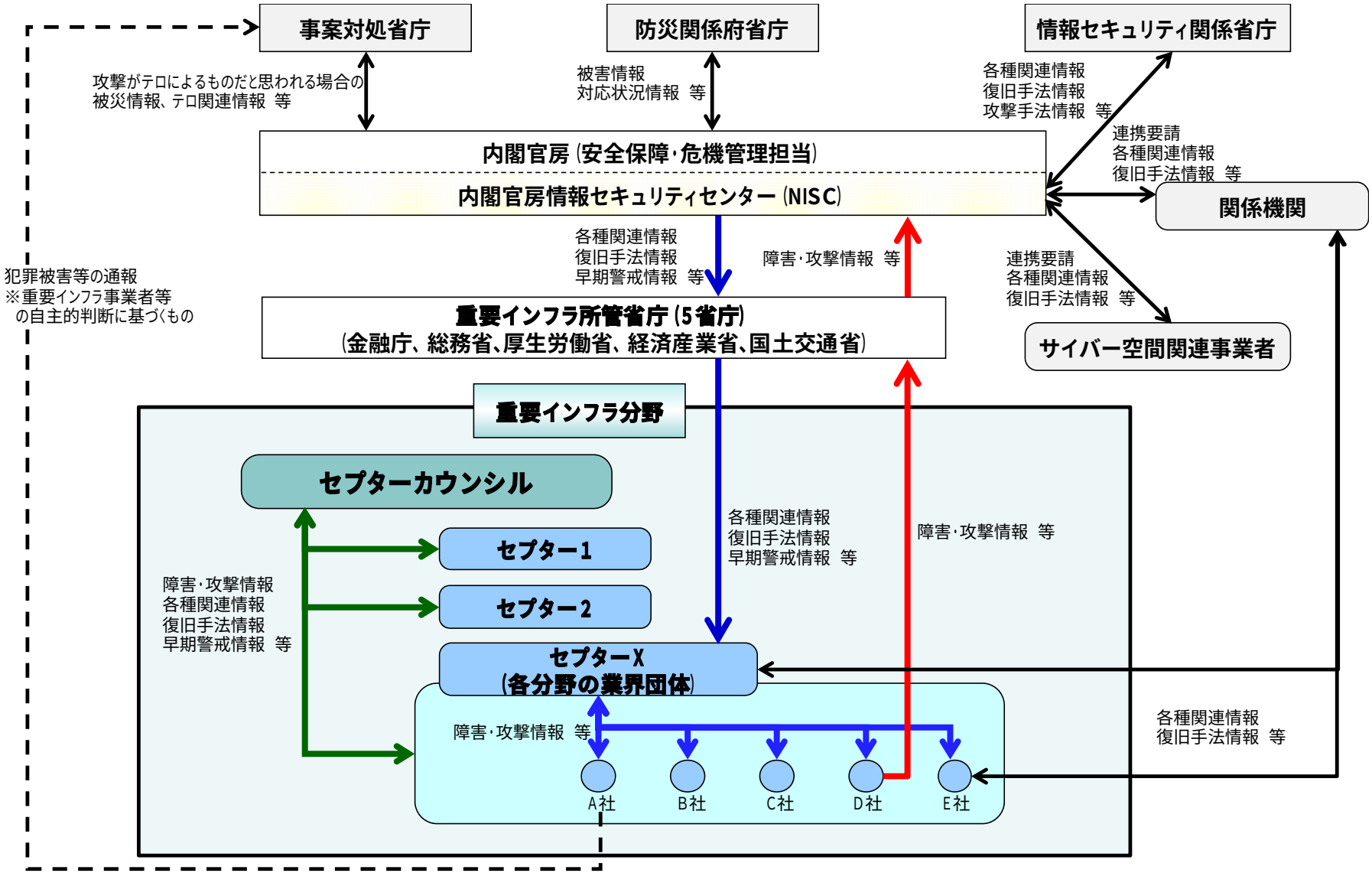
事象の類型		事象の例	説明
未発生の事象		予兆、ヒヤリハット	サイバー攻撃の予告や事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信等によるヒヤリハットなどの発生
発生した事象	機密性を脅かす事象	情報の漏えい	組織の機密情報等の流出など、機密性が脅かされる事象の発生
	完全性を脅かす事象	情報の破壊	Webサイト等の改ざんや組織の機密情報等の破壊など、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やWebサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記に繋がる事象	マルウェア等の感染	マルウェア等に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、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	システムの脆弱性等、その他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		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	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

別紙６　定義・用語集

AIST	独立行政法人産業技術総合研究所
IPA	独立行政法人情報処理推進機構
ＩＴ障害	重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、ＩＴの機能不全が引き起こすもの。
JPCERT/CC	有限責任中間法人 JPCERT コーディネーションセンター
NICT	独立行政法人情報通信研究機構
Telecom-ISAC Japan	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
関係機関	警察庁サイバーフォース、NICT、AIST、IPA、Telecom-ISAC Japan、JPCERT/CC 等
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、関係機関、重要インフラ事業者等、セプター、セプターカウンシル等をさす。
脅威	ＩＴ障害を引き起こしうる要因。
サービス維持レベル	重要インフラサービスが一定水準を下回った場合にこれを検証対象する水準の状態。
サイバー空間関連事業者	サイバー空間に係る製品、サービスや技術等を提供する事業者。
事案対処省庁	警察庁、消防庁、海上保安庁、防衛省
システムベンダー	顧客（主にここでは重要インフラ事業者等を指す）の業務内容を分析し、業務システムの設計、構築、運用等の業務を行う事業者。企画・立案から、構築・導入、完成したシステムの保守・管理までを行う。
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。 「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」及び「物流」の 10 分野。【Ｐ】
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、重要インフラ分野の対象となる事業者等に指定された者及びこれらの者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、国土交通省【Ｐ】
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	見聞や知識、ノウハウを、仲間に伝達し共有すること。組織やメンバー間で知識や情報などを伝達し合うこと。
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、防衛省
情報セキュリティ対策	重要インフラの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	重要インフラ事業者等の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をいう。
情報連絡	重要インフラ事業者等におけるＩＴ障害等の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をいう。
セキュリティベンダー	主にウィルス対策ソフトウェアをはじめとするセキュリティ対策ソフトウェアや関連サービスを開発・提供している事業者。
セプター (CEPTOAR)	官民の情報共有体制の整備、情報共有体制である「情報共有・分析機能。 Capability for Engineering of Protection, Technical Operation, Analysis and Response
セプターカウンシル (CEPTOAR-Council)	重要インフラそれぞれの分野で整備された CEPTOAR の代表で構成される協議会。

プラットフォームベンダー	業務システムを構成するにあたり、ハードウェア、ソフトウェアの根幹となるプラットフォームを提供する事業者。
防災関係府省庁	内閣府、警察庁、消防庁、防衛省【Ｐ】