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

「安心があたりまえ」
～誰もが安心できる社会基盤に～
【案】

情報セキュリティ政策会議

年　月　日

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
「安心があたりまえ」　～誰もが安心できる社会基盤に～

Ⅰ　総論

１　目標

（１）行動計画の目標

「重要インフラの情報セキュリティ対策に係る行動計画（2005 年 12 月 13 日情報セキュリティ政策会議決定）」（以下「第１次行動計画」という。）の目的は、「官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化すること」であった。また、我が国全体の情報セキュリティ政策の中長期の戦略として定めた「第１次情報セキュリティ基本計画（2006 年 2 月 2 日情報セキュリティ政策会議決定）」に位置づけを得てからは、「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」ことを目指して政府及び重要インフラ[1]10 分野等からなる関係主体[2]による取組みを進めてきた。

この結果 2008 年度末までに、「重要インフラにおける情報セキュリティの確保に係る「安全基準等[3]」策定にあたっての指針」（以下「指針」という。）の策定、及びこれに基づく分野毎の安全基準等の策定・見直しが行われ、これらを定期的に見直すサイクルが確立した。また、官民の情報共有体制の構築が進められ、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（CEPTOAR[4]）」（以下「セプター」という。）の整備が完了し、各セプター間での横断的な情報共有体制である「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）[5]（以下「セプターカウンシル」という。）が整備される見込みである。さらに、IT 障害[6]発生時の事業継続等に対応するために分野間の相互依存性の解析や、具体的なシナリオに基づく分野横断的な演習を行った。

これによって、関係主体間の連携の基礎が整うとともに、各関係主体において情報セキュリティ対策[7]の充実に資する気付きや共通認識の醸成を進める土壌が育ちつつある。

第１次行動計画の取組みを進める間にも、IT の利用はさらに広範にわたるものとなっており、重要インフラ事業者等の業務効率化や、サービスの

---

1 「重要インフラ事業者等」とは、後述「２　定義と対象範囲」を参照のこと。
2 「関係主体」とは、後述「２　定義と対象範囲」を参照のこと。
3 「安全基準等」とは、重要インフラ事業者等が、様々な判断、行為を行うに当たり、基準又は参考にするものとして策定された文書類を指す。
4 CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response
5 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）：第１次行動計画において平成 20 年度までに設置することが目標とされている、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。本行動計画策定時点では創設に向けた検討が進められているところであり、正式名称が決定していない。そのためその名称や創設時期については検討状況によって変更が生じうる。
6 「IT 障害」とは、後述「２　定義と対象範囲」を参照のこと。
7 「情報セキュリティ対策」とは、後述「２　定義と対象範囲」を参照のこと。

利便性向上などの面で様々な工夫や進歩が続いている。また、サービス利用者においても、ネットワーク環境の充実やITリテラシーの高まりによって、IT を利用したサービスに触れる機会が増えている。今後も国民生活や社会経済活動は引き続きITの利用を拡大しながら発展を続けると予想されるが、これは同時に社会がITへの依存度を高める傾向にあることを意味する。

これに伴いIT障害の発生の可能性やその影響範囲も潜在的に広がっていくことが予想される。今後も引き続き重要インフラ事業者等のサービスの安定的供給と事業継続性を確保するためには、一般に「業法」と呼ばれる当該分野に属する事業を営む者を規律する法制度の枠組みに加えて、これと整合を図りつつ各重要インフラ事業者等の自主的な取組みを充実させることが求められる。

そのため、重要インフラ防護に責任を有する政府と重要インフラ事業者等が自主的な取組みを進めるにあたっての共通の行動計画として、「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。）を取りまとめた。

第２次行動計画の策定にあたっては、第１次行動計画の進捗を踏まえて認識された課題を中心に検討を行った。検討に際しては、「継続」と「発展」の二つの側面を踏まえることとした。

「継続」の観点からは、第１次行動計画に引き続き、「重要インフラにおける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重要インフラを防護するとともに、重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図る」こととした。また、引き続き「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」ことを目指すこととした。これは、重要インフラの情報セキュリティ対策に取り組む関係主体が保持すべき、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ための不断の努力を怠らないという基本的な姿勢を端的に表すものである。

情報セキュリティ対策を講じるにあたっては、費用対効果や利便性の観点からの制約によって、一定のリスク[8]を受容することが合理的となる場合がある。また、予見し得ない脅威が引き起こすIT障害に対処するためには、IT 障害の発生を想定した対策も必要である。こうした制約や不確定要素を考慮すれば、IT障害の発生を可能な限り未然に防止する予防的対策と、IT障害が発生した際の影響を可能な限り最小化する事後的対策の両方について、技術開発や対策手法の改善を進めるとともに、両方の対策をバランスよく取り入れて対策の実効性を高める事が必要である。

そこで「発展」の観点から、各分野の特性を踏まえつつ現実に即して情報セキュリティ対策の実効性を継続的に改善できるようにするために、新

[8] 本行動計画で「リスク」とは、IT障害やITの機能不全がもたらす不利益全般について、その損害の可能性を指す。

たに分野毎の重要インフラサービス[9]について合理的な水準をサービスレベル[10]として定めることとした。これを踏まえて、第２次行動計画の目標は「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」とする。

そのため、第２次行動計画では、「重要インフラ事業者等のサービスの維持」のための IT 障害の予防的対策と、「IT 障害発生時の迅速な復旧等の確保」のための IT 障害の事後的対策の両方について、必要な対策を広く具体化している。

また、目標の実現に向けて第２次行動計画では各関係主体による様々な情報セキュリティ対策を、重要インフラ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及び関係機関[11]等において実施する事が望ましい施策からなる体系的な枠組みとして整理した。第２次行動計画では目標の達成を期すとともに、この枠組み自体の継続的な改善サイクルを確立することを目指す。

重要インフラの情報セキュリティ対策に取り組む関係主体は第２次行動計画に基づき、官民の緊密な連携の下、情報セキュリティ対策の強化に努めるとともに、重要インフラサービスの維持及び IT 障害発生時の迅速な復旧等の確保に努めることとする。また、第２次行動計画の枠組みの着実な改善を図ることとする。

また、各関係主体がそれぞれの取組みを行うに当たっては、第２次行動計画に示された対策に加えて、現在の技術の改善、協働体制の整備、法制度や経営、人材の総合的開発等に関する事項にも積極的な取組みを行うこととする。

（２）基本的な方向性

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。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んでいる。また、政府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みに対して必要な支援を行っている。

他方、多様なサービスが複雑に絡み合い、また IT の浸透が著しい今日においては、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、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。情報セキュリティ対策に死角を生じさせないよう、分野内の他事業者や他分野の事業者等との連携を充実させなければならない。

しかし、重要インフラ事業者等の取組みはそれが自主的なものであるが故に、その基本的な方向性においても多様性を有する。このような多様性を越えて、分野横断的な視点から互いの経験を活かし合い、また主体的な連携が進めやすい環境を構築するために、各主体が努めるべき基本的な方

---

9 「重要インフラサービス」とは、後述「２　定義と対象範囲」を参照のこと。
10 「サービスレベル」とは、後述「２　定義と対象範囲」を参照のこと。
11 「関係機関」とは、後述「２　定義と対象範囲」を参照のこと。

向性を以下のとおり整理した。
　ここに示す方向性は特定の関係主体に対して一方的に義務を課すものではない。基本的な方向性を具体的に示すことで、各関係主体において自主的な連携が生まれやすくすることと、また各関係主体の取組みが総体としての一貫性を保てるようにすることを期待するものである。

１）指針の遵守に加えて、先進的な対策の活用に努めること
　個別の重要インフラ事業者等の IT への依存度や、他分野との相互依存性の内容は様々である。また、それに応じた各分野における取組みにも多様性が存在する。そのため、規範としての最低基準である指針を設けることによって分野に依らず一律に必要な対策を徹底する取組みと、個別の進んだ対策を整理して自主的な対策に活かせるようにする取組みのそれぞれが重要である。また、こうした取組みについて分野横断的な連携を図ることが重要である。

２）技術面、経営面、法制面での対応の調和を図ること
　情報セキュリティ対策においては技術的な側面に関心が集まりがちである。しかし、重要インフラサービスの維持という観点からは、IT 担当部門だけで取り組むのではなく、いわゆる「情報セキュリティガバナンス[12]」の考え方を踏まえ、情報セキュリティ対策への適切な資源配分、情報セキュリティ対策に関する内部統制、といった要素についても配慮することが重要である。また、官民による適切な関与の下で、法令や業界ルール等との整合性の確保に配慮することが重要である。また、必要な範囲でこうした要素について関係主体間のコミュニケーションを図ることが重要である。

３）顧客サービスの視点と社会的責任の視点の双方に配慮すること
　重要インフラの事業においては、顧客へのサービスという側面から期待される対応と、公益の観点から期待される対応があるが、これらは必ずしも一致するものではない。これまでも各重要インフラ事業者等は自主的な対応によって両方の責任を果たしているところであり、引き続き重要インフラに依存する様々な主体とのリスクコミュニケーション[13]とセキュリティ対策促進のため、社会への説明責任を果たすことが重要である。

４）IT 障害の予防的対策に努め、また予防的対策を過信しないこと
　IT 障害が国民生活や社会経済活動に重大な影響を与えないように重要インフラを防護する観点からは、IT 障害の予防的対策だけでなく、IT 障害発生時に国民生活や社会経済活動への影響を最小限に抑えるための事後的対策も重要である。IT 障害の発生を仮定した上でその影響を最小化するための検討を行い、官民双方がそれぞれ自らの置かれる状況と果たすべき役割を自覚できるようにすることが重要である。

---

[12] 「情報セキュリティガバナンス」とは、企業経営の一環として、情報セキュリティ対策を適切に実施することを意味する。
[13] 「リスクコミュニケーション」については、後述Ⅱ５（２）を参照のこと。

５）IT 障害に関する情報は可能な限り共有すべきと理解すること

個々の重要インフラ事業者等による情報セキュリティ対策は進んでいるものと考えられるが、IT 障害の予防的対策や事後的対策の経験に関する知見や、IT 障害の原因となる脅威に関する知見の共有については、積極的な共有が不十分になりがちである。しかし、これらは対策の改善のための貴重な情報となるとの認識の上で、なお一層の情報共有の取組みを進めることが重要である。

（３）理想とする将来像

第２次行動計画に基づく取組み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。

情報セキュリティ対策に取り組む各関係主体は、各々守るべき重要インフラサービスと維持すべきサービスレベルを踏まえて、自らがなすべき必要な対策を理解している。各関係主体は自らの置かれている状況を正しく認識しており、自らの活動目標を主体的に定めている。各関係主体は各々必要な取組みを進めており、これについて定期的に自己検証を行っている。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。

関係主体は 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。自らの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。

特に重要インフラ事業者等においては、いわゆる「情報セキュリティガバナンス」という考え方が十分に浸透し、情報セキュリティ対策は単に情報システムの構築、運用の観点からだけではなく、企業経営の観点からも検討が必要であることを理解しており、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ようになっている。また、情報セキュリティ対策の対外的な説明に努めている。また、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。

この体制において、重要インフラ事業者等は自らの事業における IT 障害の発生は隠すべきものではなく、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。対策に取り組む関係者は 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毎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。

第２次行動計画に基づき、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、IT 障害は発生していないか、発生しても国民生活や社会経済活動に重大な影響を与えるような事

態には至っていない。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。

重要インフラ事業者等は、各種の対策が進む事や環境が変化することによる、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。こうした関係が対策の継続的な改善の原動力のひとつとなっている。

第２次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。内閣官房はこれを踏まえて関係主体との連携を図り、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。

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、内閣官房、重要インフラ専門委員会、セプターカウンシルの連携によって、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。

このような、各関係主体の自覚に基づく自主的な取組み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。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。また、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。

これらの各関係主体の各々の情報セキュリティ対策に関する取組み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。

２　定義と対象範囲

（１）重要インフラと重要インフラ事業者等

「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、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ある。

第２次行動計画では、「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」及び「物流」の 10 分野の重要インフラを防護対象とする。

「重要インフラ事業者等」とは上記 10 分野に属する事業を営む者のうち、別紙１の「対象となる事業者」に指定された者及びこれらの者から構成される団体である。

（2）重要インフラサービスと重要システム

「重要インフラサービス」とは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毎に定めるものである。第２次行動計画で対象とした分野毎の重要インフラサービスを別紙２に示す。なお、分野によっては対象としたサービスの代表例のみを示している場合がある。

「重要システム」とは、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毎に定めるものである。第２次行動計画で対象となる重要システムの例を別紙１に示す。

なお、別紙１及び別紙２は、情報セキュリティ対策の対象を当該重要インフラサービス及び当該重要システムに限定することを意図してまとめたものではない。ここに挙げていない重要インフラサービス及び重要システムについても、国民生活や社会経済活動に影響を与えるおそれがあるものに対しては、第２次行動計画に基づき情報セキュリティ対策に取り組む必要がある。

（3）サービスレベルと検証レベル

第２次行動計画においては、重要インフラサービスが国民生活や社会経済活動にとって許容可能な水準で安定的に提供され、また利用可能であると見做される状態を「サービスレベル」とする。サービスレベルは別紙２を参考として各重要インフラ事業者毎に定めるものとする。

各重要インフラ事業者等はサービスレベルを維持することを目標として情報セキュリティ対策に取り組むことが望ましい。また、サービスレベルは各重要インフラ事業者等の事業継続計画の目標と乖離しないものとすることが望ましい。

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とすることとし、この水準を「検証レベル」とする。各分野毎の検証レベルを別紙２に示す。

（4）IT 障害

「IT 障害」とは、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である。

ここで IT の機能不全とは、重要システムをはじめとした重要インフラサービスの提供に必要な情報システムが設計時の期待通りの機能を発揮しない状態を指す。

第２次行動計画に基づく取組みの評価・検証に際しては、IT 障害のうち検証レベルを逸脱するものの発生状況を検証することとしている。

（5）脅威

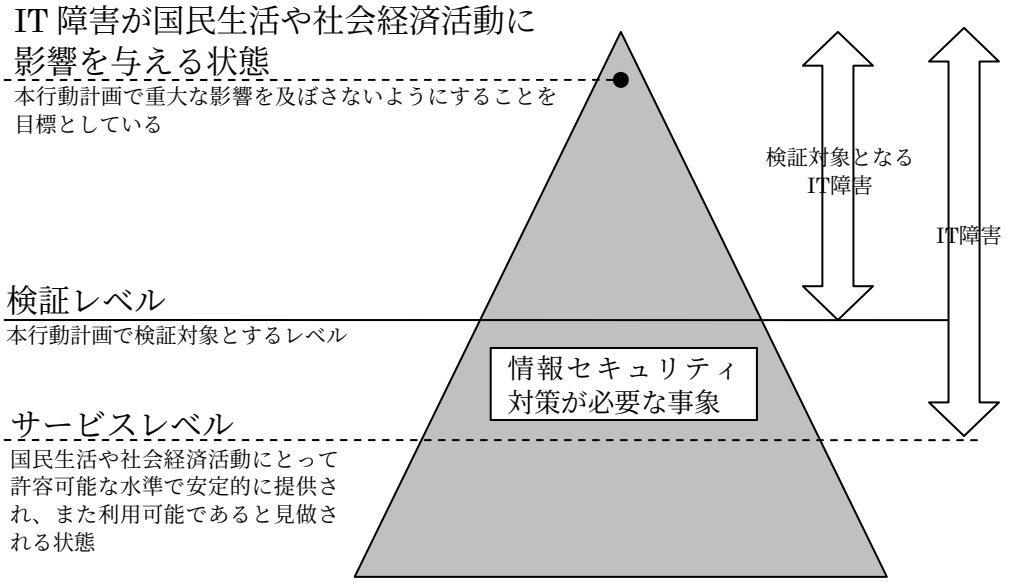
第２次行動計画においては、IT 障害を引き起こしうる要因を「脅威」と呼ぶ。脅威には多種多様なものがあり、またその態様は分野毎の特性によって様々であるが、第２次行動計画では別紙３のとおり４種に類型化している。

重要インフラ事業者等は自らの重要インフラサービスの安定的供給と事業継続性を確保すると共に、自らの IT 障害が他の重要インフラ事業者等の重要インフラサービスの安定的供給と事業継続性の確保への脅威になる可能性にも留意することが必要である。

また、脅威は大きく社会全体で対策が望まれる脅威と、個別の重要インフラ事業者等が中心となって対策する脅威がある。特に前者については分野横断的な連携を積極的に図る事が求められる。

（6）情報セキュリティ対策

第２次行動計画においては「情報セキュリティ対策」とは、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みを指す。情報セキュリティ対策には IT 障害への対策に加えて、IT の機能不全への対策を含む。情報セキュリティ対策の対象となる事象のイメージは下図のとおりである。



図：情報セキュリティ対策が必要な事象のイメージ

情報セキュリティ対策には大別して、IT 障害の発生を可能な限り未然に防止する予防的対策と、IT 障害発生時の迅速な復旧等の確保によりその影響を可能な限り最小化する事後的対策がある。

予防的対策の観点からは、IT 障害を引き起こす原因となる IT の機能不全

そのものを取り除く対策を講じる手法と、IT の機能不全を一定の範囲で受容した上でそのサービスへの影響を制御する対策を講じる手法のふたつがある。これらのいずれの手法に従って対策を講じるべきかは状況によって異なる。

この際、IT の機能不全を受容することとしていたとしても、当該機能不全の重要インフラサービスへの影響の制御に失敗し、結果的に IT 障害が発生することとなれば、事後の改善策としては当該機能不全を取り除く対策が必要となる場合がありえる。そのため第２次行動計画では、IT 障害に対する情報セキュリティ対策と同様に、IT の機能不全に対する情報セキュリティ対策も重視している。

第２次行動計画では重要インフラ事業者等による情報セキュリティ対策を単に「対策」と、また政府による情報セキュリティ対策を「施策」と呼ぶ。

（７）関係主体

第２次行動計画に基づいて情報セキュリティ対策に取り組むことを想定している「関係主体」は、内閣官房、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）、情報セキュリティ関係省庁（警察庁、総務省、経済産業省、防衛省）、事案対処省庁（警察庁、消防庁、海上保安庁、防衛省）、関係機関（警察庁サイバーフォース、NICT[14]、AIST[15]、IPA[16]、Telecom-ISAC Japan[17]、JPCERT/CC[18]　等）、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。

各関係主体が各々の役割に応じて情報セキュリティ対策に取り組むに当たっては、当該関係主体が単独で取り組むほか、IT ベンダーとの連携によって取り組むことが適切な場合がある。また、情報の共有に当たっては、必要に応じて内閣府及び関係省庁間等の既存の情報共有体制と連携を行う。

３　第１次行動計画の成果

第１次行動計画の所期の目標は全て計画期間内に達成される見込みである。主な成果は以下のとおりである。これらは第２次行動計画の基礎を構成している。

（１）安全基準等の整備及び浸透

重要インフラ分野において事業継続及び国民の信頼に応えるとの観点から、各分野毎の安全基準等の策定・改定を支援するために、情報セキュリティ対策を実施する場合、何らかの対処がなされていることが望ましい項

---

[14] NICT：独立行政法人情報通信研究機構
[15] AIST：独立行政法人産業技術総合研究所
[16] IPA：独立行政法人情報処理推進機構
[17] 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
[18] JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター

目を指針として情報セキュリティ政策会議において決定した。これを踏まえて、各分野は必要又は望ましい情報セキュリティ対策の水準を安全基準等として策定した。社会的動向の変化等を踏まえて指針を適時適切なものとするため、指針の見直しを行うとともに、これに伴う安全基準等の見直しが行われた。安全基準等の見直し状況及び安全基準等の浸透状況等の調査の実施等を通じて、指針と安全基準等の一体的な見直しサイクルを確立した。

（２）情報共有体制の強化

官民の各主体が連携するための枠組みとして、「『重要インフラの情報セキュリティ対策に係る行動計画』の情報連絡・情報提供に関する実施細目」（以下「実施細目」という。）を定め、内閣官房と重要インフラ所管省庁との情報提供・情報連絡を開始した。「情報提供」は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であり、「情報連絡」は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である。

また、各重要インフラ分野内にセプターが整備された。さらに、各セプター間での横断的な情報共有体制として、政府機関とは独立した活動が可能な位置づけのセプターカウンシルが創設される見込みである。

（３）相互依存性解析

重要インフラ分野間の連携対処のための基盤を構築すべく、「相互依存性解析」を実施した。「静的相互依存性解析」によって主に重要システムが他の重要インフラにどのように依存しているか、また、「動的相互依存性解析」によってIT障害時において時間経過とともに分野間の関係性がどのように変化するかを明らかにした。

（４）分野横断的演習

段階的に「研究的演習」及び「机上演習[19]」を経て「機能演習[20]」を実施した。「機能演習」には、重要インフラ事業者等、セプター、重要インフラ所管省庁、内閣官房等が参加し、緊急時における情報共有・情報連絡について、具体的事象を想定したシナリオによる演習を実施した。これらの演習を通じて、IT 障害発生時における情報共有・情報連絡手法等の確認と検証を実施した。

４　第２次行動計画期間における取組みの要点

第１次行動計画では、各重要インフラ事業者等の取組みに加えて、分野横断的な観点からの取組みを連携させる体制である「新しい官民連携モデル」の構築が進められた。これによって各重要インフラ事業者等の取組み

[19]机上演習：演習参加者が１つのシナリオを元に会議形式で課題討議を行いながら実施する演習
[20]機能演習：実際の組織の指示判断系統機能を用いて模擬的に検証するための演習

に、分野横断的な知見を加えることと、分野横断的な知見を内閣官房等に蓄積することが可能となった。また、行動計画の枠組みに対して改善サイクルを駆動する準備が整った。しかし、行動計画で対処すべき脅威や守るべきサービスの水準について、具体的な改善を検証するための指標は設定されていなかった。

第２次行動計画では、第１次行動計画の成果を活用して、関係主体が日々蓄積している経験を互いに活かしあう改善のサイクルの確立を目指す。そのため、対処すべき脅威や守るべきサービスの水準を可視化して継続的な検証に取り組むための施策を盛り込んでいる。これは第１次行動計画で構築された「新しい官民連携モデル」をより高次に発展させるものである。すなわち、関係主体等の自主的な取組みが互いの効果を最大化するように連携できるようになること、また関係主体の個別の自立的な取組みが行動計画の枠組みそのものを自己組織的に成長させる原動力となるようになることを目指す。

この改善の取組みは第２次行動計画に関わる全ての関係主体毎に行われる。すなわち、個別重要インフラ事業者等における改善、各重要インフラ分野毎の改善、政府における分野横断的な施策の改善というように、各層で改善に取り組む。これらの取組みは各々従来から進められているところであるが、第２次行動計画の枠組みによってこれらの取組みが有機的に互いを支え、各々の取組みをより確実なものとなるようにすることを目指す。

これによって重要インフラ事業者等が自らの経験のみならず、分野全体の重要インフラ事業者等の経験や、分野横断的な施策の経験を、自らの対策の改善に組み込めるようになることを目指す。また、ともすれば当事者以外には見逃されがちな IT 障害等の経験を広く関係主体で共有し、これを活用することで関係主体間の連携をより高度なものへと充実させる事を目指す。

Ⅱ　計画期間内に取り組む情報セキュリティ対策

第２次行動計画期間においては以下の５つを情報セキュリティ対策の柱として、取組みを進める。

１　安全基準等の整備及び浸透

第２次行動計画期間においては、事業継続の観点からの具体的内容の補充を含め、指針の位置づけや記載内容の具体性のレベルの見直しを行う。また、重要インフラ事業者等の PDCA サイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。

（１）指針の継続的改善

社会動向の変化等に対応し、また新たな知見を適時反映していくために、指針の分析・検証を１年毎、及び必要に応じて実施し、その結果を公表することとする。なお、指針の改定に関する検討は原則として３年に１度実施するものとする。ただし、必要に応じて追加的に検討を実施し、必要があると認められた場合には指針の改定を行うこととする。

なお、指針の改定に関する検討にあたっては、重要インフラ事業者等において事業継続計画の策定が進みつつある状況や、事業継続計画に関する国際規格化の進展状況等を踏まえつつ、分野横断的な観点からも実効的であるかを検証できるように指針の内容を充実させるものとする。

各重要インフラ事業者等の自主的な取組みに資する項目を充実させるために、指針に記載される事項を「要検討事項」と「参考事項」に分類し、対策項目の具体化の例示を行う事により、引き続き記載事項の充実を図ることとする。

「要検討事項」とは対策の底上げの観点から全分野共通で特段の理由のない限り対策することが望まれる事項であり、安全基準等に規定する必要性を各分野が検討するべき事項とする。また「参考事項」とは進んだ対策として盛り込む事が望ましい事項とし、各分野が任意で参考とする事項とする。

要検討事項及び参考事項は、現行指針の項目に加え、行動計画に基づく各重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を候補として必要に応じて充実させていくこととする。

（２）安全基準等の継続的改善

各分野においては、対策の経験から得られた知見を安全基準等に反映するため、安全基準等の継続的な改善に取り組むこととする。なお、安全基準等の検証に際しては、指針や毎年実施される指針の分析・検証の結果を踏まえた検討を行うこととし、必要に応じて安全基準等の改定を行うこととする。

情報セキュリティ対策に関する知見の共有を促進するために、従来検証対象となっている安全基準等の他に、情報セキュリティ対策に関する基準又は参考文書類を、可能な範囲で共用できるよう改めて広く安全基準等として整理することとする。

安全基準等に基づく対策状況については、関係性を有する主体間で互いに把握しておくことが重要である。そのため、情報セキュリティ監査又はそれに相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等の自主的な取組みを一層推奨し、分野や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対外的な説明に努める。

（３）安全基準等の浸透

各重要インフラ分野は、安全基準等の浸透に向けて、安全基準等にて定められた対策の推進に加えて、対策を実装するための環境整備にも努める。

事業者自らが定める「内規」を含めた安全基準等の浸透を確実なものとするために、「安全基準等の浸透状況等に関する調査」を引き続き定期的に実施することとする。調査項目・調査主体等については、適宜見直しを行うこととする。

（４）推進方策

ア　指針の継続的改善

指針の改定は、第２次行動計画の初年度に実施する。また、１年毎、及び必要に応じて適時に指針の分析・検証を行うこととし、その結果を必要に応じて指針の追補版として周知することとする。

イ　安全基準等の継続的改善

各重要インフラ分野は、安全基準等の継続的な改善に努める。毎年一定時期に各重要インフラ分野の取組み等の実態把握を行い、指針の分析・検証の結果を踏まえた改善の状況や、重要インフラ分野毎の独自の改善の状況について、内閣官房が可能な範囲において、客観的な把握、検証を行うこととする。

ウ　安全基準等の浸透

各重要インフラ分野は、対策を実装するための環境整備も含め、より一層の安全基準等の浸透に努める。毎年一定時期に事業者自らが定める「内規」を含めた対策状況の客観的な把握を行うこととする。

２　情報共有体制の強化

第２次行動計画期間においては、関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカウンシルの自主的な活動の充実強化を推進する。情報共有体制の全体像は、別紙４に示すとおりとする。

（1）共有すべき情報の整理

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

IT 障害に関する情報には、1) IT 障害の未然防止、2) IT 障害の拡大防止・迅速な復旧、3) IT 障害の要因等の分析・検証による再発防止の３つの側面が含まれる。

対象とする脅威、様々な社会動向の変化等を踏まえた上で、情報セキュリティ関連情報の流通に関する既存の枠組みに配慮しつつ、共有すべき情報について整理を行うこととする。この際、IT 障害に関する情報の３つの側面を踏まえた上で、関係主体の活動や保有する情報、法制度等による制約を整理するとともに、関係主体の保有する情報毎に、重要インフラ事業者等にとって有用な情報の共有のありかた（即応性の観点等を含めたタイミング、様式、方法など）を検討することとする。

また、情報提供、情報連絡の実践等を通じて、分野横断的な観点において、必要な情報と提供可能な情報の整理を継続的に見直すこととする。

（2）情報提供、情報連絡の充実

ア　情報提供、情報連絡の基本

重要インフラ事業者等のサービスの維持・復旧がより容易になるようにするためには、官民の各主体が協力することが重要であるとの観点から、第１次行動計画の下において、「実施細目」やセプターの整備を中心とした情報共有体制の構築を進めてきており、情報の共有が開始されている。当該情報共有体制の枠組みが出来上がったところであることを考え合わせ、第２次行動計画における情報提供、情報連絡は、これまでの情報共有体制を踏襲しつつ、情報提供の内容を充実したものとすることを基本とし、別添に示すところにより情報提供、情報連絡を行うものとする。

イ　情報提供、情報連絡の充実

内閣官房、重要インフラ所管省庁、セプター、重要インフラ事業者等において各々が整備している情報共有に係るルールの整合を図ることとする。また、内閣官房から重要インフラ事業者等への情報提供について、必要に応じて情報共有に求められる機能等の検討を行い各主体間で共有を目指すこととする。

また、事例や経験の共有を強化するために、第１次行動計画で実施してきた相互依存性解析で得られた知見や、今後行われる共通脅威分析で得られる知見に基づいた波及先に関する分析を行うとともに、関係機関等の有する分析機能の活用を検討することとする。

（3）セプターの強化

セプターに具備すべき要件として、第１次行動計画で定められた以下の２点の要件については引き続きこれを維持し、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[21]）が設定されていること。

なお、今後は、セプターにおける情報の収集、把握・分析、内部での共有、他セプターやセプターカウンシルへの発信などといった機能の展開が期待される。

また、各セプターは分野内の情報集約及び情勢判断を行う能力がある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みの中で図られることが望まれる。

（4）セプターカウンシル

セプターカウンシルは、各セプターにより構成される共助・互恵の活動の取組みの場として創設を目指すものであり、相互理解及びベストプラクティス等の具体的な事例共有等の分野横断的な情報共有が行われることが望まれる。

また、政府機関等とは独立した活動が可能な位置づけにあることから、情報共有の改善等のための検討などに関し、その特徴を活かして積極的な活動に取り組むことが期待される。特に重要インフラ事業者等と政府機関等の協力関係を今後一層深めていくためには、両者の間の状況認識等の共有を進めていくことが重要であることから、重要インフラ事業者等と政府機関等との意見交換を行うなどの取組みがなされることが望まれる。

（5）推進方策

ア　共有すべき情報の整理

取り扱う具体的な情報や利用の方法等は、それぞれの重要インフラ分野や業法の特性を十分に勘案し、内閣官房、セプター、セプターカウンシル等の各主体がそれぞれの取組みの中で決めることを原則とする。

この際、内閣官房は情報共有体制の強化の中心的な役割を担うこととし、IT 障害に関する情報の３つの側面を踏まえ、関係主体の保有する情報毎に、重要インフラ事業者等にとって有用な情報提供のありかた（即応性の観点等を含めたタイミング、様式、方法など）を整理する。共有すべき情報については社会環境や情報共有の実態を踏まえて適時見直すこととする。

イ　情報提供、情報連絡の充実

内閣官房、重要インフラ所管省庁、セプター、重要インフラ事業者等における情報共有に係るルールの整合を図るため、セプター等の関係者の意見等も参考としつつ、「実施細目」の見直しを行うとともに、「実施細目」

[21] POC：Point of Contact

に基づく運用についての参考資料を整備し、関係者に示すことにより情報共有体制の運用の可視化を図ることとする。また、必要に応じて情報共有に求められる機能等の検討を行い、内閣官房、重要インフラ所管省庁、セプターの間において共有することとする。

さらに、重要インフラ事業者等の情報セキュリティ向上のために有用な活動を行う機関と幅広く連携を図ることとする。

ウ　セプターの強化

セプターの機能強化のために、定期的に各セプターの機能やセプターの活動状況等の先進的な事例の紹介を行い、セプターの強化に資することとする。

３　共通脅威分析

第２次行動計画期間においては、第１次行動計画で実施してきた、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を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。

このため、従来行ってきた「静的相互依存性解析」や「動的相互依存性解析」の結果を踏まえ、研究機関等との連携を深めつつ、内閣官房、重要インフラ所管省庁、重要インフラ事業者等が協力して活動を進める。

なお、本分析の結果は、引き続き次のような重要インフラのサービス維持・復旧への活用が期待される。

①より実効性の高い事業継続計画策定に必要な基礎資料の提供
②大規模災害発生時における復旧優先順位の決定のための基礎資料の提供
③IT 障害の被害拡大防止のための、重要インフラ分野間の連携対処のための基盤提供

（１）相互依存性解析の継続

重要インフラの情報セキュリティ確保にあたっては、重要インフラ分野間での相互依存性の認識と、問題に柔軟に対応できる対策が必要である。すなわち、相互依存性解析は、潜在的なリスク・チェーンの顕現化と、事故・障害要因の連鎖的伝搬に対してのマネジメント（回避・コントロール・想定など）に必要である。このことから、第２次行動計画でも相互依存性解析に継続的に取り組むものとする。

（２）共通脅威分析の検討

各重要インフラ分野におけるIT利用が一層の進展を見せる中、我が国全体としての重要インフラの情報セキュリティを向上させていくためには、分野横断的な状況の把握、分析が従来以上に不可欠である。このため、それぞれの重要インフラ分野に共通に起こりうる脅威が何であるかを把握するための分析を行うこととする。この分析と相互依存性解析を合せて共通脅威分析と呼ぶこととし、重要インフラ分野共通のITに関する技術、シス

テム、環境等、広い範囲を対象とする分析を実施する。

（3）推進方策

共通脅威分析については、広範な分析を効果的に進めるため、各年度の初めに関係者による課題の洗い出しと優先順位付けを行って、各年度に取り組む分析対象を明確にする。また、これらの成果については、毎年、分析結果をまとめた報告書を作成する。

分析結果の実効性を高めるために、実施上の課題、手法、研究機関との連携等の検討、見直しを行う。研究機関等との連携に際しては、情報の管理、保護について十分配慮することとする。

分析結果については、重要インフラサービスの維持、復旧への活用が期待される。また、指針や安全基準等の継続的改善に活用するほか、分野横断的演習のシナリオ作成等に反映する。更に、所管省庁を含む各省庁で広く活用することが期待される。

4　分野横断的演習

第２次行動計画期間においては、第 1 次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセプター等の協力を得て、重要インフラ分野横断的な演習を実施する。また、演習シナリオの検討、演習の実施を通じて、「分野横断的な脅威に対する共通認識の醸成」や「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」などが得られることにより、分野横断的な重要インフラ防護対策の向上を目指す。なお、重要インフラ分野における現行の法制度や重要インフラ事業者等の経営上の仕組みに関することも含め、演習で得られた課題は、改善に向けた取組みに活用できるよう、分野間及び関係主体間で共有する。

（1）分野横断的演習の実施

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、それら脅威に対する分野横断的な重要インフラ防護対策の向上を目指し、具体的な IT 障害発生を想定した演習シナリオの検討とそれに基づく分野横断的な演習を継続的に実施することにより、課題の抽出及び演習実施のための知見の整備を行う。なお、演習の実施に当たっては、重要インフラ事業者等を中心に、演習シナリオ及び適切な演習手法の検討を行うものとする。

情報セキュリティ対策に関する課題や官民の情報共有に関する課題など、演習で抽出された課題については、情報共有体制の見直しなどに活用することで、分野横断的な重要インフラ防護対策の向上を図る。

また、重要インフラ事業者等の早期復旧手順や事業継続計画などについても、各分野が任意に検討できる事項として演習シナリオに組み込むことにより、分野間及び関係主体間の自律的かつ効果的な協調・連携を図る観点からの取組みの推進が期待される。

演習は、IT 障害への対応を検証する上で有効な手法であることから、シナリオ作成、運営手法等、分野横断的演習を通じて得られた演習実施のための知見について、各重要インフラ事業者等が自分野の取組みに活用できるよう整理し、提供することにより、重要インフラ事業者等の情報セキュリティ対策の向上に資することが期待される。

（2）推進方策

演習の検討、実施を通じて得られた演習シナリオ、状況付与及び演習手法などに関する課題や知見の整理を行う。

整理した課題や知見は、次回の分野横断的演習のシナリオ作成や演習手法の検討等に反映するとともに、知見の継続的な拡充に努める。

これらの課題や知見は、関係者に示すことにより共有し、各重要インフラ分野の情報セキュリティ対策の強化のための取組みへの活用を推進する。

5　環境変化への対応

社会環境や技術環境等の状況は刻々と変化しているため、情報セキュリティ対策の有効性を保ち続けるためには、環境の変化に情報セキュリティ対策を機敏に対応させていく必要がある。

そのため、広く国民に対しての広報公聴活動、当事者間のリスクコミュニケーション、国際連携等を通じて、関係主体各々が第 2 次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努めることとする。また、こうした環境の変化に対して、第 2 次行動計画の枠組みだけでは十分に対応できない場合は、内閣官房は必要な対応が可能となるような体制の検討を行うこととする。

（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、我が国の重要インフラ防護に関わる関係主体が行動計画に基づき実施した取組み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第 2 次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。

広報活動としては、行動計画に基づく関係主体の取組みを Web 等を活用して幅広く発信することとする。特に、重要インフラ専門委員会等の会議資料については可能な限り公開することとする。関係主体は自らの取組みを可能な範囲で公表することが望ましい。

また、公聴活動としては、セミナー等の機会を広く捉えて行動計画の紹介を行うとともに意見聴取に努める。また、Web を活用して意見を受け付け、これを行動計画の推進の参考とするとともに、行動計画の見直しの材料として活用する。

（2）リスクコミュニケーションの充実

各関係主体が互いの連携を進めるためにはリスクコミュニケーションを充実させることが重要である。リスクコミュニケーションとは、情報セキュリティ対策において連携すべき関係者間で、リスクについての誤解や理解不足を解消し、また関係者間で及ぼしあうリスクについての認識を共有するためのコミュニケーションである。これによって、連携して対処すべきリスクや対策の方法についての共通認識が得られるとともに、情報セキュリティ対策において連携効果を高めることができると期待される。またより強固な信頼関係が得られると期待される。

そのため、関係主体間の直接的なコミュニケーションの機会の拡大を図ることとする。

なお、リスクコミュニケーションは関係主体間で必要な範囲で行うべきものであって、例えば機密情報に当たるものを一般に開示すること等を意図しているものではない。当然ながら、開示することによって脅威が増すことが懸念される情報については、状況に応じて慎重な扱いを要するものである。

（3）国際連携の推進

国際的には、「重要情報インフラ」と呼ばれる概念の下で、その防護のためのベストプラクティスの共有が進められている。具体的には、重要情報インフラを支える制御システム等への脅威の分析や対策のためのベストプラクティスの共有や、重要情報インフラ間の相互依存性の解析等についての議論が行われている。内閣官房は、国際連携を積極的に行う関係主体の協力を得て、国際会合や他国機関等との対話を通じて最新動向を把握し、機密情報の取扱い等に留意しつつ、情報共有に努める。

（4）情報セキュリティ基盤の強化

情報セキュリティ基盤の強化のために、人材育成、研究開発、地域レベルの取組みをそれぞれ推進することとする。

人材育成については、演習・訓練及びセミナー等を通じて、高度な IT スキルを有する人材の育成を図る。

研究開発については、情報セキュリティに関する研究開発・技術開発戦略の立案に際し、重要インフラにおける IT 障害の原因となりうる IT の機能不全への対策全体に資する視点を付与することにより、脅威への対応能力の強化に資する研究開発を促進する。

地域レベルの取組みについては、関係する政府地方支分部局、地方公共団体、重要インフラ事業者等及び地方の情報セキュリティ関係組織間での情報共有及び連絡・連携の体制を、政府の体制と連動する形で平時より整備する事に努める。

（5）推進方策

ア　広報公聴活動

内閣官房情報セキュリティセンターの Web サイトを充実させ、第２次行動計画に基づく施策に関連する広報情報に一元的にアクセスできるようにする。特に、年度計画の推進状況、対策及び施策の検証結果、情報セキュリティ対策に関連する調査の情報については、可能な限り公表に努める。

イ　リスクコミュニケーションの充実

関係主体は各々必要な範囲でのリスクコミュニケーションに努めるとともに、公表することが差し支えない範囲で情報セキュリティ対策についての開示に努める。

ウ　国際連携の推進

国際連携については、引き続き重要インフラ防護のための早期警戒・監視・警報ネットワークやメリディアン[22]及び OECD 等における重要インフラ防護に関する国際的な取組みに参画していくこととする。これによって諸外国と連携し、我が国の動向を踏まえた情報セキュリティ対策に関するベストプラクティスの作成や共同演習等の国際的な連携を図る。

エ　情報セキュリティ基盤の強化

各関係主体が現在の技術の改善、協働体制の整備、法制度や経営、人材の総合的開発等に関する事項に積極的に取り組むとともに、その状況を関係者間で適時適切に共有する。

[22] 重要情報インフラ防護に特化して議論を行う国際フォーラム。各国の重要情報インフラ防護政策担当者が集まり議論を行う。第１回が英国（グリニッジ）で開催されたことから、Meridian（子午線）と呼ばれている。

III　関係主体において取り組むべき事項

１　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み、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　各主体の取組み

（１）内閣官房の施策

ア）「安全基準等の整備及び浸透」に関する施策

①毎年、指針の分析・検証を実施することに加えて、第２次行動計画の初年度及び必要に応じて、指針の改定に関する検討を実施し、これらの結果を公表

②指針の分析・検証の結果や共通脅威分析の結果を提示すること等により、各重要インフラ分野の安全基準等の継続的改善を支援

③重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表

④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

イ）「情報共有体制の強化」に関する施策

ａ）共有すべき情報の整理

①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。また、必要により実態に即した整理の見直しを実施

②整理した共有対象とする情報及びその共有方法に基づき、関係主体からの情報を集約し、重要インフラ事業者等への情報提供を実施

③共有すべき情報の整理の過程で得られた制度上の制約及び強化に必要な施策を整理

ｂ）情報提供、情報連絡の充実

①関係主体の協力を得つつ、情報を共有する範囲の見直し等の第１次行動計画中に判明した課題の解決等のため、速やかに「実施細目」の見直しを実施

②「実施細目」の運用解釈を示す参考資料を策定し、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

③「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、適時見直しを実施

④重要インフラ所管省庁における情報提供、情報連絡の担当者をリエゾンとして内閣官房に併任する等の、政府から重要インフラ事業者等への情報共有体制の維持

⑤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、重要インフラ事業者等に提供すべき情報の集約

⑥情報セキュリティ関係省庁、事案対処省庁、関係機関等からの情報提供、重要インフラ事業者等からの情報連絡等に基づき、重要インフラ事業者等に対して情報提供を実施。この際、第１次行動計画で実施した相互依存性解析及び第２次行動計画で実施する共通脅威分析に基づいた波及先に関する分析を実施

⑦関係機関等の有する分析機能の活用の検討を実施

⑧重要インフラ事業者等への情報提供における情報共有に求められる機能等（例：各経路間の暗号化等）について、必要に応じ重要インフラ所管省庁、セプターとも連携しつつ、検討を実施
⑨情報提供の充実のため、情報セキュリティ関係省庁、事案対処省庁及び関係機関との連携を強化するとともに、情報セキュリティに関する活動を行う機関等との連携対象の拡充の検討を実施
⑩関係機関等における適切な研究課題等の抽出に資するため、関係主体の協力を得つつ、関係機関等に対して内閣官房の取組みや各重要インフラ分野の動向を伝達
⑪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、セプターの情報共有体制の維持・向上のため、情報疎通機能の確認等の機会を提供

ｃ）セプターの強化
①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
②先進的なセプターの機能や活動の紹介

ｄ）セプターカウンシル
①当分の間、セプターカウンシルの事務局を務める
②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
③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

ｅ）その他
①国民や社会に対して活動を説明するため、可能な範囲で各セプター及びセプターカウンシルの取組みについての紹介を実施

ウ）「共通脅威分析」に関する施策
①毎年、重要インフラ事業者の意向等に基づく活動方針を作成
②共通脅威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毎年、分析報告書を取りまとめ、安全基準等に反映する基礎資料として、また重要インフラの事業継続計画整備等の基礎資料として提供

エ）「分野横断的演習」に関する施策
①分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施
②分野横断的演習の機会を活用して、共通脅威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

③分野横断的演習の向上策検討
④分野横断的演習の実施方法等に関する知見の集約・蓄積

オ）「環境変化への対応」に関する施策
①脅威やリスク等の状況変化に関する情報収集に努め、特に必要があると認められる場合は、重要インフラ所管省庁の協力を得て、これに対応
②情報セキュリティ対策についての広報公聴に資する Web サイトを構築
③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
④災害、物理的テロ等への対応との連動体制の構築
⑤諸外国のベストプラクティスを収集するとともに、情報セキュリティ政策に関する国際機関の動向や標準化の動向を把握
⑥国際的な脅威・脆弱性情報に関する情報収集を行い、関係主体に提供
⑦諸外国の政府機関及び国際機関と連携しながら、共同演習等の国際連携を強化するための機会を重要インフラ事業者等に紹介
⑧分野横断的演習等を通じた、高度な情報セキュリティ人材の育成

カ）自らの機能強化に関する取組み
①「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（平成 16 年 12 月 7 日 IT 戦略本部決定）にある「政府機関の事案対処支援」において収集・分析した情報の活用
②各重要インフラ分野における企業情報等を扱うため、人的・物理的側面からもその機密の保持を確保し、信頼性の高い情報交換を行うことのできる環境の整備
③IT 障害の発生時等緊急時における重要インフラ事業者等間の調整を行うセンター機能の充実
④情報セキュリティ対策に必要な、環境の変化や関係主体の対策状況についての調査活動の充実

（2）重要インフラ所管省庁の施策

ア）「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づ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へ提供
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、各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

イ）「情報共有体制の強化」に関する施策
ａ）共有すべき情報の整理

①共有対象とする情報とその共有方法の整理への協力
②共有対象とする情報とその共有方法の整理をセプターが独自に実施する場合にあっては、セプターを支援

b）情報提供、情報連絡の充実
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重要インフラ所管省庁とセプターの間及び重要インフラ所管省庁と重要インフラ事業者等の間における情報共有ルールの維持並びに「実施細目」との整合を図ることを含めた改善の実施
④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、「実施細目」の運用に係る参考資料の策定、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
⑤重要インフラ事業者等への情報提供における情報共有に求められる機能等（例：各経路間の暗号化等）について、必要に応じセプターとの間での検討の実施及び内閣官房の検討への協力
⑥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
⑦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
⑧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
⑨内閣官房がセプターの情報疎通機能等の機会を提供する場合の協力

c）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

d）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

ウ）「共通脅威分析」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共通脅威分析を必要とする取組み対象に関する情報、あるいは、共通脅威分析に必要な情報を内閣官房に提供
③共通脅威分析の結果として提供される基礎資料の評価
④共通脅威分析の結果として提供される基礎資料の施策への活用

エ）「分野横断的演習」に関する施策

①分野横断的演習の実施に必要となる、演習のシナリオ、実施方法、検証課題等に関する情報を内閣官房に提供
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分野横断的演習の向上策検討への協力
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

オ）「環境変化への対応」に関する施策
①情報セキュリティ対策についての広報公聴に資する情報を内閣官房に提供
②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
③災害、物理的テロ等への対応との連動体制の構築

（３）情報セキュリティ関係省庁の施策

ア）「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

イ）自らの機能強化に関する取組み
①対処能力の向上等、情報セキュリティ関係省庁における取組みの継続的な実施

（４）事案対処省庁の施策

ア）「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
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要望があった場合、意見交換等を実施

イ）自らの機能強化に関する取組み
①対処能力の向上等、サイバーテロ等への対処に係る、事案対処省庁における取組みの継続的な実施

（５）関係機関の自主的な取組みとして期待する事項

ア）「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みに対する協力

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

イ）「分野横断的演習」に関する施策及び対策

①分野横断的演習に必要となる IT 障害を発生させる脅威、IT 障害発生事例等に関する情報を内閣官房に提供

ウ）情報セキュリティ対策に資する個別関係機関毎の取組み

①警察庁サイバーフォースは、各種関連情報等の収集能力を強化するとともに、高度な IT スキルを有する人材を育成

②NICT は、サイバー空間上で発生する各種攻撃に対する事前対策、インシデント対応、事後対策、暗号プロトコルの安全性評価及び暗号技術の新規応用分野に関わる総合技術の研究開発を実施

③AIST は、ハードウェア、ソフトウェア、またそこで用いられている暗号技術のセキュリティ解析および評価技術、新規セキュリティ技術の提案等、総合的な研究開発を実施

④IPA は、IT 障害事例とそれに関わる経験の共有を促進するための情報収集・分析機能を担うとともに、情報システムの信頼性を定量的に評価するための共通リファレンスをはじめとするソフトウェアエンジニアリング手法の開発や、情報システムの信頼性向上対策及び情報セキュリティ対策を実施するための障害対策分析によるチェックリスト等を策定。また、情報処理技術者試験に情報セキュリティに関する試験区分や項目を設け実施するとともに、各種スキル標準において情報セキュリティに関する知識項目等を整備し、普及啓発を実施。さらに、重要インフラ分野での制御システムの情報セキュリティ及びサービス継続関連について国内外の情報収集・分析を行うとともに、重要インフラ事業者等を対象とした情報セキュリティ上の管理的対策等に関する啓発活動を実施。加えて、暗号プロトコルの安全性評価及び暗号プロトコルの安全性評価に関する調査研究を実施

⑤Telecom-ISAC Japan は、電気通信事業者を中核とする事業者横断の情報セキュリティ対処連携の場を提供し、ネットワークインシデント情報の収集・分析・共有を実施。また、電気通信事業者等のサイバー攻撃等への対応能力強化を目的とした機能検証・連携強化を実施。さらに、エンドユーザへのネットワークセキュリティリテラシー向上を目的とした啓発への取組や、ネットワークセキュリティ人材の育成施策への貢献

を目指すとともに、情報通信ネットワーク防護のための技術的対策や運用面の課題などの検討を実施

⑥JPCERT/CC は、重要インフラ事業者等からの情報提供や対応依頼に基づき、インシデント対応のための関係者間のコーディネーションや、攻撃の脅威分析、対策の検討に関する支援活動を実施。また、制御系システムやソフトウエア製品、プロトコルに関する脆弱性関連情報や特定のサイトへの攻撃情報等の脅威関連情報を広く収集・分析し、重要インフラ事業者等との事前の合意に基づき、「早期警戒情報」として、重要インフラ事業者等、セプター、セプターカウンシル又は内閣官房に提供。さらに、重要インフラ事業者等を対象とした情報セキュリティ上の管理的対策等に関する啓発活動を実施

（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

ア）「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・検証を実施する事に加えて、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情報セキュリティ監査又はそれに相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等を自主的な取組みとして実施することを検討

⑤情報セキュリティ対策の対外的な説明の充実に努める

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

イ）「情報共有体制の強化」に関する対策

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

ウ）「共通脅威分析」に関する対策

①毎年、自らが単独で分析することが困難で、共通脅威として分析する価値のある脅威を共通脅威分析の取組み対象として提案

②内閣官房、及び、共通脅威分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

③共通脅威分析に必要な実際的な情報を、積極的に内閣官房に提供

④共通脅威分析の議論・検討に参画

⑤共通脅威分析の成果として提供される基礎資料の評価
⑥共通脅威分析の結果として提供される基礎情報の事業継続計画等への活用

エ）「分野横断的演習」に関する取組み
①分野横断的演習の実施に必要となる、演習のシナリオ、実施方法、検証課題等に関する情報を内閣官房に提供
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分野横断的演習の向上策検討への協力
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みに対し、分野横断的演習結果の活用に努める

オ）「環境変化への対応」に関する対策
①情報セキュリティに関する取組みを国民向けに紹介することを検討
②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

（7）セプターの自主的な対策として期待する事項

ア）「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の実施。また、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重要インフラ事業者等への情報提供における情報共有に求められる機能等（例：各経路間の暗号化等）について、内閣官房や重要インフラ所管省庁が行う検討への協力
⑤情報疎通機能の定期的な確認
⑥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
⑦関係機関との合意に基づく補完的な情報共有の実施
⑧セプターの機能強化・充実
⑨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
⑩セプターカウンシルへの参加

イ）「共通脅威分析」に関する対策
①共通脅威分析に関する重要インフラ事業者等の自主的な取組みに参加

ウ）「分野横断的演習」に関する対策

①分野横断的演習への参加

（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

ア）「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内閣官房が重要インフラ事業者等への情報提供において求められる機能等（例：各経路間の暗号化等）の検討時における改善等に関する検討の実施

④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情報共有による分野横断的な情報共有の推進

⑤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

Ⅳ　評価・検証と見直し

１　行動計画の推進体制

（１）行動計画の進捗状況の評価・検証

第２次行動計画に基づく取組みを着実に進め、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評価・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み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み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、自らの取組みを改善するよう努めるべきものである。しかし、第２次行動計画の評価・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み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みの改善に役立てるようにすることを主眼とする。

第２次行動計画の進捗状況の評価・検証は、個々の情報セキュリティ対策がどのような成果をあげたのかという「成果（アウトプット）を測る視点」と、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「結果（アウトカム）を測る視点」のふたつの視点で取り組む。この際、可能な限り客観的な指標を用いた検証を行った上で、評価に取り組むこととする。

なお、第２次行動計画においては、「検証」とは各々の取組みについてその進捗状況に関する客観的事実を指標を用いて確認することとし、また、「評価」とは目標に照らしてその取組みの妥当性を見直すこととする。

「成果（アウトプット）を測る視点」からの検証は、第２次行動計画に基づく個別の情報セキュリティ対策の柱に着目して行う。第２次行動計画に基づく情報セキュリティ対策の柱は、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、検証のための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検証のための指標と、政府機関等による施策の検証のための指標を設定することとする。これらの検証は、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、内閣官房が行う。

個別の重要インフラ事業者等による対策の評価については、それが自主的なものである事に鑑み、基本的には事業者自らが行うこととする。また、政府機関等による施策の評価は情報セキュリティ政策会議が行うこととする。

この際、情報セキュリティ対策の柱毎の指標については、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。

「結果（アウトカム）を測る視点」からの評価・検証は、第２次行動計画の目標と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に対して評価・検証を行うのではなく、情報セキュリティ対策の全体、すなわち第２次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。

また、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柱毎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。

対策の成果検証、施策の成果検証、補完調査は年に１度、情報セキュリティ政策会議が実施することとし、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。

また、行動計画に基づく取組みの結果の評価は、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。

（２）対策の成果検証

重要インフラ事業者等は重要インフラサービスの安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。この取組み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み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。

対策の成果検証は、第２次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毎に検証対象とした重要インフラサービスについて、検証レベルを逸脱した IT 障害の発生状況を検証することとする。検証対象とする重要インフラサービスと検証レベルは別紙２に示すとおりとする。具体的な指標は、検証レベルを逸脱する IT 障害事例のうち内閣官房が認知したものの 10 分野全体での総数とする。

なお、個別の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、事業者等毎又は分野毎の 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。

（３）施策の成果検証

第２次行動計画の施策は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の施策である。第１次行動計画期間においては、これらの施策の枠組みの構築に重点がおかれたが、第２次行動計画においてはこの枠組みの構築が計画通り完了する見込みであることを踏まえ、各施策の効果の検証に着手する。

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柱毎に、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。

ア）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、重要インフラ事業者等における各種の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、個別事業者等の安全基準等に基づいた取組み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、指針及び参考資料に採録した対策項目数、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数、指針の重要インフラ事業者等による評価とする。

イ）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、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。

ウ）共通脅威分析

「共通脅威分析」に期待される成果は、指針の継続的改善及び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することである。そのため、毎年度当初に、重要インフラ事業者等の必要性を勘案して策定する共通脅威分析の検討項目に対する年度末時点の達成度に着目した指標を設定する。具体的な指標は、実施した検討項目件数、各検討結果の重要インフラ事業者等による評価とする。

エ）分野横断的演習

「分野横断的演習」に期待される成果は、重要インフラ事業者等の IT 障害発生時の早期復旧手順、事業継続計画の検証などに対する貢献である。演習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、より現実の状況に近い演習の実施

が重要であり、それぞれの役割を担当する多くのプレイヤーの参加が望ましい。そのため、演習参加者の拡大と演習で得られた知見が、重要インフラ事業者等の取組み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、演習の延べ参加者数と、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重要インフラ事業者等の数とする。

オ）環境変化への対応

「環境変化への対応」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、第２次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、第２次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、「環境変化への対応」に挙げた施策のうち、「リスクコミュニケーション」に期待される成果は、関係主体間で互いの活動への理解の向上と、連携を図りやすい環境の醸成である。そのため、関係主体間のコミュニケーション機会の充実に着目した指標を設定する。具体的な指標は、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とする。

カ）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。

（４）結果の評価のための補完調査

指標を用いた成果検証は実態を捉えるために不可欠なものであるが、それは一側面を捉えるものに過ぎない。第２次行動計画の期待する結果（アウトカム）の評価をより実態に即すようにするために、指標では捉えられない側面を補完的に調査する事が必要である。そのため、IT 障害等の事例について補完調査を実施し、第２次行動計画に基づく施策と対策を評価するため材料を得ることとする。

補完調査は毎年１回行うこととし、調査結果を可能な範囲で公表する。

（５）行動計画に基づく取組みの結果の評価

第２次行動計画の理想とする将来像を踏まえて、行動計画に基づく取組みの結果の評価に取り組む。

理想とする将来像に着目すると、個別の対策や施策の成果がこの結果に

それぞれどの程度貢献したかを分析的に評価することは困難である。また、個別の対策や施策の成果が結果に結びつくまでには時間差があり、それぞれの取組みを一律に同じ時系列で評価することも適当ではない。そこで、第２次行動計画のどの施策や対策がどの程度貢献したかを個別に分析するのではなく、これらの総体である行動計画そのものを総合的に評価することとする。

行動計画の結果の評価では、対策の検証、施策の検証、補完調査の結果を内閣官房でとりまとめ、行動計画に基づく取組みが、全体として第２次行動計画の結果（アウトカム）の達成に適ったものであるかを評価する。この際、個別の対策や施策の及ばない面のみに着目するのではなく、むしろ全体のバランスを見た上で更に取組みを前進させるためにはどうすれば良いかという面にも着目することが重要である。

（６）行動計画の見直し

第２次行動計画については、対策の成果、施策の成果、補完調査、評価の内容（以下「評価等」という。）を踏まえ、また、脅威、IT 障害、IT を利用したサービス等に関する社会情勢等の変化等をふまえ、３年毎又は必要に応じ、見直しを行う。第２次行動計画期間においては、少なくとも策定から２年後から 12 ヶ月かけて見直すこととする。

特に見直しの要点となるのは、目標とそれに基づく基本的な方向性、重要インフラ事業者等の対象範囲、関係主体とすべき主体の対象範囲、対策や施策の追加や廃止、想定すべき脅威の例示、対象とすべき重要インフラサービスの範囲、サービスレベル、検証レベル、評価指標の設定等である。またこれに併せて、各用語の定義や行動計画の対象範囲についても、必要に応じて見直しを行うものとする。

第２次行動計画の見直しに際しては、各分野の特性や取組状況に配慮しつつ、事業者の取組みが自主性に基づくものであることを踏まえた検討を行うことが必要である。また、第２次行動計画が想定し得なかった事象が発生した場合はこれに対応できるようにすることが重要である。

行動計画の見直しは重要インフラ専門委員会において行うこととし、委員会の合意を経て、情報セキュリティ政策会議で新たな行動計画を決定するものとする。

２　既存の情報共有体制との連携

緊急事態時や災害対策等においては、第２次行動計画の情報共有の枠組みの他にも、既存の情報共有体制がある。既存の情報共有体制が想定している事態のもと IT 障害が発生した場合には、第２次行動計画とこれら情報共有体制との連携が望まれる。このため、内閣官房は関係する府省庁の協力を得て情報共有の円滑化に向けた検討を行うこととする。

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、1) IT 障害の未然防止、2) IT 障害の拡大防止・迅速な復旧、3) IT 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　　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　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

（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、情報提供元が予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）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

（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。

（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。

（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

（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、以下の①から④に掲げる場合であって、法令等で報告が義務づけられている場合、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
- ア）IT 障害が発生した場合
- イ）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
- ウ）サイバー攻撃による被害を検知した場合
- エ）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
- ア）IT 障害が発生した場合
- イ）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
- ア）IT 障害が発生した場合
- イ）2 次被害により IT 障害が発生すると考えられる場合
- ウ）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
- ア）IT 障害が発生した場合

イ）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恐れがある場合など、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。

（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）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。

（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。以下「情報公開法」という。）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、当該情報が情報公開法第 5 条第 2 号本文但し書き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。

４　災害やテロ等の緊急事態における情報の集約及び共有

災害やテロ等の緊急事態においては、前述の１から３に定めるところにかかわらず、「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）等に基づき、内閣官房及び関係府省庁間で情報を集約及び共有するものとする。

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 ・ニュース・番組制作システム ・編成・運行システム
金融	銀行 生命保険・損害保険 証券会社 金融商品取引所	・預金の払い出し、振込等資金移動、融資業務の停止 ・保険金の支払い停止 ・有価証券売買の停止　　等	・銀行、信用金庫、信用組合、農業協同組合等 ・生命保険・損害保険・証券会社　等 ・金融商品取引所　　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 ・保険業務システム ・証券取引システム ・取引所システム　　等 （オープンネットワークを利用したサービスを含む。）
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 （いわゆる電子カルテ、遠隔画像診断）
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検証レベル

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）		検証レベル	
		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2条）	・ITの機能不全により、放送の停止が生じないこと	
金融	銀行	・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1項1号） ・資金の貸付け又は手形の割引（銀行法第10条1項2号） ・為替取引（銀行法第10条1項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または近隣店舗の他の ATM や窓口において対応が可能な場合等）を除く
	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
	証券会社 金融商品取引所	・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 ・金融商品市場の開設	・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8項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8項2号） ・有価証券等清算取次ぎ（金融商品取引法 第2条8項5号） ・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14項、同条16項、80条、84条）	・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 ・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 ・金融商品取引所等に関する内閣府令第112条7項を参照

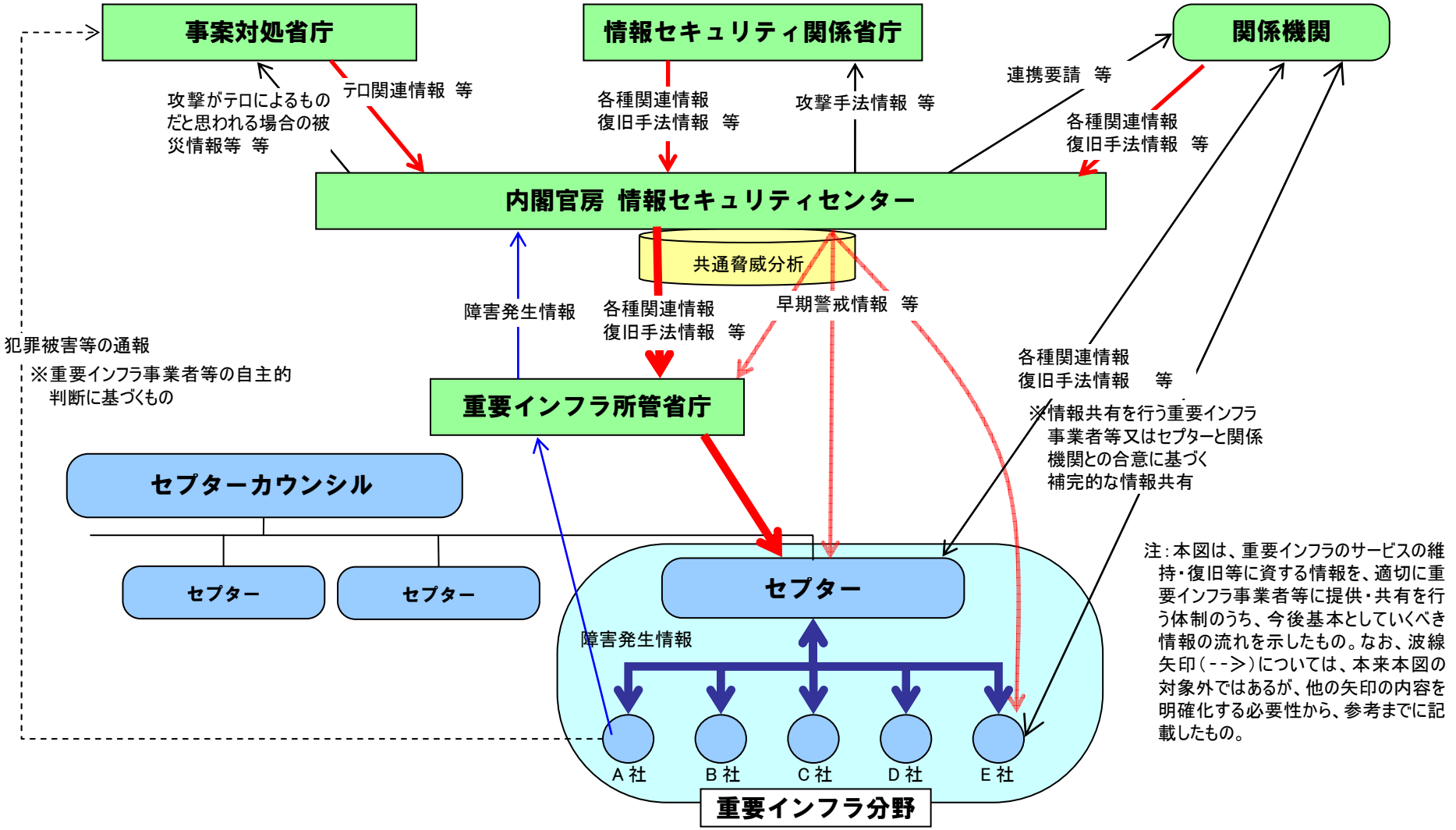
重要インフラ分野	重要インフラサービス（手続きを含む）（注）		検証レベル	
	呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
航空	・旅客、貨物の航空輸送サービス ・航空交通管制業務 ・気象情報配信 ・予約、発券、搭乗・搭載手続き ・運航整備 ・飛行計画作成	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法　第2条） ・空域の適正な利用及び安全かつ円滑な航空交通の確保（航空法　第９５条の２） ・航空機の利用に適合する予報・警報等の配信（気象業務法　第14条） ・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・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	
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	
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、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	例：ホームページによる各種情報提供サービスの場合 ・個人情報の漏えいが生じないこと ・サービスの提供不能又は誤った内容の提供が発生した場合、概ね 24 時間以内にシステムを復旧し、通常どおりサービスを提供できること
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 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、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
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	

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 障害を引き起こす脅威の例

脅威の類型	脅威の例	
	社会全体で対応が望まれる脅威	個別の重要インフラ事業者等が 中心となって対応する脅威
①サイバー攻撃をはじめとする意図的要因	分野横断的に多発するサービス不能攻撃、不正侵入、重要情報の詐取　等	不正侵入、データ改ざん・破壊、不正コマンド実行、ウイルス攻撃、サービス不能攻撃（DoS：Denial of Service）、情報漏えい、重要情報の詐取、内部不正　等
②非意図的要因	大規模な操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備が予想される社会環境変化や制度改正（例：西暦 2000 年問題、暗号の危殆化、IPv6 への移行）　等	操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障　等
③災害や疾病	大規模な地震、水害（例：首都圏直下地震、荒川の氾濫）による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等
④他分野の障害からの波及	大規模な電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等

別紙４　情報共有体制



注：本図は、重要インフラのサービスの維持・復旧等に資する情報を、適切に重要インフラ事業者等に提供・共有を行う体制のうち、今後基本としていくべき情報の流れを示したもの。なお、波線矢印（- - ≫）については、本来本図の対象外ではあるが、他の矢印の内容を明確化する必要性から、参考までに記載したもの。

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	各分野におけるセキュリティ対策等の検討体制
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 ・災害対策基本法に基づく、災害応急対策における電気通信設備の被害状況等報告 ・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 の連絡体制を活用して実施 ・放送における情報共有体制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	・ウィルス発生等の情報共有体制を活用して実施
金融	銀行 生命保険 損害保険 証券会社 金融商品取引所	(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	・全国銀行協会、（財）金融情報システムセンター（FISC）等の事業者団体を通じて実施
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、IT障害の連絡体制により実施。 (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	

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	各分野におけるセキュリティ対策等の検討体制
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	・事業者団体を通じて実施
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 ・GAS CEPTOAR の連絡体制を活用して実施 ・事業者団体を通じて実施	・業界内の委員会等を通じて実施
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」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」に基づく情報提供 (3) 地方公共団体→政府 ・「地方公共団体の情報システムに係る緊急時の連絡等について」に基づく情報提供 (4) 政府→地方公共団体 ・「地方公共団体の情報システムに係る緊急時の連絡等について」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	・政府部内連絡体制で実施
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 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 (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	・事業者団体を通じて実施