資料１

重要インフラの情報セキュリティ対策に係る第４次行動計画（案）

資料１－１　「重要インフラの情報セキュリティ対策に係る第４次行動画（案）」に対する意見募集の結果

資料１－２　「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に対する意見募集の結果一覧

資料１－３　「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」の概要

資料１－４　重要インフラの情報セキュリティ対策に係る第４次行動計画（案）

「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に対する意見募集の結果

資料１－１

意見募集期間：平成29年1月26日から2月16日まで　意見数**20件**（7団体18件、2個人2件）

【】は通し番号

主な御意見	考え方
1．経営層による計画的な投資【6,7,9,11,13】	
ライフサイクルの長い重要インフラにおいては、経営層が率先して、中長期的な投資計画に情報セキュリティ対策を織り込むことを検討することが重要。	Ⅱ.本行動計画の要点④「重要インフラ事業者等の経営者層の在り方」の記述に加え、Ⅲ.5.5「経営層への働きかけ」、Ⅳ.5.(5)「防護基盤の強化」に関する対策にも、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である旨を追記。 本文修正　p.25,33
2．今後における取組事項への提言【5,8,10,18,20】	
情報セキュリティ対策を保安規制として位置付けるには、業種の特性を踏まえて、慎重な検討が必要【18,20】	「安全」の確保が前提であることを明らかにするため、「安全等を維持する観点」が重要である旨を追記。 本文修正　p.7,12,28,30
提供される情報の重複が発生しないような、窓口の一本化を含めた体制の構築を期待【5,18】	必要な情報が確実に届くことを確保しつつ、情報共有システムの整備による効率化を目指す。
調達機器の脆弱性等に係るナレッジDBの構築を進めるべき【8】	既存の情報共有に加え、今後の情報共有システムの整備においても、そのような情報共有ができるよう検討。
製品のサプライチェーンが信頼できることを確認するための技術や制度について検討を深めることが必要【10】	「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改定で反映。

その他の御意見

・対象となる重要インフラ事業者等の表記【17】 本文修正　p.50
・法令・ガイドライン等の修正【19】 本文修正　p.54
・表現ぶりの明確化（内部統制とペネトレーションテスト）【4】 本文修正　p.11
・用語の解釈に係る照会等（OT【3】、予兆・ヒヤリハット【14】）
・分野を超えた認識の共有【1】
・通信事業者の取組強化【2】
・事業者が日常的に使用する文書にも要件を記載【12】
・ヒヤリハットの報告に資する社内検知体制整備【15】
・C（確認）及びA（是正）の定着【16】

「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に対する意見募集の結果一覧

資料１－２

意見募集期間：平成29年1月26日(木)から同年2月16日(木)まで　　20件

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
1	Ⅲ.5.5	24	－	重要インフラ事業者に対する実行方法についての記載について以下の通り意見を述べる。 ・現在各会社でセキュリティ教育が経営層の指揮によってなされているが、会社の垣根を越えて、 重要インフラに対するセキュリティの重要性を改めて共有する機会を設けたほうが良いのではないか。 理由としてはオリンピック・パラリンピックを3年後に控え、様々な企業がそれぞれのインフラでかかわることになる。 例を挙げると、道路交通、鉄道などについていえば、鉄道会社と高速道路、一般道路それぞれにかかわる会社に関する、ITのセキュリティが連携することで、一つのインフラが危機にあったときに、他のインフラでカバーできるのではないだろうか。	御意見のとおり、重要インフラ事業者等や関係者間において、サイバーセキュリティに係るリスクやサイバー攻撃等に係る情報を共有することは重要です。第3次行動計画に掲げた「リスクマネジメント」について、第４次行動計画(案)では「リスクマネジメント及び対処態勢の整備」としており、各重要インフラ事業者等がその機能保証のため、内部統制を強化し、主体的かつ自立的に対処態勢を整備することが求められていますが、同時に「リスクコミュニケーション及び協議」も推進することとしています。この取組は、重要インフラ事業者等がステークホルダーとの間においてリスクに関する役割や責任の分担等に係る合意形成を行い、重要インフラサービスの提供に関して期待される責任を果たす上で重要です。それぞれの重要インフラ事業者等が各セプターやセプターカウンシル、分野横断的演習等を利活用して、各関係主体と協力しつつ、情報・意見交換の充実を図ることとしています。	なし
2	不明	－	－	重要インフラの情報セキュリティ対策について、情報セキュリティインシデントはほぼ例外無く情報通信インフラを利用して脅威が拡大することから、情報通信分野の企業には独自の責任ある対応が求められると思うが、その視点が盛り込まれていない。重要インフラセキュリティ対策において脅威の大本を無害化するためには攻撃発信元特定のための法執行機関への協力や積極的なマルウェア感染拡大防止等が不可欠であるが、情報通信事業者は責務を果たすことができる立場にありながら、通信の秘密教条主義から、その役割を担っているとは言い難い。諸外国の事例等についてもまとめるとともに、通信の秘密教条主義から脱した現実的な情報通信事業者の責務について提言を望みます。	第４次行動計画（案）では、第３次行動計画と同様に、「情報セキュリティ対策は、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」ことを基本的な考え方としており、「Ⅳ．関係主体において取り組むべき事項」においても、「重要インフラ事業者等」については「自主的な対策として期待する事項」を示しています。 なお、重要インフラ事業者（情報通信）は、これまでも関係機関と協力して、マルウェア感染に係る利用者への注意喚起等の取組を行ってきています。	なし
3	Ⅰ.1 Ⅲ.5.6	1 26	全国銀行協会	「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）（以下、行動計画（案）という。）から「OT（ITを利用した制御システム等の運用技術）」という用語が使用されている（1頁）。また、各関係主体における人材育成について「OTの管理部門（中略）においても情報セキュリティ対策が要求される」との記述がある（26頁）。この用語を使用した背景と定義（制御技術そのものを指すのか、制御技術および技術を使ったシステムの運用まで指すのか等）をご教示いただきたい。	重要インフラ事業者等を取り巻く環境は、情報通信技術(IT)の活用が進展し、制御システム等の運用技術(OT)とも融合して広く実装されつつある一方 、情報セキュリティ対策を講じるべき防護対象が拡大・複雑化し、影響の範囲や程度を想定することが困難化している状況にあります。こうした背景を踏まえ、本行動計画では、機能保証の考え方に基づき「重要インフラサービスの安全かつ持続的な提供」を実現することを重要インフラ防護の目的の中で明確化しました。当該目的を果たすためには、重要インフラ事業者等にあっては、様々な役割や能力を持つ人材が組織横断的に連携し、情報セキュリティ対策に当たることが必要となります。 P.1脚注に記載のとおり、本行動計画においては「ITを利用した制御システム等の運用技術」を「OT」と表記していますが、P.26の「OTの『管理部門等』」については、上記背景を踏まえ、運用技術自体の管理に限らず、運用技術を用いた制御システムの管理、運用、保守等を担う部門も含めて、機能保証の考え方に基づき連携が必要となるOTに関わる部門を表す概念として整理しています。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
4	Ⅲ.1.1	11	全国銀行協会	「内部統制」の一般的な定義に鑑みると、「内部統制を図るための取組」として、「ペネトレ―ション」が例示されている点には違和感がある。例えば、「ペネトレ―ションテスト」を独立して記述することを検討いただきたい。	内部統制の基本的要素として「ITへの対応」が含まれることから、ITへの適切な対応に欠かせない情報セキュリティ確保のための取組の一例としてペネトレーションテストを挙げていますが、御指摘を踏まえ、関係部分を以下のとおり修正します。 「対処態勢整備や内部統制の基本的要素としてのITへの適切な対応に欠かせない情報セキュリティ確保の~~意識を持った企業経営の強化に向けた内部統制を図る~~ための取組（※一例として、内部監査や~~、~~ペネトレーションテスト等が考えられる。）」	11
5	Ⅲ.2.2	14	全国銀行協会	当セプターの構成員は、内閣官房内閣サイバーセキュリティセンター（以下、「NISC」という。）から所管省庁および当セプター事務局を経由して提供されるサイバー攻撃等に関する情報のほか、JPCERTおよび金融ISAC（注）等からも同種の情報を得ている。 今後、本行動計画（案）にもとづき、更なる情報共有体制の強化が進められると、NISCから各セプター構成員に展開されるサイバー攻撃等に関する情報の数が多くなるものと考えられる。 一方、セプター構成員の立場に立つと、当セプターを含めた複数の先から展開されるサイバー攻撃等に関する情報に重複が生じた場合、不要な確認作業に労力を費やすおそれがある。 ついては、可能であれば、JPCERTおよび金融ISAC等の機関とも連携し、情報の重複等が極力発生しないような情報共有体制の構築について検討いただきたい。 （注）金融ISACはセプター構成員の一部が加盟。	御指摘のとおり、NISCが提供する情報と関係機関等から展開される情報に重複が生じる可能性がありますが、それだけ当該情報は分野横断的な影響等が懸念されるものであると考えられます。 情報共有体制の強化に向けては、関係主体間での連携を密に、各セプター事務局とも連携しつつ情報の峻別をはじめとした取組を進めてまいります。 また、御指摘のような効率的な情報共有体制の実現に向け、情報共有システムの整備にも取り組んでまいります。	なし
6	Ⅰ.4.3	6	内閣府SIP	本行動計画における重点的な取組方針 第4次行動計画案に示された通り、重要インフラ事業者等における先導的取組において、更に強化・推進していくことが重要である。特に、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する必要がある。このような重要インフラ事業者等における先導的取組の推進と他の分野への拡大を積極的に推進すべきである。	御意見のとおり、重要インフラの情報セキュリティ対策を強化・推進するためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第4次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
7	Ⅰ.4.4 表2	8	内閣府 SIP	表2 本行動計画における施策群と補強・改善の方向性等 5．防護基盤の強化において、「〇セキュリティ・バイ・デザインの推進」に加え、セキュリティ・バイ・デザインを反映した「セキュリティ対策への長期的・継続的な投資」を加えるべきである。	御意見のとおり、重要インフラ事業者等がセキュリティ・バイ・デザインの考え方にのっとり、制御系機器・システム等の調達及び運用を行うためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第４次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
8	Ⅲ.2.2	14	内閣府 SIP	情報共有の更なる推進 第４次行動計画案に示された通り、情報共有体制の強化が重要である。 「共有すべき情報」の考え方について、ここに例示されている「システムの不具合等に関する情報」とは、現に運用中のシステムについての情報を念頭においていると見受けられるが、これに限らず、今後調達予定の機器についての情報も共有することが、重要インフラ防護に有効である。 一般に重要インフラ事業者が運用するシステムは規模が大きいため、調達すべき機器も数多い。調達する機器の選定にあたっては、セキュリティ強度が高いものを求めるとともに、セキュリティ強度が低いものは避けなければならない。この際、エビデンスに基づく非推奨製品や事故事例を共有してナレッジベースを構築することが、調達時のセキュリティ対策として有効である。 このようなナレッジベースの構築は、内閣官房、重要インフラ所管省庁、重要インフラ事業者が相互に協力・分担しながら推進すべきである。	御指摘のとおり、調達機器の脆弱性等に係る各種情報も極めて有用であり、既に関連する情報は情報セキュリティ関係機関等でも提供されているところです。今後の情報共有システムの整備にあたっては、御指摘のような情報の共有に向けた検討も進めてまいります。	なし
9	Ⅲ.4	18	内閣府 SIP	リスクマネジメント及び対処態勢の整備 第４次行動計画案に示された通り、「リスクアセスメントの結果を踏まえた適切な対処態勢が整備されること」が必要である。この「適切な対処態勢」に加えて、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、経営層が率先して中長期的な「セキュリティ対策投資計画への反映」が重要である。	御意見のとおり、重要インフラ事業者等において「適切な対処態勢」を整備するには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第４次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
10	Ⅲ.5.1	23	内閣府 SIP	重要インフラに係る防護範囲の見直し 第４次行動計画案に示された通り、「サプライチェーンを含めた「面としても防護」を確保する」ことが重要である。 上述のような、製品そのもののセキュリティ強度の評価を共有することに加え、その製品のサプライチェーンが信頼できることを確認するための技術や制度について検討を深めることが必要である。	御指摘の事項については、「面としての防護」に向けて取り組むにあたり、重要な要素のひとつであると考えます。現行の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）」においては、本編「Ⅲ6.1.5(2)」に関連して「同対策編」の「Ⅱ1.5(2)」に、サプライチェーンリスクへの対応に関する記述をしていますが、当該指針を2017年度に改定する必要があり、サプライチェーンが信頼できることを確認するための技術の動向等について考慮すること等を記載したいと考えています。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
11	Ⅲ.5.4	25	内閣府SIP	セキュリティ・バイ・デザインの推進 第４次行動計画案に示された通り、「システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの考え方を関係主体が共通の価値として認識することを促していく」ことが重要である。特に、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する必要がある。	御意見のとおり、重要インフラ事業者等がセキュリティ・バイ・デザインの考え方にのっとり、制御系機器・システム等の調達及び運用を行うためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第４次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
12	Ⅲ.5.8	26	内閣府SIP	規格・標準及び参照すべき規程類の整備 第４次行動計画案に示された通り、規程類を整理することが重要である。 対策の実効性を持たせるためには、セキュリティ要件を定めた規程類を整理するだけでなく、重要インフラ事業者が日常的に参照している（重要インフラの安定運用に向けた）ガイドライン等に直接要件を追記していくことが重要である。	各重要インフラ分野における、ガイドラインを含む安全基準等の策定・改定に当たっては、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第4版)」が活用されています。重要インフラ事業者等が日常的に参照している重要インフラサービス提供に係る既存のガイドライン等に、当該指針を踏まえた情報セキュリティに関する事項を追記することで、実効性の向上が期待できる場合は、そのようにしていただくべきと考えます。	なし
13	Ⅳ.5.(5)	33	内閣府SIP	Ⅳ. 関係主体において取り組むべき事項（P33） 5. 重要インフラ事業者等の自主的な対策として期待する事項 (5)「防護基盤の強化」に関する対策 「○4 制御系機器・システムの第三者認証制度の認証を受けた製品の活用を検討。」に加え、「設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する。」を追記すべきである。	御意見のとおり、重要インフラ事業者等において設備のライフサイクルも勘案した計画的なセキュリティ対策を講じることが必要であると認識しています。こうした取組については、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に実施することが重要であると考えています。このため、第４次行動計画案のⅣ(ローマ数字の4)章の「5.(5)「 防護基盤の強化」に関する対策」の⑤として、以下の項目を追加します。 「情報セキュリティ対策に関する各取組に必要な予算・体制・人材等の経営資源を計画的に確保、配分。」	33
14	別紙3	56	S&J株式会社	別紙3 情報連絡における事象と原因の類型 「発生した事象」のうち「上記につながる事象」は、「未発生の事象」の「予兆・ヒヤリハット」に含まれるべきと考えられます。理由は、「2.2 情報連絡の仕組み」に記載されている「予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象を報告する場合」において、「上記につながる事象」が含まれるかどうかがあいまいな解釈ができてしまうためです。また、より「予兆・ヒヤリハット」の目的を明確にするためには、「マルウェアが添付された不審メールの受信」は省くべきと思われます。 私の「未来投資会議構造改革徹底推進会合「第４次産業革命（Society5.0）・イノベーション」会合 （第４次産業革命）（第２回） 配布資料」の資料１０におけるP.7にヒヤリハットの事例が記述されています。	別紙3では、「上記につながる事象」の例として実際にマルウェアの感染等が確認されたことをもって「発生した事象」と整理するとともに、情報連絡の対象であることを明確化しています。また、「マルウェアが添付された不審メールの受信」それ自体は「未発生の事象」であり、原案のとおりとします。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
15	別添	44	S&J株式会社	「別添：情報連絡・情報提供について」の「1. システムの不具合等に関する情報」 「予兆・ヒヤリハットに関する情報」の報告について記述されているが、そもそも、このような事象を検知できるシステムと体制が無ければならないことを明記すべきです。言い換えれば、検知しなければ報告しなくてもいい、ということにならないようにしなければならない、ということです。	重要インフラ事業者等に対しては自らの責任において、予兆・ヒヤリハットに限らず情報セキュリティ全般についてその実施や対策を実装するための環境整備を求めており（p32）、御指摘の箇所はその取組から得られた情報の共有を促すことを意図していますので、原案のとおりとします。	なし
16	Ⅰ.3	3	特定非営利活動法人日本ネットワークセキュリティ協会	施策の「安全基準等の整備及び浸透」にある現状の課題として、 「自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である」 とあるが、施策としては、指針や基準の浸透しかなく、実務的に有効なCheck（確認）がなされているかの策がない。 確実に推進するための、具体的な取り組みを明示いただきたい。	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り、 政府機関は、重要インフラ事業者等による情報セキュリティ対策のPDCAサイクルの定着化等に必要な支援を行います。 具体的な支援策としては、従前から、安全基準等の浸透状況等調査により、重要インフラ事業者等の情報セキュリティ対策の取組状況等を把握し、施策の改善に活用するなどしておりますが、これに加え、指針に記載されたPDCAプロセスのさらなる明確化や、Check（確認）に係る観点の整理（「4.2.5 モニタリング及びレビューの推進」）等を実施します。	なし
17	別紙1	50	電気事業連合会	P50の別紙１　対象となる重要インフラ事業者等と重要システム例に関して、電力分野については、対象となる重要インフラ事業者等の記載を見直してはどうか。 今後、電力システム改革の過程で会社が分割される際に、様々な会社形態が考えられ、場合によっては発電事業等を行わない持株会社がセキュリティ統括の役割を担う可能性もあるため、現行案の範疇を尊重しつつ、このようなケースを考慮して「一般送配電事業者、主要な発電事業者　等」とするべきではないか。	御指摘のとおり、修正いたします。	50
18	Ⅰ.4.4 表2	7	石油化学工業協会	「第4次行動計画(案)」の7ページ 表2「本行動計画における施策群と補強・改善の方向性」に、第3次行動計画からの主な補強・改善の方向性として「情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点からサービス維持レベルを関係法令等において具体化するなど、制度的枠組みを適切に改善する取組を継続的に実施」との記述がある。 重要インフラ事業者は「サイバーセキュリティ基本法」に則って自主的に取組んできているところである。法制化の検討に際しては、初めから法制化ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提である。対象となる事業者へのサイバー攻撃による障害の影響の大きさと、これに対応するための事業者の負担に十分に配慮されたい。 また同表2の「情報共有体制の強化」に関して、情報は単に収集するだけでなく、有効に活用することこそが肝要と考える。サイバーインシデントの増加に伴って情報共有すべき関係先も増えており、窓口の一本化など効率化も望まれる。情報共有体制が有効かつ効率的に機能するような仕組み作りをお願いしたい。	御指摘の「制度的枠組みを適切に改善する取組」は、法制化のみを念頭に置いたものではありません。重要インフラを取りまく環境は分野により様々であると考えられ、技術の進展等により重要インフラサービスの形態そのものが変化するケースのほか、サービス形態は変わらなくても、コスト削減や利便性の向上等を目的としてサービスの提供に必要なシステムが大きく変わるケースもあると考えられます。御指摘のとおり重要インフラ分野毎の事業特性等を踏まえつつ、法制化も含めた制度見直しの検討を行い、その結果、必要と判断された場合に法制化を実施すべきと考えられます。 また、御指摘のような有効かつ効率的な情報共有体制の実現に向け、関係主体間で連携した情報共有システムの整備に取り組んでまいります。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
19	別紙2	54	石油化学工業協会	「第4次行動計画(案)」の別紙2「重要インフラサービスの説明と重要インフラサービス障害の例」で、化学分野に係る法令、ガイドラインとして「石油化学分野における情報セキュリティ確保に係る安全基準」が制定されているので、これに改めていただきたい。	御指摘のとおり、修正いたします。	54
20	Ⅰ.4.4 表2 Ⅲ 2.1	7 13	日本化学工業協会	化学セプター(主要石油化学事業者)が供給するサービスは、ポリエチレン、ポリプロピレン、塩化ビニル等国民生活に幅広く使用されている財を構成する主要部材の一つである。従来から、かかるサービスの供給途絶に備えた対応としては、供給するサービスが部材の供給であり、地域を越えた代替供給が可能であることを踏まえ、緊急時の事業者間の融通や緊急時を想定した余裕を持った製品在庫等により必要な備えを進めてきているところである。 一方、本行動計画案において重要インフラサービスとして位置づけられているセプターの供給するサービスは、化学を除けば、地域を越えた代替供給が困難なものであり、また、関連する業法により事業者に対して供給責任を負わせているものである。 一方、化学セプターの存立する産業基盤においては、化学的、物理的にリスクを内在する物質を、多くの場合高温、高圧で処理するものであり、同様のプロセスを扱う他製造業と同様に、サイバー攻撃による施設の安全の確保に重点を置いた対策が必要であり、かかる観点から従来からNISCと定期的に情報交換を行い、その対策の継続的な改善を進めているところである。これらの状況を政府においてはご理解頂き、各事業者において適切な対応がとられることが促進されるような方策をとっていただきたいと考えている。 なお、「4.4本行動計画における施策群と補強・改善の方向性等」の表2中の「1．安全基準等の整備及び浸透」において、情報セキュリティ対策を関係法令等における保安規制として位置付ける、とあるが、サービス供給継続の観点から保安規制としてセキュリティ対策を位置付けるのは必ずしも適切ではないと考えられる。保安規制としてセキュリティ対策を位置付けるのであれば、物理的な安全、保安の確保の観点から別途の視点で審議を尽くすべきと考えるところ、「保安規制として位置付けること」の部分を削除していただきたい。 また、サイバー攻撃情報の報告を法的に義務付けたとしても、そのことにより、事業者における対応の促進が図られるとは考えられず、それよりもむしろ、従来から行われているIPAやNISC、事業者相互間の情報共有・交換を一層充実させることにより、事業者の自主的な対応を促すことが、セキュリティ対策の向上に資するのではないかと考えられる。 したがって、はじめから規則や法規制ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提であると考える。 また、「Ⅲ. 計画期間内に取り組む情報セキュリティ対策」の「2.1 本行動計画期間における情報共有体制」に、24時間365日体制による迅速かつ効率的なサーバー攻撃に関する情報共有の実現に向け、内閣官房と重要インフラ事業者等の間のホットライン構築とあるが、報告時刻については、実効性ある現実的な方策にすべきと考えられる。	「安全」が確保されるということも、事案の性質に応じて、機能保証の重要な要素であると考えています。御指摘を踏まえ、関係部分を以下のとおり修正します。 「安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、」 なお、御指摘の「情報セキュリティ対策を関係法令等における保安規制として位置付ける」ことについては、「制度的枠組みを適切に改善する取組」の一例として挙げているものであり、法制化のみを念頭に置いたものではありません。重要インフラを取りまく環境は分野により様々であると考えられ、技術の進展等により重要インフラサービスの形態そのものが変化するケースのほか、サービス形態は変わらなくても、コスト削減や利便性の向上等を目的としてサービスの提供に必要なシステムが大きく変わるケースもあると考えられます。御指摘のとおり重要インフラ分野毎の事業特性等を踏まえつつ、法制化も含めた制度見直しの検討を行い、その結果、必要と判断された場合に法制化を実施すべきと考えられます。 また、御指摘のとおり、ホットライン構築に向けては報告タイミングも含め実効性ある現実的なものとなるよう情報共有システムの整備・運用に取り組んでまいります。	7,12, 28,30

「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」の概要

資料１－３

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系(ＩＴ)に限らず、制御系(ＯＴ)を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

３．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

①　先導的取組の推進(クラス分け)

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

②　オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③　リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

４．本行動計画の期間

➢　第４次行動計画（案）はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

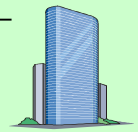
重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ（１３分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

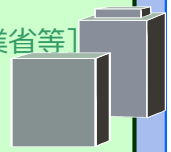
ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５省庁）



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

関係機関等



- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

重要インフラの情報セキュリティ対策に係る第４次行動計画（案）

安全基準等の整備・浸透

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

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

第４次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

「基本的な考え方」

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。
重要インフラ全体の機能保証の観点から、官民が一丸となった重要インフラ防護の取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

第４次行動計画 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的として、セキュリティ対策のPDCAに沿って「指針」及び「安全基準等」の継続的改善を推進する。

※安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称
※指針・・・・・・安全基準等の策定・改定に資するため、分野横断的に必要度の高い対策項目を収録したもの

現状の課題

- 自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である

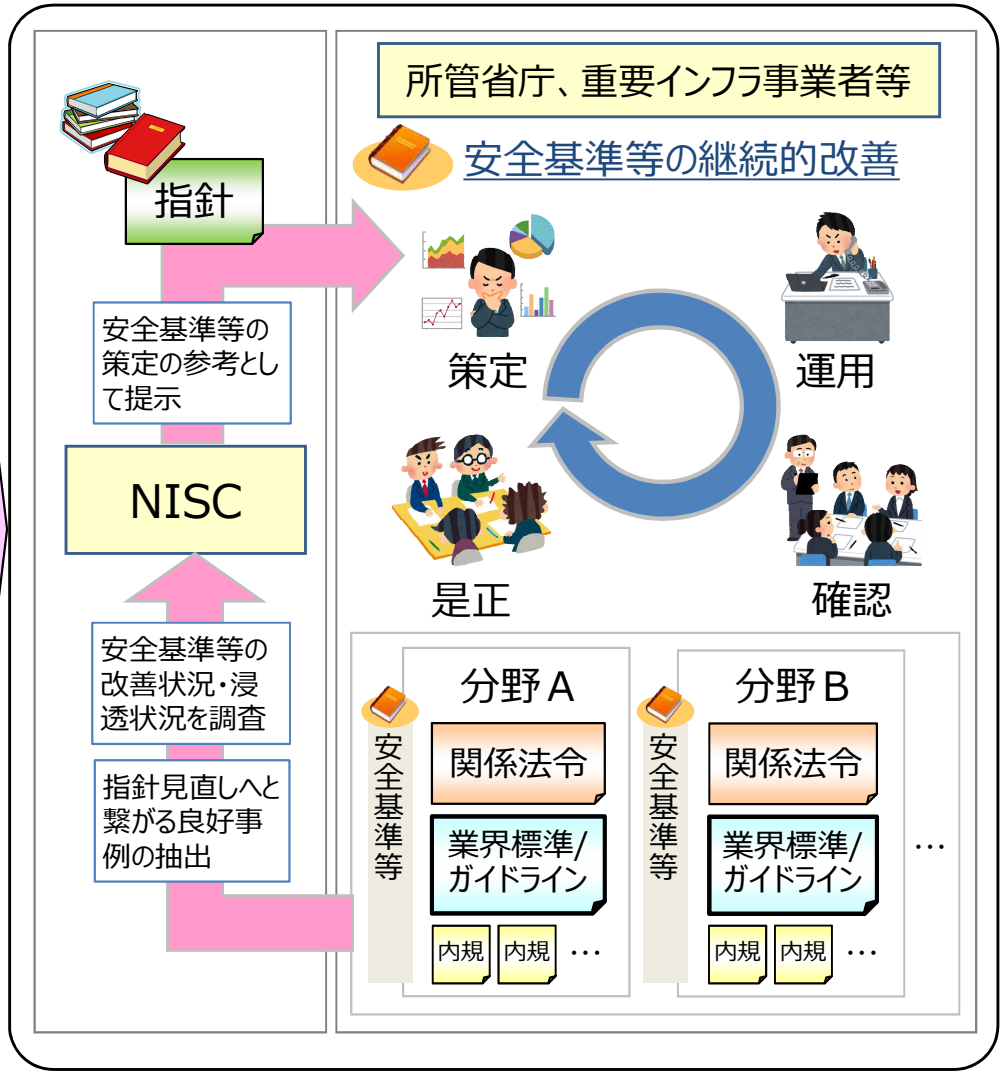
行動計画期間中の施策

（１） 指針の継続的改善
- 情報セキュリティ文化の醸成やPDCAサイクルの実行に責任を持つ経営層が認識すべき事項及び行動を指針改定時に詳細化
- 機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の対処態勢整備の必要性を指針改定時に明記

（２） 安全基準等の継続的改善
- セキュリティ対策のPDCAサイクルに沿った業界標準/ガイドラインの改善プロセスの推進
- 情報セキュリティの取組の保安規制への位置付けや、関係法令等におけるサービス維持レベルの具体化等、制度的枠組みを適切に改善する取組の継続的な実施

（３） 安全基準等の浸透
- 重要インフラ事業者等への毎年のアンケート調査により、セキュリティ対策状況を把握するとともに、アンケートへの回答を通じ、事業者等が対策の課題、解決策等を認識可能となるよう支援

第４次行動計画に基づく取組



第４次行動計画 施策②：情報共有体制の強化

個々の重要インフラ事業者等が日々変化する情報セキュリティ動向に迅速に対応できるよう、官民間や分野内外間における情報共有の強化に取り組む。

現状の課題

- 情報共有を行う意義・必要性の訴求
- 迅速かつ効果的な情報共有体制の検討
- 共有すべき情報の理解・浸透・活性化
- 民間の自主的取組に関する普及・促進　　等

行動計画期間中の施策

（１）情報共有体制の充実

- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（２）情報共有の更なる促進

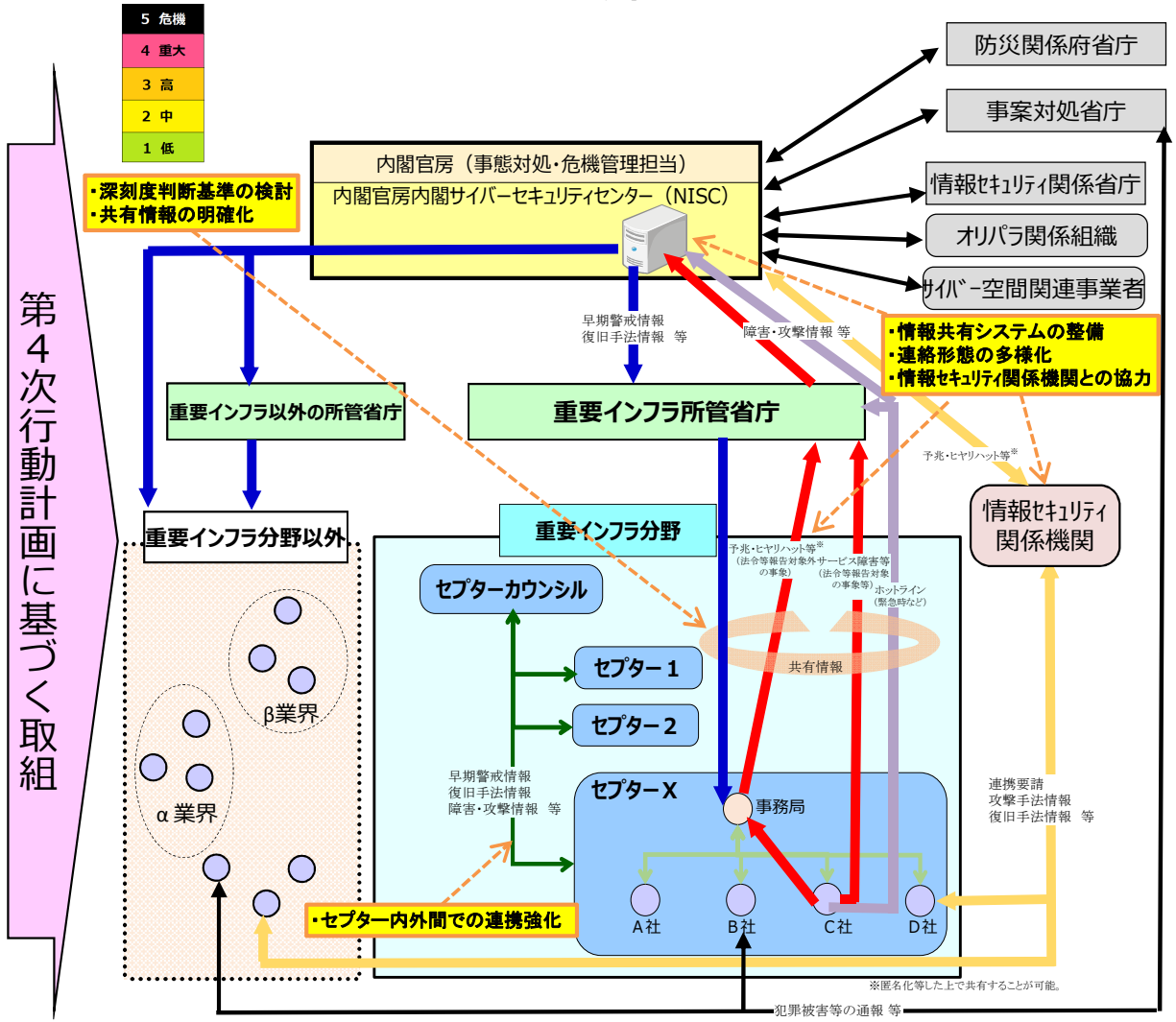
- 重要インフラサービス障害の深刻度判断基準の検討
- 共有すべき情報の明確化※

※情報系だけでなく制御系やIoTシステムも対象となること等を明示

（３）民間活動の更なる活性化

- セプター内、セプター間の情報共有の更なる充実
- 先導的な取組を行うISAC等の活動の展開

【本行動計画期間で取り組む情報共有体制】



第４次行動計画 施策③：障害対応体制の強化

重要インフラ事業者における重要インフラサービス障害対応の実態や演習ニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上。

現状の課題

- より効果的で実用的な分野横断的演習の企画推進
- 参加者拡大や、重要インフラサービス障害発生時の関係主体間の在り方に適合した演習成果の普及・浸透

行動計画期間中の施策

（１）分野横断的演習の継続と改善

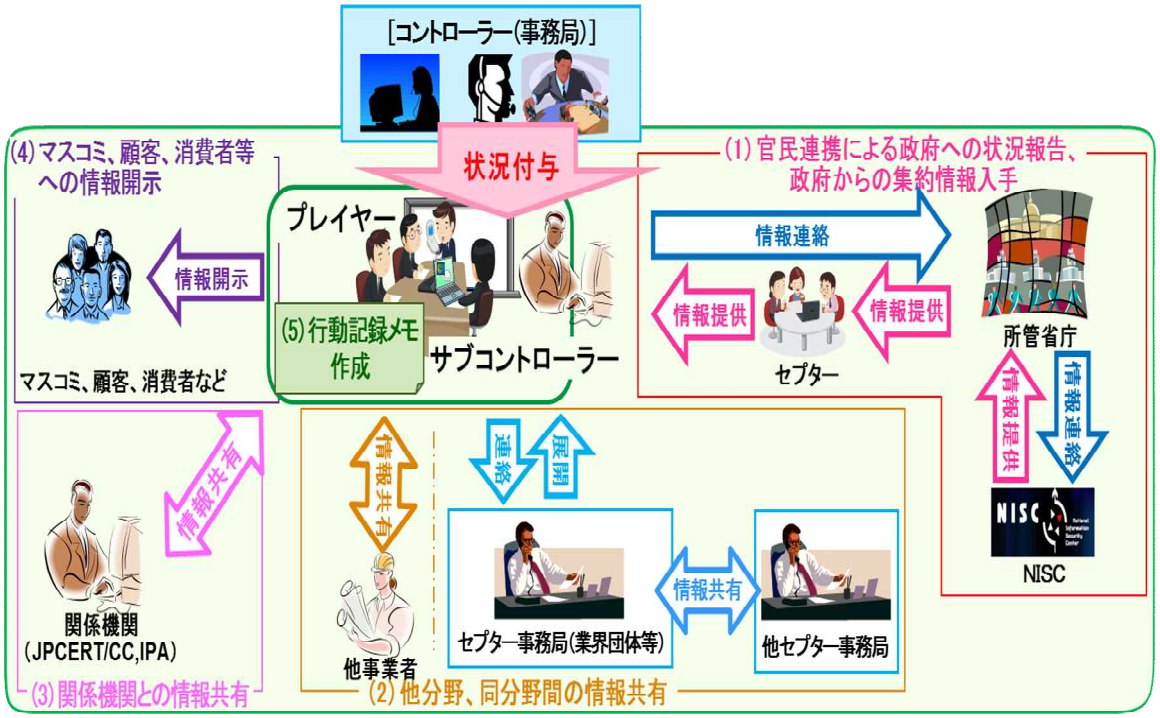
- 重要インフラ事業者の実態に即した演習企画
  - ・重要インフラ事業者の演習ニーズ取り込み
  - ・最新の攻撃手法を考慮した演習シナリオ整備
  - ・外縁の事業者や密接に関連する関係主体の参画

（２）参加者大幅増に即した演習成果の浸透

- 新規参加への促進
- 他演習・訓練との相互連携
- 経営理解増進に寄与する演習企画
- 自社演習実施に資する演習ノウハウの還元
  - ・仮想的な演習環境の提供　等

第４次行動計画に基づく取組

分野横断的演習の概要（ステークホルダー相関図）



分野横断的演習の継続と充実

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上

第４次行動計画 施策④：リスクマネジメント及び対処態勢の整備

重要インフラサービスの安全・持続的な提供に向けて、重要インフラ事業者等が実施するリスクマネジメント及びこれを踏まえた対処態勢整備を推進する。

現状の課題

- リスクアセスメントの重要性については認識が広まりつつあるが、その考え方や実施方法については十分に浸透していない。
- 重要インフラサービス障害が発生した際に備えた対処態勢整備の必要性が高まっているが、具体的な方向性・支援策等が示されていない。

行動計画期間中の施策

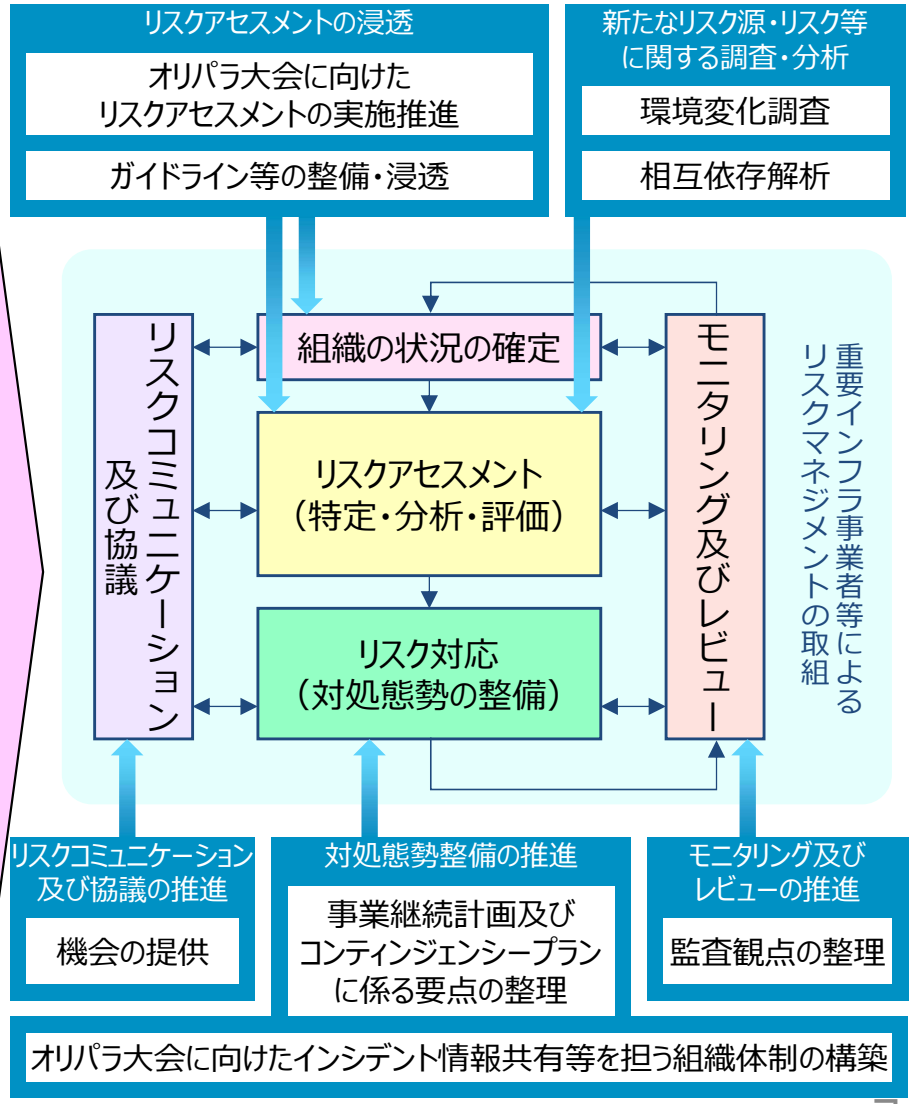
（１）リスクマネジメントの標準的な考え方

（２）リスクマネジメントの推進

- リスクアセスメントの浸透
  - ・オリパラ大会に向けたリスクアセスメントの実施推進
  - ・機能保証の考え方に立脚したリスクアセスメントガイドライン等の整備・浸透
- 新たなリスク源・リスク等に関する調査・分析
  - ・環境変化調査　・相互依存性解析
- 対処態勢整備の推進
  - ・機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの要点の整理
  - ・オリパラ大会に向けたインシデント情報共有等を担う組織体制の構築
- リスクコミュニケーション及び協議の推進
  - ・内部ステークホルダー間、関係主体間での情報・意見交換の機会の提供
- モニタリング及びレビューの推進
  - ・重要インフラ事業者等が自主的に行う内部監査等の監査観点の整理

（３）本施策と他施策との相互反映プロセスの確立

第４次行動計画に基づく取組



第４次行動計画 施策⑤：防護基盤の強化

防護範囲の見直し、広報広聴活動、国際連携、経営層への働きかけ、人材育成等、行動計画の全体を支える共通基盤的な取組を強化する。

現状の課題

- 環境変化に対応するための「面としての防護」の確保
- 広報広聴活動の一層の推進
- 国際的な情報セキュリティ対策水準の向上
- 情報セキュリティに関する経営層の意識の向上
- 人材の質的・量的な充実

行動計画期間中の施策

（１）重要インフラに係る防護範囲の見直し
- 「面としての防護」に向けた取組、国の安全等の確保の観点からの取組

（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

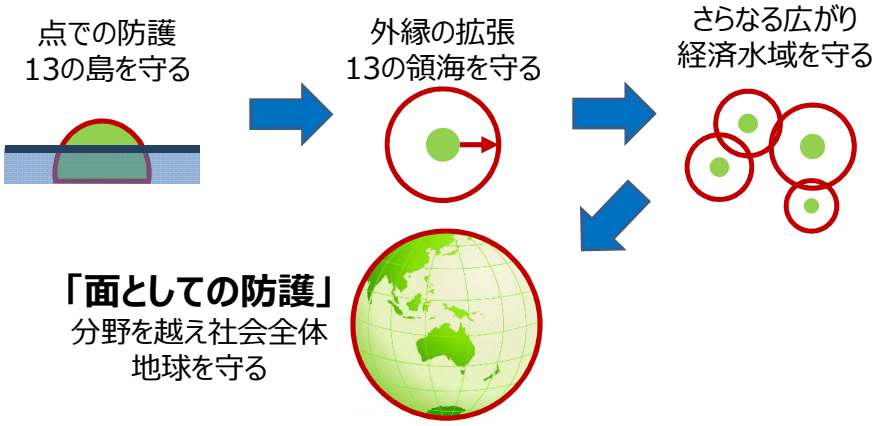
（３）国際連携の推進
- 国際的な情報セキュリティ対策の水準向上のための積極的な寄与

（４）経営層への働きかけ
- 情報セキュリティに関する経営層の意識向上のための働きかけ

（５）人材育成等の推進
- 橋渡し人材の育成、組織横断的体制の構築、情報セキュリティに係る訓練、資格取得等の人材育成策の推進等

第４次行動計画に基づく取組

重要インフラに係る防護範囲の見直し



広報広聴活動

Webサイト、講演等を通じた発信

国際連携

二国間、地域間、多国間の連携

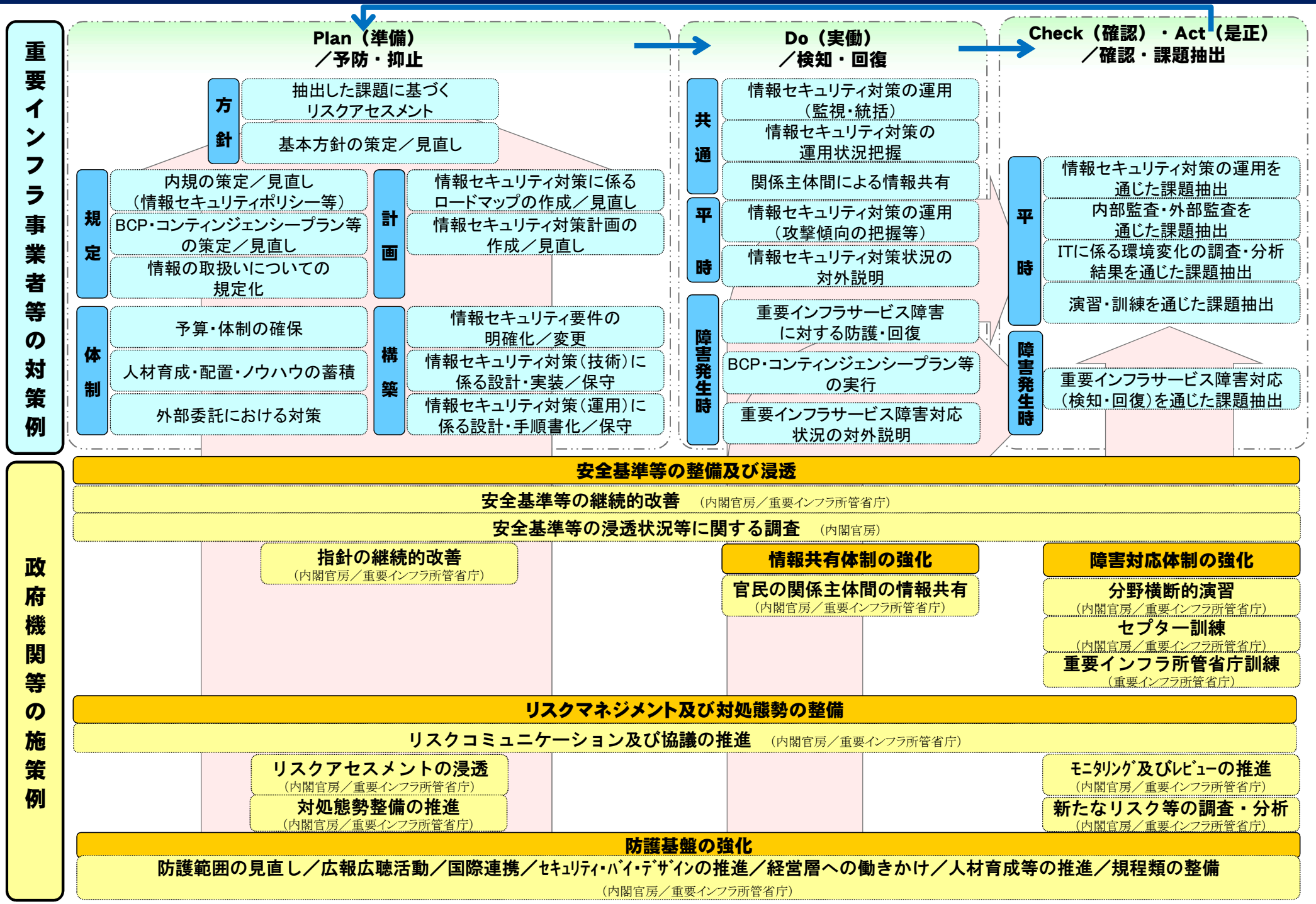
経営層への働きかけ

情報セキュリティに関する
意識向上・施策改善

人材育成等

「サイバーセキュリティ人材育成プログラム」
に基づく取組みの推進

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



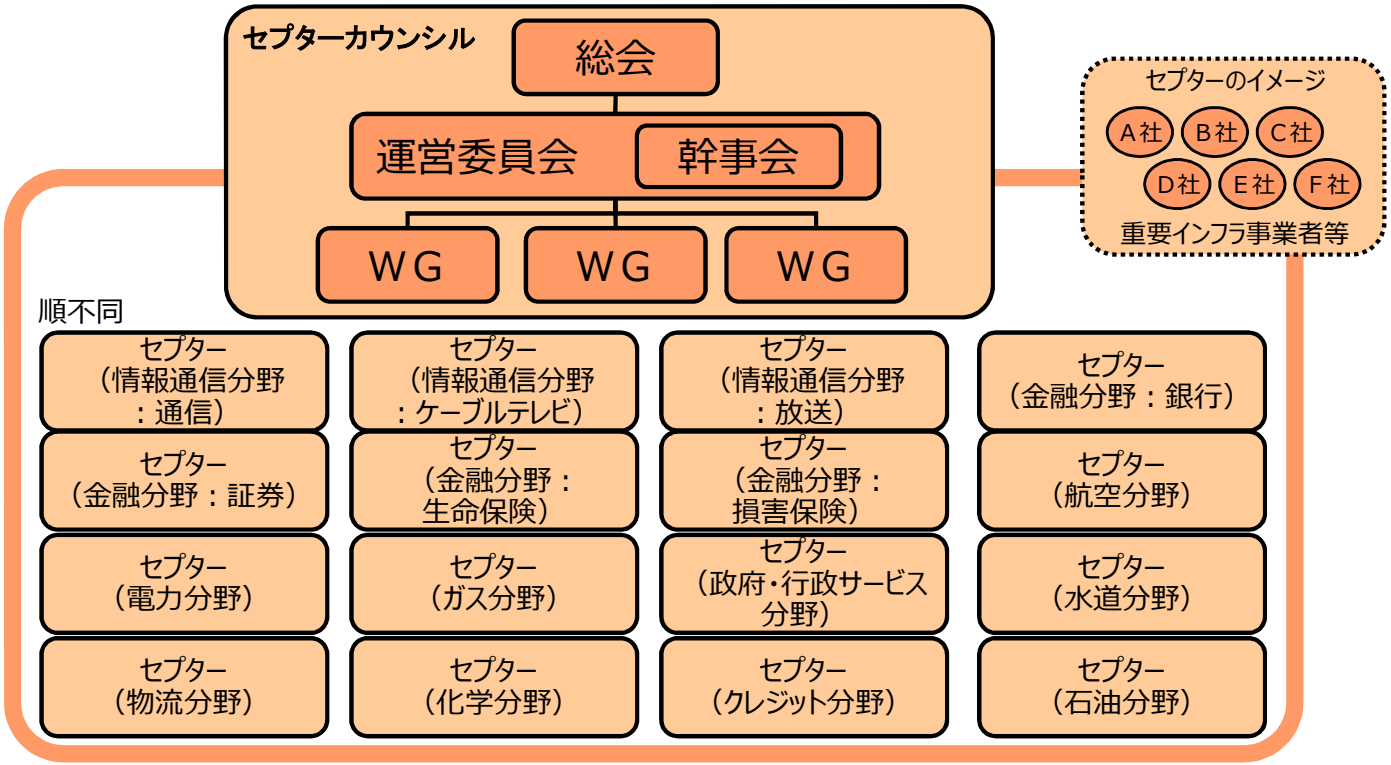
セプターとセプターカウンシル

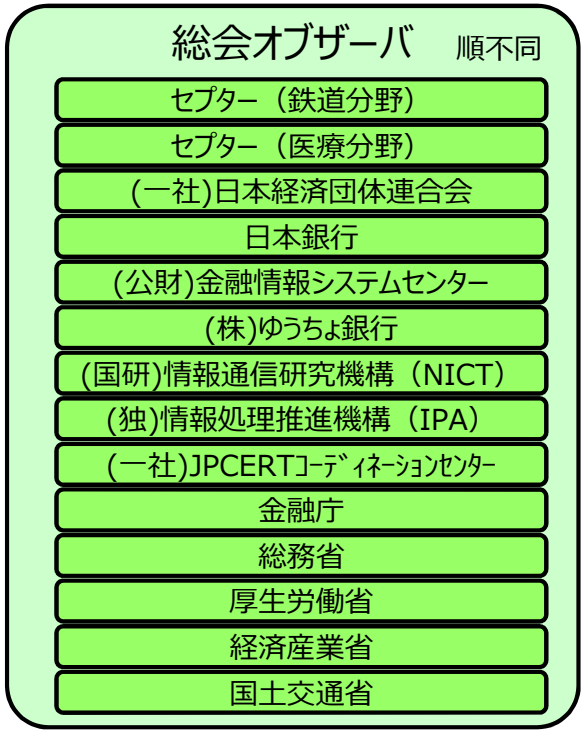
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

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

セプターカウンシル

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





情報共有体制の強化・防護範囲の見直しに関する取組状況

2017年3月末日現在

■ セプターの拡充等

重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会 銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一社) ICT-ISAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟、日本放送協会	(一社) 全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社) 生命保険協会 総務部組織法務グループ	(一社) 日本損害保険協会 ＩＴ推進部品質グループ	定期航空協会	(一社) 日本鉄道電気技術協会	電気事業連合会 情報通信部	(一社) 日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社) 日本水道協会 総務部総務課	(一社) 日本物流団体連合会	石油化学工業協会	(一社) 日本クレジット協会	石油連盟
構成員（のべ数）	23社 1団体	335社 1団体	195社 1団体	1,428社	261社 ７機関	41社	29社 （オブザーバ３社含む）	14社 1団体	22社 1団体	12社 2機関	10社	47 都道府県 1,741 市区町村	1グループ 6機関	8水道 事業体	6団体 16社	13社	28社	13社
2014年4月時点	27社 1団体	250社 1団体	194社 1団体	1,411社	251社 ７機関	43社	30社 （オブザーバ３社含む）	2ｸﾞﾙｰﾌﾟ 3機関	22社 1団体 1機関	12社 2機関	10社	47 都道府県 1,742 市区町村	1グループ 2機関	8水道 事業体	6団体 16社	—	—	—
NISCからの情報の展開先（構成員以外）	376 社・団体	438社	—	3社・団体	—	—	—	—	—	—	38社	—	377 社・機関	内容に応じ1,351事業体へ展開	—	—	—	—
	その他（核物質防護等の措置が要求される企業（内容に応じ展開先を選定）、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等（内容に応じ展開先を選定））																	
事務局の民間移行	2016年7月　航空分野（国土交通省航空局 → 定期航空協会）、鉄道分野（国土交通省鉄道局 →（一社）日本鉄道電気技術協会）																	

■ その他

既存事業領域を越える連携等	情報通信（Telecom-ISACの活動を新たに設立されたICT-ISACに移行し一部の放送事業者及びケーブルテレビ事業者が加盟）、電力（電力ISACを設立、４月より運用開始予定）、 化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者への拡張）、制御システム（JPCERT/CCが提供するConPaS等） J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報WAISE（JPCERT/CC：セキュリティ情報全般）

（※）本頁は、2017年3月時点の状況を示すものであり、セプターの構成員に関する情報は、定期的（２回/年）に更新し、内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰのＨＰ（http://www.nisc.go.jp/）に掲載。

重要インフラサービス障害等に係る深刻度判断基準（素案）

○ 概要

重要インフラサービス障害の深刻度や当該障害に関する情報の重要度に応じて影響範囲や対処行動等が異なってくることも踏まえ、関係主体間で認識の共有を図り、迅速な対応要否等の判断に資するため、下表のとおり、重要インフラサービス障害に係る深刻度の判断基準の例を設け、具体化に向けた検討を進める。（第4次行動計画案別添抜粋）

○ 目的

①可視化された深刻度により、発生した事象について関係主体間で共通の理解を助ける（客観性、国際的整合性に留意）

②深刻度レベルを政府の対応を判断する基準とする

③事象に関する情報共有の体制や方法の基準とする

表1　重要インフラサービス障害に係る深刻度判断基準（例）

深刻度	定　義
レベル5（危機）	複数の重要インフラサービスに著しい影響を与えるおそれが切迫している事象
レベル4（重大）	重要インフラサービスに著しい影響を与えるおそれが高い事象
レベル3（高）	重要インフラサービスに一定の影響を与えるおそれが高い事象
レベル2（中）	重要インフラサービスに影響を与えるおそれがある事象
レベル1（低）	重要インフラサービスに影響を与えるおそれが小さい事象

（第4次行動計画案別添抜粋）

具体化

表2　検討のための素案

深刻度	国民・社会への影響	システムへの影響	
		非常用系	常用系
レベル5（危機）	国民生活等に広範かつ著しい影響を与えるおそれが切迫		
レベル4（重大）	国民生活等に著しい影響を与える可能性が高い	重要インフラサービスの安全性・持続性への影響により評価	
レベル3（高）	国民生活等に明らかな影響を与える可能性が高い		重要インフラサービスの提供への影響により評価
レベル2（中）	国民生活等に何らかの影響を与える可能性がある		
レベル1（低）	国民生活等に影響を与える可能性は低い		
レベル0（なし）	国民生活等に影響を与える可能性はない		

資料１－４

重要インフラの情報セキュリティ対策に係る
第４次行動計画（案）

平　成　　年　　月　　日
サイバーセキュリティ戦略本部

目次

Ⅰ．はじめに

1.　行動計画策定に当たっての方向性

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、特に情報通信、電力、金融等、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる。また、重要インフラはその性質上、安全かつ持続的なサービス提供が求められていることから、その防護に当たっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を可能な限り減らすとともに、障害発生の早期検知や、障害の迅速な復旧を図ることが重要である。

このため政府では、重要インフラ防護に係る基本的な枠組みとして、重要インフラ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（以下「行動計画」という。）を策定し、これを推進してきた。

この枠組みは、「重要インフラのサイバーテロ対策に係る特別行動計画」（平成１２年１２月情報セキュリティ対策推進会議決定）（以下「特別行動計画」という。）に始まり、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や、刻々と変化する社会環境・技術環境や複雑化・巧妙化するサイバー攻撃の趨勢等に対する適切な対応を反映し、また枠組みにおける施策の評価等に基づく必要な見直しを行いながら、直近の「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成２６年５月情報セキュリティ政策会議決定、平成２７年５月サイバーセキュリティ戦略本部改訂）（以下「第３次行動計画」という。）に至るまで、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１６年以上にわたる実績を積み上げ、一定の効果を上げてきたところである。

こうした背景を踏まえ、重要インフラ防護に係る基本的な枠組みについては、これを継続し、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「本行動計画」という。）を策定した。本行動計画の策定に当たっては、「サイバーセキュリティ基本法」（平成２６年法律第１０４号）の基本理念にのっとり、後述の第３次行動計画の評価及び「サイバーセキュリティ戦略」（平成２７年９月閣議決定）を踏まえ、関係主体に定着している第３次行動計画の５つの施策群の基本的骨格を維持することにした。一方で、重要インフラを標的とするサイバー攻撃の状況や、その背景としての社会環境・技術環境の変化は著しく、情報通信技術（ＩＴ）が制御システム等の運用技術（ＯＴ）と融合して社会経済システムに広く実装されてきている[1]ほか、サイバー攻撃の対象となり得るＩｏＴシステムが普及しつつある。また、２０２０年東京オリンピック・パラリンピック競技大会（以下「オリパラ大会」という。）の開催を控え、今後、重要インフラを取り巻くリスクは増大していくおそれがある。こうした状況を勘案して重点的な方針を定め、各施策における取組を強化・改善していくこととした。

[1] 本計画の以下においては、情報通信技術（ＩＴ）を利用した制御システム等の運用技術（ＯＴ）を単に「ＯＴ」と表記する。

2.　本行動計画の構成

本行動計画の構成及び各章の概要は、表１のとおり。

なお、本行動計画に基づく各取組の実施主体については、Ⅳ章を参照のこと。

表１　本行動計画の構成

章	概要
Ⅰ．はじめに	第３次行動計画の評価結果等を踏まえた本行動計画の策定に当たっての方向性や、本行動計画の取組方針、考え方等について記載
Ⅱ．本行動計画の要点	本行動計画を推進するに当たっての、①重要インフラ防護の目的、②基本的な考え方、③関係主体の在り方、④重要インフラ事業者等の経営層の在り方について記載
Ⅲ．計画期間内に取り組む情報セキュリティ対策	本行動計画の５つの施策群ごとに、情報セキュリティ対策の実施方針や具体的な取組内容について記載
Ⅳ．関係主体において取り組むべき事項	上記Ⅲ．の情報セキュリティ対策に関し、各関係主体が実施する取組及び各関係主体に期待される取組について記載
Ⅴ．評価・検証	本行動計画の評価・検証の方針及び実施方法について記載
Ⅵ．本行動計画の見直し	上記Ⅴ．の評価を踏まえた本行動計画の見直し方針について記載

3.　第３次行動計画の評価

第３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] 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

第３次行動計画の評価として、施策群ごとの分析的な評価（結果及び課題の洗出し）を行った上、これを踏まえた第３次行動計画全体としての総合的な評価（第３次行動計画期間の目標（理想とする将来像）に照らした成果及び課題の洗出し）を行った。

総合的な評価の概要については、以下のとおりである

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

＜評価＞

第３次行動計画においては、基本的な考え方として「情報セキュリティ対策は、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」ことを明示し、本将来像について訴求した。

また、重要インフラ事業者等の自主的な取組を促すことを目的として、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」及びその付属文書（以下これらを「安全基準等の策定指針」という。）をＰＤＣＡ（Plan, Do, Check, Act）サイクルに沿った構成に改定した。また、各重要インフラ分野におけるガイドライン等及び各重要インフラ事業者等における内規等の行動規範については、安全基準等の策定指針の改定を受けて、それぞれ自主的な見直しが進められているところである。

このことから、自主的に見直しの必要性を判断して改善できるサイクル自体は、重要インフラ事業者等の行動規範として浸透しつつあると認められる。

他方、ＰＤＣＡサイクルのうち、Check（確認）及びAct（是正）の取組については、内閣官房が実施した情報セキュリティ対策の状況を把握するための安全基準等の浸透状況等の調査の結果からも、いまだ十分に定着しているとは言えず、行動様式として根付いているとは認められない状況であり、その定着が課題である。

今後、上記の行動規範に基づく行動様式が各関係主体に根付き、これに沿った取組が継続されることによって、各関係主体及び関係主体間における情報セキュリティ文化が形成されることが期待される。

＜将来像＞
各関係主体間において、重要インフラサービス障害の予防的対策を強化するためのコミュニケーションが日常的に行われるとともに、重要インフラサービス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。

＜評価＞

官民の情報共有については、重要インフラ事業者等から所管省庁・内閣官房への情報連絡の件数が着実に増加しており、より積極的な情報共有が行われつつある。

また、民間における情報共有については、セプターカウンシルの事務局を民間主体に移行するなど、セプター間の情報共有等の活動に関する主体性及び積極性の向上が図られるとともに、各セプターにおけるセプター構成員の拡大もあり、幅広い情報交換による情報セキュリティに関する知識の向上や、情報セキュリティ担当者間の人的つながりの形成が進んでおり、関係主体間のコミュニケーションの環境整備に着実な進展が見られた。加えて、幾つかの分野においてＩＳＡＣ[2]が組織されるなど、情報共有の活性化やサイバー攻撃対策の高度化も進んでいる。

障害対応体制については、分野横断的演習及びセプター訓練を継続的に実施しており、演習参加者の大幅な増加やシナリオの高度化が見られるところであり、これらの取組が、重要インフラ事業者等のニーズに応え、防護能力の向上に寄与していると認められる。

一方、脅威がより深刻化する中、重要インフラサービス障害の予防的対策を強化するためには、その目的に照らしてコミュニケーション手法を分類・具体化し、質・量ともに改善し続ける必要がある。また、障害発生時の対応について、演習や訓練を通じてその能力の向上が図られている一方、重要インフラサービス障害の対応経験等を分野横断的に将来の対策に生かす取組が十分とは言えず、こうした取組の強化が課題である。加えて、重要インフラの「面としての防護」を図るためには、障害対応事例等の分析・共有による継続的改善が重要であり、今後もその取組を継続していく必要がある。

[2] ＩＳＡＣ：Information Sharing and Analysis Center

＜将来像＞
関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている。また、多様な主体間でのコミュニケーションが充実し、重要インフラサービス障害の発生時に冷静に対処できるようになっている。

＜評価＞

関係主体間のコミュニケーションは、前述のとおり、着実に進展している。また、関係主体以外に向けては、第３次行動計画及びその取組結果を公表しているほか、分野横断的演習に関する動画の配信を行うなど、第３次行動計画に基づく取組に係る認知度を高めて国民に安心感を与えることを目的とした広報活動を推進してきた。

一方、標的型メール攻撃による情報漏えい等の報道を目にする機会が増加しているなどの背景的要因もあり、重要インフラ防護に関する国民の不安感が拭い切れていないことも事実であり、これを払拭することが課題である。

重要インフラサービス障害発生時の対応については、前述のとおり、演習や訓練を通じてインシデント対応の確認を行うとともに、改善のための取組を行ってきた。また、海外の関係機関等との間においても、各種枠組みを通じた情報共有を行うなどの連携を推進してきた。

国民に安心感を与え、重要インフラサービス障害発生時の冷静な対処を可能とするためには、国内外の多様な主体と連携し、新たなリスク源・リスクやインシデントについての情報を収集・分析し、関係主体間で共有するとともに、機能保証の観点も踏まえ、積極的に国民に向けて発信するなど、取組の継続・強化が必要である。

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

＜評価＞

重要インフラの情報セキュリティ対策については、平成１２年以後、行動計画として策定・公表され、当該行動計画に基づく取組に関しては、個々の取組がどのような結果をもたらしたのかという「結果（アウトプット）を測る視点」から、各年度における進捗状況の確認・検証を行ってきた。また、３年ないし５年の間隔で、行動計画における取組により社会が実際にどの程度理想とする将来像に近づいたのかという「成果（アウトカム）を測る視点」から、行動計画期間中における成果の評価を行い、その評価に基づく行動計画の見直しを行ってきた。

こうした取組により、我が国の重要インフラ防護は、特別行動計画から見て１６年間、現行の形態となった行動計画で１１年間の実績を有しており、５つの施策群に基づく対策が着実に進展していることから、定期的な評価により適切な見直しが行われたものと評価できる。

今後も行動計画として重要インフラ防護に係る基本的な枠組みを維持し、これに基づく取組を継続していくことが必要である。

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

＜評価＞

前述のとおり、行動計画に基づく取組は、着実に進展していると認められる。

このため、今後も関係主体に定着している第３次行動計画の５つの施策群の基本的骨格を維持しつつ、各施策において取組を深化させる。この際、重要インフラを標的とするサイバー攻撃の状況や、その背景としての社会環境・技術環境の変化を勘案した上、機能保証の観点から、①重要インフラ全体の防護を図るための一部事業者による先導的な取組の更なる推進、②オリパラ大会を見据えた情報共有体制の強化、③リスクマネジメントを踏まえた対処態勢の整備といった事項を考慮することが求められる。こうした事項については、本行動計画の重点的な方針として定めた上、これを踏まえて各施策における取組を強化・改善していく必要がある。

4.　本行動計画策定に当たっての検討結果

前述のとおり、本行動計画の策定に当たっては、第３次行動計画の評価により抽出された課題に加え、「サイバーセキュリティ戦略」を踏まえ、関係主体に定着している第３次行動計画の５つの施策群の基本的骨格を維持することにした。この際、重要インフラを標的とするサイバー攻撃の状況や、その背景としての社会環境・技術環境の変化を勘案し、重要インフラ防護の目的を機能保証の観点から明確化するとともに、重点的な方針を定めた上、本行動計画の取組を強化・改善していくことにした。

4.1 重要インフラ防護の目的

本行動計画においては、第３次行動計画における重要インフラ防護の目的を継承しつつ、重要インフラにおける機能保証の考え方を踏まえ、重要インフラサービスに重点を置き、「重要インフラサービスの安全かつ持続的な提供の実現」を重要インフラ防護の目的の中で明確化した。

4.2 「機能保証」の考え方

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

(1) 重要インフラ事業者等に求められる取組

重要インフラ事業者等にあっては、経営層が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じるとともに、サイバー攻撃等に遭遇した場合であっても、重要インフラサービスの安全を確保し、かつ、自ら及びステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続できるように、適切な対処態勢を整備することなどが求められる。また、経営層は、情報セキュリティ対策に係る内部統制システムを整備した上、こうした機能保証のための取組が適切に講じられていることについて、自らのステークホルダーに対するアカウンタビリティを果たすことが重要である。

(2) 政府機関に求められる取組

政府機関にあっては、国民生活及び社会経済活動を支える基盤として防護すべき重要インフラの範囲及び重要インフラサービスの範囲について、関係主体と連携の上でこれを設定又は見直すとともに、上記重要インフラ事業者等の取組への必要な支援を行うことが求められる。また、こうした取組が適切に講じられていることについて、本行動計画の評価や広報広聴活動等を通じて、国民に対するアカウンタビリティを果たすことが重要である。

4.3 本行動計画における重点的な取組方針

本行動計画策定に当たっては、以下のとおり、３つの重点的な取組方針を定め、各施策の取組に反映することにした。

4.3.1　重要インフラ事業者等における先導的取組の推進（相互依存性等を踏まえた重要インフラ事業者等のクラス分け）

各重要インフラ事業者等における情報通信技術の活用が進展し、また重要インフラ分野間の相互依存関係が増大している中、他の重要インフラ分野からの依存度が高く、かつ、比較的短時間の重要インフラサービス障害であってもその影響が大きくなるおそれのある重要インフラ分野（例：電力、情報通信、金融）にあっては、当該重要インフラ分野における主要な重要インフラ事業者等を中心として、相対的に高度な情報セキュリティ対策を自主的に推進している実態がある。高度化するサイバー攻撃等から重要インフラ全体の防護を図るためには、こうした一部の重要インフラ事業者等による先導的取組について、これを更に強化・推進していくとともに、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野に広めていくことが望まれることから、これを本行動計画の各施策に反映した。

4.3.2　オリパラ大会も見据えた情報共有体制の強化

オリパラ大会を始めとする国際的なビッグイベントに向けて、我が国は、国際的に大きな注目を集める一方で、悪意ある者の関心の対象ともなり、サイバー攻撃等のリスクが高まりつつあると予想される。こうした深刻化するサイバー攻撃等の脅威からオリパラ大会や重要インフラを防護するためには、各関係主体にあっては、脅威を早期に検知し、また脅威に適切に対応するための有益で実用的な情報に基づく対処

を迅速かつ適切に行うことが求められる。このため、これを本行動計画の「情報共有体制の強化」の施策に反映した。

また、こうした取組については、オリパラ大会終了後においても活用できるレガシーとして引き継ぐことを想定し、その体制構築等に係るノウハウ等のモデル化についても検討を進める。

4.3.3.　リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラを標的とするサイバー攻撃の深刻化や、その背景としての社会環境・技術環境の変化を踏まえると、重要インフラがサイバー攻撃等に遭遇した場合であっても、重要インフラサービスの安全を確保し、かつ、重要インフラ事業者等及びそのステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続できるように、各重要インフラ事業者等が適切な対処態勢を整備することが必要である。また、機能保証の観点から適切な対処態勢を整備するためには、リスクマネジメントのプロセスにおけるリスクアセスメント、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等の取組を強化・推進することが求められる。このため、これを本行動計画の「リスクマネジメント及び対処態勢の整備」の施策に反映した。

4.4 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群と補強・改善の方向性等については、下表のとおり。

表２　本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群	第３次行動計画の施策群との対応	第３次行動計画からの主な補強・改善の方向性
１．安全基準等の整備及び浸透	「[1] 安全基準等の整備及び浸透」を基本的に踏襲	○経営層に期待される認識・行動、コンティンジェンシープラン等の作成を含めた対処態勢整備、ＯＴを視野に入れた組織整備や人材育成などの重要性を訴求し、指針を充実 ○安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点からサービス維持レベルを関係法令等において具体化するなど、制度的枠組みを適切に改善する取組を継続的に実施 ○重要インフラ事業者等の安全基準等浸透及び改善につながるように、浸透状況調査の調査項目を見直し
２．情報共有体制の強化	「[2] 情報共有体制の強化」を基本的に踏襲	○情報共有の更なる推進 ・連絡形態の多様化（情報連絡元の匿名化等を可能とするセプター事務局経由の省庁報告ルートの新設）による情報共有の障壁の排除 ・サービス障害の深刻度判断基準に基づく情報共有による効率的かつ有効な事案対応の促進 ・ホットライン構築も可能な情報共有システムの整備による２４時間３６５日体制での迅速かつ効率的なサイバー攻撃に関する情報共有の実現

		・情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことについて、範囲の明確化による関係主体間の認識の共有
３．障害対応体制の強化	「[3] 障害対応体制の強化」を基本的に踏襲	○重要インフラ事業者等の実用性に即した分野横断的演習及びセプター訓練の継続的な改善 ○分野横断的演習の実施結果から得た知見、ノウハウ等を重要インフラ事業者等に広く浸透させることや、仮想的な演習環境を提供することにより、各重要インフラ事業者等による自主的な演習の実施を促進
４．リスクマネジメント及び対処態勢の整備	「[4] リスクマネジメント」を基本的に踏襲した上、発展的に「リスクマネジメント及び対処態勢の整備」として捉え直した	○施策のスコープを拡大し、機能保証の観点から、リスクアセスメント結果を踏まえた対処態勢の整備支援に係る取組（オリパラ大会も見据えた取組を含む。）を追加 ○機能保証の観点で重要となる「リスクコミュニケーション及び協議」並びに「モニタリング及びレビュー」係る取組を推進
５．防護基盤の強化	「[5] 防護基盤の強化」を基本的に踏襲	○重要インフラ分野内外の情報共有等を行う範囲の見直しを継続 ○国際会議等で得た情報の関係主体への積極的な提供 ○セキュリティ・バイ・デザインの推進 ○重要インフラ事業者等の経営層に対する働きかけ ○人材育成の支援（具体的な人材育成について産学官が連携して推進）

Ⅱ．本行動計画の要点

本行動計画を推進するに当たっての、①「重要インフラ防護」の目的、②基本的な考え方、③重要インフラ事業者等・政府機関・情報セキュリティ関係機関等の関係主体の在り方、その中でも④重要インフラ事業者等の経営層に期待する在り方を以下に示す。

①「重要インフラ防護」の目的

重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的とする。

②基本的な考え方

重要インフラ事業者等における情報セキュリティ対策は、一義的には当該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。ただし、重要インフラ全体の機能保証の観点からは、各関係主体が連携して重要インフラ防護の目的を果たすために努力を払うことが必要である。このため、重要インフラ防護における関係主体が一丸となった取組を通じて、重要インフラ防護の目的を果たすとともに、あわせて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

- 重要インフラ事業者等は、事業主体として、また社会的責任を負う立場として、それぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に対して必要な支援を行う。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

③関係主体の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況の把握に努め、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携や統制の取れた対応ができる。

④重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実践すること。

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

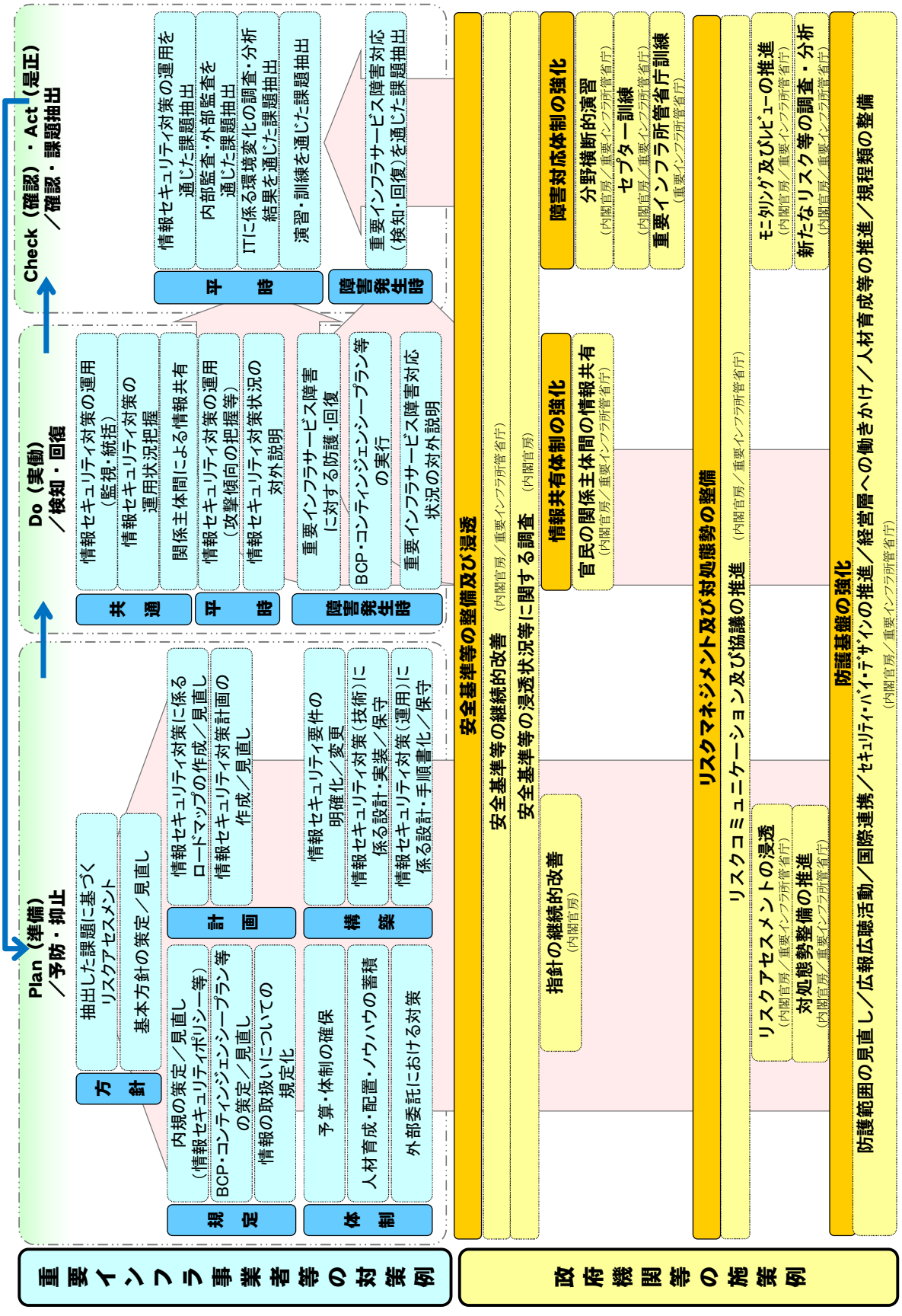


図　「重要インフラ事業者等の対策例」と各施策に関連する「政府機関等の施策例」

Ⅲ．計画期間内に取り組む情報セキュリティ対策

1.　安全基準等の整備及び浸透

各重要インフラ分野に共通して求められる情報セキュリティ対策を「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」として策定し、必要に応じた改定を行っており、同指針を受けた形で、各重要インフラ分野におけるガイドライン等の見直し、そして重要インフラ事業者等の内規等の見直しが進められ、全体として必要な安全基準等の整備が図られている。

さらに、各重要インフラ事業者等において、安全基準等が情報セキュリティ対策の規範として浸透することにより、重要インフラサービスの安全かつ持続的な提供に必要な取組の推進が図られている。

本行動計画期間においては、内閣官房は、重要インフラ防護能力の維持・向上を目的に、指針改定及び安全基準等の継続的改善や浸透状況の調査を行う。

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

1.1 指針の継続的改善

重要インフラ防護能力の維持・向上、とりわけ経営層に関する取組、コンティンジェンシープラン等の作成を含めた対処態勢整備、ＩＴだけでなくＯＴも視野に入れた対策等に資することを目的に、内閣官房は、指針本編・対策編・手引書（「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」）の見直しを行う。

具体的には、「サイバーセキュリティ経営ガイドライン」等を活用するなどして、情報セキュリティ文化の醸成や情報セキュリティ対策のＰＤＣＡサイクル実行に責任を持つことなど、経営層の在り方を明確化する。あわせて、機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の作成を含めた対処態勢整備や内部統制の基本的要素としてのＩＴへの適切な対応に欠かせない情報セキュリティ確保のための取組（※一例として、内部監査やペネトレーションテスト等が考えられる。）について追記する。

また、サイバーインシデント発生時の対応組織であるＣＳＩＲＴ[3]の構築に加え、プラントや工場等の制御系システムへのサイバー攻撃等の脅威に迅速に対応するため、ＩＴとＯＴの横断的な組織整備や、ＯＴのセキュリティ人材の育成の重要性を訴求する。

加えて、重要インフラサービス障害が発生した場合にその経験を確実に将来の対策に生かすため、情報共有の取組の一つとして、重要インフラ事業者等の間で過去のインシデント対応に係るケーススタディの実施等を例示する。

指針本編・対策編・手引書の見直しについては、３年に１度の実施を原則とする。ただし、社会動向の大きな変化等、指針本編・対策編・手引書が想定しえなかった事象が発生した場合は、３年に１度の実施は、その限りとしない。また、２０２０年にオリパラ大会を控えていることを勘案し、本行動計画の見直

[3] Computer Security Incident Response Team。情報システムに情報セキュリティ上の問題が発生していないか監視するとともに、問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。

しに伴う指針本編・対策編・手引書の見直しについては、時宜を得て実施するものとする。

1.2 安全基準等の継続的改善

重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。

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

加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を継続的に進める。

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より精緻な把握を目的に、内閣官房は、毎年、重要インフラ事業者等の対策状況についてのアンケート調査及び往訪調査を実施する。アンケート調査については、重要インフラ事業者等における安全基準等の浸透及び取組の改善につながるよう、随時調査項目の見直しを行う。

具体的には、対策状況をより詳細かつ精緻に確認するための調査項目を追加するとともに、各施策によって、理想とする将来像へどの程度到達したかを把握するための調査項目を追加する。さらに、調査への回答を通じて、重要インフラ事業者等がセルフチェックを行い、自らの情報セキュリティ対策の充足度や課題点、解決策等を認識可能となるように調査票等を構成する。

また、アンケート調査結果から得られた仮説の検証及び良好事例の収集を目的に、重要インフラ事業者等へ往訪調査を行う。

なお、アンケート調査及び往訪調査によって得られた調査結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。

2.　情報共有体制の強化

重要インフラを取り巻く社会環境・技術環境や情報セキュリティの動向が刻々と変化する中、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、単独で取り組む情報セキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組むことが必要である。また、攻撃者情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じることは、当該攻撃の被害を最小限に留めるだけでなく、新たなサイバー攻撃の抑止にもつながる。

こうした背景を踏まえ、これまでの行動計画でも円滑な情報共有を促進するための取組を進めており、一部の分野では情報共有が活性化するなど一定の成果を得たが、まだ重要インフラ全体として十分な情報共有が行われるまでには至っていない。このため、本行動計画においても引き続き、本件取組の意義・必要性の理解を深め、その活性化を図るための施策を推進することが重要である。

なお、我が国の基本的考え方として、情報セキュリティ対策は一義的に重要インフラ事業者等が自らの責任において実施し、他の関係主体とは相互に自主的に協力することとしていることを踏まえ、官民・分野横断的に情報共有しやすい環境整備に向けた取組を優先して取り組んでいくものである。

2.1 本行動計画期間における情報共有体制

我が国ではオリパラ大会をはじめとする国際的なイベントの開催が多数予定されており、重要インフラに対するサイバー攻撃が質・量とも更なる深刻化が想定されるため、関係者間における速やかな情報共有体制の整備が急務となる。第３次行動計画で構築された情報共有体制が関係主体の間で定着していることも踏まえ、これを引き続き継承・発展させ、内閣官房では、以下のとおり情報共有体制の改善や新たなスキームの検討等に取り組み、重要インフラ事業者等は共有された情報をリスクマネジメントや事案対処等へ積極的に活用していくものとする。

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

さらに、２４時間３６５日体制による迅速かつ効率的なサイバー攻撃に関する情報共有の実現に向け、緊急時における内閣官房と重要インフラ事業者等の間のホットライン構築も可能な情報共有システムの整備に取り組む。

また、情報セキュリティ関係機関は、企業から独立した中立的な観点から、国内外のインシデントに係

る情報収集や分析、インシデント対応の支援等に当たっており、このことを踏まえれば、内閣官房及び重要インフラ事業者等と情報セキュリティに関する知見を有する同機関とが密に連携することは有効かつ望ましい姿であると言える。あわせて、同機関については、連絡元の了解が得られた情報の匿名化等を行い、積極的に関係主体と共有するなど、我が国の情報共有体制におけるメインプレーヤーの一つとしての活動が期待される。

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

以上を踏まえ、本行動計画期間中の体制を「別紙４－１　情報共有体制」に、各関係主体の役割を「別紙４－２　情報共有体制における各関係主体の役割」に示す。なお、連絡経路の多様化に際しては、情報共有システム導入前であっても試行的な取組を進めるものとする。また、重要インフラ分野の重要システムや重要インフラサービス障害の事例等について、「別紙１　対象となる重要インフラ事業者等と重要システム例」及び「別紙２　重要インフラサービスの説明と重要インフラサービス障害の例」に表した。

以上の取組を着実に進めるとともに、ＩｏＴのような分野をまたがる情報セキュリティ上の脅威についても迅速かつ的確に対応できるよう、前述の情報共有システムも活用し、重要インフラサービス障害に係る情報及び脅威情報を内閣官房に分野横断的に集約し、分析の上、関係主体と共有する仕組みの構築を進める。

2.2 情報共有の更なる推進

本行動計画期間における情報共有の活性化に向け、内閣官房では、重要インフラ事業者等との間で共有すべき情報の明確化を図るとともに、社会環境・技術環境の変化や重要インフラ分野内外の相互依存性を踏まえた継続的な防護範囲の見直し（情報共有範囲の拡充を含む）に取り組む。

共有すべき情報について、第３次行動計画における定義を継承して「重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システムの不具合等に関する情報」という。）」とし、「別添：情報連絡・情報提供について」及び「別紙３　情報連絡における事象と原因の類型」の考え方のとおりとする。ただし、重要インフラサービス障害に係る深刻度や当該障害に関する情報の重要度に応じて影響範囲や対処行動も異なることから、関係主体間における認識の共有を図り、迅速かつ効果的な情報共有を実現するため、別添の中で重要インフラサービス障害に係る深刻度の判断基準の例を示し、具体化に向けた検討を進める。これにより、分野内外への影響拡大が懸念されるサイバー攻撃等に係る情報について、一定の判断基準に基づき関係主体間での効果的な情報共有の促進に取り組んでいく。また、近年、情報システムのうち、クローズドで安全と考えられていた制御システム等においてもサイバー攻撃が確認されており、今後の普及が見込まれるＩｏＴシステムも含め、これらに対する攻撃等についても共有すべき情報の対象であることを明確化した。

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

む。

なお、これにあわせ、重要インフラサービスを安全かつ持続的に提供するための「面としての防護」を実現するため、防護範囲の見直しについても継続的に取り組む（詳細については、本章5.1(1)に記載）。

2.3 重要インフラ事業者等の活動の更なる活性化

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

具体的には、重要インフラ事業者等においては、自ら積極的に情報共有に取り組むとともに、ＣＳＩＲＴ等の重要インフラサービス障害対応体制を構築・強化することが期待される。また、セプターにおいては、第３次行動計画期間に引き続き、内閣官房が提供する情報の取扱いに関する取決め、機密保持及び構成員外への情報提供に関し、構成員間で合意されたルールが適用され、緊急時に各構成員及び構成員外との連絡が可能な窓口（ＰｏＣ[4]）が設定されている状況において、内閣官房が提供する情報を共有することの継続が期待される。

加えて、セプター内の情報集約及び情勢判断を行うコーディネータの設置、予兆情報や平時の重要インフラサービス障害事例の共有、セプター間やセプターカウンシル等との情報共有に必要な機能の充実を通じた活動の更なる活性化が期待される。また、一部の先導的な取組を行う事業者間ではＩＳＡＣを設置し、ＩＳＡＣ内で情報セキュリティ対策に資する情報の共有・調査・分析、更には海外のＩＳＡＣ等との情報共有等も進められている。ＩＳＡＣへの参画やＩＳＡＣ間の情報共有を促進することで、更なる事業者間の情報共有の活発化や情報セキュリティ対策に係る積極的な取組が期待される。

また、セプター構成員の拡大や新規セプターの設定等、セプター内外の情報共有における継続的な拡充が期待される。重要インフラ事業者等で扱われる情報共有においては、国内外の多様な主体との連携やサービスの安全かつ持続的な提供のため、ＩＴだけでなく、ＯＴを含めた情報共有の質・量の改善等が期待される。

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

このように、各セプターの積極的な参画により、重要インフラ事業者等におけるサービスの維持・復旧能力の向上に資する自発的かつ幅広い取組を通じて、セプター間の情報共有の一層の充実等、重要インフラ事業者等の活動の更なる活性化が期待される。

---

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

3.　障害対応体制の強化

本行動計画期間においては、第３次行動計画から行われている重要インフラサービス障害対応に関する能力向上及び検証を目的とする各種演習・訓練の実績を踏まえ、引き続き重要インフラサービス障害対応体制の総合的な強化に取り組む。

その中で、分野横断的演習については、最新の攻撃手法を考慮した演習シナリオの検討等を行うことにより、重要インフラ分野の重要インフラサービス障害対応体制を強化する中核的な取組として、重要インフラ事業者のニーズを取り込んだ現状の仕組みを継続しつつ更なる充実を図る。具体的には、重要インフラ事業者等におけるインシデントハンドリングや組織内規程等の実態に即した演習となるよう改善を進める。なお、分野横断的演習がセプター訓練及び重要インフラ所管省庁が実施する他の演習・訓練と相互に連携・補完し、相乗効果を発揮できるよう、引き続き各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の体制の強化を行う。

3.1 分野横断的演習の改善

本行動計画期間においては、内閣官房は、重要インフラ分野全体への分野横断的演習の成果の浸透を通じた重要インフラ防護能力の維持・向上に資することを目的に、重要インフラ事業者等を一堂に会した我が国唯一の取組である分野横断的演習を改善しつつ引き続き実施する。

その際、障害対応体制の強化に資するよう、これまでに蓄積した運営手法や成果を用いて分野横断的演習の充実を図る。

3.1.1 分野横断的演習の企画立案に係る質的改善

本行動計画期間において、内閣官房は、分野横断的演習の改善を継続的に行うことを目的として、演習運営を通じて得た知見・課題、他施策や他組織が実施する訓練から得られた課題及び重要インフラサービス障害を引き起こす要因であるリスク源に係る最新動向を演習に取り込む。さらに、重要インフラ事業者等が保有する情報システムの維持に密接に関連する関係主体、重要インフラサービスを支える重要インフラ分野以外の事業者等の参画も視野に入れた演習の企画立案に取り組む。

また、内閣官房は、演習成果が重要インフラ事業者等の情報セキュリティ対策並びに重要インフラサービス障害時の早期復旧手順及び IT-BCP 等に係る検証の更なる強化に資することを目的に、継続的な演習プロセスの改善を行う。

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

3.1.2 重要インフラ全体への分野横断的演習の成果の浸透

第３次行動計画期間中、演習参加者数は大幅に増加し、演習を有意義と評価する参加者が８割を超えていることから、引き続き演習未経験者への新規参加を促すことで、重要インフラ分野における演習成果の浸透を目指す。一方、参加者拡大には一定の限界があることから、更なる重要インフラ全体への演習成果の普及・浸透を行うためには、新規参加の促進に加え、各事業者から本演習に参加した者が本演習のノウ

ハウを活用した個別の自社演習や分野内演習に自主的に取り組めるよう、人材を育成していくことも必要である。

そのため、内閣官房は、演習のメリットについての説明資料を作成・公表することにより、重要インフラ分野全体における経営層の理解や積極的な参画を促し、各重要インフラ分野及び重要インフラ事業者等内での演習実施を促進する。

また、個別の重要インフラ事業者等による演習実施の支援に資することを目的に、これまでの演習において蓄積してきた実施・評価・助言手法の整備及びその共有化の実現に向け、仮想的な演習環境の提供等に取り組む。

3.1.3 重要インフラ所管省庁等との連携

重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練は、内閣官房が実施する分野横断的演習と期待する効果が異なるが、分野横断的演習と相互に連携・補完しつつ実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図っていくことが期待される。

このことから、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の対応能力の向上を目的に、それぞれが実施する演習における主な対象者や検証目的の明確化及び相互連携の在り方について具体化に取り組む。

また、一部の重要インフラ分野で既に設立されているＩＳＡＣ等の民間機関と連携し、参加事業者にとって効果的な演習や情報連携の在り方等についても具体化に取り組む。

なお、重要インフラサービス障害対応に当たっては、物理的な重要インフラサービス障害等の様々な要因が考えられることから、各府省庁や各重要インフラ事業者等の情報セキュリティ部門だけでなく防災・危機管理部門との情報共有を要する可能性もあるため、関係主体からのニーズも踏まえ、必要に応じて当該部門との連携に取り組む。

3.2 セプター訓練

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

実施に際して、セプター訓練では多くの重要インフラ事業者等の参加実績があることを踏まえ、本件機会を有効に活用するという観点からも、各分野の特性や最新の攻撃トレンドに係る注意喚起も兼ねた模擬情報のカスタマイズ化、全セプターにおいて日程を定めない抜き打ち訓練の実施、緊急時における情報連絡体制・手段の検証等、セプターや重要インフラ所管省庁からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有訓練の実現を目指す。

4.　リスクマネジメント及び対処態勢の整備

情報通信技術の活用の進展に伴い、サイバー攻撃や情報システムの不具合に起因する個人情報の漏えいやサービス提供の中断による経済的損失等の事例が頻繁に報告されており、実社会への被害が深刻化している。未公開の脆弱性を狙ったゼロデイ攻撃のような高度化したサイバー攻撃や内部不正に関しては、もはや「未然に防ぎきることは不可能である」ということを認識する必要がある。

こうした状況において、重要インフラ事業者等にあっては、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえたリスク対応を戦略的に講じることが必須の要件となっており、機能保証の観点からは、サイバー攻撃等に遭遇した場合であっても、重要インフラサービスを安全かつ継続的に提供できるように、リスクアセスメントの結果を踏まえた適切な対処態勢が整備されることも必要である。また、こうした活動全体（リスクマネジメント）が継続的かつ有効に機能するための仕組みを構築することも重要である[6]。

このため、重要インフラ事業者等における機能保証の考え方に立脚した施策の重点化を目的として、第３次行動計画の「リスクマネジメント」を発展的に「リスクマネジメント及び対処態勢の整備」として捉え直し、「リスクマネジメント」の各施策を引き続き実施するとともに、各重要インフラ事業者等がリスクアセスメント結果に基づく適切な意思決定を行うための内部統制の強化や、各重要インフラ事業者等が主体的かつ自律的に行う事業継続のための対処態勢の整備の支援に係る施策を新たに実施する。

4.1 リスクマネジメントの標準的な考え方

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

このことから、各関係主体は、国際的にも標準的なリスクマネジメントの考え方や、そこで利用される情報セキュリティに関する用語の定義等を利活用することが望ましい。具体的には、各施策や各種関連資料において、以下の表３に示す枠組みを軸とした考え方や枠組みの中で利用される用語の定義等を可能な限り適用する。

[6] 機能保証の観点からは、重要インフラサービスに直接関係するシステムの不具合に実施範囲を限定せず、間接的に関係するシステムの不具合の波及的な影響についても勘案し、重要インフラサービスの提供に及ぼす影響を大局的に捉えたリスクアセスメントを実施することが重要である。

表３　標準的なリスクマネジメントのプロセス（例）

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

リスクマネジメントは、基本的に各重要インフラ事業者等が自組織に最適化して取り組むものである。リスクアセスメントについては、事業者が自主的に策定している情報セキュリティ基本方針にリスクアセスメントの実施に関して記載する重要インフラ事業者等の増加が確認できるなど、既に多くの重要インフラ事業者等がその重要性を認識していることがうかがえる。その一方で、リスクアセスメントの重要性を認識しながらも、具体的にどのように進めたら良いかが分からないなどの理由により、実施できていない重要インフラ事業者等も散見されるなど、リスクアセスメントの考え方や実施方法については、十分に定着しているとは言い難い状況である。また、リスクアセスメントやリスクコミュニケーション及び協議においては、重要インフラ分野横断的な調査・分析及び意見交換等といった自組織だけでの取組が容易ではないものも存在する。

このため、次の取組を通じて、重要インフラ事業者等のリスクマネジメントの推進を行う。

4.2.1　リスクアセスメントの浸透

重要インフラサービスは、社会経済システムにおいて不可欠な役割・機能を担っていることから、安全かつ持続的に提供されている状態が維持されることが必要である。このため、各重要インフラ事業者等が自らの役割・機能を発揮し、その提供する重要インフラサービスの安全を確保し、かつ、自ら及びそのステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続させるということを目的としたリスクアセスメントを行い、その実施結果を踏まえた経営層による総合的な判断に基づくリスク対応を進めていくことにより、その目的達成を目指していくという「機能保証」の考え方が重要となる。

このことから、重要インフラ事業者等における機能保証の考え方に立脚したリスクアセスメントの浸透を図る。具体的には、次の施策を講じる。

①「機能保証に向けたリスクアセスメント・ガイドライン」[7]をオリパラ大会に係るリスクアセスメントにおいて利活用することを通じて、機能保証の考え方に立脚したリスクアセスメントの趣旨や実施方法を当該リスクアセスメントの実施主体に浸透させるとともに、リスクアセスメントに関する説明会や講習会の実施等により、当該リスクアセスメントの実施を推進する。

②「機能保証に向けたリスクアセスメント・ガイドライン」を重要インフラ事業者等における平時のリスクアセスメントに利活用できるように一般化することや、「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」を改善することなどを通じて、機能保証の考え方に立脚したリスクアセスメントの趣旨や実施方法を重要インフラ事業者等に浸透させる。

なお、これらの取組を通じて、各重要インフラ事業者等によるリスクアセスメントが将来的に一定以上の精度や水準で実施されることが期待される。

4.2.2　新たなリスク源・リスク等に関する調査・分析

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

また、重要インフラ分野において生じた重要インフラサービス障害等の影響の波及に係る解析を継続して行う。具体的には、各調査・分析の効率、他施策との相互反映等の観点も踏まえ、以下のとおりとし、その調査・分析結果については、重要インフラ事業者等に提供する。あわせて、本行動計画の取組の改善に活用する。

(1) 環境変化調査

ＩｏＴ、フィンテック（FinTech）その他中長期的な重要インフラ分野への浸透が予想される新しい技術・システムや関連する制度等を対象として、環境変化の実態調査及び環境変化に伴う新たなリスク源・リスクの分析を行う。また、当該調査・分析は、時間経過や環境変化に応じて行うことでより良い結果を得られることから、その対象や範囲を柔軟に捉えつつ、継続的に行う。また、例えば制御系、情報系等一定の分野に共通するもので、全分野に及ばずとも影響が大きい新たなリスク源・リスクについても、当該調査・分析の対象とする。

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

(2) 相互依存性解析

各重要インフラ分野における情報通信技術の活用が進展し、重要インフラ分野間及び重要インフラ以外の分野との間の相互依存関係が増大する中、重要インフラ分野における相互依存性の把握は、リスクアセスメントの実施や重要インフラサービス障害等が生じた際の効率的な復旧対策において重要である。

このことから、本行動計画において、環境変化に伴う相互依存性の変化及び新たな重要インフラ分野の

[7] オリパラ大会に向けた取組として、平成２８年９月に、内閣官房が策定した大会の運営に大きな影響を及ぼし得る重要システム・サービスを提供する事業者等に向けたガイドライン

追加が生じた場合、過去の行動計画における解析結果を基に再調査・解析を行うことを含め、相互依存性解析を継続的に行う。

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

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

4.2.3 対処態勢整備の推進

機能保証のためには、重要インフラサービス障害により影響を受けた重要インフラサービスについて、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが求められることから、重要インフラ事業者等にあっては、重要インフラサービス障害が発生した際に備えた対処態勢を整備することが必要である。

このことから、重要インフラ事業者等における対処態勢の整備を推進する。また、オリパラ大会も見据え、その関係主体における対処態勢の整備についても推進する。具体的には、次の施策を講じる。

①重要インフラ事業者等における機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの整備並びに当該計画を実行するための組織体制の構築を推進する。この際、事業継続計画及びコンティンジェンシープランが想定どおりに実行できないことがリスクとなり得ることから、これらの実行性を確保し、また検証するための教育、演習等の取組を講じることも重要である。このため、こうした取組についても併せて推進する。

②オリパラ大会も見据え、各関係主体におけるインシデント情報の共有等を担う中核的な組織体制（オリンピック・パラリンピックＣＳＩＲＴ（仮））を構築する。また、当該組織体制の整備において政府及び関連主体の役割を整理するなどの取組で得られた知見をレガシーとして上記①の施策に活用する。

なお、本行動計画において、「コンティンジェンシープラン」とは、重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたものをいい、これに基づいて適切な対応を行うことにより重要インフラサービス障害による影響を最小限に抑えることを目的とする。初動対応（緊急時対応）には、重要インフラの性質やリスクアセスメントの結果に応じて、安全を確保するために重要インフラサービスの提供を停止するなどの対応についても含まれる。また、「事業継続計画」とは、機能保証の観点から、重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準まで復旧させることを目的して、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたものをいう。

4.2.4 リスクコミュニケーション及び協議の推進

リスクコミュニケーション及び協議とは、「リスクの運用管理について、情報の提供、共有又は取得、及びステークホルダー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[8]されて

[8] JIS Q 31000:2010

いる。このプロセスは、機能保証の観点からは、サービス維持の水準等として表現される重要インフラサービスに係る組織の目的設定並びにその目的に対するリスク及びその運用管理に関する組織の意思決定を行う上で必要である。また、到来しつつある連接融合情報社会においては、重要インフラ事業者等がステークホルダーとの間においてリスクに関する役割や責任の分担等に係る合意形成を行い、重要インフラサービスの提供に関して期待される責任を果たす上でも重要となる。

このことから、重要インフラ事業者等における内部ステークホルダー間の情報や意見の交換及び関係主体間による分野横断的な情報や意見の交換の充実に資することを目的に、重要インフラ防護に関連する者によるリスクコミュニケーション及び協議を推進する。具体的には、次の施策を講じる。

①経営層、情報セキュリティ部門、情報システムや制御システムを所管する部門、ユーザ部門その他内部ステークホルダー相互間のリスクコミュニケーション及び協議を推進する。

②セプターカウンシル及び分野横断的演習を利活用し、各関係主体と協力しつつ、情報や意見の交換の充実を推進する。また、これにより、新たなリスク源・リスクに関する調査・分析に必要となる情報の収集を図る。

4.2.5 モニタリング及びレビューの推進

リスクアセスメントの結果として認識された状態は、経時的に変化すると予想される。リスクアセスメントを変更又は無効なものとするおそれのある状況及びその他の要因を特定し、リスクの変動に適切に対処するためには、リスクアセスメント結果を継続的に確認し、必要に応じて適宜にリスクアセスメント結果の見直しを実施するなど、リスクを適切に管理し、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要である。

このため、重要インフラ事業者等におけるリスクマネジメント及び対処態勢に係るモニタリング及びレビューの推進を図る。具体的には、重要インフラ事業者等が主体的に行う内部監査等の取組において、内閣官房からの機能保証の考え方を踏まえた監査観点の提供等により、モニタリング及びレビューの強化を推進する。

4.3 本施策と他施策による結果の相互反映プロセスの確立

本行動計画の他施策に資することを目的に、本施策における調査・分析結果を参考資料として他施策に活用する。

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

5.　防護基盤の強化

重要インフラを取り巻く社会環境・技術環境が刻々と変化する中、国全体の情報セキュリティに関する水準を向上させるためには、国民一人一人が情報セキュリティに対する意識を高めていくとともに、重要インフラ事業者等の経営層に対して働きかけ、共通認識を醸成することが重要である。

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

このため、本行動計画期間においては、内閣官房は、第３次行動計画に引き続き、重要インフラ分野内外に関わらず情報共有等を行う範囲の見直しについて継続的に取り組むとともに、他の関係主体と協力しつつ広報広聴活動、国際連携及び経営層への働きかけを行うことに加え、関係主体が適時に適切な関連規程類を参照し得るよう、重要インフラ防護に係る関連規程類についての手引書等を整備する。

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

5.1 重要インフラに係る防護範囲の見直し

(1) 「面としての防護」に向けた取組

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

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

(2) 国の安全等の確保の観点からの取組

昨今のサイバー攻撃の深刻化及び社会環境・技術環境の変化に伴い、国民生活及び社会経済活動の防護等に関し、安全保障上の観点を踏まえる必要性が高まっており、防護対象として情報共有等を推進すべき分野についての取組強化や、新たな重要インフラとして位置付けるべきサービスを適切に防護するため、重要インフラ分野の見直し等の継続的な取組を行う必要がある。

これまで、関係主体を含めたヒアリング等を行い現状把握等に努めてきたところであるが、今後も、社会環境の変化等を踏まえつつ、重要インフラ分野以外に対する取組を含め、防護範囲見直しに継続的に取

り組む[9]。これに当たっては、安全保障上重要な企業等[10]や我が国の国際競争力強化にとっても重要な先端技術等の知的財産や営業秘密を保有する企業等の情報セキュリティ対策の強化が必要となる関係主体を含めることとする。

なお、(1)、(2)に関し、新規の分野・事業者等については、当該分野・事業者等の状況に合わせた段階的な取組の充実を図っていくこととする。

5.2 広報広聴活動の推進

重要インフラサービス障害の影響を可能な限り極小化するためには、重要インフラ事業者等による情報セキュリティ対策の水準の向上のみならず、その他の企業や国民を含め社会全体が状況を踏まえて冷静に対応できることも重要である。

このため、各関係主体は、国民による冷静な対応に資することを目的に、行動計画の枠組みや取組について国民への積極的な発信を行う。

内閣官房は、Ｗｅｂサイト、ニュースレター及び講演等を通じ、本行動計画の取組を広く認識・理解し得るよう引き続き努めるとともに、より効果的な広報チャネルについても検討を進める。

また、情報セキュリティは、日々の環境変化や技術革新等により新たな脅威や対応が発生するため、新たな技術や新たに検討されている制度に関して早い段階で情報を収集し、変化に対応していく必要がある。

内閣官房は、往訪調査や勉強会・セミナー等を通じた各分野の状況把握や技術動向等の情報収集に努め、随時施策に反映させる。

さらには、機能保証の考え方の浸透や、「面としての防護」の実現に向けて、経営層や重要インフラ事業者等に関連する他の事業者等の理解・協力が得られるように努める。

5.3 国際連携の推進

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

このため、内閣官房は、重要インフラ所管省庁及び情報セキュリティ関係機関と連携して、二国間・地域間・多国間の枠組みを積極的に活用して我が国の取組を発信することなどにより、継続的に国際連携の強化を図る。

具体的には、我が国の分野横断的演習の取組紹介、欧米・ASEAN との協議や Meridian 等の場における講演等を通じて、我が国の特徴的な施策を積極的に発信することにより、海外の脅威情報やインシデント対

9 既存の重要インフラ以外の「空港」については、現在、関係企業による自主的な取組として情報共有等に係る枠組み（空港 SIG：Special Interest Group）が構築されるに至っている。
10 核物質防護等の措置が要求される企業を含む。

応事例、ベストプラクティスの共有等の基盤となる協力関係を強化するとともに、国際的な重要インフラ防護能力の向上にも寄与する。これによって海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。

また、重要インフラ事業者等においても、情報セキュリティ対策に係る取組の海外同業他社への展開や国際会議への参加等を通じた海外の動向把握、海外ＩＳＡＣ等との情報共有等により、多角的・多面的な国際連携に取り組むことが期待される。

5.4 セキュリティ・バイ・デザインの推進

内閣官房は、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの考え方を関係主体が共通の価値として認識することを促していく。また、各重要インフラ事業者等においては、セキュリティ・バイ・デザインの考え方にのっとり、制御系機器・システム等の調達及び運用に際して、国際標準に準拠した第三者認証制度の認証を受けた製品の活用を促進する。

5.5 経営層への働きかけ

「サイバーセキュリティ経営ガイドライン」や「企業経営のためのサイバーセキュリティの考え方」等に見られるように、情報セキュリティ対策が経営課題として重要な位置付けを持っていることが強調されるようになってきている。こうした中、重要インフラ事業者等の経営層については、その在り方として、以下の項目の必要性を認識し、実践することが期待される。

①情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。

②自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。

③情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。

④上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。

以上を踏まえ、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように働きかけを行うとともに、そのような働きかけを通して知見を得て、重要インフラ防護施策を実態に即した実効的なものとする。

5.6 人材育成等の推進

各関係主体において、「サイバーセキュリティ人材育成総合強化方針」（平成 28 年３月サイバーセキュリティ戦略本部決定）に基づく取組を推進する。また、「サイバーセキュリティ人材育成プログラム」（平成 29 年　月サイバーセキュリティ戦略本部決定）に基づく具体的な取組を推進する。具体的には、人材育成に関する次の施策を講じる。

① 重要インフラ事業者等において、経営層の意識を高め、理解を促進する。その上で、自組織の経営方針に基づく情報セキュリティ対策を提示するとともに、組織内の情報セキュリティに関係する部署間の総合調整や実務者層を指揮することができる橋渡し人材の育成を進める。

②ＩＴの管理部門に限らず、ＯＴの管理部門や法務部門等の間接部門においても情報セキュリティ対策が要求されるようになっている昨今の状況を踏まえ、様々な役割や能力を持つ人材が組織横断的に連携し、情報セキュリティ対策に当たることを可能とする体制の構築を推進する。

③ 産学官が互いに連携し、必要なセキュリティ人材像の定義、情報セキュリティに係る訓練・演習、資格取得等の具体的な人材育成策を推進する。

5.7 マイナンバーに関するセキュリティ確保

政府機関は、地方公共団体等、マイナンバーを利用する重要インフラ事業者等の情報セキュリティを確保するため、必要な支援の実施や対策の検討を行い、マイナンバーを利用する重要インフラ事業者等は、情報セキュリティを確保するために必要な取組を行う。

5.8 規格・標準及び参照すべき規程類の整備

重要インフラの情報セキュリティ対策の有効性の確保において、関係主体がその検討を行う上で、関連文書や関連規格を必要なときに参照できるようにすることなどは重要である。また、オリパラ大会も見据え、リスクアセスメント・ガイドライン等を作成する必要がある。この規程類の整備等についての内閣官房の取組は、以下のとおりである。

(1) 重要インフラ防護に係る関連規程集の発行

内閣官房は、重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照するサイバーセキュリティ戦略、本行動計画等の各関連文書を合本し、「重要インフラ防護に係る規程集」として発行する。

(2) 重要インフラ防護に係る関連規格の体系的な可視化

内閣官房は、重要インフラ防護に係る関連規格について、適切な版を必要なときに参照できるようにするため、他の関係主体との協力の下、国内外で策定される関連規格について調査を行った上で整理し、そ

の結果を明示する。

Ⅳ. 関係主体において取り組むべき事項

1. 内閣官房の施策

(1)「安全基準等の整備及び浸透」に関する施策

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

② 必要に応じて社会動向の変化及び新たに得た知見に係る検討を実施し、その結果を公表。

③ 上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。

④ 重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。加えて、所管省庁とともに、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等の保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を継続的に進める。

⑤ 重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、安全基準等の浸透状況等の調査を実施し、結果を公表。

⑥ 安全基準等の浸透状況等の調査結果を、本行動計画の各施策の改善に活用。

(2)「情報共有体制の強化」に関する施策

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

② 重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供。

③ 国内外のインシデントに係る情報収集や分析、インシデント対応の支援等にあたっている情報セキュリティ関係機関との協力。

④ サイバーセキュリティ基本法に規定された勧告等の仕組みを適切に運用。

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

⑥ 重要インフラ所管省庁の協力を得つつ、各セプターの機能・活動状況等を把握するための定期的な調査・ヒアリング等の実施、先導的なセプター活動の紹介。

⑦ 情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。

⑧ セプターカウンシルに参加するセプターと連携し、セプターカウンシルの運営及び活動に対する支援の実施。

⑨ 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。

⑩ 必要に応じてサイバー空間関連事業者との連携を個別に構築し、重要インフラサービス障害発生時に適時適切な情報提供を実施。

⑪ 新たに情報共有範囲の対象となる重要インフラ分野内外の事業者に対する適時適切な情報提供の実施。

(3)「障害対応体制の強化」に関する施策

① 他省庁の重要インフラサービス障害対応の演習・訓練の情報を把握し、連携の在り方を検討。

② 重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプターの情報疎通機

能の確認（セプター訓練）等の機会を提供。

③ 分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。

④ 分野横断的演習の改善策検討。

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

⑥ 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供（仮想演習環境の構築等）。

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。

⑧ 職務・役職横断的な全社的に行う演習シナリオの実施による人材育成の推進。

(4)「リスクマネジメント及び対処態勢の整備」に関する施策

① オリパラ大会に係るリスクアセスメントに関する次の事項

ア. 当該リスクアセスメントの実施主体への「機能保証に向けたリスクアセスメント・ガイドライン」の提供。

イ. リスクアセスメントに関する説明会や講習会の主催又は共催。

② 重要インフラ事業者等における平時のリスクアセスメントへの利活用のための「機能保証に向けたリスクアセスメント・ガイドライン」の一般化及び「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」の必要に応じた改善。

③ 本施策における調査・分析の結果を重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に反映する参考資料として提供。

④ 本施策における調査・分析の結果を本行動計画の他施策に反映する参考資料として利活用。

⑤ 重要インフラ事業者等が取り組む内部ステークホルダー相互間のリスクコミュニケーション及び協議の推進への必要に応じた支援。

⑥ セプターカウンシル及び分野横断的演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議の支援。

⑦ 機能保証の考え方を踏まえて事業継続計画及びコンティンジェンシープランに盛り込まれるべき要点やこれらの実行性の検証に係る観点等を整理し、重要インフラ事業者等に提示するなどの支援。

⑧ オリパラ大会も見据えた各関係主体におけるインシデント情報の共有等を担う中核的な組織体制の構築。

⑨ リスクマネジメント及び対処態勢における監査の観点の整理及び重要インフラ事業者等への提供。

(5)「防護基盤の強化」に関する施策

① 機能保証のための「面としての防護」を念頭に、サプライチェーンを含めた防護範囲見直しの取組を継続するとともに、関係府省庁（重要インフラ所管省庁に限らない）の取組に対する協力・提案を継続。

② Ｗｅｂサイト、ニュースレター及び講演会を通じた広報を実施。

③ 往訪調査や勉強会・セミナー等を通じた広聴を実施。

④ 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

⑤ 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

⑥ 重要インフラ所管省庁と連携し、重要インフラ事業者等の経営層に対し働きかけを行うとともに、知見を得て、本行動計画の各施策の改善に活用。

⑦ 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行。

⑧ 関連規格を整理、可視化。

⑨ 重要インフラ事業者等に対する第三者認証制度の認証を受けた製品活用の働きかけ。

2. 重要インフラ所管省庁の施策

(1)「安全基準等の整備及び浸透」に関する施策

① 指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。

② 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。さらに、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等の保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を内閣官房とともに継続的に進める。

③ 重要インフラ分野ごとの安全基準等の分析・検証を支援。

④ 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透に向けた取組を実施。

⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。

⑥ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。

(2) 「情報共有体制の強化」に関する施策

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

② 重要インフラ事業者等との緊密な情報共有体制の維持と必要に応じた見直し。

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

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

⑤ セプターの機能充実への支援。

⑥ セプターカウンシルへの支援。

⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。

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

(3) 「障害対応体制の強化」に関する施策

① 内閣官房が情報疎通機能の確認（セプター訓練）等の機会を提供する場合の協力。

② 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。

③ 分野横断的演習への参加。

④ セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。

⑤ 分野横断的演習の改善策検討への協力。

⑥ 必要に応じて、分野横断的演習成果を施策へ活用。

⑦ 分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の

連携への協力。

(4) 「リスクマネジメント及び対処態勢の整備」に関する施策

① オリパラ大会に係るリスクアセスメントの実施に際し、内閣官房、重要インフラ事業者等その他関係主体が実施する取組への協力。

② 内閣官房により一般化された「機能保証に向けたリスクアセスメント・ガイドライン」及び改善された「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」の重要インフラ事業者等への展開その他リスクアセスメントの浸透に資する内閣官房への必要な協力。

③ 本施策における調査・分析に関し、当該調査・分析の対象に関する情報及び当該調査・分析に必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査・分析が本施策における調査分析と関連する場合には、必要に応じて内閣官房と連携。

④ 本施策における調査・分析の施策への活用。

⑤ 重要インフラ事業者等のリスクコミュニケーション及び協議の支援。

⑥ 重要インフラ事業者等が実施する対処態勢の整備並びにモニタリング及びレビューの必要に応じた支援。

(5) 「防護基盤の強化」に関する施策

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

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

③ 内閣官房と連携し、重要インフラ事業者等の経営層に対し働きかけを行う。

④ 内閣官房と連携し、関連規格を整理、可視化。

⑤ 機能保証のための「面としての防護」を確保するための取組を継続。

⑥ 情報セキュリティに係る演習や教育等により、情報セキュリティ人材の育成を支援。

⑦ 重要インフラ事業者等に対する第三者認証制度の認証を受けた製品活用の働きかけ。

3. 情報セキュリティ関係省庁の施策

(1) 「情報共有体制の強化」に関する施策

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

② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。

③ セプターカウンシル等からの要望があった場合、意見交換等を実施。

4. 事案対処省庁及び防災関係府省庁の施策

(1) 「情報共有体制の強化」に関する施策

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

② 被災情報、テロ関連情報等の収集。

③ 内閣官房に対して、必要に応じて情報連絡の実施。

④ セプターカウンシル等からの要望があった場合、意見交換等を実施。

(2) 「障害対応体制の強化」に関する施策

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

② 分野横断的演習の改善策検討への協力。
③ 必要に応じて、分野横断的演習と事案対処省庁及び防災関係府省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。
④ 重要インフラ事業者等からの要望があった場合、重要インフラサービス障害対応能力を高めるための支援策を実施。

5. 重要インフラ事業者等の自主的な対策として期待する事項

(1)「安全基準等の整備及び浸透」に関する施策

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の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及び重要インフラサービス障害対応から課題を抽出し、リスク評価を経た安全基準等の継続的改善。
⑤ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。

(2) 「情報共有体制の強化」に関する対策

① セプターカウンシル、セプター、重要インフラ所管省庁及び内閣官房と連携し、平時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。
② システムの不具合等に関する情報連絡を実施。
③ 攻撃手法及び復旧手法に関する情報等の収集。
④ 情報セキュリティ関係機関との合意に基づく補完的な情報共有。
⑤ セプターカウンシルにおける活動の実施。
⑥ ＩＴ・ＯＴを含む事案の深刻度のレベル分け。

(3)「障害対応体制の強化」に関する対策

① 内閣官房が提供する情報疎通機能の確認（セプター訓練）等を活用するなどして、自らの情報共有体制を強化。
② 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。
③ 分野横断的演習への参加。
④ 分野横断的演習の改善策検討への協力。
⑤ 必要に応じて、自らの重要インフラサービス障害発生時の早期復旧手順及び IT-BCP 等への取組に対し、分野横断的演習成果を活用。

(4) 「リスクマネジメント及び対処態勢の整備」に関する対策

① オリパラ大会に係るリスクアセスメントの実施主体である場合には、当該リスクアセスメントの実施及びその結果を踏まえたリスク対応の実施。また、これらの実施に際し、内閣官房その他の関係主体との情報共有、意見交換等の必要に応じた連携。

② 機能保証の考え方に立脚したリスクアセスメントの推進及び強化。また、これに必要な資源の配分及び自組織における体制の整備。

③ 本施策における調査・分析の結果として提供される参考情報の自組織のリスクアセスメントへの活用。

④ 重要インフラサービスの提供に関するリスクの運用管理に直接的又は間接的に関係する関係主体間でのリスクコミュニケーション及び協議の推進及び強化に資する次の取組の実施。

ア．経営層、情報セキュリティ部門、情報システムや制御システムを所管する部門、ユーザ部門その他内部ステークホルダー相互間のリスクコミュニケーション及び協議の充実。また、これに必要な資源の配分及び自組織における体制の整備。

イ．セプターカウンシル、分野横断的演習その他の情報共有の機会の利活用による関係主体とのリスクコミュニケーション及び協議の充実。

⑤ 自らが単独で分析することが困難で、調査・分析する価値のある環境変化やリスク源を本施策における調査・分析の取組対象として提案。

⑥ 本施策における調査・分析の議論・検討に参画。

⑦ 対処態勢の整備に係る次の取組の実施。

ア．機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの整備並びに当該計画を実行するための組織体制の構築並びにこれらの実行性の検証

イ．自らがオリパラ大会に係るリスクアセスメントの実施主体である場合には、インシデント情報の共有等を担う中核的な組織体制（オリンピック・パラリンピックＣＳＩＲＴ（仮））に係る関係主体との協力

⑧ 内閣官房から提供された監査観点等に基づく内部監査（自主的に外部機関に委託して実施する監査を含む。）等の実施等のモニタリング及びレビューの強化の推進。

(5) 「防護基盤の強化」に関する対策

① 情報セキュリティ対策に係る取組の海外同業他社への展開や海外の動向把握等により、多角的・多面的な国際連携を促進。

② 「重要インフラ事業者等の経営層の在り方」に示す各項目の必要性を認識し、実践。

③ 内閣官房と連携し、関連規格を整理、可視化。

④ 制御系機器・システムの第三者認証制度の認証を受けた製品の活用を検討。

⑤ 情報セキュリティ対策に関する各取組に必要な予算・体制・人材等の経営資源の計画的な確保及び配分

6. セプター及びセプター事務局の自主的な対策として期待する事項

(1) 「情報共有体制の強化」に関する対策

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

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

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

④ 情報セキュリティ関係機関との合意に基づく補完的な情報共有の実施。

⑤ セプターの機能強化・充実。

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

⑦ セプターカウンシルへの参加。

(2)「障害対応体制の強化」に関する対策

① 情報疎通機能の定期的な確認。

② 重要インフラ事業者等の分野横断的演習への参加及び成果展開を支援。

③ 分野横断的演習への参加。

(3)「リスクマネジメント及び対処態勢の整備」に関する対策

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

(4)「防護基盤の強化」に関する施策

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

7. セプターカウンシルの自主的な対策として期待する事項

(1)「情報共有体制の強化」に関する対策

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

② 共有対象とする情報及びその共有方法の整理の実施。

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

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

(2)「障害対応体制の強化」に関する対策

① 必要に応じて分野横断的演習への参加。

8. 情報セキュリティ関係機関の自主的な取組として期待する事項

(1)「情報共有体制の強化」に関する対策

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

② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。

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

④ 内閣官房が実施する分析機能の強化の検討に対しての協力。

⑤ セプターカウンシルから要望があった場合、意見交換等を実施。

(2)「障害対応体制の強化」に関する対策

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

(3) 「リスクマネジメント及び対処態勢の整備」に関する対策

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

(4) 「防護基盤の強化」に関する対策

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

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

9. サイバー空間関連事業者の自主的な対策として期待する事項

(1) 「情報共有体制の強化」に関する対策

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

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

Ⅴ．評価・検証

本行動計画の評価・検証は、次の二つの視点で行う。

○「成果（アウトカム）を測る視点」からの評価

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

○「結果（アウトプット）を測る視点」からの検証

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

1.　本行動計画の評価

1.1 評価運営

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

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

行動計画の評価運営は、行動計画の性質上、毎年の変化を追っても直ちに改善策を検討することが困難であることから、３年に１度の実施を原則としているが、本行動計画の評価については、２０２０年にオリパラ大会を控えていることを勘案し、時宜を得て実施する。また、社会動向の大きな変化等、本行動計画が想定しえなかった事象が発生した場合は、３年に１度の実施は、その限りとしない。

1.2 理想とする将来像

1.2.1 将来像の概要

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、以下のような状態である。

○各関係主体の自覚に基づく自主的な取組が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、重要インフラサービス障害の予防的対策を強化するためのコミュニケーションが日常的に行われるとともに、重要インフラサービス障害が発生した場合には、その経験を確実に将来の対策に活かすための継続的な改善がなされている。

○関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている。また、多様な主体間でのコミュニケーションが充実し、重要インフラサービス障害の発生時に冷静に対処できるようになっている。

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

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

1.2.2 各関係主体の具体化した将来像

(1) 関係主体共通

関係主体共通の具体化した将来像は、以下のような状態である。

○自らの置かれている状況が正しく認識され、かつ、自らの活動目標が主体的に定められている。

○各々必要な取組が進められており、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が行われている。また、他の関係主体の活動状況が把握されており、相互に自主的な協力をすることができる。

○重要インフラサービス障害発生時の対応において、重要インフラサービス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が理解されている。

○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、統制の取れた対応ができる。

(2) 重要インフラ事業者等

重要インフラ事業者等の具体化した将来像は、以下のような状態である。

○「情報セキュリティガバナンス」に関する次の事項が重要インフラ事業者等の間で十分に浸透している。

－情報セキュリティ対策が単に情報システムの構築・運用の観点だけでなく、企業経営の観点からも検討されていること。

－システムの構築・運用及び企業経営の各責任者が適切に相互関与する体制が整備されていること。

－守るべき重要インフラサービス及びサービス維持レベルを踏まえ、自らがなすべき必要な対策が理解されていること。

－平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示などが取り組まれていること。

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

－事業における重要インフラサービス障害の発生について、これを隠すべきものではなく、重要インフラ事業者等内の情報セキュリティ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が醸成されていること。

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

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

－各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス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。

－重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、重要インフラサービス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を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一つとなっていること。

○「情報共有」に関する次の事項が十分に浸透している。

－重要インフラサービス障害の発生状況等に関する情報の把握ができており、必要に応じて当該情報が各分野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され、公式又は非公式の連携が行われていること。

(3) 内閣官房

内閣官房の具体化した将来像は、以下のような状態である。

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

○特に、重大なリスク源や重要インフラサービス障害に係るリスクについての認識が得られるようになっている。また、その対処を重要インフラ事業者等だけで行うことが困難な場合は、解決策の検討及びその実現に向けた有機的な連携・調整が速やかに実施できている。

1.3 本行動計画の目標

理想とする将来像の実現に向け、本行動計画期間中に達成が期待される目標は、以下のようなものである。

(1) 「安全基準等の整備及び浸透」における目標

「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、安全基準等によって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着実に実践するという行動様式が確立されることである。

(2) 「情報共有体制の強化」における目標

「情報共有体制の強化」に期待される成果は、最新の情報共有体制、情報連絡・情報提供に基づく情報共有及び各セプターの自主的な活動の充実強化を通じて、重要インフラ事業者等が必要な情報を享受し活用できていることである。

(3) 「障害対応体制の強化」における目標

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

(4) 「リスクマネジメント及び対処態勢の整備」における目標

「リスクマネジメント及び対処態勢の整備」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・強化により、重要インフラ事業者等において、機能保証の考え方を踏まえたリスクアセスメントの浸透、新たなリスク源・リスクを勘案したリスクアセスメントの実施及び対処態勢の整備が図られた上、これらのプロセスを含むリスクマネジメントが継続的かつ有効に機能していることである。

(5) 「防護基盤の強化」における目標

「防護基盤の強化」における各取組において期待される成果は以下のとおり。

○「防護範囲の見直し」については、環境変化及び重要インフラ分野内外の相互依存関係等を踏まえた防護範囲見直しの取組が継続して行われ、それぞれの事業者の状況に合わせた取組が進められていること。

○「広報広聴活動」については、行動計画の枠組みについて国民や関係主体以外に理解を広めるとともに、技術動向に合わせて適切に対応されていること。

○「国際連携」については、二国間・地域間・多国間の枠組み等を通じた各国との情報交換の機会や支援・啓発が充実していること。

○「規格・標準及び参照すべき規程類の整備」については、整備した規程類が重要インフラ事業者等に浸透し利活用されていること。

1.4 補完調査

本行動計画の評価を行う際には、各施策群の個別の成果からは把握しきれない状況についても適切に把握し、総合的な評価を行うことが重要である。このため、評価の実施に際しての補完的な情報を収集するための調査（以下「補完調査」という。）を原則として各年度において実施する。

補完調査は、重要インフラ事業者等による情報セキュリティ対策の課題やグッドプラクティス等の本行動計画に基づく取組の妥当性の確認に資する材料を得ることを実施目的とし、重要インフラサービス障害等の実例をサンプリングして追跡することにより実施する。

なお、調査結果については、可能な範囲で公表する。

2.　本行動計画の検証

2.1　検証運営

「結果（アウトプット）を測る視点」からの検証（各年度における進捗状況の確認）は、「Ⅲ．計画期間内に取り組む情報セキュリティ対策」に示した施策群ごと（以下「本行動計画の各施策」という。）に、その進捗状況の確認として行う。この際、本行動計画の施策がいずれも複数の関係主体による多層構造をなしており、取組結果を表す指標についても多様なものが考えられるが、大別して「重要インフラ事業者等による対策」の検証に用いる指標及び「政府機関等による施策」の検証に用いる指標をあらかじめ設定した上、本行動計画の各施策に対して分析的に行うこととする。本行動計画の各施策の指標については、その数値自体の多寡や増減にとらわれるのではなく、その数値の意味するところを適切に解釈することが重要である。

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

2.2 「重要インフラ事業者等による対策」の検証

重要インフラ事業者等は、重要インフラサービスの安全かつ持続的な提供に一義的な責任を負うものとして、日々情報セキュリティ対策に取り組んでいる。この取組を継続し、かつ、着実な改善を期すために、また重要インフラ事業者等の取組に対する政府の支援策をより効果的なものへと改善させていくためには、情報セキュリティ対策の結果を客観的に検証することが重要である。

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

なお、「重要インフラ事業者等による対策」の評価については、個別の重要インフラ事業者等の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

重要インフラサービス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ことから、重要インフラ事業者等による自己評価によるものとし、各々の重要インフラ事業者等が自ら改善に取り組むことが適当である。また、重要インフラ事業者等は、重要インフラサービス障害への対策の状況を検証するとともに、実際に重要インフラサービス障害を被った場合には、その重要インフラサービス障害への対処の内容を自己評価し、可能であれば、これらの実施状況を明らかにすることが望ましい。

2.3 「政府機関等による施策」の検証

本行動計画の各施策は、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。

施策の結果検証は、重要インフラ事業者等による情報セキュリティ対策に対する本行動計画の各施策による寄与の状況を検証することとする。

なお、具体的な指標については、前記「本行動計画の目標」を踏まえ、以下のとおり設定するものとする。

(1) 「安全基準等の整備及び浸透」に係る指標

○安全基準等の浸透状況等の調査により把握したベースラインとなる情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合

○安全基準等の浸透状況等の調査により把握した先導的な情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合

(2) 「情報共有体制の強化」に係る指標

○情報連絡・情報提供の件数

○各セプターのセプター構成員数

(3) 「障害対応体制の強化」に係る指標

○分野横断的演習の参加事業者数

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

○分野横断的演習を含め組織内外で実施する演習・訓練への参加状況

(4) 「リスクマネジメント及び対処態勢の整備」に係る指標

○「機能保証に向けたリスクアセスメント・ガイドライン」の配付数（Ｗｅｂサイトに掲載する場合には、掲載ページの閲覧数）及びリスクアセスメントに関する説明会や講習会の参加者数

○内閣官房が実施した環境変化調査や相互依存性解析の実施件数

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

○浸透状況調査結果が示す内閣官房の提示する要点を踏まえた対処態勢整備及び監査の実施件数

(5) 「防護基盤の強化」に係る指標

○Ｗｅｂサイト、ニュースレター及び講演会等による情報の発信回数

○往訪調査や勉強会・セミナー等による情報収集の回数

○二国間・地域間・多国間による意見交換等の回数

○重要インフラ防護に資する手引書等の整備状況

○制御系機器・システムの第三者認証制度の拡充状況

Ⅵ. 本行動計画の見直し

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

行動計画の見直しについては、行動計画の評価と併せて３年に１度の実施を原則としているが、本行動計画の見直しについては、２０２０年にオリパラ大会を控えていることを勘案し、大会終了後に実施する。また、社会動向の大きな変化等、本行動計画が想定しえなかった事象が発生した場合は、その限りとしない。

別添：情報連絡・情報提供について

1.　システムの不具合等に関する情報

重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システム[11]の不具合等に関する情報」という。）には、①重要インフラサービス障害の未然防止、②重要インフラサービス障害の拡大防止・迅速な復旧、③重要インフラサービス障害の原因等の分析・検証による再発防止の３つの側面が含まれ、政府機関等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間及び相互依存性のある重要インフラ分野間においてはこうした情報を共有する体制を強化することが必要である。

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

したがって、本行動計画における情報共有の範囲は、図に示すものとする。

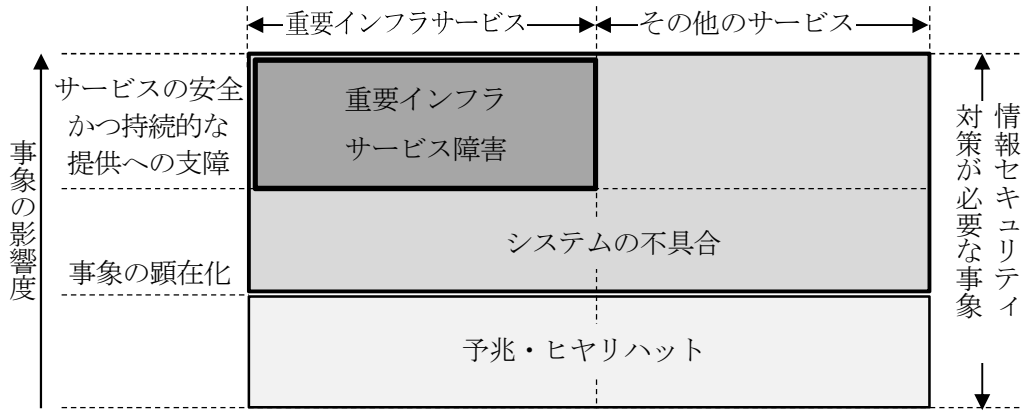


図　情報共有の対象範囲

11 ここでいうシステムには、いわゆる情報系システムに限らず、各重要インフラ分野のプラントやシステム監視等でも用いられる制御システムや、今後の急速な普及が見込まれるＩｏＴシステム等も含まれることに留意。

また、重要インフラサービス障害の深刻度や当該障害に関する情報の重要度に応じて影響範囲や対処行動等が異なってくることも踏まえ、関係主体間で認識の共有を図り、迅速な対応要否等の判断に資するため、下表のとおり、重要インフラサービス障害に係る深刻度の判断基準の例を設け、具体化に向けた検討を進める。

表　重要インフラサービス障害に係る深刻度判断基準（例）

深刻度	定　義
レベル５ （危機）	複数の重要インフラサービスに著しい影響を与えるおそれが切迫している事象
レベル４ （重大）	重要インフラサービスに著しい影響を与えるおそれが高い事象
レベル３ （高）	重要インフラサービスに一定の影響を与えるおそれが高い事象
レベル２ （中）	重要インフラサービスに影響を与えるおそれがある事象
レベル１ （低）	重要インフラサービスに影響を与えるおそれが小さい事象

関係主体が上記の深刻度判断基準を踏まえた情報共有・対応に取り組むことで、共有情報の位置付けや理解が深まり、効率的かつ有効な対応の一助になることが期待される。

2.　重要インフラ事業者等からの情報連絡

2.1 情報連絡を行う場合

システムの不具合等に関する情報[12]のうち、以下のいずれかのケースに該当する場合、重要インフラ事業者等は情報連絡を行うものとする。情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとし、全容が判明する前の断片的又は不確定なものであっても差し支えない。

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

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

2.2 情報連絡の仕組み

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

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

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

2.3 情報連絡された情報の取扱い

情報連絡された情報の取扱いについて、内閣官房及び連絡を受けた重要インフラ所管省庁は、法令等に定めがある場合又は連絡を行う重要インフラ事業者等の了承がある場合を除き開示しない。当該情報は、「行政機関の保有する情報の公開に関する法律（平成11年法律第42号）」第５条第２号ロに規定する情報と

[12]重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報を指す。

して取り扱う（不開示情報）。なお、当該情報が同号ただし書に規定する情報[13]に該当する場合には、公開されることがある。また、「3.1 情報提供を行う場合」に該当する場合はこの限りではない。

[13]人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報

3.　重要インフラ事業者等への情報提供

3.1 情報提供を行う場合

重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、情報セキュリティ関係機関、サイバー空間関連事業者及び重要インフラ事業者等から提供される幅広いシステムの不具合等に関する情報を集約、分析等した上で、以下のいずれかのケースに該当する場合、内閣官房は積極的に情報提供を行うものとする[14]。

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

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

③ そのほか重要インフラ事業者等の情報セキュリティ対策に有効と考えられる場合。

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

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

3.2 情報提供の仕組み

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

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

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

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

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

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

3.3 情報提供のための連携体制

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

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

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

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

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

別紙１　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野		対象となる重要インフラ事業者等(注１)	対象となる重要システム例
情報通信		・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融	銀行等 生命保険 損害保険 証券	・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		・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
鉄道		・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力		・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
ガス		・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス		・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		・医療機関 （ただし、小規模なものを除く。）	・診療録等の管理システム等（電子カルテシステム、遠隔画像診断システム等、医用電気機器等）
水道		・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流		・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学		・主要な石油化学事業者	・プラント制御システム
クレジット		・主要なクレジットカード会社　　等	・クレジットカード決済システム
石油		・主要な石油精製・元売事業者	・受発注システム ・生産管理システム ・生産出荷システム　　等

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

別紙２　重要インフラサービスの説明と重要インフラサービス障害の例

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

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

重要インフラ分野	重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
	・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
航空	・旅客、貨物の航空輸送サービス	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条）	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空運送事業者における情報セキュリティ確保に係る安全ガイドライン
	・予約、発券、搭乗・搭載手続	・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		
	・運航整備 ・飛行計画作成	・航空機の点検・整備 ・飛行計画の作成、航空局への提出		
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）	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告）　第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第５条
	・発券、入出場手続	・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	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条８項） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条14項）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第３条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと

重要インフラ分野	重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
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）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス事業法施行規則第112条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン
物流	・貨物自動車運送事業 ・船舶運航事業 ・港湾運送事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・他人の需要に応じ、港湾においてする船舶への貨物の積込又は船舶からの貨物の取卸の行為等を行う事業（港湾運送事業法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流分野における情報セキュリティ確保に係る安全ガイドライン
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期に渡る製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	・クレジットカード決済	・クレジットカード決済サービス（割賦販売法第２条第３項第１号及び第２号並びに第35条の16第２項）（注３）	・クレジットカード決済サービスの遅延・停止、カード情報の大規模漏えい	・クレジットCEPTOARにおける情報セキュリティガイドライン （※）今後、割賦販売法（後払分野）に基づく監督の基本方針において規定する予定
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油分野における情報セキュリティ確保に係る安全ガイドライン

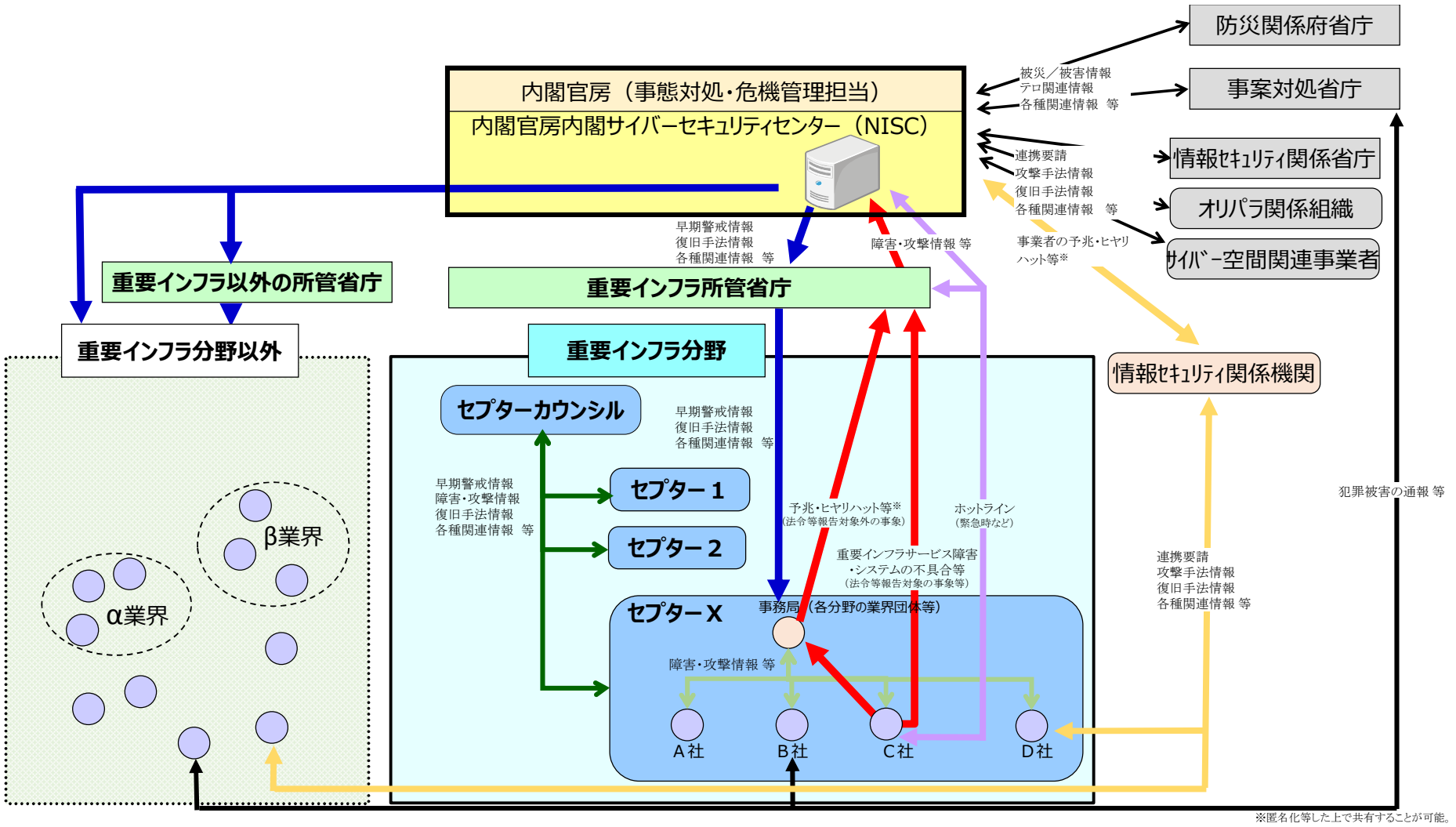
注１　ＩＴを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。
注３　改正割賦販売法（施行は、公布（2016年12月９日）から１年６か月以内の政令で定める日）においては、法第２条第３項第１号及び第２号、第35条の16第１項第２号及び第２項。

別紙３　情報連絡における事象と原因の類型

事象の類型		事象の例	説明
未発生の事象		予兆・ヒヤリハット	サイバー攻撃の予告等の予兆や、システム脆弱性等の発見、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等、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等、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やＷｅｂサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記につながる事象	マルウェア等の感染	マルウェア等によるシステム等への感染
		不正コード等の実行	システム脆弱性等をついた不正コード等の実行
		システム等への侵入	外部からのサイバー攻撃等によるシステム等への侵入
		その他	上記以外の事象

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

別紙４－１　情報共有体制


防災関係府省庁
事案対処省庁
情報セキュリティ関係省庁
オリパラ関係組織
サイバー空間関連事業者
内閣官房（事態対処・危機管理担当）
内閣官房内閣サイバーセキュリティセンター（NISC）
被災／被害情報
テロ関連情報
各種関連情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報 等
事業者の予兆・ヒヤリハット等※
重要インフラ以外の所管省庁
重要インフラ所管省庁
重要インフラ分野以外
重要インフラ分野
情報セキュリティ関係機関
セプターカウンシル
早期警戒情報
復旧手法情報
各種関連情報　等
早期警戒情報
障害・攻撃情報
復旧手法情報
各種関連情報　等
セプター１
セプター２
予兆・ヒヤリハット等※
（法令等報告対象外の事象）
ホットライン
（緊急時など）
重要インフラサービス障害
・システムの不具合等
（法令等報告対象の事象等）
犯罪被害の通報 等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報 等
β業界
α業界
セプターＸ
事務局（各分野の業界団体等）
障害・攻撃情報 等
Ａ社
Ｂ社
Ｃ社
Ｄ社
※匿名化等した上で共有することが可能。

別紙４－２　情報共有体制における各関係主体の役割

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

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

別紙５　定義・用語集

IT-BCP等	重要インフラサービスの提供に必要な情報システムに関する事業継続計画（関連マニュアル類を含む。）その他の事業継続計画。
安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称。ただし、指針は含まない。
関係主体	内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター、セプターカウンシル、情報セキュリティ関係機関及びサイバー空間関連事業者。
コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
サービス維持レベル	機能保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。
サイバー空間関連事業者	重要インフラサービスを提供するために必要な情報システムに関係する、設計・構築・運用・保守等を行うシステムベンダー、ウィルス対策ソフトウェア等の情報セキュリティ対策を提供するセキュリティベンダー及びハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
指針	安全基準等の策定・改定に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。本編はサイバーセキュリティ戦略本部決定による。対策編は対策項目のチェックリストとして具体例を記載したもの。
システムの不具合	重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。
重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。
重要インフラサービス	重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
重要インフラ事業者等	重要インフラ分野に属する事業を営む者等のうち「別紙１　対象となる重要インフラ事業者等と重要システム例」における「対象となる重要インフラ事業者等」に指定された事業者及び当該事業者等から構成される団体。
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省、国土交通省。
重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、具体的には、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者等ごとに定めるもの。
情報共有	システムの不具合等に関する情報（重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報）や情報セキュリティの確保に資する情報について、関係主体間で相互に提供し、共有すること。情報連絡及び情報提供の双方を含む。
情報システム	事務処理等を行うシステム、フィールド機器や監視・制御システム等の制御系のシステム等のＩＴを用いたシステム全般。

情報セキュリティ関係機関	警察庁サイバーフォースセンター、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人ICT-ISAC、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
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、原子力規制庁（※）及び防衛省。 ※原子力発電所の安全の観点からサイバーセキュリティに取り組む省庁
情報セキュリティ対策	重要インフラサービス障害が国民生活や社会経済活動に影響を与えないようにするための幅広い取組。
情報提供	情報セキュリティ対策に資するための情報を、内閣官房から重要インフラ事業者等へ提供すること等。
情報連絡	重要インフラ事業者等におけるシステムの不具合等に関する情報（重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報）を、重要インフラ事業者等から内閣官房に連絡すること等。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略称（CEPTOAR）。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
大規模重要インフラサービス障害	官邸対策室等が官邸危機管理センターに設置されるなどの政府として集中的な対応が必要となる規模の重要インフラサービス障害。
防災関係府省庁	災害対策基本法（昭和36年法律第223号）第２条第３号に基づく指定行政機関等の、災害時の情報収集に関係する府省庁。
予兆・ヒヤリハット	システムの不具合が生じておらず、又は生じなかったものの、システムの不具合につながるおそれがあり、又はそのおそれがあった事象。