資料５

重要インフラ行動計画改定への提言について

資料５－１　重要インフラ行動計画改定への提言（概要）

資料５－２　重要インフラ行動計画改定への提言

資料５－３　第４次行動計画期間（2017～2020）における年次報告

資料５－４　サイバーセキュリティ関係法令 Q&A ハンドブック（抜粋）

重要インフラ行動計画改定への提言（概要）

資料5－1

現状認識

重要インフラを取り巻く環境は、予断を許さない状況まで来ている

- **第４次行動計画策定以降の状況変化**
  - ✓ サイバーセキュリティを取り巻く環境変化
  - ✓ 新たなサイバーセキュリティ戦略の策定
  - ✓ 近年のサービス障害の原因は、自然災害、管理ミスが主流、多くは管理不十分によって発生

課題の明確化

管理を適切にすれば防げた類似障害が繰り返し発生していることを踏まえ経営層を含め組織的対策が必要

- **第４次行動計画「本行動計画の検証」に基づく評価としては、一定の成果あり**
- **上記評価から直接導出されない課題が存在**
  - ✓ 経営層を含めた組織統治の在り方の検討
  - ✓ サイバーセキュリティ基本法に規定された責務等が認識されていない懸念
  - ✓ 将来を見据えた環境変化、新たなリスクへの対応

改定への提言

第４次行動計画における有効な取組は継続しつつ、特に以下の2点に留意すべき

- **（提言１）障害対応体制の強化の在り方の抜本的な見直し**
  - ✓ 現在の「経営層への働きかけ」から、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載
  - ✓ サイバーセキュリティ基本法が公布・施行されたことを踏まえ、各関係主体の責務等を明確化
- **（提言２）将来の環境変化を先取りし、サプライチェーン等を含め包括的に対応**

資料５－２

重要インフラ行動計画改定への提言

令和３年(2021 年)10 月 25 日

サイバーセキュリティ戦略本部

重要インフラ専門調査会 政策部会

目次

検討の経過

「サイバーセキュリティ戦略本部　重要インフラ専門調査会政策部会」(主査:松本勉 横浜国立大学大学院環境情報研究院教授）は、別添１のとおり、「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」（平成 29 年(2017 年) ４月 18 日サイバーセキュリティ戦略本部決定)の改定に向け、重要インフラ防護における課題、今後の方向性等について調査検討を行うため、令和３年(2021 年) ５月に設置されたものである。同政策部会委員は別添２のとおりである。

この度、同政策部会は、別添３の論点について、３回の議論を経て、重要インフラ行動計画改定への提言を取りまとめた。

第１回(令和３年(2021 年) ６月 30 日開催）

議事：政策部会の運営について

次期重要インフラ行動計画の検討の進め方

第２回(令和３年(2021 年) ８月３日開催）

議事：次期行動計画の論点整理

第３回(令和３年(2021 年) ９月 17 日開催）

議事：次期行動計画の骨子案の検討

次期重要インフラ行動計画の提言案の検討

1. 現状認識

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かかる特別行動計画(平成 12 年(2000 年)12 月 15 日情報セキュリティ対策会議決定)」に始まり、サイバーセキュリティ基本法(平成 26 年法律第 104 号)の公布・施行以降、サイバーセキュリティ戦略を踏まえ、現在は、平成 29 年(2017 年)に策定された「重要インフラの情報セキュリティ対策に係る第４次行動計画」(以下「第４次行動計画」という。)となっている。第４次行動計画に基づき、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として掲げ、理想とする将来像を実現すべく取組を推進しているところである。

第４次行動計画以降、サイバーセキュリティを取り巻く環境は大きく変化してきた。特に、2020 年代を迎えた最初の１年に、世界はコロナ禍の影響による不連続な変化に直面し、結果として人々のデジタル技術の活用は加速した。さらに、2020 年代は、サイバー空間と実空間が高度に融合した Society5.0 の実現へと大きく前進する「Digital Decade」となり得ると考えられる。一方で、国家間での競争の顕在化を含む国際社会の変化の加速化・複雑化、情報通信技術の進歩や複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず変容かつ増大している。

こうした環境変化等を背景に、サイバーセキュリティ基本法に基づき、令和 3 年(2021 年)9 月 28 日、新たなサイバーセキュリティ戦略が閣議決定された。「(1)DX とサイバーセキュリティの同時推進」、「(2)公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」、「(3)安全保障の観点からの取組強化」をテーマに、「自由、公正かつ安全なサイバー空間」の確保に取り組むこととされた。特に重要インフラ防護との関係が深い(2)においては、「任務保証[1]」の深化や、「リスクマネジメント」の取組を強化することとされた。

重要インフラに着目すると、一部分野において、環境変化に起因するサービス障害が既に発生し始めている。重要インフラサービス障害のリスクは、サイバー攻撃だけではなく、自然災害、人的要因等の多岐にわたり、特に、適切な組織管理がなされれば防げたサービス障害が目立ち始めている。さらに、システム間の連鎖が進み、サービス障害による影響が大規模化する傾向にある。

こうした現状を踏まえ、新たな行動計画を策定することが必要である。

---

[1]あらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。

2. 課題の明確化

重要インフラ防護は、特別行動計画以降 21 年間の実績を有しており、これまで着実に進展してきた。第４次行動計画について、第４次行動計画「Ⅴ.評価・検証」に基づき全行動計画期間中の取組を検証したところ、一定の成果があったと評価される。このため、第４次行動計画の取組を引き続き実施することを基本としつつ重要インフラ防護を推進していくことが期待される。他方で、第４次行動計画の評価から直接的には導出されない次に掲げる課題が存在する。

①経営層を含めた組織統治の在り方の検討

「１．現状認識」のとおり昨今の重要インフラを取り巻くサイバーセキュリティの状況は予断を許さないところまで来ている。近年のサービス障害の原因は、自然災害、管理ミスが主流であり、多くは管理不十分によって発生している。管理を適切にすれば防げた類似障害が繰り返し発生していることを踏まえ、経営層を含め、組織的対策が必要と考えられる。

サイバーセキュリティ基本法における規定のとおり、重要インフラは国民生活及び社会活動の基盤であって、その機能が停止し又は低下した場合に、国民生活及び社会活動への影響が大きいことから、重要インフラ事業者等はサービス提供に関する責務を負っている。引き続き、重要インフラ事業者等が、自らの責務を理解し自主的に取り組んでいくことが期待される。しかしながら、第４次行動計画においては、サイバーセキュリティ基本法との関係が必ずしも明確でないため、サイバーセキュリティ基本法に規定された責務等が認識されていない懸念がある。なお、重要インフラサービスの性質及びリスクを踏まえ、業務継続性を担保するために、組織ごとに最適な改善を継続的に行っていくことが必要である。

②将来を見据えた環境変化、新たなリスクへの対応

「自由、公正かつ安全なサイバー空間」を確保していくためには、サイバー空間のみならず、その空間を取り巻く変化やリスクについて将来を見据え的確に認識した上で、不確実性に対応していくことが期待される。また、公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保のために、重要インフラに関与するあらゆる組織が、経済社会活動の相互依存関係の深化が進みリスクが高度化・複雑化していることを認識しつつ、サプライチェーン全体を俯瞰し責任ある行動をとることが期待される。こうした将来を見据えた環境変化、新たなリスクへの対応が必要と考えられる。

3. 改定への提言

第４次行動計画における有効な取組は継続しつつ、現状とあるべき姿のギャップを解消する必要がある。そのため、次の取組を中心に第４次行動計画を改定すべきである。

【提言１】

重要インフラ防護は、システム担当だけで対応できるものではなく、組織全体で対応する必要があるとの考え方のもとで、障害対応体制強化の在り方を抜本的に見直す。

DX 化の進展によりデジタル技術の活用が加速しつつあるなかで、組織全体を俯瞰した上でのリスクの明確化、対応策の検討等は、システム担当だけで対応できるものではなく、経営層でなければ判断できないものとなってきている。

そのため、現在の「経営層への働きかけ」という記載にとどまらず、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載すべきである。

その際、組織がサイバーセキュリティ対策の実施において参照すべき法制度について NISC によって整理された「サイバーセキュリティ関係法令 Q&A ハンドブック」を活用すべきである。

あわせて、平成 26 年度(2014 年度)にサイバーセキュリティ基本法が公布・施行されたことを踏まえ、改めて、重要インフラ防護の目的、各関係主体の責務、実施事項等について明確化すべきである。

【提言２】

将来の環境変化を先取りし、サプライチェーン等を含め包括的な対応に係る取組を促進する。

発生したサービス障害へ事後的に対応するだけではなく、将来に向けて変容していく重要インフラサービスと社会との関係を組織ごとに適切に把握した上で、サイバー攻撃、自然災害等のリスクを明確化し対応できるようにするための取組を促進すべきである。また、自組織だけにとどまらず、外部システム、海外拠点、サプライチェーン等を含む包括的な重要インフラ防護の取組を促進すべく、例えば、サプライチェーン等を担う事業者の位置付け等を明確化すべきである。

別添１

政策部会の設置について

令　和　３　年　５　月　３１日
重要インフラ専門調査会会長決定

１　重要インフラ防護に関する官民の行動計画に係る調査検討を行うため、重要インフラ専門調査会に政策部会を置く。

２　政策部会は、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月18日サイバーセキュリティ戦略本部決定）の改定に向け、重要インフラ防護における課題、今後の方向性等について調査検討を行う。

３　政策部会の委員は、重要インフラ専門調査会（以下「専門調査会」という。）の会長が専門調査会の委員の中から指名した者とする。

４　政策部会に主査をおく。主査は政策部会の委員の互選により決する。

５　主査は、必要があると認めるときは、政策部会の委員の以外の者に対し、政策部会の会議に出席して意見を述べることを求めることができる。

６　政策部会の庶務は、関係省庁の協力を得て、内閣官房において処理する。

７　政策部会は、その設置に係る調査検討が終了したときは、廃止されるものとする。

８　前各項に掲げるもののほか、政策部会の運営に関する事項その他必要な事項は、政策部会の主査が定める。

以上

別添２

〈令和３年10月25日現在〉

サイバーセキュリティ戦略本部　重要インフラ専門調査会
政策部会　委員名簿

伊勢　勝巳	東日本旅客鉄道株式会社　代表取締役副社長　技術イノベーション推進本部長
大杉　謙一	中央大学　大学院法務研究科　教授
大森　　聡	電気事業連合会　理事・事務局長
亀田　浩樹	株式会社三菱ＵＦＪ銀行　取締役常務執行役員　ＣＩＯ
志済　聡子	中外製薬株式会社　執行役員　デジタル・ＩＴ統括部門長
高橋　正和	株式会社Preferred Networks　執行役員　最高セキュリティ責任者
長島　公之	公益社団法人日本医師会　常任理事
奈良由美子	放送大学　教養学部　教授
塗師　敏男	横浜市　最高情報セキュリティ責任者補佐監
野口　和彦	横浜国立大学　客員教授
前川　　篤	株式会社シグマクシス　シニアフェロー、大阪大学　招聘教授、京都大学　特任教授
松本　　勉	横浜国立大学　大学院環境情報研究院　教授
横浜　信一	日本電信電話株式会社　執行役員　セキュリティ・アンド・トラスト室長　ＣＩＳＯ
渡辺　研司	名古屋工業大学　大学院工学研究科　教授

（五十音順・敬称略）

次期重要インフラ行動計画において特に明確にすべき事項

別添３

論点１ 重要インフラに対する脅威の変化とその対応

- 重要インフラを取り巻く脅威の変化(2000年から現在まで)
- 分野や事業者に共通する脅威の増大
- 組織固有の脅威の増大
- 重要システムを支える外部システムが重要システムに大規模な障害を引き起こすリスク(システミック・リスク)の顕在化
- サプライチェーンリスクマネジメントの必要性
- ハードウェアに関する脆弱性管理の必要性

論点２ 重要インフラと我が国の経済・社会との関係

- 重要インフラサービスの途絶が国民生活や経済社会活動に与える影響
- 重要インフラ事業者等の社会的責任

論点３ サイバーセキュリティ基本法と行動計画の関係

- 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の責務の明確化
- サイバーセキュリティ基本法(以下「基本法」という。)等の関係法令における行動計画の位置付けの明確化
- 基本法第５条事業者(地方公共団体)と基本法第６条事業者(重要社会基盤事業者)の特性に応じた役割の検討
- 重要インフラと基本法第７条事業者(サイバー関連事業者その他の事業者)との関係の明確化

論点４ 重要インフラ防護の範囲について

- 各分野における重要インフラ事業者の明確化
- 重要システムや防護対象の妥当性の検討(例：海外拠点等)
- 新たな重要インフラ分野の検討

論点５ デジタル庁設置に伴う対応

- 政府のデジタル改革への対応(例：地方公共団体との関係)

論点６ 関係主体の責任及び権限並びに実施事項の明確化

- 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の責任及び権限並びにそれらに基づく各関係主体の実施事項の明確化

論点７ 重要インフラ事業者等におけるコミットメントの確保

- 上層部(経営層)、CISO、戦略マネジメント層、担当の責務の明確化
- ビジネスとセキュリティのバランスの在り方

論点８ 重要インフラ事業者等が自らの組織に最適な防護対策

- 組織の特性を踏まえた経営層による組織のリスクの明確化
- CSIRT概念の明確化(経営におけるサイバーとCISOの役割の明確化)
- 既存の基準類をどのように当てはめればよいかを示すガイダンスの整備
  - ✓ サイバーセキュリティ確保のための組織に根差した枠組みモデル

論点９ 情報共有の強化

- 情報共有における共助の推進(自助ありきの共助、自助と共助(互助)を促進させるための公助)
- 重要インフラ事業者等の情報収集の活性化
- NISCの情報提供の在り方
- サイバーセキュリティ協議会との連携
- ISAC連携等による民主導での分野間連携の枠組みの整備

論点10 環境変化に対する柔軟な対応

- DX、コロナウイルス感染症の拡大等の様々な社会的・技術的な環境変化に応じたサイバーセキュリティの実現

論点11 東京2020大会のレガシーの活用

論点12 これまでの施策の検証・評価

資料５－３

第４次行動計画期間（2017～2020）における年次報告

令 和 ３ 年 １ ０ 月 ２ ５ 日

内閣サイバーセキュリティセンター

重 要 イ ン フ ラ グ ル ー プ

目次

2017 年度（サイバーセキュリティ政策に係る年次報告

（2017 年度） 抜粋）

別添４－２　重要インフラにおける取組の進捗状況

本章では、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「第４次行動計画」という。）に基づく取組について、2017年度の進捗状況の確認・検証結果を報告する。

１　重要インフラと第４次行動計画全体に関する取組

(1)　第４次行動計画の概要

第４次行動計画は、「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月）」、「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）」、「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（2009年２月、2012年４月改定）」及び「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（2014年５月、2015年５月改定）」に続く、我が国の重要インフラの情報セキュリティ対策として位置付けられたものであり、2017年４月にサイバーセキュリティ戦略本部で策定された。

第４次行動計画においては、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」及び「防護基盤の強化」の５つの施策が掲げられており、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである。施策ごとの取組の進捗状況については次節に示す。

(2)　取組の進捗状況

第４次行動計画は、第３次行動計画の基本的骨格（５つの施策）を維持しつつ、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、策定した。この策定に当たっては、「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ほか、重要インフラサービスに重点を置き、これまで「IT障害」としていた表記を「重要インフラサービス障害」とするなど、機能保証の考え方を踏まえたものとした。

2017年度は、第４次行動計画の初年度に当たり、同計画に従って機能保証の考え方に基づき、５つの施策それぞれについて取組を進めた。各施策の取組等の詳細は次節以降に示すが、過去最大規模での分野横断的演習の開催、「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５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」のとりまとめなど、各種取組の着実な成果を得た。なお、第４次行動計画における施策の枠外の取組として、2016年度に引き続き、重要インフラサービス障害等の事例についての現地調査である補完調査を実施した（参考：別添４－10）。

(3)　今後の取組

内閣官房と重要インフラ所管省庁等が一体となり、第４次行動計画に基づく取組を推進し、重要

インフラ事業者等に対して必要な支援を実施する。

２　第４次行動計画の各施策における取組

本節においては、第４次行動計画における施策ごとの取組の進捗状況について示す。なお、進捗状況の確認・検証は、第４次行動計画のV.1.3及びV.2.3に記載される各施策における目標及び具体的な指標を踏まえたものである。

(1)　安全基準等の整備及び浸透

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

安全基準等の整備及び浸透に関して、以下の取組を実施した。本取組の中で、重要インフラ事業者等における情報セキュリティ対策のPDCAサイクルとの整合性の確保、第４次行動計画の他施策との連携強化を図ることにより、情報セキュリティ対策の重要性を重要インフラ事業者等に訴求する仕組みを構築した。

〇安全基準等策定指針の改定等

2015年５月にサイバーセキュリティ戦略本部において決定され、497の対策項目を採録している「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）」（以下「指針」という。）に関し、往訪調査等の各種機会を通じて、重要インフラ事業者等へ説明を行い、周知を図った。

また、第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を定める際の考慮すべき事項を整理することなどを柱とする指針の改定作業を進め、「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５版）」をとりまとめた。

〇安全基準等の改善状況調査

各重要インフラ分野における安全基準等の継続的な改善状況について調査した（参考：別添４－３）。各分野において、安全基準等の改善の必要性について検討・確認し、４つの分野

において安全基準等の改善を行ったほか、11の分野において改善に向けた分析・検証に着手している。なお、各分野における制度的な枠組みについて現状の把握に努めた。

〇安全基準等の浸透状況等調査

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状況について調査を実施した（参考：別添４－４）。アンケート調査では、3,142件の回答が得られ、分析の結果、重要インフラ事業者等が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割合は約５割であった。また、重要インフラ事業者等が先導的な情報セキュリティ対策に取り組んでいる割合は約２割であった。良好な点として、ほぼ全ての事業者等で何らかの情報セキュリティ対策が取られていることから、セキュリティマインドが醸成されていること等が認められた。一方、CSIRTを設置している事業者がほとんど増えていないことから、CSIRTの設置等について呼びかけていく必要がある。

また、往訪調査を実施し、情報セキュリティに係る体制や規程等について意見交換を行うとともに、政府への意見・要望の収集を実施し、良好事例及び課題を整理した（参考：別添４－５）。

イ　今後の取組

2017年度の取組結果を活用しつつ、第４次行動計画に基づき、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を推進するとともに、重要インフラ事業者等への安全基準等の浸透を図る。具体的には、「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５版）」を策定した上で、同指針の普及・浸透を図るとともに、重要インフラ所管省庁と連携し、制度的枠組みを必要に応じて適切に改善する取組を継続する。また、浸透状況等調査については、アンケートの回答が事業者等に資する内容となるよう、取組の充実を図る。

(2)　情報共有体制の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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。
＜具体的な指標＞
・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

ア　取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。こうした取組により、官民の各関係主体が協力する情報共有体制の維持・強化を推進するとともに、重要インフラ事業者等による情報共有活動の活性化を図った。

○官民の情報共有体制

第４次行動計画に基づき、重要インフラ所管省庁と連携して具体的な取扱手順にのっとって情報共有体制を運営した。2017年度も前年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場などを通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。その結果、重要インフラ事業者等から内閣官房に対して388件の情報連絡が行われ、内閣官房からは54件の情報提供を行っている（参考：別添４－６）。

表１：重要インフラ事業者等との情報共有件数

年度	2014	2015	2016	2017
重要インフラ事業者等から内閣官房への情報連絡件数	124件	401件	856件	388件
内閣官房からの情報提供件数	38件	44件	80件	54件

重要インフラ事業者等におけるセキュリティ対策の取組（Web・メール等の無害化等）が進んだこと等により、情報連絡の件数は前年度に比べ減少しているものの、内閣官房からの情報提供件数も含め、情報共有件数は依然として多い状況である。なお、第４次行動計画において、セプター事務局を経由した新たな情報連絡ルートの導入が明記されたところであり、セプター事務局経由で匿名化された情報が出てくるなど、一定の効果が出ている。

大規模重要インフラサービス障害対応時の情報共有体制における各関係主体の役割については、平時から大規模重要インフラサービス障害対応時への体制切替の手順について確認を行うとともに、内閣官房（事態対処・危機管理担当）及び関係省庁と連携し、大規模サイバー攻撃事態等対処訓練に参加し、関係主体の役割の在り方及び当該手順の実効性に関する検証を実施した。

○セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、13分野で18セプターが設置されている（参考：別添４－７）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど重要インフラ防護の関係主体間における情報連携の結節点としても機能している。また、一部の分野については、ICT-ISAC、金融ISAC及び電力ISACの活発な活動など、自主的な分野内情報共有体制が確立されている。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、NISCはこの自主的取組を支援している。セプターカウンシルは、2017年４月の総会で決定した活動方針に基づき、2017年度に、運営委員会（４回）、相互理解WG（４回）、情報収集WG（４回）、総会準備WG（３回）、企画運営WG（４回）を開催し、セプター間の情報共有や事例紹介等、情報セキュリティ対策の強化に資する情報収集や知見の共有、並びに、更なる活動活性化に向けた要望の聞き取り、その実現に向けた情報分析機能の高度化に関する討議検討を行った。

また情報共有活動である「Webサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP)」の運営を通じて、情報共有活動の更なる充実を図っている。

〇深刻度評価基準の策定に向けた取組

専門調査会の下に設置した重要インフラサービス障害に係る対処態勢検討ワーキンググループにおいて議論を行い、取組の第一段階として、発生したサービス障害が国民社会に与えた影響全体の深刻さを『事後に』評価するための評価基準の試案を策定した。

イ　今後の取組

重要インフラを取り巻く急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、情報共有をしやすくする環境整備（連絡形態の多様化、情報共有システムの整備）や共有情報の理解浸透（深刻度評価基準の策定、OT・IoT等を含む共有範囲の明確化）等、引き続き官民を挙げた情報共有体制の強化に取り組んでいく。

また、政府機関を含め、他の機関から独立した会議体であるセプターカウンシルについては、従来にも増して各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。更なるセプターカウンシルの自律的な運営体制とそれによる情報共有の活性化を目指し、NISCは運営及び活動に対する支援を継続していく。

なお、深刻度評価基準については、パブリックコメントの結果も踏まえ、議論を継続する。

(3)　障害対応体制の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。こうした取組により、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等の検証や、そのために必要な関係主体間における情報共有の有効性の検証を可能にするとともに、技術面での対処能力の向上等を図った。

〇分野横断的演習

第４次行動計画に基づく具体的な取組の方向性として「セキュリティ意識とニーズに応える演習企画」、「セキュリティ対策のPDCAサイクルの強化に資する運営」、「情報共有体制の実効性向上」、「演習運営ノウハウや知識等の還元」に取り組んだ（参考：別添４－８)。

全13分野が演習に参加し、2014年度分野横断的演習と比較すると、参加者数は約7.6倍（348

名→2,647名）に増加した。また、事後の意見交換会も実施し、分野間での情報共有の機会をもうけた。

表２　分野横断的演習参加者数の推移

年度	2014	2015	2016	2017
参加者数	348名	1,168名	2,084名	2,647名

2017年度において、事業継続計画（BCP）を関係部署と協議し的確に発動できている事業者は、2016年度から大きな変化はなく、いずれも70%以上である。また、経営層の参加率については、事前の説明会において、その重要性に言及したこと等から2016年度は23%、2017年度は29%となり、若干の増加がみられた。

○セプター訓練

各分野における重要インフラ所管省庁及びセプターとの「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訓練を実施した（参考：別添４－９）。

表３：参加セプター・参加事業者等数の推移

年度	2014	2015	2016	2017
参加セプター	14	18	18	18
参加事業者	1,644	1,658	2,020	2,106

実施に当たっては、重要インフラ事業者等に情報が届いているかを確認（受信確認）する「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下で、その旨を報告する方式の採用など、より実態に即した訓練を実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られ、本訓練の有用性があらためて確認された。

○重要インフラ所管省庁等との連携

NISCが主催する分野横断的演習及びセプター訓練以外にも、重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習（CYDER）を実施したほか、経済産業省では制御システムセキュリティセンター（CSSC）における模擬システム等を用いて、制御システムを有する電力・ガス・ビル・化学の４分野において、実践的なサイバー演習を行った。また、金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、業界横断的なサイバー

セキュリティ演習（Delta Wall Ⅱ）を実施した。

イ　今後の取組

第４次行動計画に基づき、「より実践的な演習機会の提供」、「自職場参加の推進」、「重要インフラ全体での防護能力の底上げ」、「情報共有体制の実効性の向上」について取り組む。

セプター訓練については、最近、参加事業者数が増加していることから、その機会を有効に活用し、各分野の特性や最新の攻撃トレンドを踏まえた模擬情報のカスタマイズ化、全セプターにおける日程を定めない抜き打ち訓練や（セプター事務局を経由する）新たな報告形態の導入を念頭に置いた訓練の実施等、内容の充実に取り組む。

(4)　リスクマネジメント及び対処態勢の整備

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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
＜具体的な指標＞
・「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

ア　取組の進捗状況

リスクマネジメントの推進に係る取組を以下のとおり実施した。これらの取組を通じて、重要インフラ事業者等におけるサイバー攻撃を想定したリスクマネジメント及び対処態勢整備に必要となる考え方や観点、具体的な作業手順等を整理するとともに、重要インフラ事業者等への浸透を図った。

○リスクマネジメントに対する支援

内閣官房は、2020年東京オリンピック・パラリンピック競技大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のための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リスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」をとりまとめた。さらに、重要インフラ事業者等への浸透を図るべく、セプターカウンシルにおいて、当該手引書に関する説明を実施した。

○対処態勢整備に対する支援

内閣官房は、個々の重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき、「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」について、「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（第５版）」に盛り込んだ。さらに、重要インフラ事業者等への浸透を図るべく、セプターカウンシルにおいて、当該指針に関する説明を実施した。

〇リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても各重要インフラ分野が検討に参加する検討会（２回）及び拡大作業部会（１回）をそれぞれ開催した。また、オリパラ大会に向けたリスクアセスメントの参加事業者等を対象に、説明会や意見交換会等を開催し、オリパラ大会に係るリスクコミュニケーション及び協議を支援した。

イ　今後の取組

2017年度の取組の成果等を活用し、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整備の強化を促進するとともに、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べくモニタリング及びレビューの強化を推進していく。

また、セプターカウンシルや分野横断的演習等を通じて引き続き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を行うとともに、経営層を含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を実施する。

(5)　防護基盤の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・「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の継続及びそれぞれの事業者の状況に合わせた取組の推進
・「広報公聴活動」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が広まり、技術動向に合わせた適切な対応が行われていること
・「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・啓発の充実
・「規格・標準及び参照すべき規程類の整備」については、整備した規程類の重要インフラ事業者等における利活用
＜具体的な指標＞
・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

ア　取組の進捗状況

防護基盤の強化として、以下の取組を実施した。こうした取組により、第４次行動計画の全体を支える共通基盤の強化が図られた。

なお、「情報共有体制の強化」とも関連する施策として、防護範囲見直し及び情報共有範囲の拡充を推進した。これにより、セプター事務局の民間主体への移行（医療セプター）、各セプターにおける中小事業者を含めたセプター構成員の拡大、標的型攻撃に関する情報共有体制であるC4TAPの運用改善などの成果や、民間事業者におけるICT-ISAC、金融ISAC及び電力ISACの活発な活動など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上に着実な成果があったと認められる。

〇広報広聴活動

NISCのWebサイトにおいて、分野横断的演習やセプターカウンシルの開催について広報を行うとともに、重要インフラ専門調査会の会議資料等の掲載を通じ、第４次行動計画の進捗状況等を公表した。

重要インフラ事業者等に対しては、政府機関、関係機関、セプター、海外機関の情報セキュリティに関する公表情報の紹介等を記載した重要インフラニュースレターを24回発行した。

また、重要インフラ防護に関する講演を16回実施し、第４次行動計画の考え方や取組状況について重要インフラ事業者等や国民への周知を図った。

〇国際連携

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、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者とのFace-to-Faceの会合等による緊密な関係性の構築に向けた取組を実施した。

多国間では、2017年10月にノルウェーで開催されたMeridian会合において、日本における重要インフラ防護のための各施策や取組等の事例紹介や、各国の取組等に関する意見交換を実施した。また、国際的な情報共有の枠組みであるIWWNを利用して、サイバー攻撃や脆弱性対応についての情報を継続的に共有している。

地域間では、2017年７月に日・ASEANワークショップを開催し、海外政府関係者、国際機関及び我が国の専門家を講師に招き、ASEAN各国が自国に適した政策の検討に資する取組やベストプラクティスの共有を図った。

二国間では、日米間の重要インフラ防護をテーマとする会合における講演・意見交換や、日英サイバー協議をはじめとする政府間協議等を行った。

〇規格・標準及び参照すべき規程類の整備

第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を定める際の考慮すべき事項を整理すること等を柱とする指針の改定案をとりまとめた。さらに、2020年東京オリンピック・パラリンピック競技大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のためのリスクアセスメント・ガイドライン」を、重要インフラ事

業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」をとりまとめた。

また、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、第４次行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を配布した。

制御系機器・システムの第三者認証制度については、経済産業省において、CSSCを通じて、EDSA認証取得のために必要な機器開発・設計・検証等に関するセミナーを実施するとともに、制御システムのセキュリティ評価・認証に関する検討を実施した。

イ　今後の取組

広報広聴活動については、Webサイト、重要インフラニュースレター及び講演等を通じ、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、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。

国際連携については、引き続き、重要インフラ所管省庁や情報セキュリティ関係機関と連携して、欧米・ASEANやMeridian等の二国間・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。また、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。

規格・標準及び参照すべき規程類の整備については、引き続き、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。また、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。

3　第４次行動計画における各施策の取組詳細

第4次行動計画 IV 章記載事項	取組内容
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。	・第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を定める際の考慮すべき事項を整理すること等を柱とする指針の改定案を2018 年３月にとりまとめた。
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。	・他施策との連携強化として、安全基準等策定指針対策編の対策項目に基づいて、分野横断的演習の検証課題の設定を実施した。
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。	・内閣官房において、四半期毎に開催した重要インフラ所管省庁との連絡会議等の機会を通じて、安全基準等の継続的改善を支援した。
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。	・内閣官房において、重要インフラ所管省庁の協力を得て、各分野の安全基準等の分析・検証及び改訂等の実施状況並びに今後の実施予定等の把握を実施（2017 年 12 月～2018 年３月）し、「2017 年度　重要インフラにおける安全基準等の継続的改善状況等の調査」を 2018 年３月に公表した。 ・各分野における制度的枠組みの現状の把握に努めた。
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。	・内閣官房において、重要インフラ所管省庁の協力を得て、各分野における安全基準等の整備状況、情報セキュリティ対策の実施状況等についての調査（2017 年６月～12 月）及び事業者等への往訪による調査（2017 年１月～12 月）を実施し、「2017 年度　重要インフラにおける『安全基準等の浸透状況等に関する調査』について」及び「2017 年度 重要インフラ事業者等 往訪調査 調査報告書」を 2018 年３月に公表した。
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。	・内閣官房において、安全基準等の浸透状況等の調査結果をもとに、各施策の改善事項の検討を実施した。
(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。	・平時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、第４次行動計画に基づいた手順を確認し、訓練により手順の有効性について検証を実施した。
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。	・実施細目に基づき、重要インフラ所管省庁等や情報セキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及び情報セキュリティ関係機関へ情報提供を行った。（2017 年度　情報連絡 407 件、情報提供 54 件）

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。	・内閣官房とパートナーシップを締結している情報セキュリティ関係機関から情報を受領し、重要インフラ事業者等への情報提供を行った。また、同機関が分析した情報の横展開を行った。
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。	・ 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するため、考え方の整理を実施した。
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。	・ 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ための情報共有システムの構築に向けた検討を実施した。
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。	・ 重要インフラ所管省庁の協力を得て、2017 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
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。	・ セプター事務局や重要インフラ事業等への支援に向け、情報共有に必要となる情報共有システムの構築に向けた検討を実施した。
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。	・ セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う幹事会及び運営委員会、個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。（2017 年度のセプターカウンシル会合の回数は延べ 20 回）
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。	・ 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構築に向けた検討を実施した。
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、IT障害発生時に適時適切な情報提供を実施。	・ サイバー空間関連事業者との間での情報提供に関する秘密保持契約の締結に向けた検討を行った。
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。	・ 新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
⑶「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。	・ 重要インフラ所管省庁が実施する障害対応の演習・訓練について最新の状況を把握した。 ・ 分野横断的演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った。
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。	・ 実施日時を予め明らかにしない方式の採用、通常の連絡手段が使用不可能な状況下における代替手段の使用可能性の確認、訓練参加者が単純に受信確認するだけではなく自社の被害状況をセプター事務局や所管省庁へ報告を行うなど、より実態に即した訓練を 13 分野 18 セプターを対象に実施した。
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。	・ 重要インフラ全体の防護能力の維持・向上を図る観点から、「セキュリティ意識とニーズに応える演習企画」「セキュリティ対策の PDCA サイクルの強化に資する運営」「情報共有体制の実効性向上」「演習運営ノウハウや知識等の還元」に重点をおきつつ、分野横断的演習を実施した。2017 年度は、2,647 名が演習に参加した。

④ 分野横断的演習の改善策検討。	・ 分野横断的演習が全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。また、シナリオ作成に際しては、2020 年のオリパラ大会を見据えた情報共有体制の確認や横連携（事業者間の情報共有）における視点にも留意した。 ・ 経営層向けの内容を含む講演を実施するとともに、経営層による演習参加の意義・重要性を明確にするよう、改善を図った。
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。	・ 演習実施前に、演習の検証課題を例示することにより、演習参加効果を向上させるための取組を実施した。また、演習参加により抽出された課題・問題点等を明確にした。 ・ 演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者が各社の早期復旧手順や IT-BCP 等の有効性や実効性を確認する機会を提供した。 ・ 事後の意見交換会における討議事項に「事業継続計画」などに関する事項に加え、セキュリティに関する対策や課題等に関する意見交換を行う機会を提供した。
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）。	・ 演習の概要、目的等を整理した「テキストブック」を作成し、参加事業者に提供した。また、昨年度の演習後の取組みで他の事業者にも十分に参考となる事例を「グッドプラクティス」として提示した。 ・ 自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者に、これを分かりやすく提示した。
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。	・ 重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、対外的に明確化した資料を作成し展開した。
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。	・ 複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者における重要インフラ防護における人材育成の強化・充実に寄与する演習を実施した。
(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。	・ 2020 年東京オリンピック・パラリンピック競技大会の関連事業者等に対して、機能保証の考え方を踏まえたリスクアセスメントの実施手順を記載した「機能保証のためのリスクアセスメント・ガイドライン」を 2016 年度に整備・公表している。 ・ 2017 年度は、「機能保証のためのリスクアセスメント・ガイドライン」の内容を踏まえ、「2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明会（７回）及び情報交換会（３回）を開催するなど、2020 年東京オリンピック・パラリンピック競技大会の開催・運営を支える重要サービスを提供する事業者等（141 組織）のリスクマネジメントを促進する取組を行った。
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。	・ 2020 年東京オリンピック・パラリンピック競技大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のための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リスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を、2018 年４月に公表した。なお「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」は本手引書に統合する形とした。
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。	・ 環境変化調査として、リスクアセスメントの実施における、限られた資産を有効に使うための優先順位を判断するために必要となるサービス維持レベルの検討に資するため、各重要インフラ分野の事業者が、サービス提供に当たり設定している約款などを調査し、社会状況を反映したより実態に近い各分野におけるサービス維持に関する傾向等の把握を行った。

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。	・ 環境変化調査として、各重要インフラ分野の事業者が、サービス提供に当たり設定している約款などを調査し、社会状況を反映したより実態に近い各分野におけるサービス維持に関する傾向等の把握を行った。これが、重要インフラサービスの安全かつ持続的な提供に関する継続的な議論の深化に資するものとなることも期待している。
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。	・ 2018 年 4 月に公表した「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５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の中で内部ステークホルダー間のコミュニケーションの重要性について記載を行い、経営層と実務者間、関連部門間等におけるコミュニケーションを推進した。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象に、説明会、情報交換会等を開催し、有識者による講演やリスクアセスメントの演習等を通じて重要インフラ事業者等の内部におけるリスクコミュニケーションに資する情報の提供を行った。
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。	・ 重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても各重要インフラ分野が検討に参加する検討会（２回）及び拡大作業部会（１回）をそれぞれ開催した。
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。	・ 個々の重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき、「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」について、「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（第５版）」に盛り込み、2018 年４月に公表した。
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。	・ サイバーセキュリティ対処調整センターについて、2018 年度末の構築に向け、仕様の細部について検討を実施すると共に、情報共有・対処体制に関する基本的な方針を関係府省庁、大会組織委員会、東京都等と協議の上、改正した。また、2017 年 12 月にセキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」の中で、2018 年度末を目途に構築及び運用開始することを決定した。
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。	・ リスクマネジメントにおける内部監査の観点を、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」に記載し、2018 年４月に公表した。
⑸「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。	・ 防護範囲見直し及び情報共有範囲の拡充を推進した。これにより、セプターカウンシル事務局の民間主体への移行、各セプターにおける中小事業者を含めたセプター構成員の拡大、標的型攻撃に関する情報共有体制である C4TAP の運用改善などの成果や、民間事業者における ISAC の活発な活動など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上が図られた。
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。	・ NISC 重要インフラニュースレターを 23 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の情報セキュリティに関する公表情報の紹介等の広報を行った。第４次行動計画の実行に当たり、セプターや重要インフラ事業者等に加え海外の重要インフラ関係者に対し、第４次行動計画やその施策等について計 19 回講演を行った。
③ 往訪調査や勉強会・セミナー等を通じた広聴を実施。	・ 往訪調査を通じて、第４次行動計画やその施策等について説明を行うとともに、第４次行動計画への意見や NISC への要望についてヒアリングを行った。
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。	・ 各国とのサイバーセキュリティに関する意見交換等の二国間会合、日・ASEAN CIIP ワークショップや Meridian 会合及び IWWN 等の地域間・多国間における取組に参加し、相互理解の基盤を強化した。

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。	・ アメリカ DHS との会合等を通じて得た知見を踏まえ、国内での有識者・業界関係者等との議論・検討を行い、国際整合性も考慮した上で深刻度評価基準の素案を策定した。
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。	・ 経営層に関する取組は、基本Gをフォローしつつ、各省庁の経営ガイドライン等の調査を行った。
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。	・ 重要インフラ関係者が共通に参照する関連文書について、サイバーセキュリティ戦略、行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を配布した。
⑧ 関連規格を整理、可視化。	・ 国内外で策定される重要インフラ防護に関係する規格について、情報を収集するとともに、リスクマネジメントに関する手順書を作成するに当たって関連する規格を整理し、手順書に反映した。
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。	・ 第三者認証制度について、第４次行動計画における取組内容の検討を行い、第三者認証を受けた製品の活用を推進していくこととした。
2. 重要インフラ所管省庁の施策	**金融庁、総務省、厚生労働省、経済産業省、国土交通省**
(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。	・ 経済産業省において、2017 年 11 月に「サイバーセキュリティ経営ガイドライン」の改訂を行い、「サイバーセキュリティリスクに対応するための仕組みの構築」の追加や、委託先の組織としての活用の把握等の留意点の追記等を行った。
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。	・2018 年４月から、主要な空港ビル事業者等が「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」に基づく各種取組みを開始することから、事業者自らが情報セキュリティ対策を実施するにあたっての参考となるように、国土交通省において 2018 年３月に「空港分野における情報セキュリティ確保に係る安全ガイドライン」を作成した。 ・ 厚生労働省については、サイバー攻撃の手法の多様化・巧妙化を含めた医療情報システムを取り巻く環境の変化に対応するため、「医療情報の安全管理に関するガイドライン」の改定を行い、2017 年５月に第５版を公表した。また、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業に着手した。 ・ 金融庁及び経済産業省については、自らが安全基準等の策定主体とはなっていない。
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。	・ 重要インフラ所管省庁は、各分野における検証等に寄与するため、所管のガイドライン等を改定若しくは改定の検討を行った。
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。	・ 厚生労働省において、「医療情報システムの安全管理に関するガイドライン」及び「水道分野における情報セキュリティガイドライン」について、ツイッター等を活用した普及活動を実施した。また、2017 年５月に行った「医療情報システムの安全管理に関するガイドライン」の改定に併せて、「医療情報システムを安全に管理するために――『医療情報システムの安全管理に関するガイドライン』全ての医療機関等の管理者向け読本」についても、第２版として改定を行った。
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。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各分野における現状を把握した上で、調査の回答を行った。

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。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の浸透状況等の調査について、所管の各分野に協力を求め、3,144 者から回答を得た。 ・ なお、浸透状況等の調査として、金融庁では「金融機関等のシステムに関する動向及び安全対策実施状況調査」、総務省では「地方自治情報管理概要」を通じて、所管の各重要インフラ事業者等への調査を実施した。
⑵「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。	・ 重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあったＩＴの不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。
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。	・ 重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ所管省庁内のとりまとめ担当部局と各分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・ 国土交通省については、航空、鉄道、物流分野における、有事の情報共有・平時の知見共有を通じた集団防御を図るため、重要インフラ事業者（航空、鉄道、物流）が情報の共有・分析や対策を連携して行う体制である「交通 ISAC（Information Sharing and Analysis Center）」（仮称）の創設に向けた支援を行っている。 ・ 平成 30 年３月 17 日に医療セプター事務局を厚生労働省から公益社団法人日本医師会に移管するとともに、日本歯科医師会、日本薬剤師会、日本看護協会及び四病院団体協議会についても構成員とすることとした。
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。	・ 重要インフラ所管省庁において、重要インフラ事業者等からのＩＴ障害等に係る報告があった際に、事案の大小や重要インフラサービスの事案であるか否かに関わらず、速やかに内閣官房へ情報連絡を行った。
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。	・ 重要インフラ所管省庁において、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・ 重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。 ・ 平成 30 年４月 24 日に医療セプターを代表し、公益社団法人日本医師会がセプターカウンシルに加盟した。
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。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
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	・ 厚生労働省においては、IPA の情報収集・分析・共有の仕組み（J-CSIP）に加入するよう調整を行った。
⑶「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。	・ 重要インフラ所管省庁を通じた情報共有体制の確認として、2017 年７月から 10 月までの間に、全 18 セプターに対するセプター訓練を実施した。
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。	・ 重要インフラ所管省庁は、2017 年度分野横断的演習検討会、拡大作業部会等に出席し、演習を実施する上での方法や検証課題等についての検討を行った。
③ 分野横断的演習への参加。	・ 重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員などが、2017 年 12 月に実施された分野横断的演習に参加した。

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。	・ 重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2017 年度分野横断的演習への参加を促し、全体で過去最多の 2,647 名の参加者を得た。
⑤ 分野横断的演習の改善策検討への協力。	・ 重要インフラ所管省庁は、2017 年度分野横断的演習の事後アンケートに回答するとともに、演習における対応記録を作成し来年度以降の改善策の検討材料として内閣官房へ提出した。また、来年度以降も視野に入れた課題、方向性についての議論を行う検討会に出席した。
⑥ 必要に応じて、分野横断的演習成果を施策へ活用。	・ 重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。
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。	・ 重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習「CYDER」を実施したほか、経済産業省では制御システムセキュリティセンター（CSSC）における模擬システム等を用いて、制御システムを有する電力・ガス・ビル・化学の４分野において、実践的なサイバー演習を行った。また、金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅱ）を実施した。
⑷「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。	・ 厚生労働省においては、NISC と連携し、オリパラ大会に係るリスクアセスメントの取組を実施した。
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。	・ 重要インフラ所管省庁においては、NISC が作成したリスクアセスメント・ガイドラインや手引書等の浸透状況を把握するための調査に協力した。
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。	・ 重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・ 「ＥＵ諸国及び米国における情報共有体制に関する調査」については、重要インフラ所管省庁において今後、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として活用が予定されている。 ・ 厚生労働省においては、平成 29 年度は海外における医療分野のサイバーセキュリティに関する基礎調査を行った。平成 30 年度は海外における情報連携機能（ISAC 等）について調査する予定。
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。	・ 重要インフラ所管省庁において、重要インフラ事業者等の情報セキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象とした説明会、意見交換会等の開催に協力することにより、重要インフラ事業者間のリスクコミュニケーション及び協議を支援した。

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。	・ 厚生労働省では、医療分野においては、平成 29 年５月に改定を行った「医療情報の安全管理に関するガイドライン（第５版）」の中で、非常時の事前・事後の対応について、サイバー攻撃に関して記載を追加した。また、水道分野においては、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業を進め、コンティンジェンシープランを位置付ける予定。
(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。	・ 総務省及び経済産業省を中心として、日・ASEAN 情報セキュリティ政策会議等をはじめとした会合の開催等を行うなどにより国際連携の強化を図った。
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。	・ 総務省及び経済産業省を中心として、国際連携にて得た知見を、講演等を通じて国内の関係主体に提供した。
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。	・ 厚生労働省においては、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業を進め、経営層が果たすべき役割を位置付ける予定。
④ 内閣官房と連携し、関連規格を整理、可視化。	・ 重要インフラ所管省庁及び内閣官房において、国内外で策定される重要インフラ防護に関係する規格について、情報を収集した。
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。	・ 厚生労働省においては、医療セプターの構成員について、セプター事務局において検討・調整を行った。
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。	・ 総務省において、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。2017 年度は、重要インフラ事業者から、553 名受講した。 ・ 分野横断的演習等に参加した。
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。	・ 経済産業省において、CSSC に委託したサイバーセキュリティ演習にて制御システムのセキュリティ評価・認証を取り上げ、演習参加者である重要インフラ事業者等の意識向上を図った。
3. 情報セキュリティ関係省庁の施策	**警察庁、総務省、外務省、経済産業省、原子力規制庁、防衛省**
(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。	・ 情報セキュリティ関係省庁及び内閣官房において、相互に情報共有窓口を明らかにすることにより、情報共有体制の運用を行った。
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。	・ 情報セキュリティ関係省庁から、標的型メール攻撃に利用された添付ファイルやＵＲＬリンク情報等について内閣官房に情報連絡を実施した。
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。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
4. 事案対処省庁及び防災関係府省庁の施策	**内閣府（防災担当）、警察庁、防衛省**
(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。	・ 2017 年度において大規模重要インフラサービス障害に該当する事案は発生していないが、大規模サイバー攻撃事態等対処訓練に参加し、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。

② 被災情報、テロ関連情報等の収集。	・「サイバー攻撃特別捜査隊」を中心として、各都道府県警察においてサイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。 ・警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。
③ 内閣官房に対して、必要に応じて情報連絡の実施。	・内閣官房と必要に応じて情報共有を実施した。
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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
⑵「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。	・事案対処省庁は、2017 年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、シナリオ、実施方法、検証課題等についての検討が行われた。
② 分野横断的演習の改善策検討への協力。	・事案対処省庁は、2017 年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、演習の総括、次年度に向けた課題等についての検討が行われた。
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。	・分野横断的演習と重要インフラ防護に資するそれ以外の演習・訓練を相互に視察し、演習・訓練担当者間の連携強化に努めた。 ・都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。
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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

2018 年度（サイバーセキュリティ 2019　抜粋）

別添４－２　重要インフラにおける取組の進捗状況

本章では、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「第４次行動計画」という。）に基づく取組について、2018年度の進捗状況の確認・検証結果を報告する。

１　重要インフラと第４次行動計画全体に関する取組

(1)　第４次行動計画の概要

第４次行動計画は、「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月）」、「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）」、「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（2009年２月、2012年４月改定）」及び「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（2014年５月、2015年５月改定）」に続いて、我が国の重要インフラの情報セキュリティ対策として位置付けたものであり、2017年４月にサイバーセキュリティ戦略本部で決定した。その後、2018年７月に、重要インフラ分野として「空港分野」を追加する改定を実施している。

第４次行動計画においては、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」及び「防護基盤の強化」の５つの施策を掲げており、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである（参考：別添４－１）。施策ごとの取組の進捗状況については次節に示す。

(2)　取組の進捗状況

第４次行動計画は、第３次行動計画の基本的骨格（５つの施策）を維持しつつ、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、策定したものである。この策定に当たっては、「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ほか、重要インフラサービスに重点を置き、これまで「IT障害」としていた表記を「重要インフラサービス障害」とするなど、機能保証の考え方を踏まえたものとした。

2018年度は、2017年度に引き続き、同計画に従って機能保証の考え方に基づき、５つの施策それぞれについて取組を進めた。各施策の取組等の詳細は次節以降に示すが、過去最大規模での分野横断的演習の開催、発生したサービス障害が国民社会に与えた影響全体の深刻さを事後に評価するための基準の初版の決定など、各種取組の着実な成果を得た。なお、第４次行動計画における施策の枠外の取組として、2017年度に引き続き、重要インフラサービス障害等の事例についての現地調査である補完調査を実施した（参考：別添４－10）。

(3) 今後の取組

引き続き、内閣官房と重要インフラ所管省庁等が一体となり、第４次行動計画に基づく取組を推進し、重要インフラ事業者等に対して必要な支援を実施する。

２ 第４次行動計画の各施策における取組

本節においては、第４次行動計画における施策ごとの取組の進捗状況について示す。なお、進捗状況の確認・検証は、第４次行動計画のⅤ.1.3及びⅤ.2.3に記載される各施策における目標及び具体的な指標を踏まえたものである。

(1) 安全基準等の整備及び浸透

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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
＜具体的な指標＞
・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

ア 取組の進捗状況

安全基準等の整備及び浸透に関して、以下の取組を実施した。本取組の中で、重要インフラ事業者等における情報セキュリティ対策のPDCAサイクルとの整合性の確保、第４次行動計画の他施策との連携強化を図ることにより、情報セキュリティ対策の重要性を重要インフラ事業者等に訴求する仕組みを構築した。

〇安全基準等策定指針の改定等

第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、サイバー攻撃への初動対応や事業継続のための復旧対応方針等を定める際に考慮すべき事項を整理することなどを柱とする指針の改定作業を進め、「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５版）」をとりまとめ、2018年４月のサイバーセキュリティ戦略本部において決定、公表を行った。

また、2019年１月の重要インフラ専門調査会において、自然災害の多発やサイバーセキュリティ戦略の改定、重要インフラ分野への空港分野の追加等、指針第５版とりまとめ後の環境変化を踏まえた指針の改定について方向性が承認された。

〇安全基準等の改善状況調査

各重要インフラ分野における安全基準等の継続的な改善状況について調査した（参考：別添４－３）。各分野において安全基準等の改善の必要性について検討・確認し、2017年度より４分野増加した８つの分野において安全基準等の改善を行ったほか、７の分野において改善に向けた分析・検証に着手している。なお、各分野における制度的な枠組みについては、経済産業省においてガス事業法施行規則を改定し、「ガス工作物の運転又は操作を管理する電子計算機に係るサイバーセキュリティの確保に関すること」をガス事業法上の保安規制の一部として位置付ける取組があった。

〇安全基準等の浸透状況等調査

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状況について調査を実施した。アンケート調査（参考：別添４－４）では、2,050件の回答が得られ、分析の結果、重要インフラ事業者等が「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割合」は2017年度と同様の約５割であった。また、重要インフラ事業者等が「先導的な情報セキュリティ対策に取り組んでいる割合」は2017年度の約２割から2018年度には約３割となった。良好な点として、ほぼ全ての事業者等で何らかの情報セキュリティ対策が取られていることから、セキュリティマインドが醸成されていること等が認められた。

また、往訪調査を実施し、情報セキュリティに係る体制や規程等について意見交換を行うとともに、政府への意見・要望の収集を実施し、良好事例及び課題を整理した（参考：別添４－５）。

イ　今後の取組

2018年度の取組結果を活用しつつ、第４次行動計画に基づき、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重要インフラ分野の安全基準等の継続的改善を推進するとともに、重要インフラ事業者等への安全基準等の浸透を図る。具体的には、「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５版）」を改定した上で、同指針の普及・浸透を図るともに、重要インフラ所管省庁と連携し、制度的枠組みを必要に応じて適切に改善する取組を継続する。また、浸透状況等調査については、アンケートの回答が事業者等に資する内容となるよう、取組の充実を図る。

(2)　情報共有体制の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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。
＜具体的な指標＞
・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

ア　取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。こうした取組により、官民の各関係主体が協力する情報共有体制の維持・強化を推進するとともに、重要インフラ事業者等による情報共有活動の活性化を図った。

〇官民の情報共有体制

第４次行動計画に基づき、重要インフラ所管省庁と連携し、具体的な取扱手順にのっとって情報共有体制を運営した。また、2017年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場などを通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。その結果、重要インフラ事業者等から内閣官房に対して223件の情報連絡が行われ、内閣官房からは43件の情報提供を行っている（参考：別添４－６）。

表１：重要インフラ事業者等との情報共有件数

年度	2014	2015	2016	2017	2018
重要インフラ事業者等から内閣官房への情報連絡件数	124件	401件	856件	388件	223件
内閣官房からの情報提供件数	38件	44件	80件	54件	43件

重要インフラ事業者等におけるセキュリティ対策の取組（Web・メール等の無害化等）が進んだこと等により、情報連絡の件数は前年度に比べ減少しているものの、内閣官房からの情報提供件数も含め、情報共有件数は依然として多い状況である。

大規模重要インフラサービス障害対応時の情報共有体制における各関係主体の役割については、平時から大規模重要インフラサービス障害対応時への体制切替の手順について確認を行うとともに、大規模サイバー攻撃事態等対処訓練に参加し、内閣官房や関係省庁との連携要領、関係主体の役割の在り方及び同手順の実効性に関する検証を実施した。

〇セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、空港分野が追加となり、14分野で19セプターが設置されている（参考：別添４－７）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど、重要インフラ防護の関係主体間における情報連携の結節点としても機能している。また、一部の分野においては、ICT-ISAC、金融ISAC及び電力ISACの活発な活動など、自主的な分野内情報共有体制が確立されているほか、交通ISAC（仮称）の創設に向けた取組や、医療・水道分野における情報連携機能（ISAC）を検討するための調査などの取組も進んでいる。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2018年４月の総会で決定した活動方針に基づき、2018年度に、運営委員会（４回）、相互理解WG（４回）、情報収集WG

（４回)、総会準備WG（３回）を開催し、セプター間の情報共有や事例紹介等、情報セキュリティ対策の強化に資する情報収集や知見の共有、及び、更なる活動活性化に向けた要望の聞き取り、その実現に向けた情報分析機能の高度化に関する討議検討を行った。また情報共有活動である「Webサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP)」を通じて、情報共有活動の更なる充実を図っている。

〇深刻度評価基準の策定に向けた取組

サイバーセキュリティ戦略本部において、重要インフラ専門調査会における調査審議を踏まえ、発生したサービス障害が国民社会に与えた影響全体の深刻さを事後に評価するための基準の初版を決定した。

イ　今後の取組

重要インフラを取り巻く急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、情報共有を容易にする環境整備（連絡形態の多様化、情報共有システムの整備）や共有情報の理解浸透（共有範囲の明確化）等、引き続き官民を挙げた情報共有体制の強化に取り組んでいく。

また、政府機関を含め、他の機関から独立した会議体であるセプターカウンシルについては、従来にも増して各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。更なるセプターカウンシルの自律的な運営体制とそれによる情報共有の活性化を目指し、内閣官房は運営及び活動に対する支援を継続していく。

(3)　障害対応体制の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。こうした取組により、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等の検証や、関係主体間における情報共有の有効性の検証を可能にするとともに、技術面での対処能力の向上等を図った。

〇分野横断的演習

第４次行動計画に基づく具体的な取組の方向性として「より実践的な演習機会の提供」、「自職場参加の推進」、「重要インフラ全体での防護能力の底上げ」及び「情報共有体制の実効性の向上」に取り組んだ（参考：別添４－８)。

2018年度からは、空港分野を加えた全14分野が演習に参加し、参加者数は3,077名に増加した。また、事後の意見交換会も実施し、分野間での情報共有を促進した。

表２　分野横断的演習参加者数の推移

年度	2015	2016	2017	2018
参加者数	1,168名	2,084名	2,647名	3,077名

2018年度においては、重要インフラ全体での防護能力の底上げのため、募集の際に自職場参加について丁寧に説明したテキストブック等を添付することで、昨年度と比較し、自職場参加者が増加した（2017年度：63%→2018年度：75%）。

また、演習当日における経営層参加については、参加者募集時や事前説明会における資料に加え、ベースシナリオの中でも経営層の参加を促したものの、その参加率は28%に留まっている。

なお、2017年度分野横断的演習参加者へのフォローアップ調査の結果から、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（演習で得られた知見を踏まえ改善を実施又は検討している）と評価した参加者の割合は82%となっている。一方で、安全基準等の浸透状況等調査の結果から、組織内外で実施する演習・訓練への参加状況について、分野横断的演習を含む組織外で実施される演習・訓練への参加割合は61%、組織内で演習・訓練を実施している割合は29%に留まっている。

〇セプター訓練

各重要インフラ分野における重要インフラ所管省庁及びセプターとの「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訓練を実施した（参考：別添４－９）。

表３：参加セプター・参加事業者等数の推移

年度	2015	2016	2017	2018
参加セプター	18	18	18	19
参加事業者等	1,658	2,020	2,106	2,005

実施に当たっては、重要インフラ事業者等に内閣官房から提供する情報が届いているかを事業者等に確認（受信確認）する「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下で、その旨を報告する方式の採用等、より実態に即した訓練を実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られ、本訓練の有用性が確認された。

〇重要インフラ所管省庁等との連携

内閣官房が主催する分野横断的演習及びセプター訓練以外にも、重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習（CYDER）を実施した。また、金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）を実施した。これら演習と相互に連携・補完しつつ分野横断的演習等を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・向上を図った。

イ　今後の取組

第４次行動計画に基づき、分野横断的演習については、自職場参加の推奨等により演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図るとともに、2020年東京オリンピック・パラリンピック競技大会に関わる重要インフラ事業者等が、大会開催時に想定されるより困難な脅威にも適切に対応できる状態に達することを目指す取組を行う。また、引き続き、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についても促進していく。

セプター訓練については、引き続きその機会を有効に活用し、「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下でその旨を報告する方式の採用等を実施する。

(4)　リスクマネジメント及び対処態勢の整備

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・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

＜具体的な指標＞
・「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

ア　取組の進捗状況

リスクマネジメントの推進に係る取組を以下のとおり実施した。これらの取組を通じて、重要インフラ事業者等におけるサイバー攻撃を想定したリスクマネジメント及び対処態勢整備に必要となる考え方や観点、具体的な作業手順等を整理するとともに、重要インフラ事業者等への浸透を図った。

〇リスクマネジメントに対する支援

内閣官房は、2020年東京オリンピック・パラリンピック競技大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のためのリスクアセスメント・ガイドライン」をWebサイトへの掲載や説明会で配布することで浸透を図った。また、同ガイドラインを重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」をとりまとめ、2018年４月に公表した。さらに、重要インフラ事業者等への浸透を図るべく、重要インフラのセキュリティに関するカンファレンスや、ISACにおける勉強会、分野横断的演習の説明会などで同手引書に関する説明を実施するとともに、各重要インフラ所管省庁へも説明を実施した。

なお、「機能保証のためのリスクアセスメント・ガイドライン」の配付数について、掲載されているWebサイトの閲覧数は257件、第３回説明会の参加者数は504人、第４回説明会の参加者数は515人となっている。

〇対処態勢整備に対する支援

内閣官房は、個々の重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」について、「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（第５版）」に盛り込んだ。さらに、重要インフラ事業者等への浸透を図るべく、重要インフラのセキュリティに関するカンファレンスや分野横断的演習の説明会等で、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に関する説明を実施した。

また、2017年12月に2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議セキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを構築したほか、サイバーセキュリティ対処調整センターを含む、大会に向けたサイバーセキュリティ体制の運用方針等について、大会組織委員会、東京都等と協議の上、2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議セキュリティ幹事会サイバーセキュリティWTにおいて決定した。

〇リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動（運営委員会（４回）、相互理解WG（４回）、情報収集WG（４回）、総会準備WG（３回））を支援したほか、分野横断的演習に関しても、説明会、意見交換会、各重要インフラ分野が検討に参加する検討会（２回）及び拡大作業部会（１回）をそれぞれ開催した。また、2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象に、説明会（25回）や情報交換会（６回）を開催し、大会に係るリスクコミュニケーション及び協議を支援した。

イ　今後の取組

2018年度の取組の成果等を活用し、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整備の強化を促進するとともに、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べくモニタリング及びレビューの強化を推進していく。

また、セプターカウンシルや分野横断的演習等を通じて引き続き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を行うとともに、経営層を含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支援を実施する。

(5)　防護基盤の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜目標＞
・「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の継続及びそれぞれの事業者の状況に合わせた取組の推進
・「広報公聴活動」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が広まり、技術動向に合わせた適切な対応が行われていること
・「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・啓発の充実
・「規格・標準及び参照すべき規程類の整備」については、整備した規程類の重要インフラ事業者等における利活用
＜具体的な指標＞
・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

ア　取組の進捗状況

防護基盤の強化として、以下の取組を実施した。こうした取組により、第４次行動計画の全体を支える共通基盤の強化が図られた。

○防護範囲の見直し

重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大、民間事業者におけるICT-ISAC、金融ISAC及び電力ISACの活発な活動、交通ISAC（仮称）の創設に向けた取組など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上に着実な成果があったと認められる。

○広報広聴活動

内閣官房は、NISCのWebサイトにおいて、分野横断的演習やセプターカウンシルの開催について広報を行うとともに、重要インフラ専門調査会の会議資料等の掲載を通じ、第４次行動計画の進捗状況等を随時公表したほか、重要インフラ事業者等に対して、情報セキュリティに関する政府機関、情報セキュリティ関係機関、海外機関等の公表情報の紹介等を記載した重要インフラニュースレターを24回発行した。

また、重要インフラ防護に関する講演を14回実施し、第４次行動計画の考え方や取組状況について重要インフラ事業者等や海外等への周知を図った。

さらに、情報通信、航空、鉄道、物流、ガス及びクレジット分野の合計16事業者等を対象とした往訪調査の機会を活用し、第４次行動計画やその施策等について説明し、第４次行動計画への意見や内閣官房への要望についてヒアリング等を行った。

〇国際連携

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、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者とのFace-to-Faceの会合等による緊密な関係性の構築に向けた取組を実施した。

多国間では、2018年10月に韓国で開催されたMeridian会合において、日本のサイバー演習や2020年東京オリンピック・パラリンピック競技大会に向けた取組の紹介及び各国の取組等に関する意見交換を実施した。また、2018年12月に開催した分野横断的演習当日に合わせて海外機関を対象とした演習見学会を開催し、演習概要の説明及び各国のサイバー演習の取組に関する情報交換を実施した。加えて、国際的な情報共有の枠組みであるIWWNを利用して、サイバー攻撃や脆弱性対応についての情報を継続的に共有している。

地域間では、2019年１月にASEAN研修員向けの「ASEAN地域のサイバーセキュリティ対策強化のための政策能力向上」研修において、日本における重要インフラ防護の取組について講演した。

二国間では、日仏サイバー協議における意見交換や、日米間や日豪間における政府間協議等を行った。また、2018年４月に開催された米国サイバー演習の視察に合わせ、サイバー演習について米国と意見交換を実施したほか、2019年１月には仏国サイバー演習を視察するとともに、サイバー演習や重要インフラ防護施策について意見交換を実施した。

〇経営層への働きかけ

内閣官房において、「記述情報の開示に関する原則」の公表（金融庁）、「経営ガイドライン」の普及活動、産業サイバーセキュリティ研究会の活動（経済産業省）のほか、IPA（中小企業向けのサービス）等の取組について、第４次行動計画の関連施策の改善を実施するための参考とするとともに、関連施策を通して経営層への働きかけを実施した。

〇人材育成等の推進

内閣官房は、「サイバーセキュリティ人材育成取組方針」（2018 年６月サイバーセキュリティ戦略本部報告）に基づく取組を推進した。重要インフラ事業者等については、情報セキュリティ人材の育成カリキュラム等による組織内の人材教育について、各関連施策を通じて普及啓発を行った。

〇規格・標準及び参照すべき規程類の整備

内閣官房は、国内外で策定される重要インフラ防護に関係する規格について情報を収集するとともに、「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５版）」を作成するに当たって関連する規格を整理し、指針に反映した。

また、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、第４次行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を更新し、配布した。

制御系機器・システムの第三者認証制度については、経済産業省において、CSSCを通じて、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。

イ　今後の取組

防護範囲の見直しについては、引き続き見直しの取組及びそれぞれの事業者等の状況に合わせた取組の推進を実施する。

広報広聴活動については、Webサイト、重要インフラニュースレター及び講演等を通じ、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、往訪調査や勉強会・セミナー等を通じた各重要インフラ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。

国際連携については、引き続き、重要インフラ所管省庁や情報セキュリティ関係機関と連携して、欧米・ASEANやMeridian等の二国間・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。また、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。

経営層への働きかけについては、引き続き内閣官房及び重要インフラ所管省庁が連携し、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。

人材育成等の推進については、引き続き「サイバーセキュリティ人材育成取組方針」を踏まえ、重要インフラ事業者等の重要サービス等を防御するセキュリティ人材の育成カリキュラム等について普及啓発を行う。

規格・標準及び参照すべき規程類の整備については、引き続き、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。また、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。

3　第４次行動計画における各施策の取組内容

第4次行動計画 IV 章記載事項	取組内容
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。	・ 第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を定める際の考慮すべき事項を整理すること等を柱とする指針の改定を行い、2018 年４月のサイバーセキュリティ戦略本部において決定、公表を行った。
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。	・ 2019 年１月の重要インフラ専門調査会において、自然災害の多発やサイバーセキュリティ戦略の改定、重要インフラ分野への空港分野の追加等の環境変化を踏まえた指針の改定について、方向性が承認された。
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。	・ 2018 年４月に決定した指針（第５版）の説明を重要インフラ所管省庁やセプター等に対して行うとともに、指針の更なる改定に関して重要インフラ所管省庁やセプター等に背景や方針の説明を行うことなどを通じて、安全基準等の継続的改善を支援した。
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。	・ 重要インフラ所管省庁の協力を得て、各重要インフラ分野の安全基準等の分析・検証及び改訂等の実施状況並びに今後の実施予定等の把握を実施（2018 年 12 月～2019 年３月）し、「2018 年度　重要インフラにおける安全基準等の継続的改善状況等の調査」を 2019 年４月に公表した。 ・ 各重要インフラ分野における制度的枠組みの現状の把握に努めた。
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。	・ 重要インフラ所管省庁の協力を得て、各重要インフラ分野における安全基準等の整備状況、情報セキュリティ対策の実施状況等についての調査（2018 年６月～12 月）及び事業者等への往訪による調査（2018 年１月～12 月）を実施し、「2018 年度　重要インフラにおける『安全基準等の浸透状況等に関する調査』について」を 2019 年４月に公表した。
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。	・ 安全基準等の浸透状況等の調査結果をもとに、各施策の改善事項の検討を実施した。
(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。	・ 平時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、第４次行動計画に基づいた手順を確認し、訓練により手順の有効性について検証を実施した。
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。	・ 実施細目に基づき、重要インフラ所管省庁等や情報セキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及び情報セキュリティ関係機関へ情報提供を行った。（2018 年度　情報連絡 230 件、情報提供 43 件）

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。	・内閣官房とパートナーシップを締結している情報セキュリティ関係機関と情報を共有し、重要インフラ事業者等への情報提供を行った。また、同機関が分析した情報の横展開を行った。さらに、同機関を始めとした情報セキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。
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。	・ 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するため、考え方の整理について引き続き検討した。
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。	・ 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収集する仕組みを構築し、収集した情報をとりまとめた。
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。	・ 重要インフラ所管省庁の協力を得て、2018 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
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。	・ セプター事務局や重要インフラ事業者等との情報共有に関し、情報共有体制の更なる改善に向けた検討を実施した。
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。	・ セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。（2018 年度のセプターカウンシル会合の回数は延べ 16 回）
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。	・ 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構築に向けた検討を実施した。
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、IT障害発生時に適時適切な情報提供を実施。	・ サイバー空間関連事業者との間での情報提供に関し、検討を行った。
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。	・ 新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
⑶「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。	・ 重要インフラ所管省庁が実施する障害対応の演習・訓練について、相互に参加する等により最新の状況を把握した。 ・ 分野横断的演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った。
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。	・ 実施日時を予め明らかにしない方式の採用、通常の連絡手段が使用不可能な状況下における代替手段の使用可能性の確認、訓練参加者が単純に受信確認するだけではなく自社の被害状況をセプター事務局や重要インフラ所管省庁へ報告を行うなど、より実態に即した訓練を 14 分野 19 セプターを対象に実施した。
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。	・ 重要インフラ全体の防護能力の維持・向上を図る観点から、「より実践的な演習機会の提供」、「自職場参加の推進」、「重要インフラ全体での防護能力の底上げ」、「情報共有体制の実効性の向上」に重点をおきつつ、分野横断的演習を実施した。2018 年度は、3,077 名が演習に参加した。

④ 分野横断的演習の改善策検討。	・ 分野横断的演習が全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。また、シナリオ作成に際しては、2020 年東京オリンピック・パラリンピック競技大会を見据えた情報共有体制の確認やレピュテーションリスクにおける視点にも留意した。 ・ 事前説明会において、個別シナリオ作成における事業継続計画及びコンティンジェンシープランの重要性について説明を実施するとともに、経営層による演習参加の重要性を明確にするよう、改善を図った。
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。	・ 2017 年度分野横断的演習の事後調査により、演習に参加して得られた気づきを踏まえた改善状況等（リスク分析の成果の検証状況、復旧手順及び IT-BCP 等の検討の状況）を把握し、その分析結果を踏まえた 2018 年度分野横断的演習の企画・運営について検討した。また、効果的な取組を進めていると評価される参加事業者等について、ヒアリング等を通じて具体的な取組内容を把握し、グッドプラクティスとしてまとめ、他の演習参加者等に提供した。 ・ 演習実施前に、演習の検証課題を提示すること等により、演習参加効果を向上させるための取組を実施した。また、演習参加により抽出された課題・問題点等を明確にした。 ・ 演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者等が各社の早期復旧手順や IT-BCP 等の有効性や実効性を確認する機会を提供した。 ・ 事後の意見交換会として、討議事項にセキュリティに関する対策や課題、顔の見える関係等に関する意見交換を含む機会を提供した。
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）。	・ 演習の概要、目的等を整理し、「テキストブック」として参加事業者等のサブコントローラー向け、プレイヤー向け及びセプター事務局向けそれぞれの版を作成し、参加事業者等、セプター事務局及び重要インフラ所管省庁に提供した。 ・ 自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。 ・ 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、仮想的な演習環境の構築を進めた。
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。	・ 重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、対外的に明確化した資料を作成し展開した。
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。	・ 複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者等における重要インフラ防護における人材育成の強化・充実に寄与する演習を実施した。
(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。	・ 2020 年東京オリンピック・パラリンピック競技大会の関連事業者等に対して、機能保証の考え方を踏まえたリスクアセスメントの実施手順を記載した「機能保証のためのリスクアセスメント・ガイドライン」を 2016 年度に整備・公表している。 ・ 2018 年度は、「機能保証のためのリスクアセスメント・ガイドライン」の内容を踏まえ、「2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明会（25 回）及び情報交換会（６回）を開催するなど、2020 年東京オリンピック・パラリンピック競技大会の開催・運営を支える重要サービスを提供する事業者等（268 組織）のリスクマネジメントを促進する取組を行った。
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。	・ 2020 年東京オリンピック・パラリンピック競技大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のための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リスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」をとりまとめ、2018 年４月に公表している。なお「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」は本手引書に統合する形となっている。

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。	・ 安全基準の整備等に関わる新たなリスク源について、**安全基準等策定指針等の改定に向けて整理したほか、**新たなリスク源に関するヒアリング等を実施することで、社会状況を反映したより実態に近い各重要インフラ分野におけるサービス維持に関する状況等の把握を行った。
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。	・ 新たなリスク源に関するヒアリング等を実施することで、社会状況を反映したより実態に近い各分野におけるサービス維持に関する状況等の把握を行い、他施策の内容検討に繋げた。
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。	・ 2018 年４月に公表した「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５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の中で内部ステークホルダー間のコミュニケーションの重要性について記載を行い、経営層と実務者間、関連部門間等におけるコミュニケーションを推進した。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象に、説明会や情報交換会等を開催し、有識者による講演やリスクアセスメントの演習等を通じて重要インフラ事業者等の内部におけるリスクコミュニケーションに資する情報の提供を行った。
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。	・ 重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても、説明会や意見交換会等のほか、各重要インフラ分野が検討に参加する検討会（２回）及び拡大作業部会（１回）をそれぞれ開催した。
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。	・ 個々の重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき、「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」について、「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（第５版）」に盛り込み、2018 年４月に公表している。 ・ 事業継続計画及びコンティンジェンシープランの実行性の検証に係る観点をとりまとめ、分野横断的演習のテキストブックに掲載するとともに、演習事前説明会で重要インフラ事業者等に、これらの観点を踏まえた課題抽出と改善の重要性について説明を行った。
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。	・ 2017 年 12 月にセキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを構築した。また、サイバーセキュリティ対処調整センターを含む、2020 年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ体制の運用方針等について、大会組織委員会、東京都等と協議の上、決定した。
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。	・ リスクマネジメントにおける内部監査の観点を、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」に記載し、2018 年４月に公表している。
(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。	・ 防護範囲見直し及び情報共有範囲の拡充を推進した。これにより、重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大、民間事業者における ISAC の活発な活動など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上が図られた。

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。	・ NISC 重要インフラニュースレターを 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の情報セキュリティに関する公表情報の紹介等の広報を行った。第４次行動計画の実行に当たり、セプターや重要インフラ事業者等に加え海外の重要インフラ関係者に対し、第４次行動計画やその施策等について計 14 回講演を行った。
③ 往訪調査や勉強会・セミナー等を通じた広聴を実施。	・ 往訪調査等を通じて、第４次行動計画やその施策等について説明を行うとともに、第４次行動計画への意見や NISC への要望についてヒアリング等を行った。
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。	・ 各国とのサイバーセキュリティに関する意見交換等の二国間会合、ASEAN 研究員向けサイバーセキュリティ対策強化のための政策能力向上研修における講演、海外機関を対象とした分野横断的演習見学会の開催、Meridian 会合や IWWN での情報交換等の地域間・多国間における取組を通じて、相互理解の基盤を強化した。
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。	・ 米国サイバー演習の視察及び意見交換を通じて得た知見を踏まえ、国内での有識者・業界関係者等との議論・検討を行い、分野横断的演習内容の改善を行った。
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。	・ 「記述情報の開示に関する原則」の公表（金融庁）、「経営ガイドライン」の普及活動、産業サイバーセキュリティ研究会の活動（経済産業省）のほか、IPA（中小企業向けのサービス）等の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策を通して経営層への働きかけを実施した。
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。	・ 重要インフラ関係者が共通に参照する関連文書について、サイバーセキュリティ戦略、行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を更新、配布した。
⑧ 関連規格を整理、可視化。	・ 国内外で策定される重要インフラ防護に関係する規格について情報を収集するとともに、「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５版）」を作成するに当たって関連する規格を整理し、指針に反映した。
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。	・ 第三者認証制度について、第４次行動計画における取組内容の検討を行い、第三者認証を受けた製品の活用を推進していくこととしており、重要インフラ事業等に対する働きかけに向け、メーカーとの意見交換等を通じた状況把握を実施した。
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。	・ 経済産業省において、「サイバーセキュリティリスクに対応するための仕組みの構築」や、委託先の組織としての活用の把握等の留意点が記載されている「サイバーセキュリティ経営ガイドライン」の普及啓発を行った。
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。	・ 総務省において、「自治体情報セキュリティ対策検討チームの報告（2015 年 11 月）」を踏まえた地方公共団体におけるセキュリティ対策の抜本的強化への取組や、「政府機関の情報セキュリティ対策のための統一基準」の改定等を踏まえ、2018 年９月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」等を改定した。また、2017 年度に発生した電気通信事故の原因及び対応策等について分析・評価を行い、その結果や有識者からの意見を踏まえ、「情報通信ネットワーク安全・信頼性基準」等について、2019 年３月に改定した。 ・ 厚生労働省において、2019 年３月に「水道分野における情報セキュリティガイドライン（第４版）」を策定した。 ・ 国土交通省において、国土交通省所管の重要インフラ分野（航空、空港、鉄道、物流）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」の改訂を行い、事業者への周知・浸透を図るとともに、国土交通省のウェブサイトに掲載した。 ・ 金融庁及び経済産業省については、自らが安全基準等の策定主体とはなっていない。 ・ 制度的枠組みを適切に改善する取組として、経済産業省においてガス事業法施行規則を改定し、「ガス工作物の運転又は操作を管理する電子計算機に係るサイバーセキュリティの確保に関すること」をガス事業法上の保安規制の一部として位置付けた。

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。	・ 重要インフラ所管省庁は、各重要インフラ分野における検証等に寄与するため、所管のガイドライン等を改定若しくは改定の検討を行った。
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。	・ 厚生労働省において、「医療情報システムの安全管理に関するガイドライン」及び「水道分野における情報セキュリティガイドライン」について、ツイッター等を活用した普及活動を実施した。また、2018 年 10 月に「医療情報システムの安全管理に関するガイドライン」の周知徹底等に関して都道府県等に対し通知した。
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。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各重要インフラ分野における現状を把握した上で、調査の回答を行った。
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。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の浸透状況等の調査について、所管の各重要インフラ分野に協力を求め、2,050 者から回答を得た。なお、浸透状況等の調査として、金融庁では「金融機関等のシステムに関する動向及び安全対策実施状況調査」を通じて、所管の各重要インフラ事業者等への調査を実施した。
⑵「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。	・ 重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあったＩＴの不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。
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。	・ 重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ所管省庁内のとりまとめ担当部局と各重要インフラ分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・ 厚生労働省においては、2018 年 10 月に「医療情報システムの安全管理に関するガイドライン」の周知徹底等に関して都道府県等に対して通知した。また、医療・水道分野における情報連携機能（ISAC）を検討するための調査等を行った。 ・ 国土交通省において、2018 年４月から重要インフラ事業者（航空、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」（仮称）の仮運用が開始されたことから、事業者が参加する検討会を開催し、交通 ISAC の本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論した。また、2018 年７月に重要インフラ分野に追加された空港分野の事業者に対し、交通 ISAC への参加を促した。
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。	・ 重要インフラ所管省庁は、重要インフラ事業者等からのＩＴ障害等に係る報告があった際に、事案の大小や重要インフラサービスの事案であるか否かに関わらず、速やかに内閣官房へ情報連絡を行った。
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。	・ 重要インフラ所管省庁は、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・ 重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・ 重要インフラ所管省庁は、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。 ・ 2018 年４月 24 日に医療セプターを代表し、公益社団法人日本医師会がセプターカウンシルに加入した。 ・ 国土交通省において、2018 年７月に重要インフラ分野に追加された空港分野がセプターカウンシルに加入するよう、事業者と調整中である。
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。	・ 重要インフラ所管省庁は、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。

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	・ 厚生労働省において、医療分野におけるセプター構成員の拡充に関して支援を行った。また、IPA の情報収集・分析・共有の仕組み（J-CSIP）に加入するよう調整を行い、医療分野は、2018 年５月、水道分野は 2018 年 11 月に加入した。 ・ 国土交通省において、2018 年７月に重要インフラ分野に追加された空港分野が IPA の情報収集・分析・共有の仕組み（J-CSIP）に加入するよう、事業者と調整し、2018 年 11 月に加入した。
(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。	・ 重要インフラ所管省庁を通じた情報共有体制の確認として、2018 年８月から 10 月までの間に、全 19 セプターに対するセプター訓練を実施した。
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。	・ 重要インフラ所管省庁は、2018 年度分野横断的演習検討会、拡大作業部会等に出席し、演習を実施する上での方法や検証課題等についての検討を行った。
③ 分野横断的演習への参加。	・ 重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員などが、2018 年 12 月に実施された分野横断的演習に参加した。
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。	・ 重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2018 年度分野横断的演習への参加を促し、全体で過去最多の 3,077 名の参加者を得た。
⑤ 分野横断的演習の改善策検討への協力。	・ 重要インフラ所管省庁は、2018 年度分野横断的演習の事後調査に回答するとともに、演習における対応記録を作成し翌年度以降の改善策の検討材料として内閣官房へ提出した。また、翌年度以降も視野に入れた課題、方向性についての議論を行う検討会に出席した。
⑥ 必要に応じて、分野横断的演習成果を施策へ活用。	・ 重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。
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。	・ 重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習「CYDER」を実施した。また、金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）を実施した。
(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。	・ 重要インフラ所管省庁において、内閣官房と連携し、オリパラ大会に係るリスクアセスメントの取組を実施した。
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。	・ 重要インフラ所管省庁において、内閣官房が作成した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の浸透状況を把握するための調査に協力した。

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。	・ 重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・ 「ＥＵ諸国及び米国における情報共有体制に関する調査」については、重要インフラ所管省庁において、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として活用されている。
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。	・ 重要インフラ所管省庁において、重要インフラ事業者等の情報セキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象とした説明会、意見交換会等の開催に協力することにより、重要インフラ事業者等間のリスクコミュニケーション及び協議を支援した。
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。	・ 金融庁において、諸外国における「脅威ベースのペネトレーションテスト」の手法や海外金融機関の活用状況を把握するための外部委託調査を実施し、2018 年５月に「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」を公表した。また、大規模な金融機関に対し、サイバーセキュリティ対策の一層の高度化を図るため、「脅威ベースのペネトレーションテスト」の活用を促した。 ・ 厚生労働省において、2018 年度に策定した「水道分野における情報セキュリティガイドライン（第４版）」において、コンティンジェンシープランを位置付けた。
⑸「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。	・ 総務省及び経済産業省を中心として、日・ASEAN サイバーセキュリティ政策会議等をはじめとした会合の開催等を行うなどにより国際連携の強化を図った。
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。	・ 総務省及び経済産業省を中心として、国際連携にて得た知見を、講演等を通じて国内の関係主体に提供した。
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。	・ 厚生労働省において、2018 年度に策定した「水道分野における情報セキュリティガイドライン（第４版）」において、経営層が果たすべき役割を位置付けた。
④ 内閣官房と連携し、関連規格を整理、可視化。	・ 重要インフラ所管省庁は、内閣官房と連携し、国内外で策定される重要インフラ防護に関係する規格について、情報を収集した。
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。	・ 厚生労働省において、医療分野におけるセプター構成員の拡充に関して支援を行った。 ・ 国土交通省において、重要インフラ分野に空港分野が追加となるよう調整する（2018 年７月 25 日に重要インフラ分野に追加）とともに、空港セプターに新たに参加する事業者についてセプター事務局と検討・調整を行った。
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。	・ 重要インフラ所管省庁は、分野横断的演習等に参加し、情報セキュリティ人材の育成を支援した。 ・ 総務省において、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。
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。	・ 経済産業省において、制御系機器・システムの第三者認証制度について、CSSC を通じ、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。

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。	・ 情報セキュリティ関係省庁及び内閣官房において、相互に情報共有窓口を明らかにすることにより、情報共有体制の運用を行った。
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。	・ 情報セキュリティ関係省庁から、標的型メール攻撃に利用された添付ファイルやURLリンク情報等について内閣官房に情報連絡を実施した。
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。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
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。	・ 2018年度において大規模重要インフラサービス障害に該当する事案は発生していないが、事案対処省庁等は、大規模サイバー攻撃事態等対処訓練に参加し、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。
② 被災情報、テロ関連情報等の収集。	・ 「サイバー攻撃特別捜査隊」を中心として、各都道府県警察においてサイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。 ・ 警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。
③ 内閣官房に対して、必要に応じて情報連絡の実施。	・ 事案対処省庁及び防災関係府省庁は、内閣官房と必要に応じて情報共有を実施した。
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。	・ 警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・ 警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
(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。	・ 事案対処省庁は、2018年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、シナリオ、実施方法、検証課題等についての検討が行われた。
② 分野横断的演習の改善策検討への協力。	・ 事案対処省庁は、2018年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、演習の総括、次年度に向けた課題等についての検討が行われた。
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。	・ 分野横断的演習と重要インフラ防護に資するそれ以外の演習・訓練を相互に視察し、演習・訓練担当者間の連携強化に努めた。 ・ 都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。

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。	・ 警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・ 警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

2019 年度（サイバーセキュリティ 2020　抜粋）

別添５－２　重要インフラに関する取組の進捗状況

「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「第４次行動計画」という。）に基づく取組について、2019年度の進捗状況の確認・検証結果を報告する。

１　第４次行動計画

(1)　概要

第４次行動計画は、「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月）」、「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）」、「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（2009年２月、2012年４月改定）」及び「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（2014年５月、2015年５月改訂）」に続いて、我が国の重要インフラの情報セキュリティ対策として位置付けられるものであり、2017年４月にサイバーセキュリティ戦略本部で決定された。その後、2018年７月に重要インフラ分野として新たに「空港分野」を追加し、2020年１月には各重要インフラ分野の安全基準の名称の変更や関係法令の改正に伴う記載の変更を踏まえた改定を実施している。

第４次行動計画においては、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」及び「防護基盤の強化」の５つの施策を掲げ、内閣官房と重要インフラ所管省庁等が協力し、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っていくこととしている（参考：別添５－１）。

(2)　各施策の実施状況

第４次行動計画は、第３次行動計画の基本的骨格（５つの施策）を維持しつつ、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、策定したものである。この策定に当たっては、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として明確化したほか、これまでの「IT障害」を「重要インフラサービス障害」とするなど、機能保証の考え方を踏まえたものとしている。

2019年度は、2018年度に引き続き、同計画に従って、５つの施策それぞれについて取組を進めた。各施策における取組は次節以降に示すが、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」等の改定（2019年５月）、過去最大規模での分野横断的演習の実施（2019年11月）など、サイバーセキュリティを取り巻く環境の変化を踏まえつつ、各施策を着実に推進した。また、これらの５つの施策に基づく取組のほか、第４次行動計画について適切な評価を行うため、個別施策の指標では捉えられない側面を補完的に調査することを目的に、重要インフラサービス障害等の事例についての現地調査である補完調査を2018年度に引き続き実施した（参考：別添５－

9）。

(3) 今後の取組

重要インフラサービスの安全かつ持続的な提供の実現に向け、今後も内閣官房と重要インフラ所管省庁等が連携し、第４次行動計画に基づく積極的な取組を引き続き推進するとともに、東京2020大会後に予定されている同計画の評価・見直しに向けた検討に着手していく。

２　第４次行動計画の各施策における取組

本節では、第４次行動計画の各施策における取組の実施状況について述べる。また、第４次行動計画のⅤ.1.3及びⅤ.2.3に示す各施策における目標及び具体的な指標に対応する内容も併せて記載する。

(1) 安全基準等の整備及び浸透

＜目標＞
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

安全基準等の整備及び浸透に向け、以下の取組を実施した。

〇安全基準等策定指針の改定

サイバーセキュリティを取り巻く情勢を踏まえ、「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５版）」を2019年５月に改定し、重要インフラの各分野の安全基準等において規定することが望まれる項目として、「災害による障害の発生しにくい設備の設置及び管理」及び「データ管理」を追加した。前者は、重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい配置とする等、適切な設備の設置及び管理を行う仕組みを構築すること、後者は、システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うことを求めるものである。

また、第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、同指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。

〇安全基準等の継続的な改善

内閣官房は、重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況を調査し、安全基準等の継続的な改善状況を取りまとめた。2019年度は、指針や関係法令・ガイドラインの改定等を契機として、各重要インフラ分野において計11件の安全基準等の改定（初版制定含む）が実施されたことを確認した。（参考：別添５－３）。

また、総務省は、放送設備に義務付ける技術基準を定める省令の一部を改正し、厚生労働省は、水道施設の技術的基準を定める省令の一部を改正することで、それぞれサイバーセキュリティに係る保安規程・技術基準の一部として位置づけた。

なお、各重要インフラ分野における制度的枠組みの現状については、内閣官房において取りまとめ、2019年10月の重要インフラ専門調査会に報告した。

〇安全基準等の浸透

内閣官房は、重要インフラ所管省庁等の協力を得て、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実施状況等を調査した。2019年度は2,205者から回答があり、今回の調査結果をベースラインとなる情報セキュリティ対策と先導的な情報セキュリティ対策に整理し、それぞれの実施状況を確認したところ、2018年度の調査と比較してそれらに取り組んでいる事業者の割合はおおむね増加していることが確認された（参考：別添５－４）。

イ　今後の取組

第４次行動計画に基づき、引き続き、安全基準等策定指針の整備等を通じて各重要インフラ分野の安全基準等の継続的な改善を推進するとともに、重要インフラ所管省庁等と連携し、安全基準等の整備・浸透を図っていく。

(2)　情報共有体制の強化

＜目標＞
・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。
＜具体的な指標＞
・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

ア　取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。

〇官民の情報共有体制

第４次行動計画に基づき、重要インフラ所管省庁と連携し、具体的な取扱手順にのっとって情報共有体制を運営した。また、2018年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場などを通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。さらに、「「重要インフラの情報セキュリティ対策にかかる第４次行動計画」に基づく情報共有の手引書」を、関係機関と連携し、協働して策定し、情報共有の方法を明確化した。その結果、重要インフラ事業者等から内閣官房に対して269件の情報連絡が行われ、内閣官房からは38件の情報提供を行っている（参考：別添５－５）。

なお、2019年度第４四半期から新型コロナウイルス感染症の世界的な拡大が始まり、感染拡大防止策として、テレワークの活用が余儀なくされる状況となった。これまで、テレワークを導入していない重要インフラ事業者等が、テレワーク導入に伴うサイバーセキュリティリスクを的確に把握し、許容可能な程度に低減を行うための検討に着手し、緊急事態宣言が発出される前の2020年４月７日正午に注意喚起を発出するとともに、必要な問合せ対応を行った。また、2020年６月には、テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について事務連絡を発出した。

表１：重要インフラ事業者等との情報共有件数

年度	2015	2016	2017	2018	2019
重要インフラ事業者等から内閣官房への情報連絡件数	401 件	856 件	388 件	223 件	269 件
内閣官房からの情報提供件数	44 件	80 件	54 件	43 件	38 件

情報連絡の件数は、重要インフラ事業者等におけるセキュリティ対策の取組（Web・メール等の無害化等）が進んだこと等により減少していたが、自然災害やクラウドサービスで生じた障害が複数の重要インフラ事業者等のサービスに影響した事例の発生もあり、増加に転じた。内閣官房からの情報提供件数も含め、情報共有件数は依然として多い状況である。

大規模重要インフラサービス障害対応時の情報共有体制における各関係主体の役割については、平時から大規模重要インフラサービス障害対応時への体制切替えの手順について確認を行うとともに、大規模サイバー攻撃事態等対処訓練に際し、内閣官房や関係省庁との連携要領、関係主体の役割の在り方及び同手順の実効性に関する検証を実施した。

〇セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、14分野で19セプターが設置されている（参考：別添５－６）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど、重要インフラ防護の関係主体間における情報連携の結節点

としても機能している。また、一部の分野においては、ICT-ISAC、金融ISAC及び電力ISACの活発な活動など、自主的な分野内情報共有体制が確立されているほか、交通ISACの創設に向けた検討や、医療・水道分野における情報連携機能（ISAC）を検討するための調査などの取組も進んでいる。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2019年４月の総会で決定した活動方針に基づき、2019年度に、運営委員会（３回）、相互理解WG（２回）、情報収集WG（３回）、総会準備WG（２回）を開催し、セプター間の情報共有や事例紹介等、情報セキュリティ対策の強化に資する情報収集や知見の共有、及び、更なる活動活性化に向けた要望の聞き取り、その実現に向けた情報分析機能の高度化に関する討議検討を行った。また情報共有活動である「Webサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP）」を通じて、情報共有活動の更なる充実を図っている。

〇深刻度評価基準の策定に向けた取組

サイバーセキュリティ戦略本部が決定した発生したサービス障害が国民社会に与えた影響全体の深刻さを「事後に」評価するための基準の初版について、過去のサイバー攻撃事案に適用し、検証・評価を行った。

イ　今後の取組

重要インフラを取り巻く急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、効果的かつ迅速な情報共有に資するため、情報共有体制の改善に係る検討を行い、引き続き官民を挙げた情報共有体制の強化に取り組んでいく。

また、政府機関を含め、他の機関から独立した会議体であるセプターカウンシルについては、従来にも増して各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。更なるセプターカウンシルの自律的な運営体制とそれによる情報共有の活性化を目指し、内閣官房は運営及び活動に対する支援を継続していく。

(3)　障害対応体制の強化

＜目標＞
・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
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。

〇分野横断的演習

第４次行動計画に基づく具体的な取組の方向性として「重要インフラの防護能力の強化」、「オリパラを見据えた演習」、「官民・政府機関内連携」及び「演習参加形態の整理」に取り組んだ（参考：別添５－７）。

また、事前説明会において、「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」に基づく情報共有の手引書」について説明を実施し、情報共有の方法を明確化するよう、改善を図った。

2019年度は、全14分野が演習に参加し、参加者数は4,967に増加した。また、事後の意見交換会も実施し、分野間での情報共有を促進した。

表２　分野横断的演習参加者数の推移

年度	2016	2017	2018	2019
参加者数	2,084 名	2,647 名	3,077 名	4,967 名

2019 年度においては、重要インフラ全体での防護能力の底上げのため、見学会に代わり、演習参加のハードルが高いと感じている事業者向けに、「演習疑似体験プログラム」を実施し、９割弱の参加者から有意義であると回答を得た。

また、2018 年度分野横断的演習参加者へのフォローアップ調査の結果から、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（演習で得られた知見を踏まえ改善を実施又は検討している）と評価した参加者の割合は 93%となっている。

一方で、演習当日における他部門参加については、参加者募集時や事前説明会における資料に加え、事前説明会で参加を促したものの、その参加率は広報部門 37%、防災・危機管理部門 27%に留まっている。

なお、分野横断的演習を含め組織内外で実施する演習・訓練への参加割合は、73.6%であった。

〇セプター訓練

各重要インフラ分野における重要インフラ所管省庁及びセプターとの「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訓練を実施した（参考：別添５－８）。

表３：参加セプター・参加事業者等数の推移

年度	2016	2017	2018	2019
参加セプター	18	18	19	19

参加事業者等	2,020	2,106	2,005	1,958

実施に当たっては、重要インフラ事業者等に内閣官房から提供する情報が届いているかを事業者等に確認（疎通確認）する「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下で、その旨を報告する方式の採用等、より実態に即した訓練を実施すると共に、疎通確認が取れなかった事業者に対して各セプター事務局にてフォローを実施し、疎通確認がなぜできなかったのか、原因調査とその対策を実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られ、本訓練の有用性が確認された。

〇重要インフラ所管省庁等との連携

内閣官房が主催する分野横断的演習及びセプター訓練以外にも、重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習（CYDER）を実施した。また、金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）を実施した。これら演習と相互に連携・補完しつつ分野横断的演習等を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・向上を図った。

イ　今後の取組

第４次行動計画に基づき、分野横断的演習については、自職場参加の推奨等により演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図るとともに、東京2020大会に関わる重要インフラ事業者等が、大会開催時に想定されるより困難な脅威にも適切に対応できる状態に達することを目指す取組を行う。また、引き続き、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についても促進していく。

セプター訓練については、引き続きその機会を有効に活用し、「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自組織における被害状況を確認の上、「被害あり」という仮定の下でその旨を報告する方式の採用等を実施する。

(4)　リスクマネジメント及び対処態勢の整備

＜目標＞
・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
＜具体的な指標＞
・「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

ア　取組の進捗状況

リスクマネジメント及び対処態勢の整備に向け、以下の取組を実施した。

〇リスクマネジメントに対する支援

東京2020大会の関連事業者等がリスクアセスメントの際に利活用できるよう、内閣官房は「機能保証のためのリスクアセスメント・ガイドライン」を提供している。内閣官房では、Webサイトへの掲載や説明会での配布を通じて本ガイドラインの普及促進を図っており、2019年度におけるWebサイトの閲覧数は4830件、第５回説明会の参加者数は423人となっている。

また、同ガイドラインを重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加し、2018年４月に策定・公表した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」について、脅威及びリスク源の例として「法令・政策の不認識」を追加する改定を2019年５月に行った。さらに、重要インフラ事業者等への浸透を図るべく、重要インフラのセキュリティに関するカンファレンスなどで同手引書に関する説明を実施するとともに、各重要インフラ所管省庁へも説明を実施した。

〇対処態勢整備に対する支援

内閣官房では、重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき「対応及び対策の考慮事項」を「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５版）」において提示している。これらについて、重要インフラのセキュリティに関するカンファレンスや分野横断的演習の説明会等で、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に関する説明を実施した。

また、2017年12月に2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議セキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを設置し、東京2020大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において

運用したほか、サイバーセキュリティ対処調整センターの情報共有システムを使用した情報共有及びインシデント発生時の対処に係る訓練・演習を実施した。

〇リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動（運営委員会（３回）、相互理解WG（２回）、情報収集WG（３回）、総会準備WG（２回））を支援したほか、分野横断的演習に関しても、説明会や意見交換会等のほか、各重要インフラ分野が検討に参加する検討会（２回）及び有識者部会（２回）をそれぞれ開催した。また、東京2020大会に向けたリスクアセスメントの参加事業者等を対象に、説明会（15回）や情報交換会（１回）を開催し、大会に係るリスクコミュニケーション及び協議を支援した。

イ　今後の取組

これまでの取組の成果等を活用し、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整備の強化を促進するとともに、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べくモニタリング及びレビューの強化を推進していく。特に新型コロナウイルス感染症拡大防止対策に伴う、これまでと大きく異なる新たな生活様式の定着などに対応するための新たなデジタル技術の活用とサイバーセキュリティ対策を一体的に進めていくことが重要との観点から、これに伴う新たなリスクを的確に把握し、必要な対応を行っていくことに重点を置く。

また、セプターカウンシルや分野横断的演習等を通じて引き続き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を行うとともに、経営層を含む内部の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支援を実施する。

(5)　防護基盤の強化

＜目標＞
・「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の継続及びそれぞれの事業者の状況に合わせた取組の推進
・「広報公聴活動」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が広まり、技術動向に合わせた適切な対応が行われていること
・「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・啓発の充実
・「規格・標準及び参照すべき規程類の整備」については、整備した規程類の重要インフラ事業者等における利活用
＜具体的な指標＞
・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

ア　取組の進捗状況

防護基盤の強化に向け、以下の取組を実施した。

〇防護範囲の見直し

内閣官房はサイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しの検討を行った。

また、民間においても、ICT-ISAC、金融ISAC、電力ISAC等の活発な活動や交通ISACの創設に向けた検討など、サイバーセキュリティに関する協力関係拡大や充実を図る動きが進んだ。

加えて、総務省及び経済産業省において地域に根付いたセキュリティ・コミュニティの形成促進に取り組んだ。

〇広報広聴活動

内閣官房は、重要インフラ事業者等に対し、重要インフラニュースレターを24回発行し、サイバーセキュリティに関する政府機関、情報セキュリティ関係機関、海外機関等の取組を周知した。

また、重要インフラ防護に係る計画や指針、その他の関連情報をWebサイトに掲載し、重要インフラ事業者等に対して情報発信を行っており、計画や指針の改定を行った際は、掲載内容を更新するとともに、報道資料等を通じてその内容を周知している。重要インフラ事業者等を対象とした講演会やセミナーでは、第４次行動計画等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等を説明するとともに、分野横断的演習等の内閣官房の取組について紹介を行った。

〇国際連携

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、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者とのFace-to-Faceの会合等による緊密な関係性の構築に向けた取組を実施した。

二国間では、日英サイバー協議や日ウクライナサイバー協議における意見交換を行った。また、日米間、日独間、日豪間や日加間における政府間協議等を行った。

多国間及び地域間では、国際的な情報共有の枠組みであるIWWNを活用し、サイバー攻撃や脆弱性対応についての情報の継続的な共有を行っている。また、スイスで開催されたMeridian会合（2019年10月）や日ASEAN CIIPワークショップ（2019年７月）では、日本における官民連携の取組の紹介及び各国の取組等に関する意見交換を実施した。その他、分野横断的演習当日（2019年11月）に合わせて海外機関を対象とした演習見学会の開催や、「ASEAN地域のサイバーセキュリティ対策強化のための政策能力向上」研修（2020年１月）を通じて、日本における重要インフラ防護の取組を紹介した。

〇経営層への働きかけ

内閣官房において、経済産業省・情報処理推進機構（IPA）が作成している「サイバーセキュ

リティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。

さらに、経済産業省による電力分野における「電力サイバーセキュリティ対策会議」の開催等によって、経営層を交えたサイバーセキュリティの取組が着実に推進された。

〇人材育成等の推進

内閣官房は、「サイバーセキュリティ人材育成取組方針」（2018 年６月サイバーセキュリティ戦略本部報告）に基づく取組を推進した。重要インフラ事業者等については、情報セキュリティ人材の育成カリキュラム等による組織内の人材教育について、各関連施策を通じて普及啓発を行った。

〇規格・標準及び参照すべき規程類の整備

内閣官房は、重要インフラ防護に経理関係主体における安全基準等の整備等に資するよう、「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」等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラグループ　関係規程集」を作成し、2019年４月に発行した。

また、制御系機器・システムの第三者認証制度については、経済産業省において、CSSCを通じて、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。

イ　今後の取組

防護範囲の見直しについては、重要インフラを取り巻く環境の変化や社会的な要請を踏まえつつ、引き続き必要に応じ行っていく。

広報広聴活動については、Webサイト、重要インフラニュースレター、講演等を通じ、行動計画の取組を引き続き周知していくとともに、各重要インフラ分野の状況、技術動向等の情報収集に努め、随時施策に反映させる。

国際連携については、引き続き、重要インフラ所管省庁や情報セキュリティ関係機関と連携し、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。また、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。

経営層への働きかけについては、引き続き内閣官房及び重要インフラ所管省庁が連携し、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。

人材育成等の推進については、引き続き「サイバーセキュリティ人材育成取組方針」を踏まえ、重要インフラ事業者等の重要サービス等を防御するセキュリティ人材の育成カリキュラム等に

ついて普及啓発を行う。

規格・標準及び参照すべき規程類の整備については、重要インフラ防護に係る関連文書の改定等を継続的に調査し、必要な対応を行う。

３　第４次行動計画における各施策の取組内容

第4次行動計画 IV 章記載事項	取組内容
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。	・第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」を 2019 年５月に改定し、本指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。また、サイバーセキュリティを取り巻く情勢を踏まえ、安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」をあわせて追加した。同改定版については、NISC の Web サイトで公表した。
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。	・サイバーセキュリティを取り巻く情勢を踏まえ、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」を 2019 年５月に改定し、安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加した。同改定版については、NISC の Web サイトで公表した。
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。	・「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」に安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加し、各重要インフラ分野の安全基準等の継続的改善を支援した。
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。	・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況等について調査を実施した。同調査結果については、毎年度、重要インフラ専門調査会に報告するとともに、NISC の Web サイトで公表している。 ・各重要インフラ分野における制度的枠組みの現状について取りまとめのうえ、2019 年 10 月の重要インフラ専門調査会において報告するとともに、NISC の Web サイトで公表した。

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。	・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て、重要インフラの各分野の重要インフラ事業者等に対して情報セキュリティ対策の実施状況等について調査を実施した。また、重要インフラ事業者等に対してヒアリングを実施し、情報セキュリティ対策の取組事例を収集した。これらの調査結果については、毎年度、重要インフラ専門調査会に報告するとともに、NISC の Web サイトで公表している。
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。	・安全基準等の浸透状況等の調査結果については、各施策の改善に向けた取組の参考となるよう、重要インフラ専門調査会に報告するとともに、NISC の Web サイトで公表している。
(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。	・平時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、第４次行動計画に基づいた手順を確認し、手順の有効性について検証を実施した。
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。	・実施細目に基づき、重要インフラ所管省庁等や情報セキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及び情報セキュリティ関係機関へ情報提供を行った。(2019 年度　情報連絡 269 件、情報提供 38 件)
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。	・内閣官房とパートナーシップを締結している情報セキュリティ関係機関と情報を共有し、分析した上で重要インフラ事業者等へ情報提供を行った。また、同機関を始めとした情報セキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。
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。	・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するため、考え方の整理について引き続き検討した。
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。	・「「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」に基づく情報共有の手引書」を、関係機関と連携し、協働して策定し、情報共有の方法を明確化した。
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。	・重要インフラ所管省庁の協力を得て、2019 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
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。	・「「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」に基づく情報共有の手引書」を、関係機関と連携し、協働して策定し、情報共有の方法を明確化した。
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。	・セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。(2019 年度のセプターカウンシル会合の回数は延べ 11 回)
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。	・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構築に向けた検討を実施した。

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、IT障害発生時に適時適切な情報提供を実施。	・サイバー空間関連事業者との間での情報提供に関し、検討を行った。
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。	・新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
(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。	・重要インフラ所管省庁が実施する障害対応の演習・訓練に参加する等により最新の状況を把握した。 ・分野横断的演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った。
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。	・実施日時を予め明らかにしない方式の採用、通常の連絡手段が使用不可能な状況下における代替手段の使用可能性の確認、訓練参加者が単純に受信確認するだけではなくセプターによっては自社の被害状況をセプター事務局や重要インフラ所管省庁へ報告を行うなど、14 分野 19 セプターを対象に、より実態に即した訓練を実施した。
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。	・重要インフラ全体の防護能力の維持・向上を図る観点から、「より実践的な演習機会の提供」、「自職場参加の推進」、「重要インフラ全体での防護能力の底上げ」、「情報共有体制の実効性の向上」に重点をおきつつ、分野横断的演習を実施した。2019 年度は、4,967 名が演習に参加した。
④ 分野横断的演習の改善策検討。	・分野横断的演習が全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。また、シナリオ作成に際しては、東京 2020 大会を見据えた情報共有体制の確認やレピュテーションリスクにおける視点にも留意した。 ・事前説明会において、「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」に基づく情報共有の手引書」について説明を実施し、情報共有の方法を明確化するよう、改善を図った。
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。	・過去の事案から復旧手順及び IT-BCP 等の状況を把握し、その内容を踏まえた 2019 年度分野横断的演習の企画・運営について検討した。 ・演習実施前に、演習の検証課題を提示すること等により、演習参加効果を向上させるための取組を実施した。 ・演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者等が各社の早期復旧手順や IT-BCP 等の有効性や実効性を確認する機会を提供した。 ・事後の意見交換会として、討議事項にセキュリティに関する対策や課題、顔の見える関係等に関する意見交換を含む機会を提供した。
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)。	・演習の概要、目的等を整理し、「テキストブック」として参加事業者等のサブコントローラー向け、プレイヤー向け及びセプター事務局向けそれぞれの版を作成し、参加事業者等、セプター事務局及び重要インフラ所管省庁に提供した。 ・自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。演習参加のハードルが高いと感じている事業者向けの支援に資することを目的に、「演習疑似体験プログラム」を作成し、提供した。
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。	・重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、対外的に明確化した資料を作成し展開した。
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。	・複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者等における重要インフラ防護における人材育成の強化・充実に寄与する演習を実施した。
(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。	・東京 2020 大会の関連事業者等に対して、機能保証の考え方を踏まえたリスクアセスメントの実施手順を記載した「機能保証のためのリスクアセスメント・ガイドライン」を 2016 年度に整備・公表している。 ・2019 年度は、「機能保証のためのリスクアセスメント・ガイドライン」の内容を踏まえ、「2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明会（15 回）及び情報交換会（１回）を開催するなど、東京 2020 大会の開催・運営を支える重要サービスを提供する事業者等（322 組織）のリスクマネジメントを促進する取組を行った。
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。	・東京 2020 大会の関連事業者等がリスクアセスメントを円滑に行えるよう内閣官房が提供している「機能保証のための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リスクアセスメントに利活用できるよう一般化するとともに、内部監査等の観点を追加し、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」として 2018 年４月に策定・公表している。また、2019 年５月には、脅威及びリスク源の例として「法令・政策の不認識」を追加する改定を行った。
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。	・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供するため、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を NISC の Web サイトで公表している。また、内閣官房が過去に実施した調査の結果を NISC の Web サイトに引き続き掲載し、参考資料として提供している。
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。	・他施策の検討において活用すべく、重要インフラを取り巻く環境の変化に伴う新たなリスク源等について調査した。
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。	・「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５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」における内部ステークホルダー間のコミュニケーションの重要性についての記載を踏まえ、経営層と実務者間、関連部門間等におけるコミュニケーションを推進している。 東京 2020 大会に向けたリスクアセスメントの参加事業者等を対象に、説明会や情報交換会等を開催し、リスクアセスメントの演習等を通じて重要インフラ事業者等の内部におけるリスクコミュニケーションに資する情報の提供を行った。
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。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても、説明会や意見交換会をそれぞれ開催した。
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。	・「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５版）」において、事業継続計画及びコンティンジェンシープランの策定・改定における考慮事項を整理し、重要インフラ事業者等に提示している。 ・また、分野横断的演習においては、事業継続計画及びコンティンジェンシープランの実行性の検証に係る観点を取りまとめ、同演習の事前説明会において、重要インフラ事業者等に対し、これらの観点を踏まえた課題抽出と改善の重要性について説明を行った。
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。	・2017 年 12 月にセキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを設置し、東京 2020 大会までの大規模イベント（G20 大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用した。また、サイバーセキュリティ対処調整センターの情報共有システムを使用した情報共有及びインシデント発生時の対処に係る訓練・演習を実施した。
⑨ リスク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。	・「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」において、情報セキュリティ確保に係るリスクアセスメントの考え方や作業手順に関するフレームワークを整理し、重要インフラ事業等に提示している。
⑸「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。	・民間事業者における ISAC の活発な活動や分野横断的演習への参加者の増加等を通じて、セキュリティの取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。
②Web サイト、ニュースレター及び講演会を通じた広報を実施。	・NISC 重要インフラニュースレターを 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の情報セキュリティに関する公表情報の紹介等の広報を行った。 ・重要インフラ防護に係る計画や指針、その他の関連情報を Web サイトに掲載し、重要インフラ事業者等に対して情報発信を行っている。また、計画や指針の改定を行った際は、掲載内容を更新するとともに、報道資料等を通じてその内容を周知している。 ・重要インフラ事業者等を対象とした講演会やセミナーでは、「重要インフラの情報セキュリティ対策に係る第４次行動計画」をはじめとする重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等を説明するとともに、分野横断的演習等の内閣官房の取組について紹介を行った。
③往訪調査や勉強会・セミナー等を通じた広聴を実施。	・重要インフラ事業者等への往訪調査、セミナー等の機会を活用し、NISC の取組を紹介するとともに、情報セキュリティ政策等について意見交換を行った。
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。	・各国とのサイバーセキュリティに関する意見交換等の二国間会合、海外機関を対象とした分野横断的演習見学会の開催、Meridian 会合や IWWN での情報交換等の地域間・多国間における取組を通じ、国際連携を強化した。
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。	・二国間・地域間・多国間会合等を通じて得た知見を関係主体に提供した。
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。	・経済産業省・情報処理推進機構（IPA）が作成している「サイバーセキュリティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。 ・国土交通省と連携し、一般財団法人運輸総合研究所が主催する交通分野の経営層向けのサイバーセキュリティ対策に関する検討会への参画及び関連セミナーに対する後援を通じ、支援・協力を行った。
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。	・「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」等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラグループ　関係規程集」を作成・発行した。
⑧関連規格を整理、可視化。	・重要インフラ所管省庁及び重要インフラ事業者等の安全基準等の整備に資するよう、サイバーセキュリティ、リスクマネジメント等の重要インフラ防護に関係する規格を整理し、「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５版）」に参考文献として記載している。

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。	・第三者認証制度について、第４次行動計画における取組内容の検討を行い、第三者認証を受けた製品の活用を推進していくこととしており、重要インフラ事業者等に対する働きかけに向け、メーカーとの意見交換等を通じた状況把握を実施した。
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。	・経済産業省において、Society5.0 におけるセキュリティ対策の全体像を整理し、産業界が自らの対策に活用できるセキュリティ対策例をまとめた、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を 2019 年４月に策定した。 また、経済産業省において、経営者のリーダーシップの下でサイバーセキュリティリスクに対応するための仕組みの構築や委託先の状況把握等を行うべきであることが記載されている「サイバーセキュリティ経営ガイドライン」の普及啓発を行った。
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。	・総務省において、放送設備等のサイバーセキュリティ確保に関する省令改正を 2020 年３月に実施した。なお、2017 年８月に発生した大規模なインターネット障害を踏まえ、誤った経路制御情報やサイバー攻撃による障害等のネットワークを跨がって発生する障害に関する電気通信事業者間での情報共有等について、また、2018 年 12 月の携帯電話事業者からは確認できなかったソフトウェアに関する有効期限切れによる重大事故を踏まえ、ソフトウェアの信頼性向上対策について、「情報通信ネットワーク安全・信頼性基準」等を 2019 年３月に改正している。 ・厚生労働省において、「医療情報システムの安全管理に関するガイドライン」の改定を検討しており、2020 年３月に改定素案を策定した。また、水道施設におけるサイバーセキュリティ対策を強化する観点から、水道施設の技術的基準を定める省令の一部を改正した（2020 年４月施行）。 ・航空、空港、鉄道及び物流分野については、国土交通省において「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（第５版）改定版」の内容を包括した、各分野における「情報セキュリティ確保に係る安全ガイドライン」を作成している。 ・金融庁については、自らが安全基準等の策定主体とはなっていない。
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。	・重要インフラ所管省庁は、各重要インフラ分野における検証等に寄与するため、所管のガイドライン等を改定若しくは改定の検討を行った。
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。	・総務省において、平成 30 年度に報告された電気通信事故について、電気通信分野の専門家等で構成する電気通信事故検証会議による検証から得られた再発防止のための教訓等をとりまとめ、2019 年８月に報告書として公表し、関係事業者団体を通じて周知等を行った。
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。	・重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各重要インフラ分野における現状を把握した上で、調査の回答を行った。調査結果については、各施策の改善に向けた取組の参考となるよう、内閣官房が NISC の Web サイトで公表している。
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。	・重要インフラ所管省庁は、内閣官房に協力し、重要インフラ事業者等に対して情報セキュリティ対策の実施状況等について調査を実施し、安全基準等の浸透状況を確認した。調査結果については、各施策の改善に向けた取組の参考となるよう、内閣官房が NISC の Web サイトで公表している。 ・浸透状況等の調査として、金融庁では「金融機関等のシステムに関する動向及び安全対策実施状況調査」を通じて、所管の重要インフラ事業者等への調査を実施した。
(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。	・重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあったＩＴの不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。

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。	・重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ 所管省庁内のとりまとめ担当部局と各重要インフラ分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を立ち上げ、連携態勢の強化に取り組んだ。 ・総務省において、平成 30 年度に報告された電気通信事故について、電気通信分野の専門家等で構成する電気通信事故検証会議による検証から得られた再発防止のための教訓等をとりまとめ、2019 年 8 月に報告書として公表し、関係事業者団体を通じて周知等を行った。 ・厚生労働省において、医療機関におけるセキュリティ対策について、医療機関の実態や各国の状況等に関する知見を収集するとともに、情報共有の在り方について議論することを目的に、医療関係者との意見交換会を開催した。 ・国土交通省において、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」の運営形態等について事業者による検討・議論の支援を行った。また、2019 年 11 月に、事業者有志による一般社団法人交通 ISAC 設立準備委員会が設置されたことから、2020 年 4 月に法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った。
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。	・重要インフラ所管省庁は、①の情報共有体制のもと、重要インフラ事業者等からのＩＴ障害等に係る報告があった場合は、速やかに内閣官房へ情報連絡を行った。
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。	・重要インフラ所管省庁は、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・重要インフラ所管省庁は、セプターカウンシル総会及び幹事会にオブザーバーとして出席し、意見交換、支援等を行った。 ・2019 年 4 月に空港セプターがセプターカウンシルに加入した。
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。	・重要インフラ所管省庁は、セプターカウンシル総会及び幹事会にオブザーバーとして出席し、意見交換、支援等を行った。
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	・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を立ち上げ、連携態勢の強化に取り組んだ。 ・厚労省において、医療機器のサイバーセキュリティの確保に関するガイダンスについて（通知）を医療機器の製造販売業者向けの講習会にて周知し、製造販売業者が行うべきサイバーセキュリティへの取組及び対応を具体的に提示した。
⑶「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。	・重要インフラ所管省庁を通じた情報共有体制の確認として、2019 年 10 月から 2020 年 1 月までの間に、全 19 セプターに対するセプター訓練を実施した。
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。	・重要インフラ所管省庁は、2019 年度分野横断的演習検討会、拡大作業部会 等に出席し、演習を実施する上での方法や検証課題等についての検討を行った。
③ 分野横断的演習への参加。	・重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員などが、2019 年 11 月に実施された分野横断的演習に参加した。
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。	・重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2019 年度分野横断的演習への参加を促し、全体で過去最多の 4,967 名の参加者を得た。
⑤ 分野横断的演習の改善策検討への協力。	・重要インフラ所管省庁は、2019 年度分野横断的演習の事後調査に回答するとともに、演習における対応記録を作成し翌年度以降の改善策の検討材料として内閣官房へ提出した。また、翌年度以降も視野に入れた課題、方向性についての議論を行う検討会に出席した。

⑥ 必要に応じて、分野横断的演習成果を施策へ活用。	・重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。
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。	・金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）を実施した。 ・重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。
(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。	・重要インフラ所管省庁において、内閣官房と連携し、東京 2020 大会の関連事業者を対象にリスクアセスメントを実施した。 ・総務省においては、内閣官房および東京 2020 大会に関係する地方公共団体と連携し、東京 2020 大会に係るリスクアセスメントの取組を実施した。
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。	・重要インフラ所管省庁は、内閣官房と協力し、「機能保証に向けたリスクアセスメント・ガイドライン」等を踏まえ、東京 2020 大会の関連事業者等のリスクアセスメントを推進している。
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。	・重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・内閣官房が実施した「ＥＵ諸国及び米国における情報共有体制に関する調査」等については、重要インフラ所管省庁において今後、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として活用されている。
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。	・重要インフラ所管省庁において、重要インフラ事業者等の情報セキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。
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。	・金融庁において、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2018 年 10 月公表）に基づく取組みにおいて把握した実態や共通する課題等について、「金融分野のサイバーセキュリティレポート」として公表した。また、クラウドの活用事例（グッドプラクティス）や適切なリスク管理の在り方等について外部委託調査を実施し、2019 年６月に「クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書」を公表した。
(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。	・総務省及び経済産業省を中心として、日・ASEAN サイバーセキュリティ政策会議等をはじめとした会合の開催等を行うなどにより国際連携の強化を図った。
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。	・総務省及び経済産業省を中心として、国際連携にて得た知見を、講演等を通じて国内の関係主体に提供した。

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。	・経済産業省において、2020 年 2 月に「電力サイバーセキュリティ対策会議」を開催し、電力分野におけるサイバーセキュリティの取組の更なる推進を図った。 ・国土交通省は、内閣官房と連携し、一般財団法人運輸総合研究所が主催する交通分野の経営層向けのサイバーセキュリティ対策に関する検討会への参画及び関連セミナーに対する後援を通じ、支援・協力を行った。
④ 内閣官房と連携し、関連規格を整理、可視化。	・重要インフラ所管省庁は、内閣官房と連携し、国内外で策定される重要インフラ防護に関係する規格について、情報を収集した。
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。	・国土交通省において、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」の運営形態等について事業者による検討・議論の支援を行った。また、2019 年 11 月に、事業者有志による一般社団法人交通 ISAC 設立準備委員会が設置されたことから、2020 年 4 月に法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った。 ・総務省は、一般社団法人 ICT-ISAC が中心となり実施しているサイバー攻撃に関する情報を収集・分析・共有するための基盤の高度化を推進するなど、関係事業者等における情報共有の取組を強化した。 ・総務省及び経済産業省において、地域に根付いたセキュリティ・コミュニティの形成促進に取り組んだ。
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。	・重要インフラ所管省庁は、分野横断的演習等に参加し、情報セキュリティ人材の育成を支援した。 ・総務省において、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。
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。	・経済産業省において、制御系機器・システムの第三者認証制度について、CSSC を通じ、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。
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。	・情報セキュリティ関係省庁及び内閣官房において、相互に情報共有窓口を明らかにすることにより、情報共有体制の運用を行った。
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。	・情報セキュリティ関係省庁から、標的型メール攻撃に利用された添付ファイルや URL リンク情報等について内閣官房に情報連絡を実施した。あわせて、攻撃手法及び復旧手法に関する情報等の収集を行い、事業者と共有した。
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。	・情報セキュリティ関係省庁とセプターカウンシル等（セプターカウンシル相互理解 WG）との間で意見交換等を実施し、相互理解の促進や信頼関係の深化を図った。
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。	・2019 年度において大規模重要インフラサービス障害に該当する事案は発生していないが、事案対処省庁等は、大規模サイバー攻撃事態等対処に備え、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。
② 被災情報、テロ関連情報等の収集。	・「サイバー攻撃特別捜査隊」を中心として、各都道府県警察においてサイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。 ・警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。
③ 内閣官房に対して、必要に応じて情報連絡の実施。	・事案対処省庁及び防災関係府省庁は、内閣官房と必要に応じて情報共有を実施した。

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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報を Web サイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
⑵「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。	・事案対処省庁は、2019 年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、シナリオ、実施方法、検証課題等についての検討が行われた。
② 分野横断的演習の改善策検討への協力。	・事案対処省庁は、2019 年度分野横断的演習検討会及び拡大作業部会にオブザーバーとして出席するとともに、当該検討会等においては、演習の総括、次年度に向けた課題等についての検討が行われた。
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。	・事案対処省庁は、分野横断的演習と重要インフラ防護に資するそれ以外の演習・訓練を相互に視察し、演習・訓練担当者間の連携強化に努めた。 ・都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。
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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報を Web サイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

2020 年度（サイバーセキュリティ 2021　抜粋）

別添５－２　重要インフラに関する取組の進捗状況

「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「第４次行動計画」という。）に基づく取組について、2020年度の進捗状況の確認・検証結果を報告する。

１　第４次行動計画

(1)　概要

第４次行動計画は、「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月）」、「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）」、「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（2009年２月、2012年４月改定）」及び「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（2014年５月、2015年５月改訂）」に続いて、我が国の重要インフラの情報セキュリティ対策として位置付けられるものであり、2017年４月にサイバーセキュリティ戦略本部で決定された。その後、2018年７月に重要インフラ分野として新たに「空港分野」を追加し、2020年１月には各重要インフラ分野の安全基準の名称の変更や関係法令の改正に伴う記載の変更を踏まえた改定を実施している。

第４次行動計画においては、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」及び「防護基盤の強化」の５つの施策を掲げ、内閣官房と重要インフラ所管省庁等が協力し、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っていくこととしている（参考：別添５－１）。

(2)　各施策の実施状況

第４次行動計画においては、機能保証の考え方を踏まえ、サイバー攻撃や自然災害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目的としている。

2020年度は、2019年度に引き続き、同計画に従って、５つの施策それぞれについて取組を進めた。各施策における取組は次節以降に示すが、新型コロナウイルス感染症の対応として、テレワークを採用する組織が増加している状況など、サイバーセキュリティを取り巻く環境の変化を踏まえつつ、各施策を着実に推進した。また、これらの５つの施策に基づく取組のほか、第４次行動計画について適切な評価を行うため、個別施策の指標では捉えられない側面を補完的に調査することを目的に、重要インフラサービス障害等の事例についての現地調査である補完調査を2019年度に引き続き実施した（参考：別添５－９）。

(3)　今後の取組

重要インフラサービスの安全かつ持続的な提供の実現に向け、今後も内閣官房と重要インフラ所管省庁等が連携し、第４次行動計画に基づく積極的な取組を引き続き推進するとともに、東京2020大会後に策定が予定されている新たなサイバーセキュリティ戦略の検討内容を踏まえながら、次期行動計画の検討を行っていく。

２　第４次行動計画の各施策における取組

本節では、第４次行動計画の各施策における取組の実施状況について述べる。また、第４次行動計画のⅤ.1.3及びⅤ.2.3に示す各施策における目標及び具体的な指標に対応する内容も併せて記載する。

(1)　安全基準等の整備及び浸透

＜目標＞
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

安全基準等の整備及び浸透に向け、以下の取組を実施した。

〇安全基準等の継続的な改善

内閣官房は、重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況を調査し、安全基準等の継続的な改善状況を取りまとめた。2020年度は、指針や関係法令・ガイドラインの改定等を契機として、各重要インフラ分野において計８件の安全基準等の改定が実施されたことを確認した。（参考：別添５－３）。

〇安全基準等の浸透

内閣官房は、重要インフラ所管省庁等の協力を得て、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実施状況等を調査した。2020年度は2,162者から回答があり、今回の調査結果を「ベースラインとなる情報セキュリティ対策」と「先導的な情報セキュリティ対策」に整理し、それぞれの実施状況を確認したところ、2019年度の調査と比較してそれらに取り組んでいる事業者の割合は多くの項目で増加しており、改善傾向が継続していることが確認された（参考：別添５－４）。

イ　今後の取組

第４次行動計画に基づき、安全基準等策定指針の整備等を通じて各重要インフラ分野の安全基準等の継続的な改善を引き続き推進するとともに、重要インフラ所管省庁等と連携し、安全基準等の浸透を図っていく。

(2) 情報共有体制の強化

＜目標＞
・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。
＜具体的な指標＞
・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

ア 取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。

○官民の情報共有体制

第４次行動計画に基づき、重要インフラ所管省庁と連携し、具体的な取扱手順にのっとって情報共有体制を運営した。また、2019年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場などを通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。さらに、関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラの情報セキュリティ対策にかかる第４次行動計画」に基づく情報共有の手引書」を、活用しつつ、情報共有を行った。その結果、重要インフラ事業者等から内閣官房に対して309件の情報連絡が行われ、内閣官房からは64件の情報提供を行っている（参考：別添５－５）。

なお、2020年に入ってから新型コロナウイルス感染症の世界的な拡大が始まり、感染拡大防止策として、テレワークの活用が余儀なくされる状況となった。これまで、テレワークを導入していない重要インフラ事業者等が、テレワーク導入に伴うサイバーセキュリティリスクを的確に把握し、許容可能な程度に低減を行うよう、緊急事態宣言が発出される前の2020年４月７日正午に注意喚起を発出するとともに、必要な問合せ対応を行った。また、2020年６月には、テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について事務連絡を発出した。この後も、こうした取組が継続的に求められることを見据え、数度にわたり注意喚起を発出した。さらに、2021年１月の再度の緊急事態宣言を受けて、テレワーク時のセキュリティ対策を意識するよう改めて注意喚起を発出した。この間、これまで以上に積極的に注意喚起を発出してきており、重要で可能なものはウェブサイトに掲載して広く周知した。

表１：重要インフラ事業者等との情報共有件数

年度	2016	2017	2018	2019	2020
重要インフラ事業者等から内閣官房への情報連絡件数	856 件	388 件	223 件	269 件	309 件
内閣官房からの情報提供件数	80 件	54 件	43 件	38 件	64 件

情報連絡の件数は、重要インフラ事業者等におけるセキュリティ対策の取組（Web・メール等の無害化等）が進んだこと等により減少していたが、自然災害やクラウドサービスで生じた障害、VPN を始めとした重要機器の脆弱性が複数の重要インフラ事業者等のサービスに影響した事例の発生もあり、増加に転じた。内閣官房からの情報提供件数も含め、情報共有件数は依然として多い状況である。

大規模重要インフラサービス障害対応時の情報共有体制における各関係主体の役割については、平時から大規模重要インフラサービス障害対応時への体制切替えの手順について確認を行うとともに、大規模サイバー攻撃事態等対処訓練に際し、内閣官房や関係省庁との連携要領、関係主体の役割の在り方及び同手順の実効性に関する検証を実施した。

〇セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、14分野で19セプターが設置されている（参考：別添５－６）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど、重要インフラ防護の関係主体間における情報連携の結節点としても機能している。また、一部の分野においては、ICT-ISAC、金融ISAC、交通ISAC及び電力ISACの活発な活動など、自主的な分野内情報共有体制が確立されているほか、医療・水道分野における情報連携機能（ISAC）を検討するための調査などの取組も進んでいる。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2020年４月の総会で決定した活動方針に基づき、2020年度に、運営委員会（４回）、情報収集WG（４回）、総会準備WG（１回）を開催し、セプター間の情報共有や事例紹介等、情報セキュリティ対策の強化に資する情報収集や知見の共有、及び、更なる活動活性化に向けた要望の聞き取り、その実現に向けた情報分析機能の高度化に関する討議検討を行った。なお、新型コロナウイルス感染症拡大防止の観点から、相互理解WGは、開催できなかった。また情報共有活動である「ウェブサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP）」を通じて、情報共有活動の更なる充実を図っている。

〇深刻度評価基準の策定に向けた取組

サイバーセキュリティ戦略本部が決定した発生したサービス障害が国民社会に与えた影響全体の深刻さを「事後に」評価するための基準の初版について、過去のサイバー攻撃事案に適用し、検証・評価を行った。

イ　今後の取組

重要インフラを取り巻く急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、効果的かつ迅速な情報共有に資するため、脅威の動向や環境変化に柔軟に対応できるよう検討を行い、引き続き官民を挙げた情報共有体制の強化に取り組んでいく。

また、政府機関を含め、他の機関から独立した会議体であるセプターカウンシルについては、従来にも増して各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。更なるセプターカウンシルの自律的な運営体制とそれによる情報共有の活性化を目指し、内閣官房は運営及び活動に対する支援を継続していく。

(3)　障害対応体制の強化

＜目標＞
・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
・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
＜具体的な指標＞
・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

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。

○分野横断的演習

第４次行動計画に基づく重要インフラ防護能力の維持・向上に資することを目的として分野横断的演習を実施した。2020年度は「テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応」、「東京2020大会時における対応」を特徴として取り組んだ。（参考：別添５－７）。

また、事前説明会において、「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」の浸透を図るため、演習における事前準備・演習当日の行動・事後の改善で留意すべき点等について、第４次行動計画に記載されているサイバーセキュリティ対策のPDCAサイクルに従って見直しを行うことを推奨した。

2020年度は、全14分野が演習に参加し、参加者数は4,721名であった。

表２　分野横断的演習参加者数の推移

年度	2017	2018	2019	2020
参加者数	2,647 名	3,077 名	4,967 名	4,721 名

2020 年度は、テレワークの活用の急速な進展を踏まえ、テレワーク環境からの参加を 25%の事業者等が実施した。また、東京 2020 大会を支える重要サービス事業者に該当する事業者等のうち、62%が東京 2020 大会を想定した体制で参加した。

さらに、2019 年度分野横断的演習参加者へのフォローアップ調査の結果によれば、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（演習で得られた知見を踏まえ改善を実施又は検討している）と評価した参加者の割合は 98%となっている。

一方で、重要インフラ全体での防護能力の底上げのため、2019 年度に引き続き、演習参加のハードルが高いと感じている事業者向けに、「演習疑似体験プログラム」を実施し、82%の参加者から有意義であると回答を得た。

なお、「安全基準等の浸透状況等に関する調査」によれば、 分野横断的演習以外の演習・訓練を含め、組織内外で実施する演習・訓練への参加割合は、76.4%であった。

〇セプター訓練

各重要インフラ分野における重要インフラ所管省庁及びセプターとの「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訓練を実施した（参考：別添５－８）。

表３：参加セプター・参加事業者等数の推移

年度	2017	2018	2019	2020
参加セプター	18	19	19	19
参加事業者等	2,106	2,005	1,958	1,995

実施に当たっては、重要インフラ事業者等に内閣官房から提供する情報が届いているかを事業者等に確認（疎通確認）する「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下で、その旨を報告する方式の採用等、より実態に即した訓練を実施するとともに、疎通確認が取れなかった事業者に対して各セプター事務局にてフォローを実施し、疎通確認がなぜできなかったのか、原因調査とその対策を実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られ、本訓練の有用性が確認された。

〇重要インフラ所管省庁等との連携

内閣官房が主催する分野横断的演習及びセプター訓練以外にも、重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、実践的サイバー防御演習（CYDER）を実施した。また、金融庁では金融業界

全体のサイバーセキュリティの底上げを図ることを目的に、業界横断的なサイバーセキュリティ演習（Delta WallⅤ）を実施した。これら演習と相互に連携・補完しつつ分野横断的演習等を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・向上を図った。

イ　今後の取組

第４次行動計画に基づき、分野横断的演習については、さらなる行動計画の浸透の場として活用するとともに、演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図り、より困難な脅威にも適切に対応できる状態に達することを目指す取組を行う。また、引き続き、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についても促進していく。

セプター訓練については、現在運用している情報共有体制を活用し、所管省庁、セプター及び重要インフラ事業者の各段階で疎通確認状況を把握するとともに、「「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」に基づく情報共有の手引書」を活用し、レビューを行うことにより疎通確認率の向上、体制強化等の適切な改善に資する。

(4)　リスクマネジメント及び対処態勢の整備

＜目標＞
・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
＜具体的な指標＞
・「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（ウェブ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

ア　取組の進捗状況

リスクマネジメント及び対処態勢の整備に向け、以下の取組を実施した。

○リスクマネジメントに対する支援

東京2020大会の関連事業者等がリスクアセスメントの際に利活用できるよう、内閣官房は「機能保証のためのリスクアセスメント・ガイドライン」を提供している。内閣官房では、ウェブサイトへの掲載等での配布を通じて本ガイドラインの普及促進を図っており、2020年度におけるウェブサイトの閲覧数は3116件となっている。また、その内容を踏まえ、「2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明資料の提供、質疑応答等を実施するなど、東京2020大会の開催・運営を支える重要サービスを提供する事業者等（297組織）のリスクマネジメントを促進する取組を行った。

さらに、同ガイドラインを重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点や、脅威及びリスク源の例として「法令・政策の不認識」を追加した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を提供しており、2020年度におけるウェブサイトの閲覧数は2021件となっている。

〇対処態勢整備に対する支援

内閣官房では、重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき「対応及び対策の考慮事項」を「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５版）」において提示している。これらについて、重要インフラのセキュリティに関するカンファレンスや分野横断的演習の説明会等で、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に関する説明を実施した。

また、2017年12月に2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議セキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを設置し、東京2020大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用したほか、サイバーセキュリティ対処調整センターの情報共有システムを使用した情報共有及びインシデント発生時の対処に係る訓練・演習を実施した。

〇リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動（運営委員会（４回）、情報収集WG（２回）、総会準備WG（１回））を支援したほか、分野横断的演習に関しても、説明会等のほか、各重要インフラ分野が検討に参加する検討会（２回）及び有識者部会（２回）をそれぞれ開催した。また、東京2020大会に向けたリスクアセスメントの参加事業者等を対象に、取組に係る説明資料の提供、質疑応答等を実施し、大会に係るリスクコミュニケーション及び協議を支援した。

イ　今後の取組

これまでの取組の成果等を活用し、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整備の強化を促進する。特にリスクアセスメントでは自律的な取組が重要であることから、内閣官房は、それを導く知見を提供することに重点を置く。

新型コロナウイルス感染症拡大防止対策に伴うテレワークの導入や新たなデジタル技術の浸透によって、これまでにないセキュリティリスクが顕在化している。したがって、新たなデジタル技術の活用とサイバーセキュリティ対策を一体的に進めることが求められるため、これに伴

うリスクの洗い出しや必要な対応を実施することを引き続き推進していく。

また、セプターカウンシルや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を行うとともに、経営層を含む内部の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支援を継続して実施する。

(5) 防護基盤の強化

＜目標＞
・「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の継続及びそれぞれの事業者の状況に合わせた取組の推進
・「広報公聴活動」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が広まり、技術動向に合わせた適切な対応が行われていること
・「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・啓発の充実
・「規格・標準及び参照すべき規程類の整備」については、整備した規程類の重要インフラ事業者等における利活用
＜具体的な指標＞
・ウェブサイト、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

ア 取組の進捗状況

防護基盤の強化に向け、以下の取組を実施した。

○防護範囲の見直し

内閣官房はサイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しの検討を行った。

また、民間においても、ICT-ISAC、金融ISAC、電力ISAC等の活発な活動や交通ISACの設立など、サイバーセキュリティに関する協力関係拡大や充実を図る動きが進んだ。

加えて、経済産業省において、2020年11月に設立された「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」と連携し、大企業と中小企業を含めた産業界のサイバーセキュリティ対策を促進した。

○広報広聴活動

内閣官房は、重要インフラ事業者等に対し、重要インフラニュースレターを24回発行し、サイバーセキュリティに関する政府機関、情報セキュリティ関係機関、海外機関等の取組を周知した。

また、ウェブサイト上やSNSでの情報セキュリティに関する脅威・警戒情報の発信や、重要インフラ関係規定集を更新しウェブサイト上で公表する等、効果的な広報チャネルを通じた情報発信を行った。重要インフラ事業者等を対象とした講演会やセミナーでは、第４次行動計画等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等

を説明するとともに、分野横断的演習等の内閣官房の取組について紹介を行った。

〇国際連携

内閣官房は、重要インフラ所管省庁、情報セキュリティ関係省庁及び情報セキュリティ関係機関と連携し、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者とのオンラインでの会合等による緊密な関係性の構築に向けた取組を実施した。

二国間では、日米間、日英間、日独間や日豪間等における政府間協議等を行った。

多国間及び地域間では、国際的な情報共有の枠組みであるIWWNを活用し、サイバー攻撃や脆弱性対応についての情報の継続的な共有を行っている。また、2021年２月には、NISCが主催した「国際サイバーセキュリティワークショップ・演習」において、2020年12月に実施した分野横断的演習の取組内容を海外機関へ広く紹介した。

〇経営層への働きかけ

内閣官房において、経済産業省・情報処理推進機構（IPA）が作成している「サイバーセキュリティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。

また、経済産業省から企業経営者向けに、最近のサイバー攻撃の状況を踏まえた注意喚起を発出するなど、経営層を交えたサイバーセキュリティの取組が着実に推進された。

〇人材育成等の推進

内閣官房は、サイバーセキュリティ２０２０や「サイバーセキュリティ人材育成取組方針」（2018 年６月サイバーセキュリティ戦略本部報告）に基づく取組を推進した。重要インフラ事業者等については、情報セキュリティ人材の育成カリキュラム等による組織内の人材教育について、各関連施策を通じて普及啓発を行った。

〇規格・標準及び参照すべき規程類の整備

内閣官房は、重要インフラ防護に係る関係主体における安全基準等の整備等に資するよう、「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」等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラグループ　関係規程集」を2020年８月に更新し、ウェブサイト上で公表した。

また、制御系機器・システムの第三者認証制度については、経済産業省において、CSSCを通じて、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。

イ　今後の取組

防護範囲の見直しについては、重要インフラを取り巻く環境の変化や社会的な要請を踏まえつつ、引き続き必要に応じ行っていく。

広報広聴活動については、ウェブサイト、SNS、重要インフラニュースレター、講演等を通じ、行動計画の取組を引き続き周知していくとともに、各重要インフラ分野の状況、技術動向等の情報収集に努め、随時施策に反映させる。

国際連携については、引き続き、重要インフラ所管省庁、情報セキュリティ関係省庁及び情報セキュリティ関係機関と連携し、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。また、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。

経営層への働きかけについては、引き続き内閣官房及び重要インフラ所管省庁が連携し、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。

人材育成等の推進については、引き続き「サイバーセキュリティ人材育成取組方針」を踏まえ、重要インフラ事業者等の重要サービス等を防御するセキュリティ人材の育成カリキュラム等について普及啓発を行う。

規格・標準及び参照すべき規程類の整備については、重要インフラ防護に係る関連文書の改定等を継続的に調査し、必要な対応を行う。

３　第４次行動計画における各施策の取組内容

第4次行動計画 IV 章記載事項	取組内容
1. 内閣官房の施策	
⑴「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。	・サイバーセキュリティを取り巻く情勢を踏まえ、指針において安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加する等の改定を行っており、この改定の内容を NISC のウェブサイトで公表するとともに、「内閣サイバーセキュリティセンター 重要インフラグループ　関係規程集」（電子版）として新たに取りまとめ、同サイト上に掲載した。
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。	・サイバーセキュリティを取り巻く情勢を踏まえ、指針において安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加する等の改定を行っており、この改定の内容を NISC のウェブサイトで公表するとともに、「内閣サイバーセキュリティセンター 重要インフラグループ　関係規程集」（電子版）として新たに取りまとめ、同サイト上に掲載した。
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。	・「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」等を通じて、各重要インフラ分野の安全基準等の継続的改善を支援している。各重要インフラ分野においては、指針や関係法令・ガイドラインの改定等を契機として、安全基準等の継続的な改善が着実に実施されている。
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。	・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況等について調査を実施した。同調査結果については、毎年度、重要インフラ専門調査会に報告するとともに、NISC のウェブサイトで公表している。 ・2020 年度は、指針や関係法令・ガイドラインの改定等を契機として、各重要インフラ分野において計８件の安全基準等の改定が実施された。 ・重要インフラの各分野における制度的枠組みの改善状況について、進捗があった重要インフラ所管省庁から重要インフラ専門調査会において報告を受けるとともに、同内容を NISC のウェブサイトで公表した。

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。	・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て、重要インフラの各分野の重要インフラ事業者等に対して情報セキュリティ対策の実施状況等について調査を実施した。また、重要インフラ事業者等に対する情報セキュリティ対策の取組事例の収集については、新型コロナウイルス感染症の感染拡大防止のため、インターネットを活用して Web 会議等により実施した。これらの調査結果については、毎年度、重要インフラ専門調査会に報告するとともに、NISC のウェブサイトで公表している。
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。	・安全基準等の浸透状況等の調査結果については、重要インフラ所管省庁における各施策の改善に向けた取組の参考となるよう、重要インフラ専門調査会で報告して NISC のウェブサイトで公表するとともに、内閣官房においては次期行動計画の検討に活用した。
⑵「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。	・平時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、第４次行動計画に基づいた手順を確認し、手順の有効性について検証を実施した。
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。	・実施細目に基づき、重要インフラ所管省庁等や情報セキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及び情報セキュリティ関係機関へ情報提供を行った。（2020 年度　情報連絡 309 件、情報提供 64 件）
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。	・内閣官房とパートナーシップを締結している情報セキュリティ関係機関と情報を共有し、分析した上で重要インフラ事業者等へ情報提供を行った。また、同機関を始めとした情報セキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。
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。	・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するため、考え方の整理について引き続き検討した。
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。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「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」に基づく情報共有の手引書」を活用しつつ、情報共有を行った。
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。	・重要インフラ所管省庁の協力を得て、2020 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
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。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「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」に基づく情報共有の手引書」を活用しつつ、情報共有を行った。

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。	・セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。(2020 年度のセプターカウンシル会合の回数は延べ 7 回)
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。	・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構築に向けた検討を実施した。
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、IT障害発生時に適時適切な情報提供を実施。	・サイバー空間関連事業者との間での情報連携体制を構築し、重要インフラ事業者等に向けた注意喚起等の情報提供に活用した。
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。	・新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
⑶「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。	・重要インフラ所管省庁が実施する障害対応の演習・訓練に参加する等により最新の状況を把握した。 ・分野横断的演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った
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。	・実施日時を予め明らかにしない方式の採用、通常の連絡手段が使用不可能な状況下における代替手段の使用可能性の確認、訓練参加者が単純に受信確認するだけではなくセプターによっては自社の被害状況をセプター事務局や重要インフラ所管省庁へ報告を行うなど、14 分野 19 セプターを対象に、より実態に即した訓練を実施した。
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。	・第４次行動計画に基づく重要インフラ防護能力の維持・向上に資することに重点をおきつつ、分野横断的演習を実施した。2020 年度は 4,721 名が演習に参加した。
④ 分野横断的演習の改善策検討。	・分野横断的演習が全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。また、シナリオ作成に際しては、テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応、東京 2020 大会を見据えた情報共有体制の確認やレピュテーションリスクにおける視点にも留意した。 ・事前説明会において、「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」の浸透を図るため、演習における事前準備・演習当日の行動・事後の改善で留意すべき点等について、第４次行動計画に記載されているサイバーセキュリティ対策の PDCA サイクルに従って見直しを行うことを推奨した。
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。	・過去の事案から復旧手順及び IT-BCP 等の状況を把握し、その内容を踏まえた 2020 年度分野横断的演習の企画・運営について検討した。 ・演習実施前に、演習の検証課題を提示すること等により、演習参加効果を向上させるための取組を実施した。 ・演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者等が各社の早期復旧手順や IT-BCP 等の有効性や実効性を確認する機会を提供した。

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)。	・自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。 ・演習参加のハードルが高いと感じている事業者向けの支援に資することを目的に、「演習疑似体験プログラム」を作成し、提供した。
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。	・重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、分野横断的演習の関係者に資料を共有した。
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。	・複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者等における重要インフラ防護における人材育成の強化・充実に寄与する演習を実施した。
(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。	・東京 2020 大会の関連事業者等に対して、機能保証の考え方を踏まえたリスクアセスメントの実施手順を記載した「機能保証のためのリスクアセスメント・ガイドライン」を 2016 年度に整備・公表している。 ・2020 年度は、「機能保証のためのリスクアセスメント・ガイドライン」の内容を踏まえ、「2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明資料の提供、質疑応答等を実施するなど、東京 2020 大会の開催・運営を支える重要サービスを提供する事業者等（297 組織）のリスクマネジメントを促進する取組を行った。
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。	・東京 2020 大会の関連事業者等がリスクアセスメントを円滑に行えるよう内閣官房が提供している「機能保証のための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リスクアセスメントに利活用できるよう一般化するとともに、内部監査等の観点を追加し、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」として 2018 年４月に策定・公表している。また、2019 年５月には、脅威及びリスク源の例として「法令・政策の不認識」を追加する改定を行い、NISC のウェブサイトで公表している。
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。	・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供するため、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を NISC のウェブサイトで公表している。また、内閣官房が過去に実施した調査の結果を NISC のウェブサイトに引き続き掲載し、参考資料として提供している。
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。	・他施策の検討において活用すべく、これまでに実施した調査・分析の結果は NISC のウェブサイトに掲載している。 ・2020 年度往訪調査において、事業者に対して情報セキュリティに関するリスクへの対処について調査した。

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。	・「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５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」における内部ステークホルダー間のコミュニケーションの重要性についての記載を踏まえ、経営層と実務者間、関連部門間等におけるコミュニケーションを推進している。 ・東京 2020 大会に向けたリスクアセスメントの参加事業者等を対象に、説明資料の提供、質疑応答等を実施し、重要インフラ事業者等の内部におけるリスクコミュニケーションに資する情報の提供を行った。
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。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても、説明会を開催した。
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。	・「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５版）」において、事業継続計画及びコンティンジェンシープランの策定・改定における考慮事項を整理し、重要インフラ事業者等に提示している。 ・また、分野横断的演習においては、事業継続計画及びコンティンジェンシープランの実行性の検証に係る観点を取りまとめ、同演習の事前説明会において、重要インフラ事業者等に対し、これらの観点を踏まえた課題抽出と改善の重要性について説明を行った。
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。	・2017 年 12 月にセキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを設置し、東京 2020 大会までの大規模イベント（G20 大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用した。また、サイバーセキュリティ対処調整センターの情報共有システムを使用した情報共有及びインシデント発生時の対処に係る訓練・演習を実施した。
⑨ リスク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。	・「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」において、情報セキュリティ確保に係るリスクアセスメントの考え方や作業手順に関するフレームワークを整理し、重要インフラ事業等に提示している。
⑸「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。	・民間事業者における ISAC の活発な活動や分野横断的演習への参加を通じて、セキュリティ対策の取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。
②ウェブサイト、ニュースレター及び講演会を通じた広報を実施。	・NISC 重要インフラニュースレターを 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の情報セキュリティに関する公表情報の紹介等の広報を行った。 ・重要インフラ防護に係る計画や指針、その他の関連情報をウェブサイトに掲載し、重要インフラ事業者等に対して情報発信を行っている。また、公式サイトや SNS を通じて注意・警戒情報を発信し、セキュリティ対策の取組の一層の強化を図った。 ・重要インフラ事業者等を対象とした講演会やセミナーでは、「重要インフラの情報セキュリティ対策に係る第４次行動計画」をはじめとする重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等を説明するとともに、分野横断的演習等の内閣官房の取組について紹介を行った。

③往訪調査や勉強会・セミナー等を通じた広聴を実施。	・重要インフラ事業者等への往訪調査、セミナー等の機会を活用し、NISC の取組を紹介するとともに、情報セキュリティ政策等について意見交換を行った。
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。	・各国とのサイバーセキュリティに関する意見交換等の二国間会合、国際的なワークショップへの参加や IWWN での情報交換等の地域間・多国間における取組を通じ、国際連携を強化した。
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。	・二国間・地域間・多国間会合等を通じて得た知見を関係主体に提供した。
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。	・経済産業省・情報処理推進機構（IPA）が作成している「サイバーセキュリティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。
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。	・「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」等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラグループ 関係規程集」を更新し、ウェブサイト上で公表した。
⑧関連規格を整理、可視化。	・国内外で策定される重要インフラ防護に関係する規格について情報収集を実施した。
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。	・重要インフラ防護に関係する第三者認証制度の動向等について情報収集を実施し、認証を受けた製品活用の推進に向けた検討を行った。
2. 重要インフラ所管省庁の施策	
⑴「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。	・経済産業省において、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」の社会実装を推進するために、フィジカル空間とサイバー空間のつながりの信頼性の確保の考え方を整理した「IoT セキュリティ・セーフティ・フレームワーク」を 2020 年 11 月に策定した。 また、経済産業省において、サイバーセキュリティ経営ガイドラインを講演会等で周知し、普及啓発を促進。ダウンロード数は 2021 年 1 月末時点で 10 万件を超えた。加えて、可視化ツール V1.0 開発のため、β 版ベースでユーザ企業及び投資家等ステークホルダーへのヒアリングを実施。その結果を V1.0 の企画としてまとめ、V1.0 開発に着手した。

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。	・重要インフラ所管省庁では、各重要インフラを取り巻く情勢を踏まえ、必要に応じて安全基準等の分析・検証や安全基準等の見直しを行っており、2020年度は主に以下の改定が実施された。 ・政府・行政サービス分野に関し、総務省は、2020年12月に地方自治体分野における安全基準等である「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定を行った。 ・情報通信分野に関し、総務省は、通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方及び災害に強い通信インフラの維持・管理方策について検討した結果を取りまとめた情報通信審議会からの一部答申を踏まえ、令和２年６月に「情報通信ネットワーク・安全・信頼性基準」の改定を行った。 ・医療分野に関し、厚生労働省は、「医療情報システムの安全管理に関するガイドライン」を令和３年１月29日付で第5.1版に改定し、クラウド化の拡大を念頭において、クラウドの概要、クラウド利用に係る責任分界についての追記等を行った。 ・また、水道分野に関し、厚生労働省は、令和２年４月に施行された「水道施設の技術的基準を定める省令の一部を改正する省令」（厚生労働省令第59号）において、水道事業の施設基準としてサイバーセキュリティ対策を位置づけた。 ・航空、空港、鉄道及び物流分野に関し、国土交通省は、各分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。 ・なお、金融庁については、自らが安全基準等の策定主体とはなっていない。
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。	・重要インフラ所管省庁は、各重要インフラ分野における検証等に寄与するため、所管のガイドライン等を改定若しくは改定の検討を行った。
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。	・総務省において、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を改定し、地方公共団体における安全基準の整備等を支援した。 ・厚生労働省において、医療関係者向けに、医療分野におけるサイバーセキュリティ対策の強化を図ることを目的として研修を実施した。
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。	・重要インフラ所管省庁は、所管の各重要インフラ分野における安全基準等の改善状況を取りまとめ、内閣官房に報告した。
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。	・重要インフラ所管省庁は、内閣官房に協力し、重要インフラ事業者等に対して情報セキュリティ対策の実施状況等について調査を実施し、安全基準等の浸透状況を確認した。調査結果については、各施策の改善に向けた取組の参考となるよう、内閣官房がNISCのウェブサイトで公表している。 ・なお、金融庁では金融情報システムセンター（FISC）を通じ、浸透状況等の調査として所管の重要インフラ事業者等への調査を実施した。
⑵「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。	・重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあったＩＴの不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。

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。	・重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ 所管省庁内のとりまとめ担当部局と各重要インフラ分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2020 年度は演習等の実施により連携態勢の更なる強化に取り組んだ。 ・総務省においては、地方公共団体の情報セキュリティ担当者の連絡先等をとりまとめており、担当者の異動時には最新の情報を報告する体制をとることで、綿密な情報共有体制を維持している。 ・総務省において、令和元年度に報告された電気通信事故については、電気通信分野の専門家等で構成する電気通信事故検証会議による検証から得られた再発防止のための教訓等をとりまとめ、令和２年９月に報告書として公表し、関係事業者団体を通じて周知等を行った。また、 有識者及び電気通信分野の事業者団体で構成する事故報告・検証制度等タスクフォースを設置し、事故報告・検証制度等の在り方について議論を行っている。 ・厚生労働省において、医療機関間のサイバーセキュリティに関する情報共有・相談体制の検討に向けて、医療機関同士が情報共有ツールを活用して情報交換を行う試行を令和 3 年１～3 月に実施した。医療分野のサイバーセキュリティ対策に関する意見交換においては医療機関のみならず、製薬メーカーの参画も得られた。 ・国土交通省において、法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」が、2020 年４月に一般社団法人として設立され、2021 年３月現在 79 会員まで増加している。
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。	・重要インフラ所管省庁は、①の情報共有体制のもと、重要インフラ事業者等からのＩＴ障害等に係る報告があった場合は、速やかに内閣官房へ情報連絡を行った。
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。	・重要インフラ所管省庁は、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・重要インフラ所管省庁は、セプターカウンシル総会及び幹事会にオブザーバーとして出席し、意見交換、支援等を行った。
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。	・重要インフラ所管省庁は、セプターカウンシル総会等にオブザーバーとして出席し、意見交換、支援等を行った。
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	・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2020 年度は演習等の実施により連携態勢の更なる強化に取り組んだ。
⑶「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。	・重要インフラ所管省庁を通じた情報共有体制の確認として、2020 年 9 月に、全 19 セプターに対するセプター訓練を実施した。
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。	・重要インフラ所管省庁は、2020 年度分野横断的演習検討会、拡大作業部会等に出席し、演習を実施する上での方法や検証課題等についての検討を行った。
③ 分野横断的演習への参加。	・重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員などが、2020 年 12 月に実施された分野横断的演習に参加した。
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。	・重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2020 年度分野横断的演習への参加を促し、4721 名の参加者を得た。

⑤ 分野横断的演習の改善策検討への協力。	・重要インフラ所管省庁は、2020 年度分野横断的演習の事後調査に回答するとともに、演習における対応記録を作成し翌年度以降の改善策の検討材料として内閣官房へ提出した。
⑥ 必要に応じて、分野横断的演習成果を施策へ活用。	・重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。
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。	・金融庁では金融業界全体のサイバーセキュリティの底上げを図ることを目的に、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅴ）を実施した。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2020 年度に各関係団体間で大規模インシデント発生時を想定した演習を実施した。 ・重要インフラ事業者等を対象とした演習として、総務省においては、情報システム担当者等のサイバー攻撃への対処能力向上のため、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。 ・総務省において、地方公共団体に対して、国立研究開発法人情報通信研究機構（NICT）の実践的サイバー防御演習「CYDER」の積極的受講を推進した。
⑷「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。	・重要インフラ所管省庁において、内閣官房と連携し、東京 2020 大会の関連事業者を対象にリスクアセスメントを実施した。
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。	・重要インフラ所管省庁は、NISC が作成したリスクアセスメント・ガイドラインや手引書等の浸透状況を把握するための調査に協力した。
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。	・重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・総務省においては、今後、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として「ＥＵ諸国及び米国における情報共有体制に関する調査」の活用が予定されている。
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。	・重要インフラ所管省庁において、重要インフラ事業者等の情報セキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。
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。	・金融庁において、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2018 年 10 月公表）に基づく取組みにおいて把握した実態や共通する課題等について、2020 年６月に「金融分野のサイバーセキュリティレポート」を公表した。また、サイバー空間の脅威を迅速に把握し、金融システム全体のセキュリティ向上等に取り組むため、2020 年７月に「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」を公表した。
⑸「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。	・総務省及び経済産業省を中心として、日・ASEAN サイバーセキュリティ政策会議等をはじめとした会合の開催等を行うなどにより国際連携の強化を図った。
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。	・総務省及び経済産業省を中心として、国際連携にて得た知見を、講演等を通じて国内の関係主体に提供した
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。	・経済産業省において、2020 年 12 月、企業経営者向けに最近のサイバー攻撃の状況を踏まえた注意喚起を発出し、経営層を交えたサイバーセキュリティ対策の更なる推進を図った。また、2019 年度に引き続き「第２回電力サイバーセキュリティ対策会議」を開催し、電力分野におけるトップマネジメントレベルで、サイバーセキュリティ対策の取組の確認を行った。
④ 内閣官房と連携し、関連規格を整理、可視化。	・重要インフラ所管省庁は、内閣官房と連携し、国内外で策定される重要インフラ防護に関係する規格について、情報を収集した。
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。	・国土交通省において、法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」が、2020 年４月に一般社団法人として設立され、2021 年３月現在 79 会員まで増加している。 ・経済産業省において、大企業と中小企業がともにサイバーセキュリティ対策を推進するために産業界が 2020 年 11 月に設立した「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」と連携し、産業界のセキュリティ対策を促進した。 ・総務省は、一般社団法人 ICT-ISAC が中心となり実施しているサイバー攻撃に関する情報を収集・分析・共有するための基盤の高度化を推進するなど、関係事業者等における情報共有の取組を強化した。 ・総務省及び経済産業省において、地域に根付いたセキュリティ・コミュニティの形成促進に取り組んだ。
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。	・重要インフラ所管省庁は、分野横断的演習等に参加し、情報セキュリティ人材の育成を支援した。 ・総務省において、地方公共団体に対して、国立研究開発法人情報通信研究機構（NICT）の実践的サイバー防御演習「CYDER」の積極的受講を推進した。
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。	・経済産業省において、制御系機器・システムの第三者認証制度について、CSSC を通じ、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。
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。	・情報セキュリティ関係省庁及び内閣官房において、相互に情報共有窓口を明らかにすることにより、情報共有体制の運用を行った。
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。	・情報セキュリティ関係省庁から、標的型メール攻撃に利用された添付ファイルや URL リンク情報等について内閣官房に情報連絡を実施した。
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。	・情報セキュリティ関係省庁とセプターカウンシル等との間で意見交換等を実施し、相互理解の促進や信頼関係の深化を図った。
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。	・2020 年度において大規模重要インフラサービス障害に該当する事案は発生していないが、事案対処省庁等は、大規模サイバー攻撃事態等対処に備え、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。

② 被災情報、テロ関連情報等の収集。	・「サイバー攻撃特別捜査隊」を中心として、各都道府県警察においてサイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。 ・警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。
③ 内閣官房に対して、必要に応じて情報連絡の実施。	**・事案対処省庁及び防災関係府省庁は、内閣官房と必要に応じて情報共有を実施した。**
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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
⑵「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。	・事案対処省庁は、2020 年度分野横断的演習検討会にオブザーバーとして出席するとともに、当該検討会等においては、シナリオ、実施方法、検証課題等についての検討が行われた。
② 分野横断的演習の改善策検討への協力。	・事案対処省庁は、2020 年度分野横断的演習検討会にオブザーバーとして出席するとともに、当該検討会等においては、演習の総括、次年度に向けた課題等についての検討が行われた。
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。	・事案対処省庁は、分野横断的演習と重要インフラ防護に資するそれ以外の演習・訓練に関して、演習・訓練担当者間の連携強化に努めた。 ・都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。
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。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

資料５－４

サイバーセキュリティ関係法令 Q&A ハンドブック

Ver1.0

（抜粋）

令和２年３月２日

内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）

「サイバーセキュリティ関係法令 Q&A ハンドブック」の公開に当たって

この度、関係者の自発的かつ精力的な努力と相互の協力により、「サイバーセキュリティ関係法令 Q&A ハンドブック」をお届けできるのは、作業に当たった全員の喜びであります。また私個人にとっても、サイバーセキュリティ戦略本部員を辞した後に、このサブワーキンググループ（サイバーセキュリティ戦略本部の普及啓発・人材育成専門調査会の中のサブワーキンググループとなります）の主査を仰せつかい、ボランティア精神に富んだ皆さんとご一緒できたのは、格別の思い出となりました。

この企画のアイディアは、副主査を務められた岡村久道氏の経験と発案に多くを負っています。同氏は、経済産業省が平成 21 年にとりまとめた「情報セキュリティ関連法令の要求事項集」（以下「要求事項集」）の編集を手掛けられ、その後、現在までの間にサイバーセキュリティ基本法をはじめとしたセキュリティに関係する重要な法律が多くなってきたことを踏まえて、その発展形として今回のような資料集刊行の必要性を強く主張されました。なぜなら、ドッグ・イヤーの比喩に従えば、この間に 70 人間イヤー相当の時間が経過したわけで、事実「想定外」の事例が多数発生していたからです。

私も岡村さんとは幾分違った観点から、このような資料集の必要性を感じていました。というのも、学者として「情報法」という法分野が存在し得ることを直感し、幾分でもその体系化に寄与することを志していましたので、「情報セキュリティ六法」のようなものができること自体が、この分野の学問の発展に資するものだと思ったからです。また実務的に言えば、官僚の皆さんの仕事は「法の原則に基づいて」行われねばなりませんから、多くの仕事は「〇〇六法」のような法令集と首っ引きでなされるのが通例です。サイバーセキュリティの重要性が増した現在では、「六法」のようなものを机上において作業する時代になったのではないか、と考えたのです。

かくして出来上がった本書は、作成側からすれば、次の 3 つの特徴を持っていると自負しています。まず、サイバーセキュリティに関連すると思われる法令を、なるべく広範に網羅するよう努めたことです。参考にした「要求事項集」は主として経済産業省所管の範囲をカバーするものでしたが、本書は関係省庁の協力を得て幅広く関連事項を収録しています。

第 2 点は、これらの法令の最新版を集めたことです。IT の展開はドッグ・イヤーと呼ばれるほど早いので、法的な対応もそれに従わざるを得ません。そこで、法律など正規の手続きを経たハード・ローよりも、ソフト・ローと呼ばれるガイドラインや技術標準などが、事実上の規範となっている場合があります。ところが、これらの規範はごく少数の関係者は知っているとしても、一般にはいつ改定されたかが分かりにくい宿命があります。本書の編集作業により、とりあえず現時点での最新情報をお届けできたかと思います。

第3点は、ソフト・ローを収録したことから当然の要請ともいえますが、「法令」だけでなく、その「解説」をも重視したことです。そのためには「解説者」が必要になりますので、サブワーキンググループの下に更に「タスクフォース」を設け、新進気鋭の弁護士を中心に、なるべく客観的な記述に努めてもらいました。参加して下さった方々は多忙にもかかわらず、「縁の下の力持ち」的な仕事をボランティア精神で遂行されたことに感謝しています。

このようにして、ようやく形を整えるに至ったドキュメントを見ると、ある種の感慨を覚えます。しかし、これが終点ではありません。本書に掲載したものは、現時点で解釈まで含めて一定の方向性が出ている法令を主な対象としており、重要性が高いとしても未確定な部分があるものについては、次回以降の改訂に際しての課題となると考えています。

サイバーセキュリティの実務に携わり、本書の主たる利用者である方々には、ぜひ「改訂版」へのご要望を伝えていただければ、と思います。また、学者として本書を利用する私たちは、これを素材にして、「情報法」や「サイバーセキュリティ法」の体系化を試みていければ、と思います。

参加者一同、「現時点では精一杯努力した」という満足感はありますが、「これで満点」などとは到底思えません。また、仮に現時点で満足度が高いにしても、ドッグ・イヤーの時代にはすぐに時代遅れになる恐れがあります。今後、利用者の皆さんの後押しをいただいて、「六法」が毎年発行されるのと同じように改訂を重ねていくことができれば、「叩き台」である初版に関与した私たちの努力も、報われるのではないかと期待しています。

令和2年2月26日
関係者を代表して　林　紘一郎

前文

サイバー空間と実空間の一体化、事業のグローバル化等に伴い、サイバーセキュリティに関係する法令が増えており、事業者が適切なサイバーセキュリティ対策を講じていく上で、サイバーセキュリティに関係する法令の知識が不可欠である。

一方で、サイバーセキュリティの関係法令は体系的に存在するものではなく、これらを取りまとめ、解説を施した資料は少ない。経済産業省が平成 21 年に「情報セキュリティ関連法令の要求事項集」（以下「要求事項集」という。）[1]をとりまとめているが、その後サイバーセキュリティに関係する法令として、サイバーセキュリティ基本法等が新たに成立し、また、個人情報の保護に関する法律や不正競争防止法が改正される等、法制度に関する状況が変化している。

このような状況を踏まえ、サイバーセキュリティ戦略（平成 30 年 7 月 27 日閣議決定）においては、企業がサイバーセキュリティ対策の実施において参照すべき法制度に関する整理を行うこととされ、サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会は、平成 30 年 10 月 10 日、サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ（以下「サブ WG」という。）を設置した（オブザーバーとして関係省庁も参加）。

サブ WG は、平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、近年増加する情報の取扱いに関する法令や、情勢の変化、技術の進展に伴い生じている法的課題等について、平易な表記による解説を付して取りまとめた関係法令集を作成することを目的とし、林紘一郎名誉教授（情報セキュリティ大学院大学）を主査、岡村久道弁護士（英知法律事務所・京都大学）を副主査として検討を進め、要求事項集をベースとしつつ、必要に応じて内容をアップデートし、また、新たに検討が必要となる法的論点を加え、解説を付すこととした。この方針を踏まえた具体的な執筆に際しては、サブ WG の下部にタスクフォースを設置し、必要に応じて有識者等にヒアリングを実施した。当該ドラフトはサブ WG に提出され、サブ WG において検討を加え、本書を取りまとめた。

読み手としては、経営層、企業においてサイバーセキュリティ対策を企画、立案し、経営層に必要な説明や助言を行う「戦略マネジメント層」及び法令対応を行う法務部門を想定し、現場で広く利用頂けるよう可能な限り平易な表現を心がけた。

本書は、基本的に、一般的なものと考えられる公刊物の内容を踏まえて作成したものであるが、個別具体的な事例において現行法がどのように解釈・適用されるかは、それぞれの状況を勘案したうえで、最終的には裁判所において判断されるものであることは言うまでもない。

いずれにせよ、本書が企業実務上の参考として、効率的・効果的なサイバーセキュリティ対策・法令遵守の促進への一助になることを期待している。

なお、本書については、サイバーセキュリティに関する法令について今後も大きな変化が予想されることを踏まえ、継続的に必要な論点の検討を行いつつ、必要に応じ改訂・拡充等を行っていく予定である。

---

[1] 平成 21 年 6 月にまとめた後に検討を行った平成 23 年 4 月版のものも参考として公開されている。

Q3 内部統制システムとサイバーセキュリティとの関係

内部統制システムとサイバーセキュリティの関係はどのようなものか。

タグ：会社法、内部統制システム、リスク管理体制、事業継続計画（BCP）、グループ・ガバナンス・システム、CSIRT、モニタリング

１．概要

会社におけるサイバーセキュリティに関する体制は、その会社の内部統制システムの一部といえる。取締役の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各会社が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各会社において決定されるべきである。また、取締役会は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定することでもよい。

２．解説

（１）内部統制システムの概念とサイバーセキュリティ

後掲の各裁判例によれば、内部統制システムとは「会社が営む事業の規模、特性等に応じたリスク管理体制」と定義される。大会社、監査等委員会設置会社及び指名委員会等設置会社においては、取締役会（取締役）は、内部統制システムの構築に関する事項を決定しなければならないこととされており（会社法第 348 条第 3 項第 4 号、第 4 項、第 362 条第 4 項第 6 号、第 5 項、第 399 条の 13 第 1 項第 1 号ハ、第 416 条第 1 項第 1 号ホ）、それ以外の会社であっても、その事情いかんによっては、内部統制システムの構築に関する事項を決定しない場合に、そのことが、取締役の善管注意義務、忠実義務違反となり得る場合がある。会社の事業継続にとってサイバーインシデントが及ぼす影響が看過できない状況下においては、この「リスク」の中に、サイバーセキュリティに関するリスクが含まれ得るため、リスク管理体制の構築には、サイバーセキュリティを確保する体制の構築が含まれ得る。

同体制の構築にあたっては、サイバーインシデントを未然に防止するための方策や方針（セキュリティポリシー）の策定に加え、事業継続に関する悪影響を最小化するための事業継続計画（BCP[1]）を策定する[2]ことも考えられる

---

[1] Business Continuity Plan の略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCP のうち情報（通信）システムについて記載を詳細化したものが IT-BCP（ICT-BCP）である（サイバーセキュリティ 2019・356 頁参照。

[2] サイバーセキュリティ基本法におけるサイバーセキュリティの定義には、情報システムの安全性および信頼性の確保のために必要な措置も含まれる（Q1 参照）ため、同法におけるサイ

このように、サイバーセキュリティを確保する体制は、内部統制システムに含まれ得るといえる。

（２）会社法の内部統制システム

会社法は、大会社、監査等委員会設置会社及び指名委員会等設置会社について、内部統制システムの構築の基本方針を取締役又は取締役会が決定すべきことを明文の義務としている（会社法第 348 条第 3 項第 4 号・4 項、第 362 条第 4 項第 6 号・5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ）。これらの規定は、善管注意義務から要求される内部統制システム構築の基本方針決定義務を念のために明文にしたものである。決定すべき内部統制システムは、類型に分けて列挙されている。その中には、①法令等遵守体制、②損失危険管理体制、③情報保存管理体制、④効率性確保体制、⑤企業集団内部統制システム等が含まれる（前記引用の会社法各条及び会社法施行規則第 98 条第 1 項、第 2 項、第 100 条第 1 項、第 110 条の 4 第 2 項、第 112 条第 2 項）。サイバーセキュリティに関するリスクが、会社に重大な損失をもたらす危険のある場合には、②の損失危険管理体制（損失の危険の管理に関する規程その他の体制をいう）に含まれる。

また、サイバーセキュリティインシデントに伴って漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）の対象となる情報の保存と管理に関するセキュリティは③の情報保存管理体制（取締役の職務の執行に係る情報の保存及び管理に関する体制をいう）の問題ともなり得るほか、個人情報保護法など法令が情報の安全管理を要求しているような場合には、①の法令等遵守体制（取締役及び使用人の職務の執行が法令及び定款に適合することを確保するための体制をいう）の問題にもなることがある。

この点に関して、持株会社の子会社から顧客等の個人情報の管理について委託を受けていた持株会社の他の子会社の再委託先の従業員が当該個人情報を不正に取得して売却した情報流出事故に関して、持株会社の株主が、内部統制システムの構築等に係る取締役としての善管注意義務違反があったなどと主張して、持株会社の取締役に対し、会社法第 423 条第 1 項に基づく損害賠償金を支払うよう求めた株主代表訴訟において、広島高裁は、持株会社及びその子会社からなる「グループにおいては、事業会社経営管理規程等の各種規程が整備され、それらに基づき、人事や事業計画への関与、グループ全体のリスク評価と検討、各種報告の聴取等を通じた一定の経営管理をし、法令遵守を期していたものであるから、企業集団としての内部統制システムがひととおり構築され、その運用がなされていたといえる。そして、会社法は内部統制システムの在り方に関して一義的な内容を定めているものではなく、あるべき内部統制の水準は実務慣行により定まると解され、その具体的内容については当該会社ないし企業グループの事業内容や規模、経営状態等を踏まえつつ取締役がそ

バーセキュリティの確保の観点からは、サイバー攻撃への対応等はもちろん、天災等への対応も含めた情報システム運用継続計画（IT-BCP）を策定することも考えられる。

の裁量に基づいて判断すべきものと解される」等と判示した[3]。

（３）取締役会が決定すべき事項

会社法は、「業務の適正を確保するための体制の整備」について取締役会が決すべきものとしているが、当該体制の具体的な在り方は、一義的に定まるものではなく、各会社が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各会社において決定されるべき事項である。

また、取締役会が決めるのは「目標の設定、目標達成のために必要な内部組織及び権限、内部組織間の連絡方法、是正すべき事実が生じた場合の是正方法等に関する重要な事項（要綱・大綱）[4]」でよいと解されている。

サイバーセキュリティに関していえば、当該体制の整備としては、「情報セキュリティ規程」「個人情報保護規程」等の規程の整備や、CSIRT（Computer Security Incident Response Team）などのサイバーセキュリティを含めたリスク管理を担当する部署の構築等が考えられる。

（４）企業集団における内部統制システム

会社法は、内部統制システムについて、会社単位での構築に加え、当該会社並びにその親会社及び子会社から成る企業集団（グループ）単位での構築を規定しており（会社法第 348 条第 3 項第 4 号、第 362 条第 4 項第 6 号、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ、及び会社法施行規則第 98 条第 1 項第 5 号、第 100 条第 1 項第 5 号、第 110 条の 4 第 2 項第 5 号、第 112 条第 2 項第 5 号など）、すなわち、親会社の取締役（会）は、グループ全体の内部統制システムの構築に関する当該親会社における基本方針を決定することが求められており、子会社における①親会社への報告体制、②損失危機管理体制、③効率性確保体制、④法令等遵守体制などを含め、業務執行の中でその構築・運用が適切に行われているかを監視・監督する義務を負っている。

サイバーセキュリティに関していえば、親会社の取締役会において、子会社を含めたグループ全体を考慮に入れたセキュリティ対策について検討されるべきである[5]。

（５）内部統制システムのモニタリング

取締役の善管注意義務には、上述のとおり内部統制システムの構築だけでなく、構築した後も環境変化を踏まえて内部統制システムが適切に機能しているか否かを継続的にモニタリングし、適時にアップデートすることも、その内容として含まれていると考えられている。平成 26 年の会社法改正の際には、その旨を明確化する趣旨からも、内部統制システムの運

[3] 広島高判令和元年 10 月 18 日判例集未登載
[4] 相澤哲ほか『論点解説新・会社法』（商事法務、平成 18 年）335 頁
[5] グループガイドライン 92 頁

用状況の概要を、事業報告の記載内容とすることが定められた（会社法施行規則第 118 条 2 号）。

内部統制システムの運用状況をモニタリングする手段として、取締役（会）は内部監査の結果を活用することも考えられる（サイバーセキュリティに関する内部監査の役割については Q5 を参照されたい。）。

（６）金融商品取引法の内部統制

金融商品取引法（昭和 23 年法律第 25 号）は、上場会社等について、財務報告に係る内部統制の有効性の評価に関する報告書（内部統制報告書）の作成及び開示を義務付けている。

３．参考資料（法令・ガイドラインなど）

・会社法第 348 条第 3 項第 4 号・第 4 項、第 362 条第 4 項第 6 号・第 5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ
・会社法施行規則第 98 条第 1 項・第 2 項、第 100 条第 1 項、第 110 条の 4 第 2 項、第 112 条第 2 項、第 118 条第 2 号
・金融商品取引法第 24 条の 4 の 4、第 25 条第 1 項第 6 号、第 193 条の 2 第 2 項
・グループガイドライン

４．裁判例

内部統制システムの整備義務に関して、
・大阪地判平成 12 年 9 月 20 日判時 1721 号 3 頁・判タ 1047 号 86 頁
・金沢地判平成 15 年 10 月 6 日判時 1898 号 145 頁・労判 867 号 61 頁
・名古屋高金沢支判平成 17 年 5 月 18 日判時 1898 号 130 頁・労判 905 号 52 頁
・東京地判平成 16 年 12 月 16 日判時 1888 号 3 頁・判タ 1174 号 150 頁
・東京高判平成 20 年 5 月 21 日資料版商事法務 291 号 116 頁
・大阪地判平成 16 年 12 月 22 日判時 1892 号 108 頁・判タ 1172 号 271 頁
・大阪高判平成 18 年 6 月 9 日判時 1979 号 115 頁・判タ 1214 号 115 頁
・最判平成 21 年 7 月 9 日判時 2055 号 147 頁
・広島高判令和元年 10 月 18 日判例集未登載

Q4 サイバーセキュリティと取締役等の責任

会社が保有する情報の漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）によって会社又は第三者に損害が生じた場合、会社の役員（取締役・監査役）は、どのような責任を問われ得るか。

タグ：会社法、個情法、損害賠償責任

１．概要

取締役（会）が決定したサイバーセキュリティ体制が、当該会社の規模や業務内容に鑑みて適切でなかったため、会社が保有する情報が漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）（以下本項において「漏えい等」という。）されたことにより会社に損害が生じた場合、体制の決定に関与した取締役は、会社に対して、任務懈怠（けたい）に基づく損害賠償責任（会社法第 423 条第 1 項）を問われ得る。また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、取締役（・監査役）がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である[1]。

個人情報の漏えい等によって第三者が損害を被ったような場合、取締役・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

他方、サイバーセキュリティインシデントに起因して、会社が保有する情報の漏えい等が生じた場合、取締役は、原則として、刑事責任を負うことはない。ただし、個人データに関して、その安全管理措置を怠ったため漏えい等が発生した場合など個情法の規定に違反した場合は、個情委による勧告・命令の対象になるほか、命令に違反した場合には、刑事罰の対象となり得る。

２．解説

（１）会社法上の責任

取締役は、内部統制システムの構築義務の一環として、サイバーセキュリティ体制を構築する義務を負うと解される（Q3 参照）。

取締役（会）が決定した内部統制システムが、当該会社の規模や業務内容に鑑みて、株式会社の業務の適正を確保するために不十分であった場合には、その体制の決定に関与した取締役は、善管注意義務（会社法第 330 条・民法第 644 条）違反に基づく任務懈怠責任（会社法第 423 条第 1 項）を問われ得る[2]。

また、内部統制システムは適切なものであったが、その内部統制システムが実際には遵守

[1] 相澤哲ほか『論点解説新・会社法』（商事法務、平成 18 年）335 頁
[2] 相澤哲ほか・同、及び大阪地判平成 12 年 9 月 20 日判タ 1047 号 86 頁

されておらず、取締役（・監査役）がそれを知り、又は注意すれば知ることができたにも関わらず、それを長期間放置しているような場合にも、善管注意義務違反に基づく任務懈怠責任を問われ得る[3]。

以上のとおり、サイバーセキュリティ体制の構築又はその運用に欠陥があり、情報の漏えい等によって会社に損害が生じたときは、取締役（・監査役）は責任を負うことがあり得る。

また、取締役（・監査役）が職務を行うについて悪意又は重過失があったときは、それにより第三者に生じた損害についても賠償責任を負う（会社法第 429 条第 1 項）。

したがって、取締役（・監査役）が、悪意・重過失により、適切なサイバーセキュリティ体制を構築せず、又は体制が適切に運用されていないのにこれを是正するのを怠り、個人情報の漏えい等によって第三者が損害を被ったときは、取締役（・監査役）は、当該第三者に対しても責任を負うことがあり得る。

（２）その他留意すべき法令

サイバーセキュリティインシデントに起因して、会社が保有する情報の漏えい等が生じた場合、取締役は原則として、刑事責任を負うことはない。ただし、会社が保有する情報のうち個人情報に関する漏えい等が生じた場合には、個情法が問題となる[4]。

個情法は、個人情報取扱事業者に対して個人情報（又は個人データ）の取扱いについての義務を規定するところ、例えば、個人情報取扱事業者である会社が、個人データに係る安全管理措置（個情法第 20 条）を怠った結果、個人データが漏えいした場合は、個情委による勧告・命令の対象となる（同法第 42 条）。この命令に違反をした者に対しては、6 月以下の懲役または 30 万円以下の罰金が科され（同法第 84 条）、法人の代表者、使用人その他の従事者（以下本項において「代表者等」という。）が、その法人の業務に関して命令違反行為を行った場合は、当該行為者を罰するほか、法人も罰金刑の対象となる（同法第 87 条第 1 項）。

したがって、個人情報の漏えい等に関して、個情法に定める義務違反がある場合には、代表者等は、刑事罰の対象となり得る。

３．参考資料（法令・ガイドラインなど）

・会社法第 330 条、第 423 条第 1 項、第 429 条第 1 項
・民法第 644 条
・個情法第 20 条、第 42 条、第 84 条、第 87 条第 1 項

４．裁判例

特になし

---

[3] 相澤哲ほか・同
[4] 個人データの漏えいがあった場合に望ましい行動について Q50 参照。

Q5 サイバーセキュリティ体制の適切性を担保するための監査等

社内のサイバーセキュリティ体制が適切であることを担保するためにどのような方策を実施することが考えられるか。

タグ：会社法、内部監査、情報セキュリティ監査、システム監査、情報開示、内部通報、CSIRT

１．概要

社内のサイバーセキュリティ体制が適切であることを担保するための方策としては、内部監査、情報セキュリティ監査、システム監査等の各種監査、内部通報、情報開示、CSIRTの設置といった方策が考えられる。

２．解説

（１）監査

ア　内部監査

会社法は、大会社、監査等委員会設置会社及び指名委員会等設置会社について、取締役（会）が内部統制システムの構築の基本方針を決定すべきことを明文の義務としているところ[1]、この内部統制システムには、会社におけるサイバーセキュリティに関する体制も含まれ得る（Q3 参照）。

内部統制システムに対する評価を行う仕組みとして内部監査部門による監査（以下「内部監査」という。）が挙げられる。

内部監査とは、「組織体の経営目標の効果的な達成に役立つことを目的として、合法性と合理性の観点から公正かつ独立の立場で、ガバナンス・プロセス、リスク・マネジメントおよびコントロールに関連する経営諸活動の遂行状況を、内部監査人としての規律遵守の態度をもって評価し、これに基づいて客観的意見を述べ、助言・勧告を行うアシュアランス業務、および特定の経営諸活動の支援を行うアドバイザリー業務」[2]とされている。

サイバーセキュリティに関する体制を内部監査の対象とすることで、社内のサイバーセキュリティ体制の適切さの担保を図ることが期待できる。

イ　情報セキュリティ監査

社内の情報資産を対象とした監査として、情報セキュリティ監査がある。これは、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専

[1] 会社法第 348 条第 3 項第 4 号・4 項、第 362 条第 4 項第 6 号・5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ

[2] 一般社団法人日本内部監査協会「内部監査基準」（平成 26 年改訂）

門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと[3]を目的とした監査である。

情報セキュリティ監査は、情報セキュリティ管理基準及び情報セキュリティ監査基準に則って実施される。情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール（管理策）を整備・運用するための実践的な規範として定められた基準であり、情報セキュリティマネジメントに関する国際規格[4]との整合をとるための改正も行われている。

情報セキュリティ監査は、社内の内部監査部門によって実施される場合は内部監査の一環として位置付けることができ、他方で、専門性の高い外部の監査機関によって実施されることもある。

なお、情報セキュリティ監査の技法を活用する形でサイバーセキュリティ体制を含めて監査を実施する場合には、リスク評価について、情報の機密性・完全性・可用性が損なわれるリスクはもちろん、企業の事業継続をはじめとした、経営レベルへの影響も重視のうえ、監査を行うこととなると考えられる[5]。

ウ　システム監査

社内の情報システム体系を対象とした監査としてシステム監査がある。これは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査[6]である。

システム監査は、システム管理基準及びシステム監査基準に則って実施される。

情報セキュリティ監査と同様、システム監査が、社内の内部監査部門によって実施される場合は、内部監査の一環として位置付けることができ、他方で、専門性の高い外部の監査機関によって実施されることもある。

なお、システム監査基準において「システム監査は各種目的あるいは各種形態をもって実施されることから、他のガイドラインや組織体独自の諸規程・マニュアル等を、システム監査上の判断尺度として用いることもできる。特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」を参照することが望ましい。」とされているとおり、情報システム監査とシステム監査については、双方が重なる部分もある[7]。

---

[3] 情報セキュリティ監査基準・2 頁参照
[4] ISO/IEC 27001:2013（JIS Q 27001:2014）及び ISO/IEC 27002:2013（JIS Q 27002:2014）
[5] この点については、経営ガイドラインも参照されたい。
[6] システム監査基準 1 頁参照
[7] この点については、経産省「情報セキュリティ管理基準参照表」も参照されたい。

（２）内部通報制度

内部監査と同様、法令遵守体制の一内容としての内部通報制度の活用が挙げられる。例えば、社内における個人情報保護法に違反する態様での個人データの管理状況について、従業員が不利益を被るおそれなしにその事実を通報できる制度を整備することにより、サイバーセキュリティ体制の適切性を担保することが期待できる。

（３）情報開示

サイバーセキュリティに関する企業の情報を開示することは、サイバーセキュリティ体制の強化につながることが期待できる。情報開示に耐えるだけのサイバーセキュリティ体制の構築が必要となるからである。

現在のところ、サイバーセキュリティに特化した情報開示に関する法的な根拠や具体的な指針は存在しないものの、企業としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

詳細は Q6 のとおりであるが、既存の制度開示としては、事業報告（会社法第 435 条第 2 項）、有価証券報告書（金融商品取引法第 24 条）、コーポレート・ガバナンス報告書（有価証券上場規程（平成 19 年 11 月 1 日東京証券取引所）第 204 号第 12 項第 1 号等）、適時開示（有価証券上場規程第 402 条等）が存在する。また、任意開示として、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、情報セキュリティ基本方針等が挙げられる。

（４）CSIRT の設置

CSIRT（シーサート）とは、Computer Security Incident Response Team の略称であり、企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと[8]をいう。

CSIRT は事業の規模、種類によって構成も形式も異なるため、その権限や活動範囲も各社によって異なるものの、最小構成の CSIRT であっても、CSIRT としての使命、サービス、活動範囲の 3 要素を定義づけることが重要である。また、組織内外の関係者と連携するためには、「PoC (Point Of Contact)：信頼できる窓口」が必要である。

CSIRT は組織全体で考慮すべきであり、内部統制としてのリスク管理、事業継続マネジメントの一環として CSIRT を構築する流れが望ましいとされている。専門性の高い CSIRT の設置により、サイバーセキュリティ体制の実効性の担保を図ることが期待できる。

３．参考資料（法令・ガイドラインなど）

・情報セキュリティ監査基準（平成 15 年経済産業省告示第 114 号）

[8] サイバーセキュリティ 2019・357 頁参照

・情報セキュリティ管理基準（平成 28 年経済産業省告示第 37 号）
・経産省「システム監査基準」（平成 30 年 4 月 20 日改訂）
・経産省「システム管理基準」（平成 30 年 4 月 20 日改訂）
・経産省「情報セキュリティ管理基準参照表」

４．裁判例

特になし

Q6 サイバーセキュリティと情報開示

企業は、サイバーセキュリティに関してどのような情報開示を行うことが望ましいか。

タグ：会社法、金融商品取引法、有価証券報告書、コーポレート・ガバナンス報告書、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書

１．概要

サイバーセキュリティに特化した情報開示に関する法的な根拠や具体的な指針は存在しない。

もっとも、サイバーセキュリティに関する企業の情報を開示することは、企業の社会への説明責任を果たすとともに、経営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。また、自社のサイバーセキュリティ対策の強化もつながることも期待できる。

そこで、企業としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

既存の制度開示としては、事業報告（会社法第 435 条第 2 項）、有価証券報告書（金融商品取引法第 24 条）、コーポレート・ガバナンスに関する報告書（有価証券上場規程（平成 19 年 11 月 1 日東京証券取引所）第 204 号第 12 項第 1 号等）、適時開示（有価証券上場規程第 402 条等）が存在する。

また、任意開示として、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、情報セキュリティ基本方針等が挙げられる。

なお、企業のサイバーセキュリティに関する情報開示の意義を踏まえ、総務省は、「サイバーセキュリティ対策情報開示の手引き」を公表し、情報開示の手段及び開示の在り方をまとめている[1]ため、詳細についてはそちらも参照されたい。

２．解説

（１）サイバーセキュリティに関する情報開示の重要性

現在のところ、サイバーセキュリティに特化した情報開示に関する法的な根拠や具体的な指針は存在しない。サイバーセキュリティに関する情報開示は、基本的には企業の任意の取組に位置付けられる。

もっとも、企業にとってサイバー攻撃が看過できないリスクとなりつつある状況において、企業のサイバーセキュリティへの取組は社会にとって重大な関心事である。企業としては、社会への説明責任の一環としてサイバーセキュリティに関する認識及び取組状況に関

[1] 総務省「サイバーセキュリティ対策情報開示の手引き」13 頁など
https://www.soumu.go.jp/main_content/000630516.pdf

する情報を開示することが期待されるとともに、経営上の重要課題としてセキュリティ対策に取り組んでいることを積極的に開示することでステークホルダーから正当な評価を受けることが可能となる。また、サイバーセキュリティに関する情報を開示することは、自社のセキュリティ対策の現状を正しく認識のうえ適正に運用する契機となるとともに、かつ、他社の状況との比較を通じて、さらに具体的な対策を検討・導入することで、自社のサイバーセキュリティ対策の強化につながることが期待できる。

そこで、企業としては、以下に例示する既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

（２）事業報告

会社法第 435 条第 2 項に基づき、株式会社は事業報告を作成することが義務付けられている。

株式会社は、内部統制システムに関する決定又は決議をしたときは、その決定又は決議の内容の概要及び当該システムの運用状況の概要を事業報告に記載しなければならないところ（会社法施行規則第 118 条第 2 号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる（サイバーセキュリティと内部統制システムとの関係については Q3 を参照されたい。）。

（３）有価証券報告書

金融商品取引法第 24 条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項等について、内閣総理大臣に提出することが義務づけられている。

その他事業の内容に関する重要な事項の中には、事業等のリスクが含まれるところ（企業内容等の開示に関する内閣府令第 15 条第 1 項第 1 号に定める第 3 号様式）、サイバーセキュリティに関するリスクをこの事業等のリスクとして開示することが考えられる。

（４）コーポレート・ガバナンスに関する報告書

証券取引所による開示制度の一環として、コーポレート・ガバナンスに関する報告書が挙げられる。

有価証券上場規程（東京証券取引所）第 204 条第 12 項第 1 号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する基本的な考え方などを記載したコーポレート・ガバナンスに関する報告書を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている。

コーポレート・ガバナンスに関する報告書では、内部統制システムに関する基本的な考え方及びその整備状況を記載することとされているところ（有価証券上場規程施行規則第 211 条第 4 項第 5 号）、サイバーセキュリティに関する事項をこの内部統制ステムの一部として

開示することが考えられる。

（５）適時開示

有価証券上場規程第 402 条等に基づき、上場会社は、剰余金の配当、株式移転、合併の決定を行った場合や災害に起因する損害又は業務遂行の過程で生じた損害が発生した場合等においては、直ちにその内容を開示することとされている。

サイバー攻撃に起因して損害が発生する場合には、この災害に起因する損害又は業務遂行の過程で生じた損害として損害・損失の内容や今後の見通しを開示することが考えられる。

（６）情報セキュリティ報告書

平成 19 年 9 月に経産省が「情報セキュリティ報告書モデル」[2]を公表しており、企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指している。同モデルにおいては、①報告書の発行目的といった基礎情報、②経営者の情報セキュリティに関する考え方、③情報セキュリティガバナンス、④情報セキュリティ対策の計画・目標、⑤情報セキュリティ対策の実績・評価、⑥情報セキュリティに係る主要注力テーマ、⑦（取得している場合の）第三者評価・認証等を基本構成としている。

（７）CSR 報告書、サステナビリティ報告書

CSR（企業の社会的責任）報告書は、環境や社会問題などに対して企業は倫理的な責任を果たすべきであるとする CSR の考え方に基づいて行う企業の社会的な取組をまとめた報告書であり、サステナビリティ（持続可能性）報告書とも呼ばれている。環境、労働、社会貢献などに関する情報や、事業活動に伴う環境負荷などが幅広く公表されている。

この中にサイバーセキュリティに関する情報を含めて公表することが考えらえる。

（８）情報セキュリティ基本方針

情報セキュリティ基本方針は、企業や組織の内部において実施する情報セキュリティ対策の方針や行動指針であり、社内規定といった組織全体のルールから、どのような情報資産を、どのような脅威から、どのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するものである。

---

[2] 経産省「情報セキュリティ報告書モデル」
https://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf

３．参考資料（法令・ガイドラインなど）

・会社法第 435 条第 2 項
・会社法施行規則第 118 条第 2 号
・金融商品取引法第 24 条
・企業内容等の開示に関する内閣府令第 15 条第 1 項第 1 号
・有価証券上場規程（東京証券取引所）第 204 条第 12 項第 1 号等、第 402 条
・有価証券上場規程施行規則（東京証券取引所）第 211 条第 4 項各号
・総務省「サイバーセキュリティ対策情報開示の手引き」
・経産省「情報セキュリティ報告書モデル」

４．裁判例

特になし

関係者一覧

（全て敬称略）

◇サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ

主査	林　紘一郎	情報セキュリティ大学院大学　名誉教授
副主査	岡村　久道	英知法律事務所　弁護士
		京都大学大学院　医学研究科　講師
委員	大杉　謙一	中央大学大学院　法務研究科　教授
委員	大谷　和子	株式会社日本総合研究所　法務部長
委員	奥邨　弘司	慶應義塾大学大学院　法務研究科　教授
委員	小向　太郎	日本大学　危機管理学部　教授
委員	星　周一郎	首都大学東京　法学部　教授
委員	丸山　満彦	デロイト トーマツ サイバー合同会社　執行役員
委員	宮川　美津子	ＴＭＩ総合法律事務所　弁護士
委員	湯淺　墾道	情報セキュリティ大学院大学　教授

オブザーバー

警察庁、個人情報保護委員会事務局、総務省、法務省、厚生労働省、経済産業省

◇サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ
タスクフォース　（ドラフト起草担当）

構成員	阿久津　匡美	弁護士法人北浜法律事務所東京事務所　弁護士
構成員	安藤　広人	ファイ法律事務所　弁護士
構成員	寺門　峻佑	ＴＭＩ総合法律事務所　弁護士
構成員	日置　巴美	三浦法律事務所　弁護士
構成員	北條　孝佳	西村あさひ法律事務所　弁護士
構成員	水町　雅子	宮内・水町ＩＴ法律事務所　弁護士
構成員	山岡　裕明	八雲法律事務所　弁護士
構成員	渡邊　涼介	光和総合法律事務所　弁護士
オブザーバー	大谷　和子	株式会社日本総合研究所　法務部長
事務局（編著担当）	蔦　大輔	内閣官房内閣サイバーセキュリティセンター 上席サイバーセキュリティ分析官

◇ヒアリング等協力（五十音順・敬称略）

○ 一般財団法人安全保障貿易情報センター（CISTEC）
池田　伸生　　青木　眞夫[1]　　加藤　智也　　佐藤　朋司　　千葉　晴夫
村井　則彦　　山田　尚文

○ 一般社団法人日本クラウドセキュリティアライアンス（CSA）
渥美　俊英　　高橋　郁夫　　成田　和弘　　諸角　昌宏

○ 一般社団法人日本内部監査協会
南部　芳子　　吉武　一

○ S&K Brussels 法律事務所
杉本　武重

○ 国立情報学研究所（NII）
佐藤　一郎　　高橋　克巳

○ システム監査学会（JSSA）
石島　隆

○ 特定非営利活動法人デジタル・フォレンジック研究会（IDF）
安冨　潔

○ 特定非営利活動法人日本セキュリティ監査協会（JASA）
永宮　直史

○ 独立行政法人日本貿易振興機構（JETRO）
島田　英樹　　長﨑　勇太

○ 日本シーサート協議会（NCA）法制度研究 WG
池田　香苗　　萩原　健太　　林　基樹

◇事務局

内閣官房内閣サイバーセキュリティセンター
基本戦略第１グループ・基本戦略第２グループ

[1] 独立行政法人情報処理推進機構（IPA）J-CRAT/サイバーレスキュー隊から協力