「重要インフラのサイバーセキュリティに係る行動計画」改定案

※　「重要インフラのサイバーセキュリティ対策のための統一基準」（案）とともにサイバーセキュリティ戦略本部において決定し、令和８年 10 月１日に施行予定

（下線部分は改定部分）

改　定　後	改　定　前
重要インフラのサイバーセキュリティに係る行動計画 ２０２２年　６　月　１７日 サイバーセキュリティ戦略本部 ２０２６年　　月　　日 サイバーセキュリティ戦略本部改定	重要インフラのサイバーセキュリティに係る行動計画 ２０２２年　６　月　１７日 サイバーセキュリティ戦略本部 ２０２４年　３　月　８　日 サイバーセキュリティ戦略本部改定 ２０２５年　６　月　２７日 サイバーセキュリティ戦略本部改定
この行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第25条第１項第５号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものである。	この行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第26条第１項第６号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものである。
Ⅰ．総論 1．重要インフラ防護の目的 重要インフラにおいて、任務保証[1]の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災	Ⅰ．総論 1．重要インフラ防護の目的 重要インフラにおいて、任務保証[1]の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災

害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靱性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的とする。 1 サイバーセキュリティ戦略(令和7年12月23日閣議決定)において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、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。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」 2. (略) 3. サイバーセキュリティ基本法との整合性について 3.1 サイバーセキュリティ基本法における行動計画の位置付け 行動計画は、サイバーセキュリティ基本法(平成26年法律第104号)第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、同法第14条(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)及び第25条第1項第5号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定される。 3.2・3.3 (略)	害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靱性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的とする。 1 サイバーセキュリティ戦略(令和3年9月28日閣議決定)において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、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。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」 2. (略) 3. サイバーセキュリティ基本法との整合性について 3.1 サイバーセキュリティ基本法における行動計画の位置付け 行動計画は、サイバーセキュリティ基本法(平成26年法律第104号)第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、同法第14条(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)及び第26条第1項第6号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定される。 3.2・3.3 (略)

4. 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群と補強・改善の方向性等を表に示す。

表 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群	第4次行動計画の施策群との対応	第4次行動計画からの主な補強・改善の方向性
（略）		
5.防護基盤の強化	「5.防護基盤の強化」の一部を「3.障害対応体制の強化」の一部と統合した上で整理	○　障害対応体制の有効性検証としての全分野一斉演習の推進 ○　警察による重要インフラ事業者等との協力等の必要な取組の支援 ○　デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施等に関する情報の共有を行う。

4. 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群と補強・改善の方向性等を表に示す。

表 本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群	第4次行動計画の施策群との対応	第4次行動計画からの主な補強・改善の方向性
（略）		
5.防護基盤の強化	「5.防護基盤の強化」の一部を「3.障害対応体制の強化」の一部と統合した上で整理	○　障害対応体制の有効性検証としての分野横断的演習の推進 ○　警察による重要インフラ事業者等との協力等の必要な取組の支援 ○　デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施等に関する情報の共有を行う。

II. 本行動計画の要点(エグゼクティブサマリー)

（略）

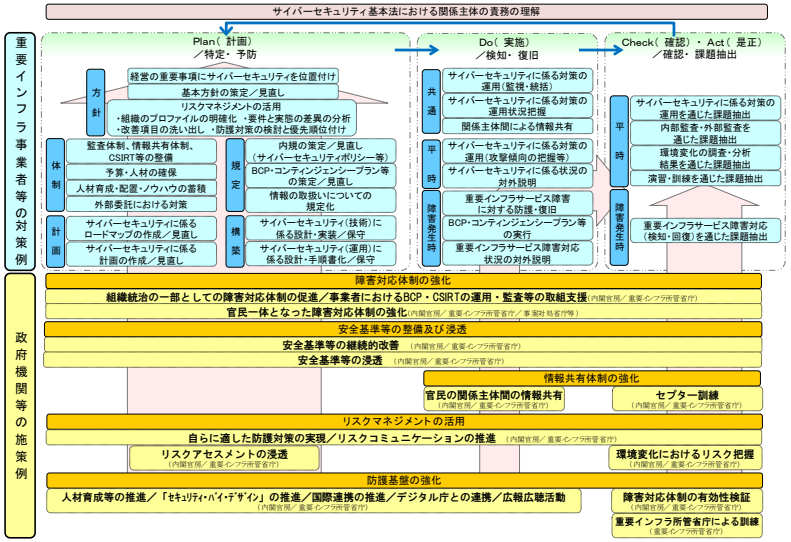

図 1 「重要インフラ事業者等の対策例」と「政府機関等の施策例」

II. 本行動計画の要点(エグゼクティブサマリー)

（略）

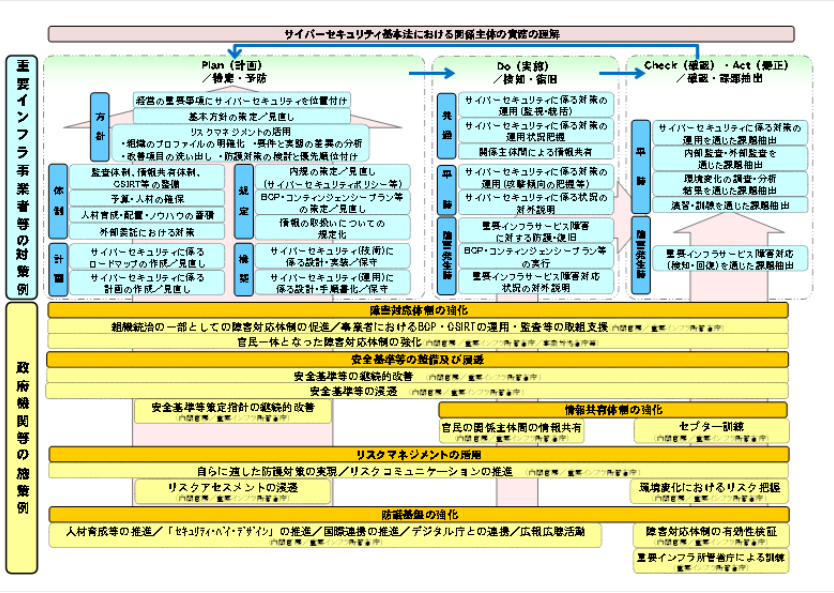

図 1 「重要インフラ事業者等の対策例」と「政府機関等の施策例」

Ⅲ．総論 （略） 1. 重要インフラを取り巻くサイバーセキュリティの環境変化 （略） こうした環境変化等を背景に、東京大会開催に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組を、我が国におけるサイバーセキュリティの向上に活用していくこととされた。また、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針において、サイバーセキュリティについても基本的な方針を示し、その実装を推進することとされた。さらに、我が国を取り巻く安全保障環境が厳しさを増している中、サイバー攻撃からの防御、サイバー攻撃の抑止、サイバー空間の状況把握に係る能力向上のため、政府全体としてのシームレスな対応を抜本的に強化していくこととされた。 （略） 2. 重要インフラ防護の範囲 重要インフラ事業者等が、各種法令等に基づき重要インフラサービスを提供する際、自らが重要インフラ防護の当事者であるという認識を持ち、重要インフラ防護に取り組む必要がある。このため、重要インフラ所管省庁は、各重要インフラ分野における重要インフラ事業者等を特定し、自らが重要インフラ事業者等であ	Ⅲ．総論 （略） 1. 重要インフラを取り巻くサイバーセキュリティの環境変化 （略） こうした環境変化等を背景に、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。この中で、東京大会開催に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組を、我が国におけるサイバーセキュリティの向上に活用していくこととされた。また、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針において、サイバーセキュリティについても基本的な方針を示し、その実装を推進することとされた。さらに、我が国を取り巻く安全保障環境が厳しさを増している中、サイバー攻撃からの防御、サイバー攻撃の抑止、サイバー空間の状況把握に係る能力向上のため、政府全体としてのシームレスな対応を抜本的に強化していくこととされた。 （略） 2. 重要インフラ防護の範囲 重要インフラ事業者等が、各種法令等に基づき重要インフラサービスを提供する際、自らが重要インフラ防護の当事者であるという認識を持ち、重要インフラ防護に取り組む必要がある。このため、重要インフラ所管省庁は、各重要インフラ分野における重要インフラ事業者等を明確化し、自らが重要インフラ事業者等で

ることを認識できるようにする。また、内閣官房及び重要インフラ所管省庁は、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しを行う。 対象となる重要インフラ分野は、「重要インフラのサイバーセキュリティ対策のための統一基準」（以下「重要インフラ統一基準」という。）に基づき、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」、「港湾」及び「郵便」の16分野とする。対象となる重要インフラ分野と重要システム例については、別紙1に、重要インフラサービスとサービス維持レベルについては、別紙2に示す。 （略）	あることを認識できるようにする。また、内閣官房及び重要インフラ所管省庁は、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しを行う。 対象となる重要インフラ分野と重要システム例については、第4次行動計画に引き続き、別紙1に示し、重要インフラ分野は、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の15分野とする。重要インフラサービスとサービス維持レベルについては、第4次行動計画に引き続き、別紙2に示す。 （略）
3.・4. （略）	3.・4. （略）
IV. 計画期間内の取組 1. 障害対応体制の強化 （略） 1.1 組織統治の一部としての障害対応体制 （略） 重要インフラ事業者等においては、組織の各階層において適切な責任と権限を明確にし、組織一丸となって重要インフラ防護を行う必要があるが、経営層のコミットメントによる組織運営上のリスクのひとつとして、重要インフラ防護の観点を含める必要がある。 重要インフラ事業者等は、本行動計画	IV. 計画期間内の取組 1. 障害対応体制の強化 （略） 1.1 組織統治の一部としての障害対応体制 （略） 重要インフラ事業者等においては、組織の各階層において適切な責任と権限を明確にし、組織一丸となって重要インフラ防護を行う必要があるが、経営層のコミットメントによる組織運営上のリスクのひとつとして、重要インフラ防護の観点を含める必要がある。 内閣官房は、本行動計画において、障害

等を踏まえ、自組織の障害対応体制の改善に努めるものとする。	対応体制の強化に資する組織統治の在り方について、安全基準等策定指針において、規定化をする。 重要インフラ事業者等は、本行動計画及び策定された安全基準等策定指針を踏まえ、自組織の障害対応体制の改善に努めるものとする。 (1)・(2) (略)
1.2 (略)	1.2 (略)
1.3 官民一体となった障害対応体制の強化 (略) 我が国を取り巻く安全保障環境は厳しさを増しており、サイバー攻撃に対する国家の強靭性を確保し、サイバー攻撃から国家を防御する力(防御力)、サイバー攻撃を抑止する力(抑止力)、サイバー空間の状況を把握する力(状況把握力)をそれぞれ高めつつ、政府全体としてシームレスな対応を抜本的に強化していくことが重要となっている。重要インフラ防護において、これらを具現化していく。 (略)	1.3 官民一体となった障害対応体制の強化 (略) 我が国を取り巻く安全保障環境は厳しさを増しており、サイバーセキュリティ戦略(令和3年9月28日閣議決定)では、サイバー攻撃に対する国家の強靭性を確保し、サイバー攻撃から国家を防御する力(防御力)、サイバー攻撃を抑止する力(抑止力)、サイバー空間の状況を把握する力(状況把握力)をそれぞれ高めつつ、政府全体としてシームレスな対応を抜本的に強化していくことが重要とされている。重要インフラ防護において、これらを具現化していく。 (略)
1.4 (略)	1.4 (略)
2. 安全基準等の整備及び浸透 (略) 安全基準等に関する体系を図2に示す。具体的には、内閣官房は、重要インフラ所管省庁の協力のもとに、各重要インフラ分野に共通して求められるサイバーセキ	2. 安全基準等の整備及び浸透 (略) 安全基準等に関する体系を図2に示す。具体的には、内閣官房は、重要インフラ所管省庁の協力のもとに、各重要インフラ分野に共通して求められるサイバーセキ

ュリティの確保に向けた取組を重要インフラ統一基準の「第３部　安全基準等において規定されるべき事項」及び「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」（以下「安全基準等策定ガイドライン」という。）において定めている。これらを踏まえ、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等(以下「安全基準等」という。)が策定されている。	ュリティの確保に向けた取組を「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」（以下「安全基準等策定指針」という。)として策定している。さらに、安全基準等策定指針で定めた手順等を具体的に示すための手引書（以下「手引書」という。）及び個別の対処方法、留意点等を示すガイダンス等の関連文書を策定している。安全基準等策定指針、手引書等を踏まえ、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等(以下「安全基準等」という。)が策定されている。

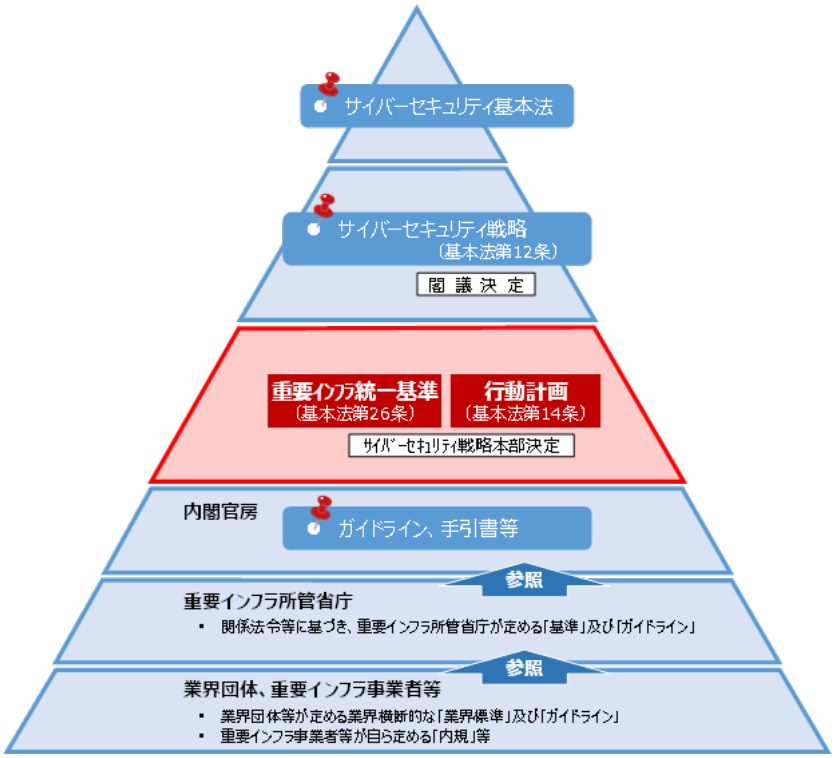

図 2 重要インフラ防護に関する安全基準等に係る体系

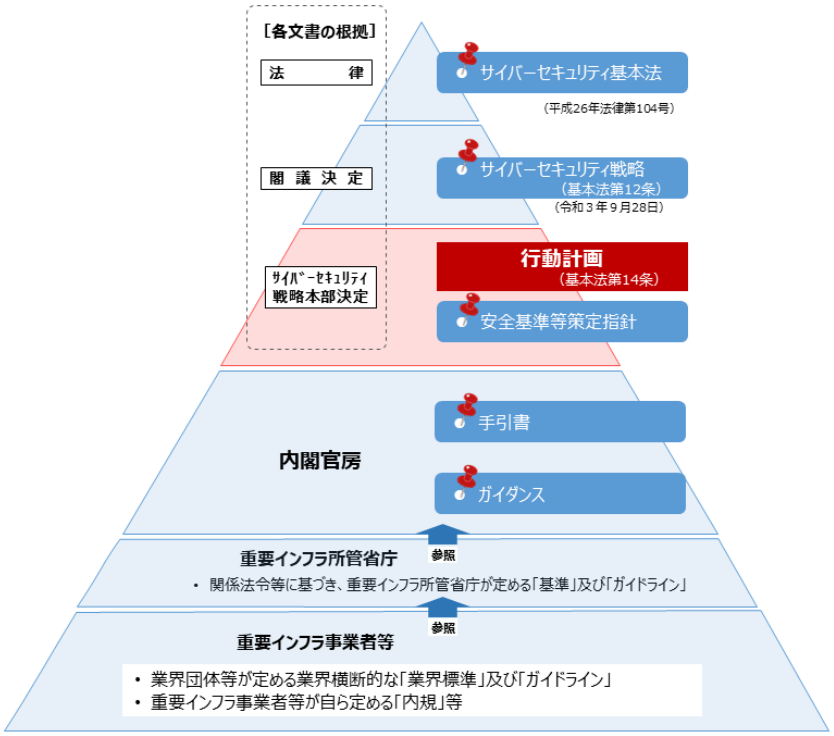

図 2 重要インフラ防護に関する安全基準等に係る体系

（削る）	2.1 安全基準等策定指針の継続的改善 内閣官房は、特に障害対応体制の強化の観点から、安全基準等策定指針及び手引書の見直しを行う。安全基準等策定指針及び手引書の見直しについては、3 年に 1 度の実施を原則とする。他方、社会動向の大きな変化等、現行の安全基準等策定指針及び手引書では十分ではない事象が発生した場合は、この限りでない。さらに、安全基準等策定指針及び手引書の関連文書であるガイダンス等については、昨今のランサムウェアによる攻撃の増加を一例とする周辺環境の激変やインシデント等に速やかに対応できるよう、運用等から得られた知見を踏まえて適時に改定する。また、国際標準や海外の指針のうち日本でも参考にすべきものがあれば適宜採り入れることを検討する。 本行動計画期間中に新たに整備を行う安全基準等策定指針に係る事項は以下のとおりとする。 (1) 組織統治に関する基準の整備 組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく、「サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0(令和５年９月内閣官房内閣サイバーセキュリティセンター)」で規定している①内部統制システムとサイバーセキュリティとの関係、②サイバーセキュリティと取締役等の責任、③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、④サイバーセキュリティと情報開示、を活用するなどして、安全基準等策定指針の記載を充実させる。

	(2) サプライチェーンに関する基準の整備 サプライチェーンに起因する重要インフラサービス障害の連鎖に係るリスク、例えば、①サプライチェーンの過程で製品に不正機能等が埋め込まれるリスク、②政治経済情勢による機器・サービスの供給途絶のリスク、③クラウドサービス等の外部サービスにおける情報の取扱い・可用性に係るリスク等の高まりを踏まえ、サプライチェーン・リスクへの対応について安全基準等策定指針の記載を充実させる。 (3) 自組織に適した継続的改善のための基準の整備 自組織に適した対策に係る基本的な考え方を安全基準等策定指針に盛り込み、具体的な実施手法を示す関連文書等の作成を実施する。 (4) その他基準の整備 プラントや工場等の制御システムへのサイバー攻撃等の脅威に迅速に対応するため、ITとOTの横断的な組織整備や、OTのセキュリティ人材の育成の重要性を訴求する。
2.1 安全基準等の継続的改善 重要インフラ所管省庁は、自らが安全基準等の策定主体の場合には、重要インフラ統一基準に基づき、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。重要インフラ事業者等は、自らが安全基準等の策定主体の場合には、関係法令の	2.2 安全基準等の継続的改善 重要インフラ所管省庁は、自らが安全基準等の策定主体の場合には、安全基準等策定指針の改定等を踏まえて、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。重要インフラ事業者等は、自らが安全基準等の策定主体の場合には、関

要求事項を遵守できるよう、重要インフラ統一基準等を踏まえつつ、継続的に安全基準等を改善する。 　具体的には、各重要インフラ事業者等の対策の経験から得た知見等をもとに、サイバーセキュリティの確保に向けた取組の運用、内部監査・外部監査、サイバーセキュリティに係る環境変化の調査・分析の結果、演習・訓練、重要インフラサービス障害対応等から課題を抽出し、リスク評価を経て、安全基準等がそれぞれの重要インフラ分野及び各組織に最適なものとなるよう取り組む。安全基準等の検証に際しては、重要インフラ統一基準及び内閣官房が公表した社会動向の変化・新たな知見を用いることとする。 　内閣官房は、重要インフラ統一基準に基づき、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。	係法令の要求事項を遵守できるよう、安全基準等策定指針の改定等を踏まえつつ、継続的に安全基準等を改善する。 　具体的には、各重要インフラ事業者等の対策の経験から得た知見等をもとに、サイバーセキュリティの確保に向けた取組の運用、内部監査・外部監査、サイバーセキュリティに係る環境変化の調査・分析の結果、演習・訓練、重要インフラサービス障害対応等から課題を抽出し、リスク評価を経て、安全基準等がそれぞれの重要インフラ分野及び各組織に最適なものとなるよう取り組む。安全基準等の検証に際しては、安全基準等策定指針及び内閣官房が公表した社会動向の変化・新たな知見を用いることとする。 　内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。
2.2 安全基準等の浸透 　重要インフラ事業者等において有効な障害対応体制の構築がなされているかを精緻に把握することを目的に、内閣官房は、重要インフラ統一基準に基づき、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段について調査分析する。結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。	2.3 安全基準等の浸透 　重要インフラ事業者等において有効な障害対応体制の構築がなされているかを精緻に把握することを目的に、内閣官房は、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段について調査分析する。結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。 　重要インフラ分野・組織ごとのリスクの多様化・複雑化に伴い、組織に応じた対策状況や、経営層の関与状況等の実態を

	より正確に把握することが重要になってきている。そのため、重要インフラ事業者等における自主的な取組を促進できる調査方法へ変更する必要がある。内閣官房は、新たな調査方法について重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を検討し、2023年度中を目処に具現化する。 　具体的には、重要インフラ事業者等において、①サイバーセキュリティの現状に係る自己評価、②自組織における本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施、を繰り返すことで、サイバーセキュリティの確保に資する継続的な改善を図ることができる合理的・効果的な調査手法を検討する。
2.3 安全基準等の文書の明確化 　内閣官房は、重要インフラ統一基準や安全基準等の理解を促進するため、その一覧をまとめ、また、文書間の関係性を明確化する。	2.4 安全基準等の文書の明確化 　内閣官房は、安全基準等策定指針、安全基準等の理解を促進するため、その一覧をまとめ、また、文書間の関係性を明確化する。
3. 情報共有体制の強化 （略） 3.1 本行動計画期間における情報共有体制 （略） 　なお、サイバーセキュリティ戦略本部長がサイバーセキュリティ基本法第27条第3項の規定に基づき、同法第32条（資料提供等）又は第33条（資料の提出その他の協力）の規定に基づき重要インフラ所管	3. 情報共有体制の強化 （略） 3.1 本行動計画期間における情報共有体制 （略） 　なお、サイバーセキュリティ戦略本部長がサイバーセキュリティ基本法第28条第3項の規定に基づき、同法第32条（資料提供等）又は第33条（資料の提出その他の協力）の規定に基づき重要インフラ所管

省庁の長又は重要インフラ事業者等の長若しくは代表者からサイバーセキュリティ戦略本部に提供された重要インフラ事業者等のサイバーセキュリティに関する資料、情報等に基づき、重要インフラ所管省庁の長に勧告できる等の仕組みを、その事務を行う内閣官房(国家サイバー統括室)は適切に運用する。 （略）	省庁の長又は重要インフラ事業者等の長若しくは代表者からサイバーセキュリティ戦略本部に提供された重要インフラ事業者等のサイバーセキュリティに関する資料、情報等に基づき、重要インフラ所管省庁の長に勧告できる等の仕組みを、その事務を行う内閣官房(国家サイバー統括室)は適切に運用する。 （略）
3.2 情報共有の更なる促進 （略） なお、内閣官房は、ナショナルサート[3]の枠組みの強化の検討と整合性を保ち、その整備の一環として、協議会[4]等との連携を一層推進する。	3.2 情報共有の更なる促進 （略） なお、内閣官房は、ナショナルサート[3]の枠組みの強化の検討と整合性を保ち、その整備の一環として、サイバーセキュリティ協議会等との連携を一層推進する。
3 （略） 4 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）第45条に基づく協議会。	3 （略） （新設）
3.3 （略）	3.3 （略）
3.4 セプター訓練 （略） 実施に際して、セプター訓練では多くの重要インフラ事業者等の参加実績があることを踏まえ、必要に応じて全分野一斉演習との連携を検討し、緊急時における情報連絡体制・手段の検証等、セプターや重要インフラ所管省庁からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有訓練の実現を目指す。	3.4 セプター訓練 （略） 実施に際して、セプター訓練では多くの重要インフラ事業者等の参加実績があることを踏まえ、必要に応じて分野横断的演習との連携を検討し、緊急時における情報連絡体制・手段の検証等、セプターや重要インフラ所管省庁からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有訓練の実現を目指す。

4. リスクマネジメントの活用 （略） 4.1 リスクマネジメントの推進 （略） (1) （略） (2) 自組織に適した防護対策の具現化 内閣官房は、前号に示した重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、既存の基準類をどのように自組織に活用するかを含めたガイダンス等を整備する。これらガイダンス等は、関係主体が自組織に適した防護対策の実現に向けて、その改善を迅速かつ的確に行えるようパフォーマンスベースとし、達成状況が監視、測定可能なものとする。なお、これらガイダンス等は、自組織で活用するほか、必要に応じて関係業界や、重要インフラ所管省庁等とともに改善していくなど考慮するものとする。 (3) リスクマネジメントに関するこれまでの取組の継続 （略） 内閣官房は、重要インフラ事業者等に対してセプターカウンシルへの参加や全分野一斉演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会を引き続き充実させる。また、内閣官房は、東京大会に向けて官民が連携してリスクマネジメントの取組を進めたことなどにより、東京大会の円滑な運営に寄与した。こうした経験やノウハウについて、重要インフラ事業者等に対しても積極的に活用することとし、その具体的な手法や手順につい	4. リスクマネジメントの活用 （略） 4.1 リスクマネジメントの推進 （略） (1) （略） (2) 自組織に適した防護対策の具現化 内閣官房は、前号に示した重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンス等を整備する。これらガイダンス等は、関係主体が自組織に適した防護対策の実現に向けて、その改善を迅速かつ的確に行えるようパフォーマンスベースとし、達成状況が監視、測定可能なものとする。なお、これらガイダンス等は、自組織で活用するほか、必要に応じて関係業界や、重要インフラ所管省庁等とともに改善していくなど考慮するものとする。 (3) リスクマネジメントに関するこれまでの取組の継続 （略） 内閣官房は、重要インフラ事業者等に対してセプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会を引き続き充実させる。また、内閣官房は、東京大会に向けて官民が連携してリスクマネジメントの取組を進めたことなどにより、東京大会の円滑な運営に寄与した。こうした経験やノウハウについて、重要インフラ事業者等に対しても積極的に活用することとし、その具体的な手法や手順につい

ての検討を行う。 4.2 （略） 5. 防護基盤の強化 （略） 特に、障害対応体制の有効性検証においては、内閣官房が全分野一斉演習を実施することで、関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくことを目指す。 （略） 5.1 障害対応体制の有効性検証 （略） 内閣官房は、重要インフラサービスの継続的提供の強靭性の確保を念頭に、引き続き、全分野一斉演習を実施する。全分野一斉演習は、内閣官房と重要インフラ所管省庁等が連携して実施し、重要インフラ事業者等に対して組織全体の障害対応体制の有効性を継続的に検証・改善する機会として提供する。 (1) 全分野一斉演習による障害対応体制の改善 （略） なお、重要インフラ事業者等による自主的な取組を促すことを目的に、全分野一斉演習の一部を疑似的に体験できる演習プログラム等の提供に取り組む。 また、障害対応体制の強化に資することを目的に、演習を通じて得た知見・課題を参考資料として本行動計画の他施策に提供する。 重要インフラ事業者等においては、演習への備えとして自組織におけるリスク	ての検討を行う。 4.2 （略） 5. 防護基盤の強化 （略） 特に、障害対応体制の有効性検証においては、内閣官房が分野横断的演習を実施することで、関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくことを目指す。 （略） 5.1 障害対応体制の有効性検証 （略） 内閣官房は、重要インフラサービスの継続的提供の強靭性の確保を念頭に、引き続き、分野横断的演習を実施する。分野横断的演習は、内閣官房と重要インフラ所管省庁等が連携して実施し、重要インフラ事業者等に対して組織全体の障害対応体制の有効性を継続的に検証・改善する機会として提供する。 (1) 分野横断的演習による障害対応体制の改善 （略） なお、重要インフラ事業者等による自主的な取組を促すことを目的に、分野横断的演習の一部を疑似的に体験できる演習プログラム等の提供に取り組む。 また、障害対応体制の強化に資することを目的に、演習を通じて得た知見・課題を参考資料として本行動計画の他施策に提供する。 重要インフラ事業者等においては、演習への備えとして自組織におけるリスク

等の把握に努め、演習に参加し、その事後においては、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマネジメント等が有効に機能しているかの見直しとその改善に取り組む必要がある。このため、重要インフラ事業者等は、全分野一斉演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証・改善することが期待される。また、重要インフラ事業者等は、有効性検証を円滑に行うことを目的に、全分野一斉演習のシナリオ・実施方法・検証課題等の企画、全分野一斉演習の実施への協力が期待される。 (2) 重要インフラ全体への全分野一斉演習の成果の浸透 （略） (3) 重要インフラ所管省庁等との連携 重要インフラ所管省庁やISAC等の民間機関が実施する重要インフラ防護に資する演習・訓練は、内閣官房が実施する全分野一斉演習と期待される効果が異なるが、それぞれが実施する演習における主な対象者や検証目的の明確化及び相互連携の在り方等を踏まえつつ、必要に応じて全分野一斉演習と相互に連携・補完しながら実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図っていくことが期待される。 （略） 5.2 人材育成等の推進 人材育成に関する次の施策を講じる。	等の把握に努め、演習に参加し、その事後においては、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマネジメント等が有効に機能しているかの見直しとその改善に取り組む必要がある。このため、重要インフラ事業者等は、分野横断的演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証・改善することが期待される。また、重要インフラ事業者等は、有効性検証を円滑に行うことを目的に、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が期待される。 (2) 重要インフラ全体への分野横断的演習の成果の浸透 （略） (3) 重要インフラ所管省庁等との連携 重要インフラ所管省庁やISAC等の民間機関が実施する重要インフラ防護に資する演習・訓練は、内閣官房が実施する分野横断的演習と期待される効果が異なるが、それぞれが実施する演習における主な対象者や検証目的の明確化及び相互連携の在り方等を踏まえつつ、必要に応じて分野横断的演習と相互に連携・補完しながら実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図っていくことが期待される。 （略） 5.2 人材育成等の推進 関係主体において、サイバーセキュリティ戦略(令和3年9月28日閣議決定)等に基づく取組を推進する。具体的には、人材育成に関する次の施策を講じる。

(1)～(3)　(略)	(1)～(3)　(略)
5.3　(略)	5.3　(略)
5.4 国際連携の推進 　(略) 　このため、内閣官房は、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携して、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進する。具体的には、我が国の全分野一斉演習の取組紹介、米豪印やASEAN等との多国間の枠組みや米国その他同志国等との二国間による協議、CSIRT間連携や海外のサイバーセキュリティ政策担当者向けの講演等を通じて、我が国の特徴的な施策を積極的に発信することにより、サイバー攻撃関連情報、海外の脅威情報、インシデント対応事例、ベストプラクティスの共有等の基盤となる協力関係を強化するとともに、国際的な重要インフラ防護能力の向上にも寄与する。これによって海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。 　(略)	5.4 国際連携の推進 　(略) 　このため、内閣官房は、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携して、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進する。具体的には、我が国の分野横断的演習の取組紹介、米豪印やASEAN等との多国間の枠組みや米国その他同志国等との二国間による協議、CSIRT間連携や海外のサイバーセキュリティ政策担当者向けの講演等を通じて、我が国の特徴的な施策を積極的に発信することにより、サイバー攻撃関連情報、海外の脅威情報、インシデント対応事例、ベストプラクティスの共有等の基盤となる協力関係を強化するとともに、国際的な重要インフラ防護能力の向上にも寄与する。これによって海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。 　(略)
5.5 サイバー犯罪対策等の強化 　サイバー空間の公共空間化を踏まえ、警察は、警察庁にサイバー事案に係る政策を一元的に担うサイバー警察局と国の捜査部隊としてのサイバー特別捜査隊を創設し、地域に密着した活動を展開する都道府県警察と合わせて警察全体としてセキュリティ確保に向けた取組を推進し	5.5 サイバー犯罪対策等の強化 　サイバー空間の公共空間化を踏まえ、サイバーセキュリティ戦略(令和3年9月28日閣議決定)では、サイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図るとされており、警察は、警察庁にサイバー事案に係

ている。 （略）	る政策を一元的に担うサイバー警察局と国の捜査部隊としてのサイバー特別捜査隊を創設し、地域に密着した活動を展開する都道府県警察と合わせて警察全体としてセキュリティ確保に向けた取組を推進している。 （略）
5.6・5.7 （略）	5.6・5.7 （略）
V. 関係主体において取り組むべき事項 1. 内閣官房 (1) （略） (2)「安全基準等の整備及び浸透」に関する事項 （削る） ① 必要に応じて社会動向の変化及び新たに得た知見を踏まえてガイダンス等の関連文書を適時に改定し、その結果を公表。 ② 上記①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。 ③ 重要インフラ所管省庁の協力を得つつ、毎年、重要インフラ統一基準に基づき、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。 ④ 重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、重要インフラ統一基準に基づき、重要インフラ事業者等における	V. 関係主体において取り組むべき事項 1. 内閣官房 (1) （略） (2)「安全基準等の整備及び浸透」に関する事項 ① 本行動計画で掲げられた各施策の推進に資するよう、安全基準等策定指針の改定を実施し、その結果を公表。 ② 必要に応じて社会動向の変化及び新たに得た知見を踏まえてガイダンス等の関連文書を適時に改定し、その結果を公表。 ③ 上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。 ④ 重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。 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、重要インフラ事業者等における安全基準等の整備状況及びサイバ

安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査を実施し、結果を公表。重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を速やかに検討し具現化。	ーセキュリティ確保に向けた取組・手段についての調査を実施し、結果を公表。重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を速やかに検討し具現化。
⑤ 上記④の調査結果を、本行動計画の各施策の改善に活用。	⑥ 上記⑤の調査結果を、本行動計画の各施策の改善に活用。
⑥ 安全基準等の整備に係る文書一覧について整理し、文書間の関係性を明確化。	⑦ 安全基準等の整備に係る文書一覧について整理し、文書間の関係性を明確化。
(3) （略）	(3) （略）
(4) 「リスクマネジメントの活用」に関する事項	(4) 「リスクマネジメントの活用」に関する事項
① （略）	① （略）
② 重要インフラ事業者等に対して、セプターカウンシルへの参加や全分野一斉演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会の提供。	② 重要インフラ事業者等に対して、セプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会の提供。
③～⑤ （略）	③～⑤ （略）
(5) 「防護基盤の強化」に関する事項	(5) 「防護基盤の強化」に関する事項
① 障害対応体制の有効性の検証が可能な全分野一斉演習のシナリオ、実施方法、検証課題等を企画し、全分野一斉演習を実施。	① 障害対応体制の有効性の検証が可能な分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。
② （略）	② （略）
③ 全分野一斉演習の改善策の検討。	③ 分野横断的演習の改善策の検討。
④ 重要インフラ事業者等による自主的な取組を促すため、全分野一斉演習の一部を疑似的に体験できる演習プログラム等を提供。	④ 重要インフラ事業者等による自主的な取組を促すため、分野横断的演習の一部を疑似的に体験できる演習プログラム等を提供。
⑤ 全分野一斉演習の機会を活用して、障害対応体制の有効性の検証等を	⑤ 分野横断的演習の機会を活用して、障害対応体制の有効性の検証等を

実施。 ⑥ 全分野一斉演習で得られた重要インフラ防護に関する知見の普及・浸透。 ⑦～⑮ （略）	実施。 ⑥ 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・浸透。 ⑦～⑮ （略）
2. 重要インフラ所管省庁 (1) （略） (2)「安全基準等の整備及び浸透」に関する事項 ① 新たな安全基準等に関する情報等を内閣官房に提供。 ②～⑥ （略） (3)・(4) （略） (5) 「防護基盤の強化」に関する事項 ① 全分野一斉演習のシナリオ、実施方法、検証課題等の企画、全分野一斉演習の実施への協力。 ② セプター及び重要インフラ事業者等の全分野一斉演習への参加を支援。 ③ 全分野一斉演習への参加。 ④ 必要に応じて、全分野一斉演習成果を施策へ活用。 ⑤ 全分野一斉演習の改善策の検討への協力。 ⑥ 全分野一斉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。 ⑦～⑩ （略）	2. 重要インフラ所管省庁 (1) （略） (2)「安全基準等の整備及び浸透」に関する事項 ① 安全基準等策定指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。 ②～⑥ （略） (3)・(4) （略） (5) 「防護基盤の強化」に関する事項 ① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。 ② 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。 ③ 分野横断的演習への参加。 ④ 必要に応じて、分野横断的演習成果を施策へ活用。 ⑤ 分野横断的演習の改善策の検討への協力。 ⑥ 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。 ⑦～⑩ （略）
3. （略）	3. （略）

4. 事案対処省庁及び防災関係府省庁 (1)・(2) （略） (3) 「防護基盤の強化」に関する事項 ① 全分野一斉演習のシナリオ、実施方法、検証課題等の企画、全分野一斉演習の実施への協力。 ② （略） ③ 全分野一斉演習の改善策の検討への協力。 ④ 必要に応じて、全分野一斉演習と事案対処省庁及び防災関係府省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。	4. 事案対処省庁及び防災関係府省庁 (1)・(2) （略） (3) 「防護基盤の強化」に関する事項 ① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。 ② （略） ③ 分野横断的演習の改善策の検討への協力。 ④ 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。
5. 重要インフラ事業者等 (1)～(3) （略） (4) 「リスクマネジメントの活用」に関する事項 ①～③ （略） ④ セプターカウンシルへの参加や全分野一斉演習等を活用し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの充実。 ⑤・⑥ （略） (5) 「防護基盤の強化」に関する事項 ① 全分野一斉演習のシナリオ、実施方法、検証課題等の企画、全分野一斉演習の実施への協力。 ② 全分野一斉演習への備えとして、自組織におけるリスク等の把握を実施。 ③ 全分野一斉演習への参加。 ④ 全分野一斉演習の事後において、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマ	5. 重要インフラ事業者等 (1)～(3) （略） (4) 「リスクマネジメントの活用」に関する事項 ①～③ （略） ④ セプターカウンシルへの参加や分野横断的演習等を活用し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの充実。 ⑤・⑥ （略） (5) 「防護基盤の強化」に関する事項 ① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。 ② 分野横断的演習への備えとして、自組織におけるリスク等の把握を実施。 ③ 分野横断的演習への参加。 ④ 分野横断的演習の事後において、洗い出された課題の分析・検証を通じて、自組織の体制や内規、リスクマ

ネジメント等が有効に機能しているかの見直しとその改善を実施。 ⑤ 全分野一斉演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証し改善を実施。 ⑥ 全分野一斉演習の改善策の検討への協力。 ⑦～⑪ （略）	ネジメント等が有効に機能しているかの見直しとその改善を実施。 ⑤ 分野横断的演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証し改善を実施。 ⑥ 分野横断的演習の改善策の検討への協力。 ⑦～⑪ （略）
6. セプター及びセプター事務局 (1)～(3) （略） (4) 「防護基盤の強化」に関する事項 ① 重要インフラ事業者等の全分野一斉演習への参加を支援。 ② 必要に応じて全分野一斉演習への参加。 ③ 全分野一斉演習で得られた重要インフラ防護に関する知見の普及・展開を支援。	6. セプター及びセプター事務局 (1)～(3) （略） (4) 「防護基盤の強化」に関する事項 ① 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。 ② 必要に応じて分野横断的演習への参加。 ③ 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・展開を支援。
7. セプターカウンシル (1) （略） (2) 「防護基盤の強化」に関する事項 ① 必要に応じて全分野一斉演習への参加。	7. セプターカウンシル (1) （略） (2) 「防護基盤の強化」に関する事項 ① 必要に応じて分野横断的演習への参加。
8. サイバーセキュリティ関係機関 (1)・(2) （略） (3) 「防護基盤の強化」に関する事項 ① 全分野一斉演習に必要となる重要インフラサービス障害の事例等に関する情報を内閣官房に提供。 ② （略）	8. サイバーセキュリティ関係機関 (1)・(2) （略） (3) 「防護基盤の強化」に関する事項 ① 分野横断的演習に必要となる重要インフラサービス障害の事例等に関する情報を内閣官房に提供。 ② （略）
9. （略）	9. （略）

Ⅵ・Ⅶ　（略）	Ⅵ・Ⅶ　（略）
附　則 この決定は、令和８年10月１日から施行する。	（新設）

別紙１　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野	対象となる重要インフラ事業者等（注１）	対象となる重要情報システム例（注２）
（略）		
行政サービス	・地方公共団体	・地方公共団体の情報システム
（略）		
郵便	・郵便事業を営む者	・配達総合情報システム

注１　ここに掲げているものは、対象となる重要インフラ事業者等の類型を例示したものであり、具体的な重要インフラ事業者等は、重要インフラ統一基準に基づき重要インフラ所管省庁において特定する。

注２　（略）

別紙２　重要インフラサービスとサービス維持レベル

重要インフラ分野	重要インフラサービス（手続きを含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
（略）				
ガス	・一般ガス導管事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】

別紙１　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野	対象となる重要インフラ事業者等（注１）	対象となる重要情報システム例（注２）
（略）		
政府・行政サービス	・地方公共団体	・地方公共団体の情報システム
（略）		
（新設）		

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

注２　（略）

別紙２　重要インフラサービスとサービス維持レベル

重要インフラ分野	重要インフラサービス（手続きを含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
（略）				
ガス	・一般ガス導管事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】

	・ガス製造事業	・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第２条第９項）		・システムの不具合により、供給支障戸数が100以上の供給支障事故が生じないこと
行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・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
（略）				
郵便	・郵便	・郵便（郵便法）		

注１・注２　（略）

別紙３～別紙４－２　（略）

	・ガス製造事業	・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第２条第９項）		・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・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
（略）				
（新設）				

注１・注２　（略）

別紙３～別紙４－２　（略）

別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における注 各関係主体の役割
○　内閣官房（国家危機管理室）	重要インフラに関連する事案の情報につき、国家サイバー統括室と相互に情報の共有を行う。	通常時の役割に加え、国家サイバー統括室と一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、国家サイバー統括室と相互に情報の共有を行う。
（略）		

注　（略）

別紙５　定義・用語集

（略）	
安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称。
（削る）	

別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における注 各関係主体の役割
○　内閣官房（事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、国家サイバー統括室と相互に情報の共有を行う。	通常時の役割に加え、国家サイバー統括室と一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、国家サイバー統括室と相互に情報の共有を行う。
（略）		

注　（略）

別紙５　定義・用語集

（略）	
安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称。ただし、安全基準等策定指針は含まない。
安全基準等策定指針	安全基準等の策定・改定に資することを目的として、サイバーセキュリティの確

			保において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。サイバーセキュリティ戦略本部決定による。
（略）		（略）	
重要インフラ	国民生活及び経済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又は経済活動に多大な影響を及ぼすおそれが生ずるもの。	重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済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又は経済活動に多大な影響を及ぼすおそれが生ずるもので、重要インフラ分野に属するもの。
（略）		（略）	
重要インフラ事業者	サイバーセキュリティ基本法第 3条第1項に規定する重要社会基盤事業者をいう。具体的には、重要インフラ分野に属する事業を行う者のうち、重要インフラ統一基準に基づき重要インフラ所管省庁において特定するもの（地方公共団体を除く）。	重要インフラ事業者	サイバーセキュリティ基本法第 3条第1項に規定する重要社会基盤事業者をいう。国民生活及び経済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又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者。具体的には、重要インフラ分野に属する事業を行う者のうち、「別紙１ 対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するも

（略）	
重要インフラ分野	重要インフラであって、他に代替することが著しく困難なサービスを提供する事業が形成するものについて、業種ごとに指定する分野。具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」、「港湾」及び「郵便」の16分野。
（略）	
情報システム	事務処理等を行うITを用いたシステム、フィールド機器や監視・制御システム等の制御系のシステム等を含むシステム全般。
（略）	

	の（地方公共団体を除く）。
（略）	
重要インフラ分野	重要インフラについて業種ごとに指定する分野であり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の15分野。
（略）	
情報システム	事務処理等を行うシステム、フィールド機器や監視・制御システム等の制御系のシステム等のITを用いたシステム全般。
（略）	