資料３

重要インフラ統一基準等の検討について

令和８年３月４日
内閣官房国家サイバー統括室

サイバー対処能力強化法及び同整備法の制定（全体イメージ）

- 国家安全保障戦略（令和4年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①官民連携の強化、②通信情報の利用、③攻撃者のサーバ等への侵入・無害化、④NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則
□ 目的規定、基本方針等（第１章）

官民連携（強化法）
□ 基幹インフラ事業者による
- 導入した一定の電子計算機の届出（第２章）
- インシデント報告

□ 情報共有・対策のための協議会の設置（第９章）
□ 脆弱性対応の強化（第42条）

〔その他、雑則（第11章）、罰則（第12章）〕

通信情報の利用（強化法）
□ 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
□ （同意によらない）通信情報の取得（第４章、第６章）
□ 自動的な方法による機械的情報の選別の実施（第22条、第35条）
□ 関係行政機関の分析への協力（第27条）
□ 取得した通信情報の取扱制限（第５章）
□ 独立機関による事前審査・継続的検査 等（第10章）

→ □ 分析情報・脆弱性情報の提供等 ←（第８章）

アクセス・無害化措置（整備法）
□ 重大な危害を防止するための警察による無害化措置
□ 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
□ 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
□ 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
□ **サイバーセキュリティ戦略本部の改組、機能強化**（サイバーセキュリティ基本法改正）
□ 内閣サイバー官の新設（内閣法改正）　等

重要インフラ統一基準の作成等

施行期日
公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

（参考）改正サイバーセキュリティ基本法（一部抜粋）

サイバーセキュリティ基本法（平成 26年法律第104号）

（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）
第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

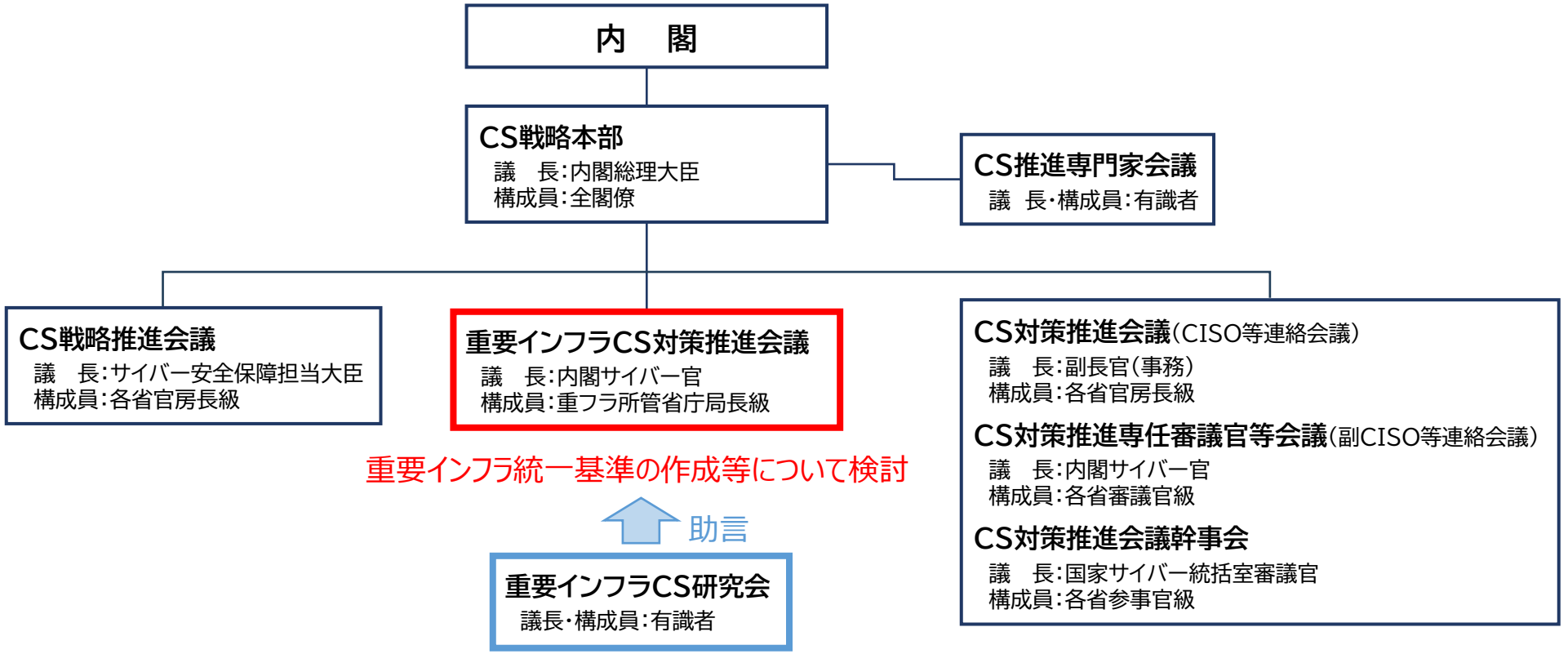
（所掌事務等）
第二十六条　本部は、次に掲げる事務をつかさどる。
三　重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュリティの確保の状況の調査を含む。）及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること

（資料の提出その他の協力）
第三十三条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長（略）に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該求めを受けた者は、正当な理由がある場合を除き、その求めに応じなければならない。
２　本部は、その所掌事務を遂行するため必要があると認めるときは、重要社会基盤事業者及びその組織する団体の代表者に対して、前項の協力を求めることができる。この場合において、当該求めを受けた者は、その求めに応じるよう努めるものとする。

※　令和８年10月(予定)にサイバー対処能力強化法が本格施行されることに伴い、基本法第十四条も改正され、国が行うべき施策として「重要な設備に係る電子計算機の被害の防止のための情報の整理及び分析を行う」ことが明記される予定。
　また、同施行により新たな官民連携の協議会が設置されることに伴い、サイバーセキュリティ基本法に基づくサイバーセキュリティ協議会は廃止される予定。

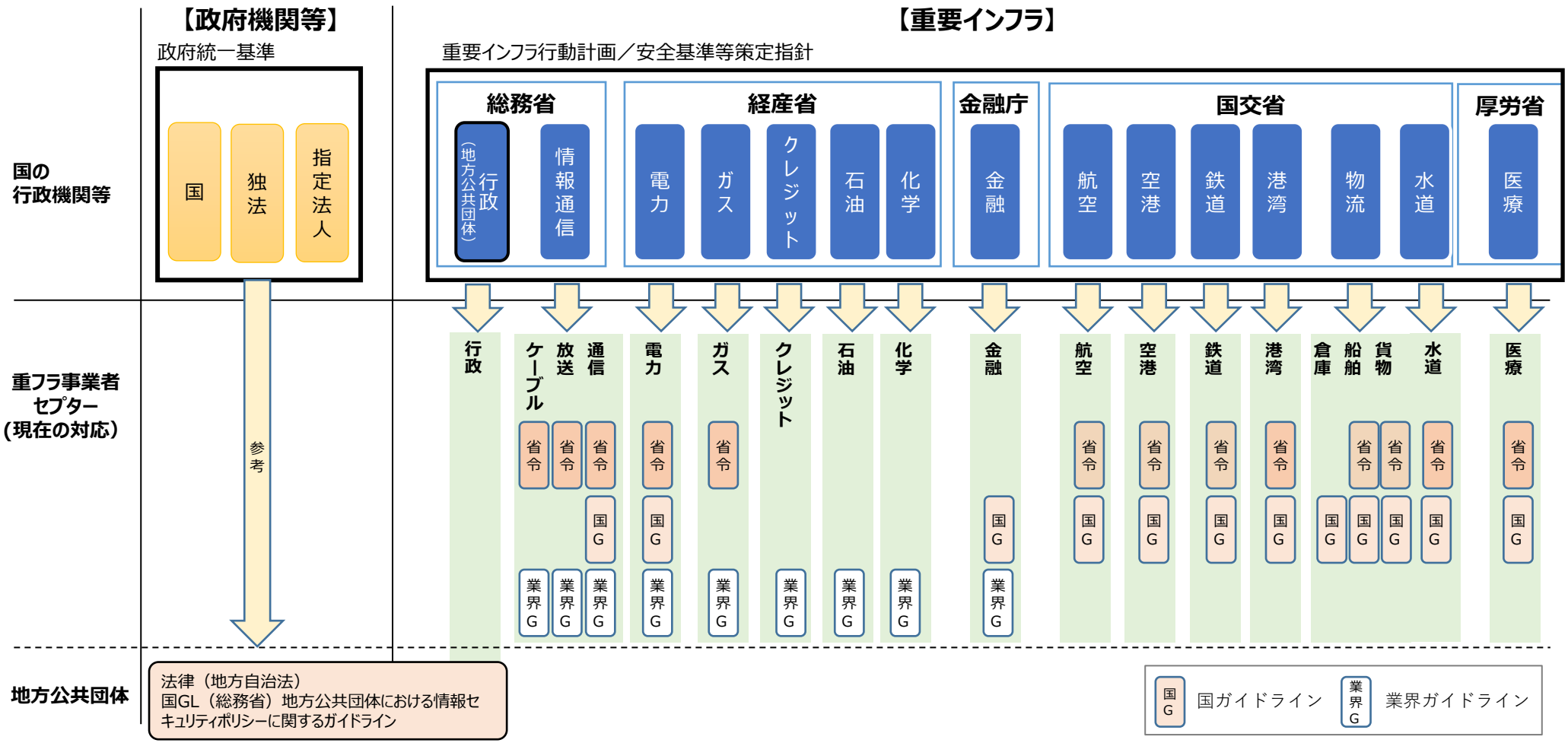
（参考）重要インフラ統一基準を検討するための関連会議

- サイバーセキュリティ（以下「CS」という。）基本法等の改正に伴いCS戦略本部の下に設置した**重要インフラCS対策推進会議**において、重要インフラ統一基準等の検討を実施（2025年8月～）。
- また、当該会議における検討に当たり、民間有識者の知見・示唆を得るため、内閣サイバー官の私的懇談会として、**重要インフラCS研究会**を開催（2025年11月～）。



現状課題①（分野・事業者によるばらつき）

- 各分野においては、行動計画を踏まえ、国・業界団体による基準やガイドラインが定められており、サイバーセキュリティ確保の取組が進められている。一方で、その**内容や水準については、分野・事業者によってばらつき**が見られる。
- 年々巧妙化・高度化の進むサイバー脅威に対応するためには、重要インフラ事業者等において**分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）の徹底**が求められる。



現状課題②（重要インフラ事業者の特定）

- 重要インフラ統一基準では、各分野の基準・ガイドラインへの反映、重要インフラ事業者等の取組への反映を進めるとともに、関係省庁における施策や重要インフラ事業者等の取組の評価・改善等を図る（PDCAサイクル）ことにより、サイバーセキュリティ強化の実効性を確保。
- この際、重要インフラ統一基準において、対象となる分野・事業者の特定が必要。

■ 行動計画における重要インフラ分野の特定等（現在）

➢ 重要インフラ分野は、行動計画の別紙で特定。

（例）

重要インフラ分野	対象となる重要インフラ事業者等	対象となる重要システム例
情報通信	・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
電力	・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
医療	・医療機関 （ただし、小規模なものを除く。）	・診療録等管理システム ・診療業務支援システム ・地域医療支援システム

➢ 具体の重要インフラ事業者（バイネーム）は、重要インフラ所管省庁において特定。

重要インフラ分野・事業者（バイネーム）ともに重要インフラ統一基準において特定する必要

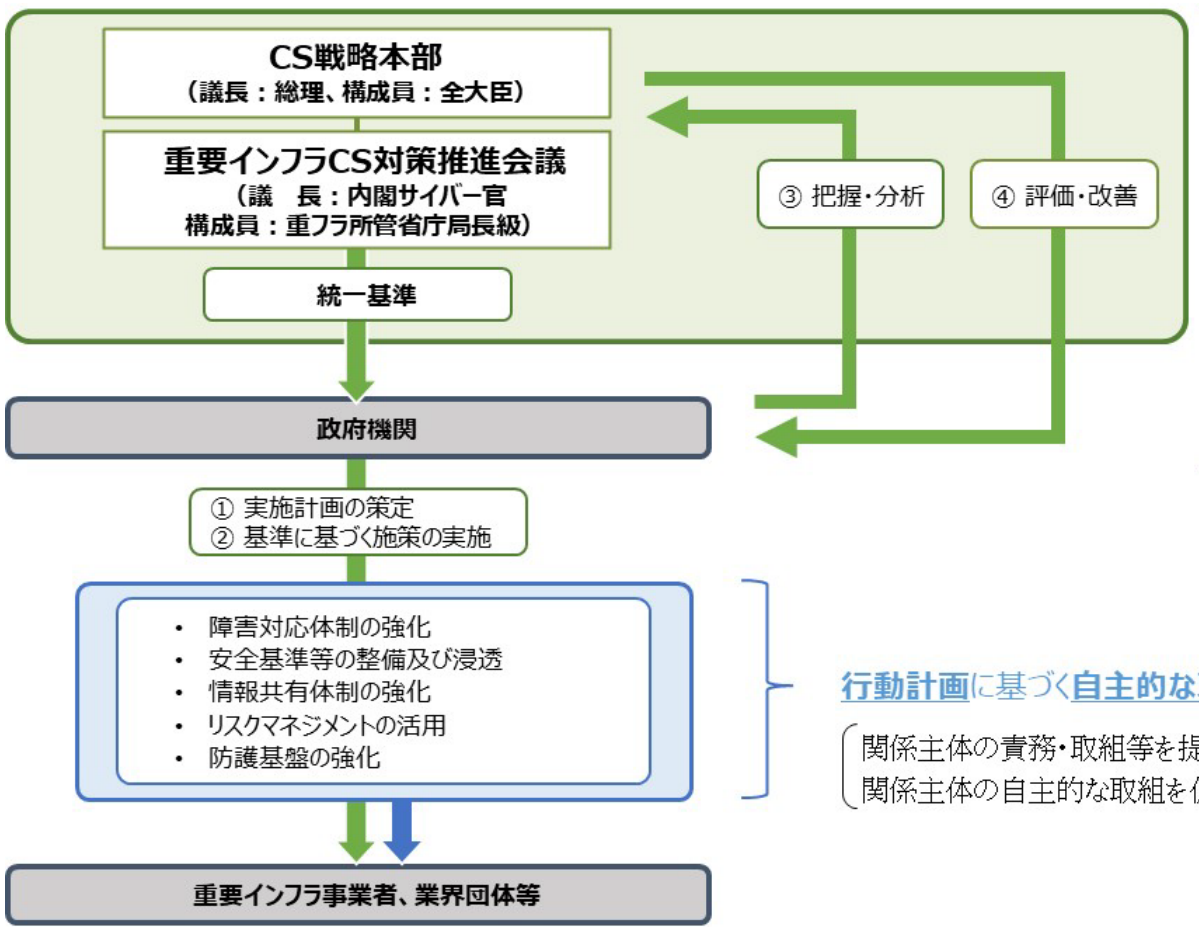
現状課題③（重要インフラと基幹インフラ）

- 重要インフラ事業者等と基幹インフラ事業者は、法律の趣旨の下に**対象範囲が定められており、それらの間には差異**がある。サイバーセキュリティ確保の観点から、例えば、現在、基幹インフラのうち重要インフラに含まれていない分野・事業者について、新たに重要インフラ分野・事業者として位置付ける等、**基幹インフラ事業者も含め、分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）の徹底を求めることが重要**。

重要インフラ		基幹インフラ	
電力	（一般送配電事業、発電事業）	電気	（一般送配電事業、送電事業、配電事業　等）
ガス	（一般ガス導管事業、ガス製造事業）	ガス	（一般ガス導管事業、特定ガス導管事業、ガス製造事業）
石油	（石油の供給）	石油	（石油精製業、石油ガス輸入業）
水道	（水道による水の供給）	水道	（簡易水道事業以外の水道事業、水道用水供給事業）
鉄道	（旅客輸送サービス、発券、入出場手続）	鉄道	（第一種鉄道事業）
物流	（貨物自動車運送事業、船舶運航事業、港湾運送事業、倉庫業）	貨物自動車運送	（一般貨物自動車運送事業）
		外航海運	（貨物定期航路事業、不定期航路事業）
港湾	（TOSによるターミナルオペレーション）	港湾運送	（一般港湾運送事業）
航空	（旅客、貨物の航空輸送サービス、予約、発券、搭乗・搭載手続、運航整備、飛行計画作成）	航空	（国内定期航空運送事業、国際航空運送事業）
空港	（空港におけるセキュリティの確保、空港における利便性の向上）	空港	（空港の設置及び管理を行う事業、空港に係る公共施設等運営事業）
情報通信	（電気通信役務、放送、ケーブルテレビ）	電気通信	（登録を要する電気通信事業、届出を要する電気通信事業）
		放送	（地上基幹放送）
—		郵便	（郵便事業）
金融	（銀行等、生命保険、損害保険　等）	金融	（銀行業、系統中央機関が行うもの、資金移動業　等）
クレジット	（クレジットサービス）	クレジットカード	（包括信用購入あっせんの業務を行う事業）
医療	（診療）	—	
化学	（石油化学工業）	—	
政府・行政サービス	（地方公共団体の行政サービス）	—	

重要インフラ統一基準

- CS戦略本部は、改正されたサイバーセキュリティ基本法第26条第１項第３号の規定に基づき、重要インフラ事業者等におけるサイバーセキュリティ確保に関する政府機関の施策の基準として、「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」（重要インフラ統一基準）の作成や、当該基準に基づく施策の評価を実施。
- これにより、政府機関として、重要インフラのサイバーセキュリティ強化のため、より積極的な役割を果たし、深刻化の進むサイバー脅威に対する重要インフラの一層の防護を図る。



統一基準を通じた**政府機関における施策のPDCAサイクル**

政府機関の施策のPDCAサイクルにより重要インフラのサイバーセキュリティ強化の実効性を確保。

行動計画に基づく**自主的な取組の促進**

関係主体の責務・取組等を提示し、重要インフラにおける関係主体の自主的な取組を促進

重要インフラ統一基準（概要）

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

第１部　総則

- 目的・適用範囲
- 統一基準に基づく施策の改善（本スキームの概要）

第２部　政府機関における施策

- 実施計画の策定
- 把握・分析
- 評価・改善

第３部　安全基準等において規定されるべき事項

- 基本的な考え方
- 組織統治
- 識別
- 防御
- 検知
- 対応及び復旧
- 技術・脅威の動向等を踏まえた対策

政府機関における施策

- 取り組むべき施策は、重要インフラ行動計画の考え方と整合性を確保し、PDCAサイクルにより各分野の施策へ反映

取り組むべき施策

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

- 実施計画の策定において対象となる重要インフラ事業者を特定

事業者において分野・事業者横断的に講ずべき対策

- 現行の安全基準等策定指針をベースとしつつ、国際標準や諸外国の取組（NIST CSF2.0等）、既存の安全基準等を踏まえ再構成・更新
  ⇒ 各分野の安全基準等へ反映

重要インフラ統一基準と行動計画との関係

重要インフラ統一基準

■概要
- PDCAサイクルの実施により重要インフラのサイバーセキュリティ強化の実効性を確保。

■主な対象
- 政府機関

※ 安全基準等を通じて重要インフラ事業者等

■主な内容
- 政府機関における施策
  - 実施計画の策定
    - 施策の実施体制
    - 取り組むべき施策
  - 把握・分析
  - 評価・改善
- 安全基準等において規定されるべき事項

考え方について整合

重要インフラ行動計画

■概要
- 関係主体の責務・取組や目指すべき将来像を提示し、自主的かつ積極的な取組を促進。

■主な対象
- 政府、重要インフラ事業者等、セプター事務局、サイバーセキュリティ関係機関、サイバー空間関連事業者等

■主な内容
- 計画期間内の取組
- 関係主体において取り組むべき事項

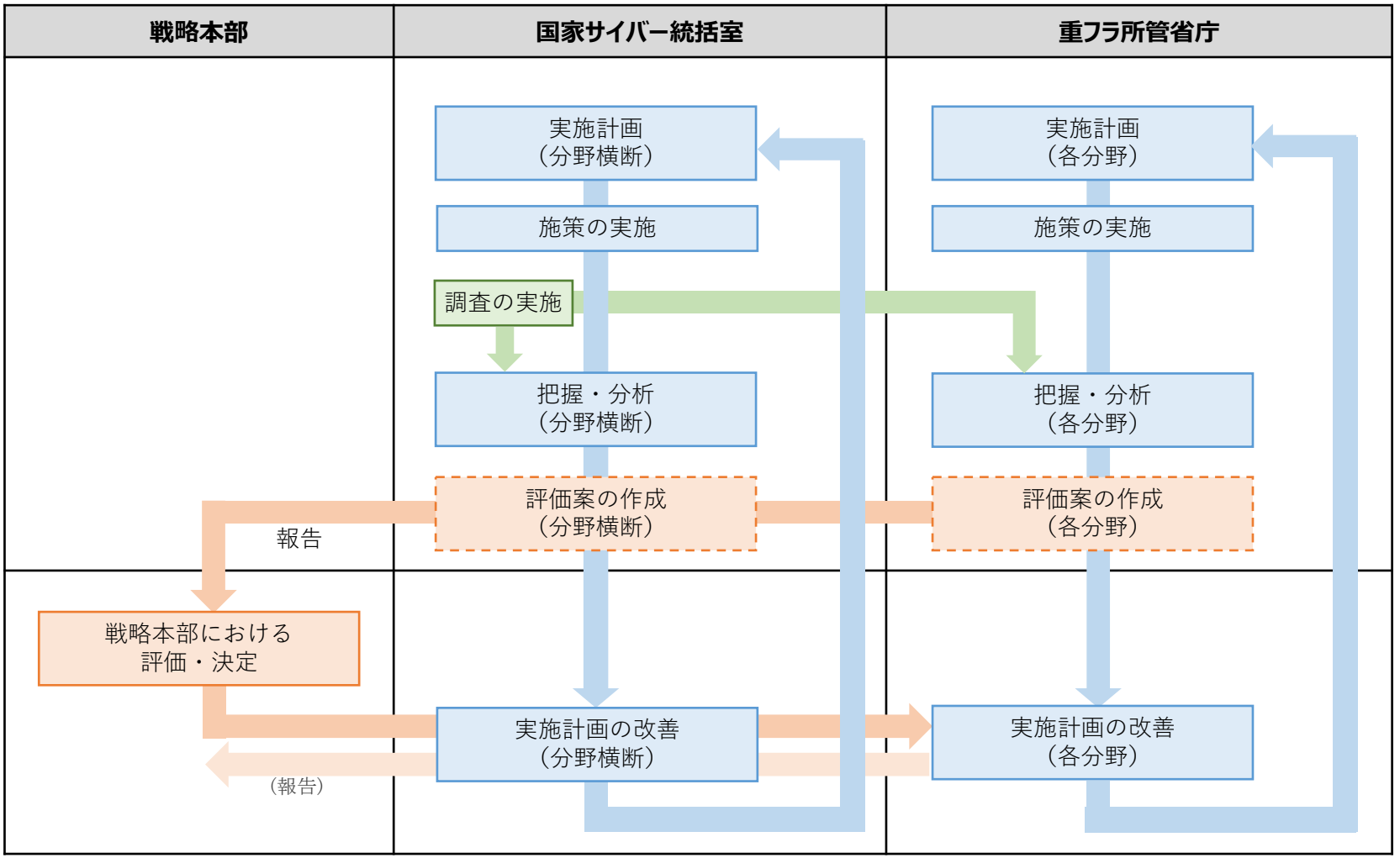
相補的な関係

重要インフラ分野全体の水準の引上げ

重要インフラにおける関係主体の自主的な取組の促進

深刻化するサイバー脅威に対し、重要インフラにおけるサイバーセキュリティの一層の確保

（参考）重要インフラ統一基準におけるPDCAサイクル



重要インフラと基幹インフラ（重要インフラ防護範囲の見直し）

	サイバーセキュリティ確保	経済安全保障
重要インフラ	**サイバーセキュリティ基本法** （目的・責務：サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める） 事業者に求められる取組： ✓ 官民連携のもと、自主的かつ積極的なサイバーセキュリティの確保	
基幹インフラ	**サイバー対処能力強化法** （目的・責務：特別社会基盤事業者による特定侵害事象等の報告の制度（省略）について定めることにより、重要電子計算機に対する不正な行為による被害の防止を図る） 事業者に求められる取組： ✓ 資産届出（義務） ✓ インシデント報告（義務） 等	**経済安全保障推進法** （目的・責務：サービスの安定的な提供を確保するため、指定を受けた事業者が主務省令で定められた設備の導入及び維持管理等の委託を行う場合には、事前にその計画を届け出るとともに、審査を受けなければならない） 事業者に求められる取組： ✓ 特定重要設備の届出（リスク管理措置） 等

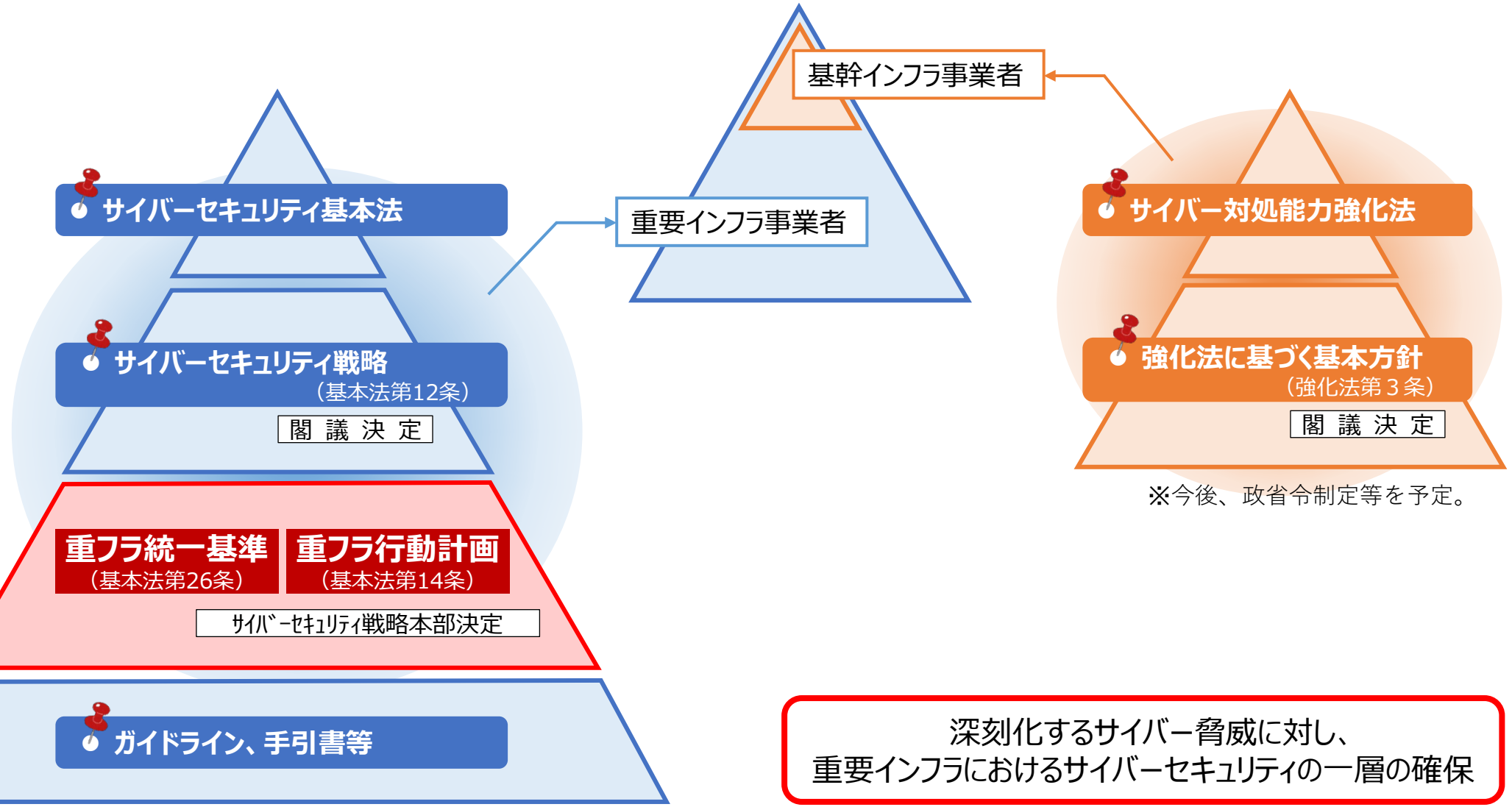
基幹インフラにおけるサイバーセキュリティ確保の重要性の高まりから新たに制定

基幹インフラ事業者における届出やインシデント報告等の対応に当たって前提となるサイバーセキュリティ対策を含め、分野・事業者横断的に講ずべき基本的な対策を徹底しサイバーセキュリティを確保
（経済安全保障推進法との整合性にも留意）

（参考）重要インフラ事業者と基幹インフラ事業者

	重要インフラ事業者 （重要社会基盤事業者）	基幹インフラ事業者 （特定社会基盤事業者）
対象 事業者	➢ 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もの（サイバーセキュリティ基本法第３条） ➢ 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あることを認識できるようにする。（重要インフラのサイバーセキュリティに係る行動計画）	➢ 主務大臣は、特定社会基盤事業を行う者のうち、その使用する特定重要設備の**機能が停止し、又は低下した場合に、その提供する特定社会基盤役務の安定的な提供に支障が生じ、これによって国家及び国民の安全を損なう事態を生ずるおそれが大きいもの**として主務省令で定める基準に該当する者を特定社会基盤事業者として指定することができる。（経済安全保障推進法第50条）
対象 分野等	➢ 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、港湾の15分野（重要インフラのサイバーセキュリティに係る行動計画）	➢ 特定社会基盤役務の提供を行うものとして政令で定めるもの（経済安全保障推進法第50条） ➢ 電気、ガス、石油、水道、鉄道、貨物自動車運送、外航海運、港湾運送、航空、空港、電気通信、放送、郵便、金融、クレジットカードの15事業分野
目的・ 責務等	➢ 基本理念にのっとり、**そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。（サイバーセキュリティ基本法第６条）	➢ その**安定的な提供を確保するため、指定を受けた事業者が主務省令で定められた設備の導入及び維持管理等の委託を行う場合には、事前にその計画を届け出るとともに、審査を受けなければならない**こととしている。（基本指針） ➢ 特別社会基盤事業者による特定侵害事象等の報告の制度（省略）について定めることにより、**重要電子計算機に対する不正な行為による被害の防止を図る**ことを目的とする。（サイバー対処能力強化法第１条）

重要インフラ防護及び基幹インフラ防護に関する制度体系



※今後、政省令制定等を予定。

深刻化するサイバー脅威に対し、
重要インフラにおけるサイバーセキュリティの一層の確保

（参考）分野別情報共有体制の現状

［2025年9月末日現在］

重要インフラ分野	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	港湾
事業の範囲	電気通信	放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油	港湾
名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会				航空 CEPTOAR	空港 CEPTOAR	鉄道 CEPTOAR	電力 CEPTOAR	GAS CEPTOAR	自治体 CEPTOAR	医療 CEPTOAR	水道 CEPTOAR	物流 CEPTOAR	化学 CEPTOAR	クレジット CEPTOAR	石油 CEPTOAR	港湾 CEPTOAR
				銀行等 CEPTOAR	証券 CEPTOAR	生命保険 CEPTOAR	損害保険 CEPTOAR	資金決済 CEPTOAR												
事務局	(一社) ICT-ISAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟 日本放送協会	(一社) 全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社) 生命保険協会 総務部	(一社) 日本損害保険協会 IT企画部	(一社) 日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社) 日本鉄道電気技術協会	電力 ISAC	(一社) 日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社) 日本医師会 情報システム課	(公社) 日本水道協会 総務部 総務課	(一社) 日本物流団体連合会	石油化学工業協会	(一社) 日本クレジット協会	石油連盟	(一社) 日本港運協会
構成員 (のべ数)	28社 1団体	299社 1団体	194社 2団体	1,216社	270社 7機関	41社	49社	188社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	5団体 15社	12社	48社	10社	30社 9団体 7地方公共団体
構成員以外の情報展開先	395社・団体	335社	13社	6社・団体	9社 1機関	–	10社	4社	–	–	–	27社・機関	194社・団体	–	376社・団体	内容に応じ1,198事業体へ展開	–	–	–	–	–

既存事業領域を越える連携等	情報通信（ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟）、金融（金融ISACにおいて、加盟金融機関間で情報共有・活動連携）、航空・空港・鉄道・物流（交通ISACにおいて、参加事業者間で情報共有・活動連携）、電力（電力ISACにおいて、加入する電気事業者間で情報共有・活動連携）、化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者と情報共有・活動連携）、J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報CISTA（JPCERT/CC: セキュリティ情報全般）

（参考）重要インフラのサイバーセキュリティに係る行動計画

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

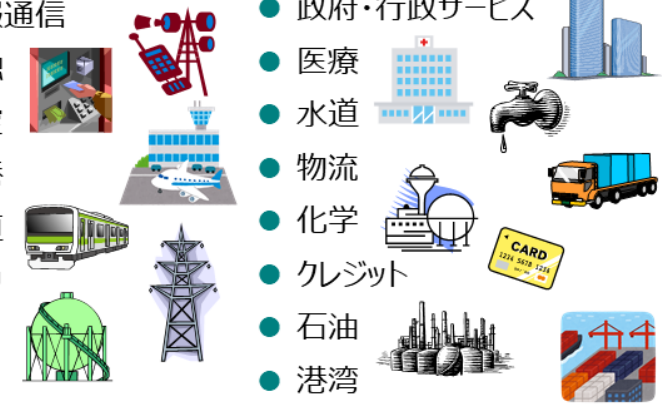
NISCによる総合調整

重要インフラ所管省庁

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

重要インフラ(全１５分野)

- 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
- 港湾



関係機関等

- サイバーセキュリティ関係省庁
  [総務省、経済産業省等]
- 事案対処省庁
  [警察庁、防衛省等]
- 防災関係府省庁
  [内閣府、各省庁等]
- サイバーセキュリティ関係機関
  [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者
  [サプライチェーン等に関わるベンダー等]

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

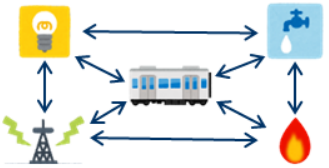
安全基準等の整備及び浸透

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

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ