

重要インフラ統一基準（案）の概要

（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）

令和 8 年 7 月 31 日
内閣官房 国家サイバー統括室（NCO）

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）

1

- 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

サイバーセキュリティ基本法 (平成26年法律第104号) ※令和8年10月施行予定

(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)

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、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とともに、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)

第二十五条 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。

3 本部は、次に掲げる場合には、あらかじめ、サイバーセキュリティ推進専門家会議の意見を聴かなければならない。

二 第一項第二号又は第三号の基準を作成しようとするとき。

三 第一項第二号又は第三号の評価について、その結果の取りまとめを行おうとするとき。

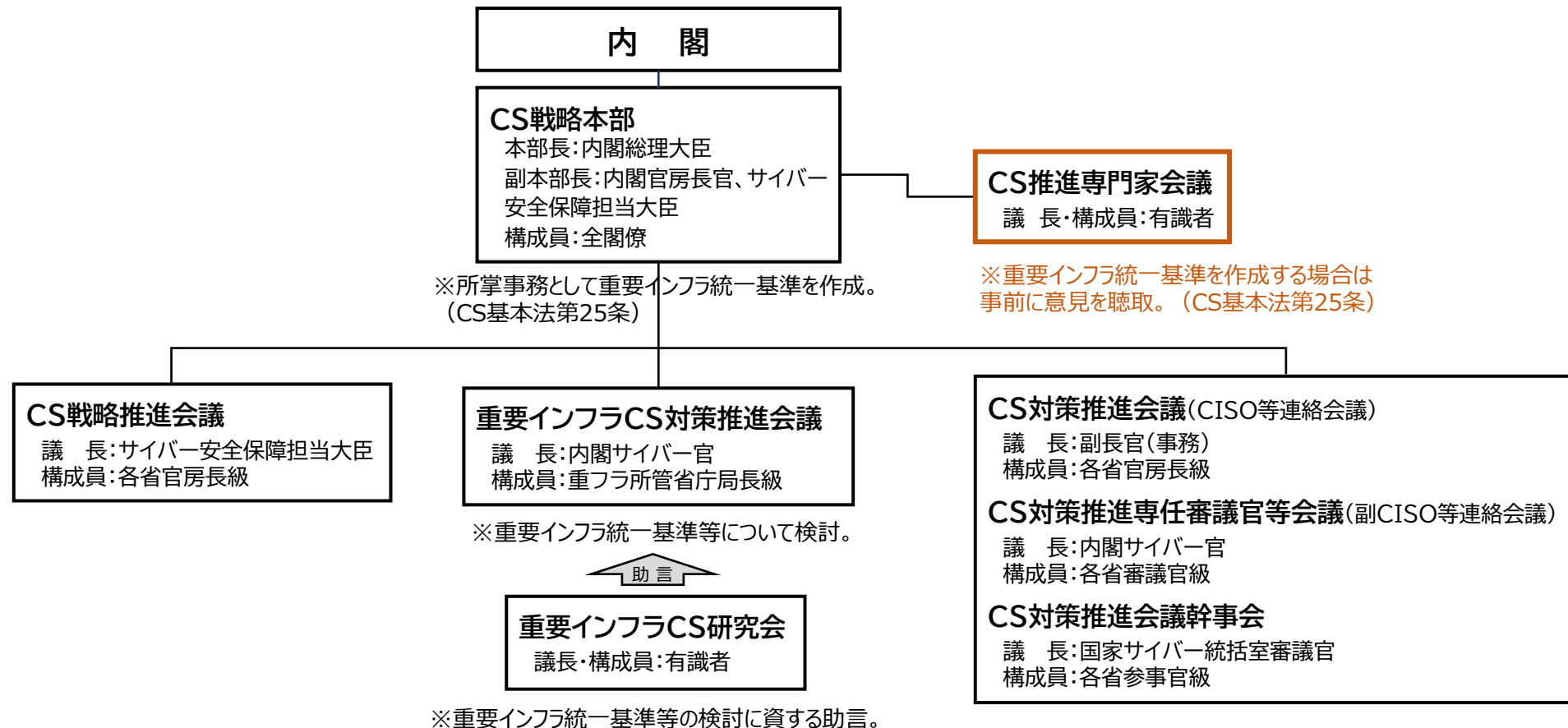
(資料の提出その他の協力)

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、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。

- 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～）。
- 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～）。
- また、CS戦略本部は、重要インフラ統一基準を作成する場合には、あらかじめCS推進専門家会議の意見を聴くこととされている。



- | | 【政府機関等】 | 【重要インフラ】 |
|---------------------|---|---|
| 国の行政機関等 | <p>政府統一基準</p> <div> <div>国</div> <div>独法</div> <div>指定法人</div> </div> | <p>重要インフラ行動計画／安全基準等策定指針</p> <div> <div>総務省</div> <div>経産省</div> <div>金融庁</div> <div>国交省</div> <div>厚労省</div> </div> |
| 重インフラ事業者セクター（現在の対応） | <p>参考</p> | <div> <div>行政</div> <div>ケーブル放送通信</div> <div>電力</div> <div>ガス</div> <div>クレジット</div> <div>石油</div> <div>化学</div> <div>金融</div> <div>航空</div> <div>空港</div> <div>鉄道</div> <div>港湾</div> <div>倉庫船舶貨物</div> <div>水道</div> <div>医療</div> </div> |
| 地方公共団体 | <p>法律（地方自治法）
国GL（総務省）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</p> | <div> <div>国G</div> <div>国ガイドライン</div> <div>業界G</div> <div>業界ガイドライン</div> </div> |

- 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

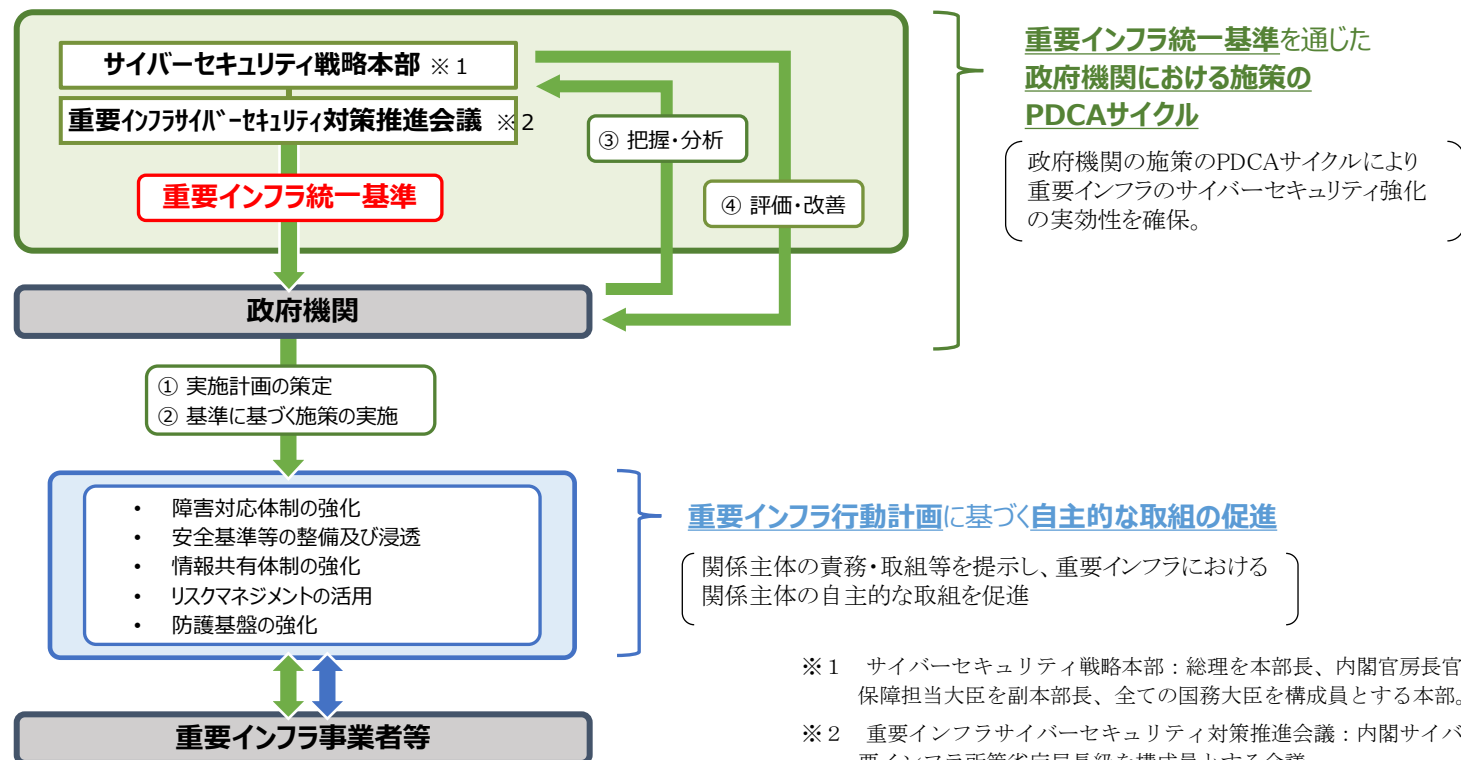
- 重要インフラ事業者等と基幹インフラ事業者は、法律の趣旨の下に**対象範囲が定められており、それらの間には差異**がある。サイバーセキュリティ確保の観点から、例えば、現在、基幹インフラのうち重要インフラに含まれていない分野・事業者について、新たに重要インフラ分野・事業者として位置付ける等、**基幹インフラ事業者も含め、分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）の徹底を求めることが重要。**

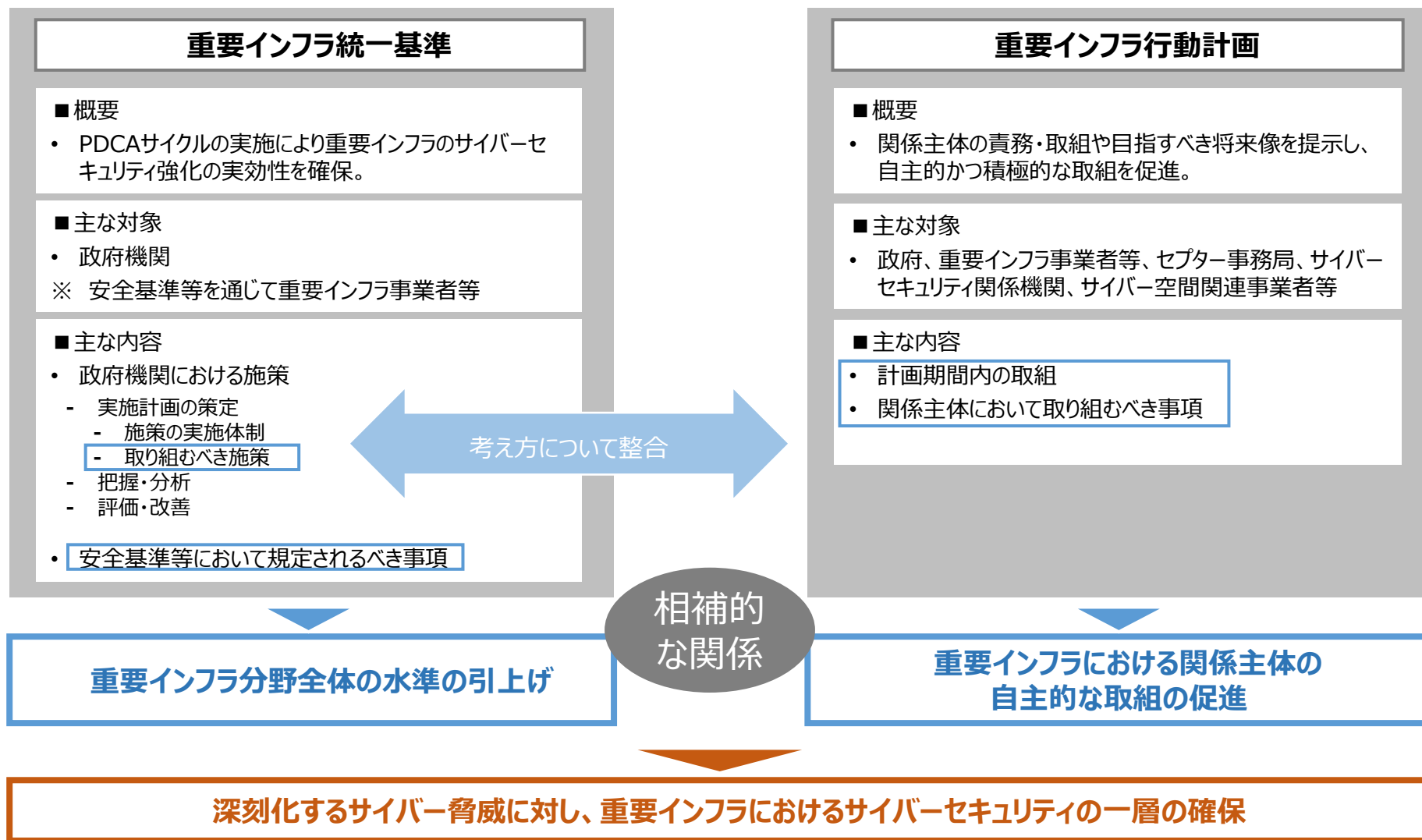
重要インフラ	基幹インフラ
電力 (一般送配電事業、発電事業)	電気 (一般送配電事業、送電事業、配電事業 等)
ガス (一般ガス導管事業、ガス製造事業)	ガス (一般ガス導管事業、特定ガス導管事業、ガス製造事業)
石油 (石油の供給)	石油 (石油精製業、石油ガス輸入業)
水道 (水道による水の供給)	水道 (簡易水道事業以外の水道事業、水道用水供給事業)
鉄道 (旅客輸送サービス、発券、入出場手続)	鉄道 (第一種鉄道事業)
物流 (貨物自動車運送事業、船舶運航事業、倉庫業)	貨物自動車運送 (一般貨物自動車運送事業)
	外航海運 (貨物定期航路事業、不定期航路事業)
港湾 (TOSによる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 (銀行等、生命保険、損害保険 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)	医療 (注) 令和8年6月17日、医療分野を追加する改正法が公布。公布日から起算して1年6月を超えない範囲内において政令で定める日から施行。
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)	—

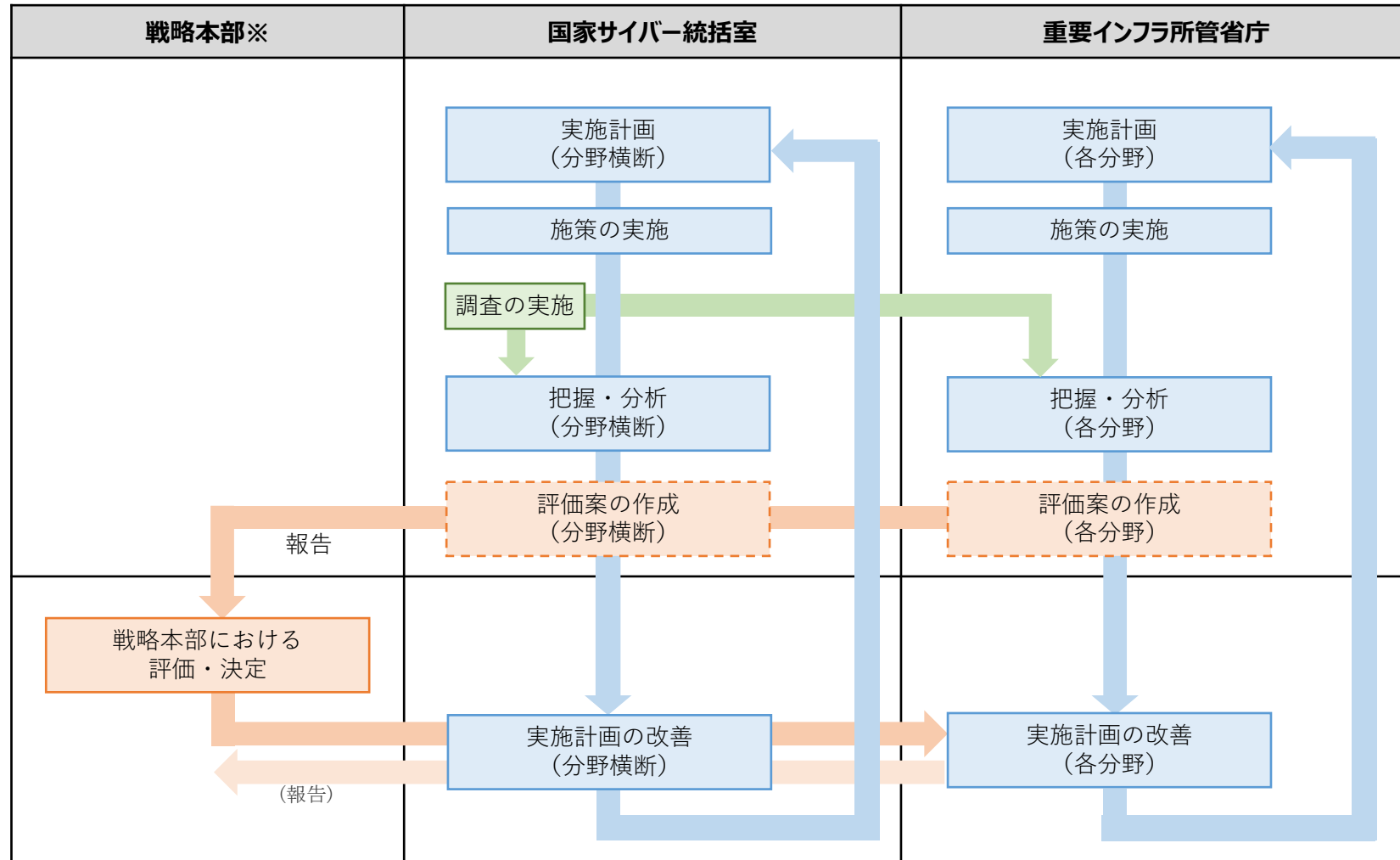
- 現在、サイバーセキュリティ対策の水準は、分野・事業者によってばらつきが見られる。
- 国家を背景とした攻撃キャンペーンの発生等、深刻化するサイバー脅威へ対応するためには、分野・事業者横断的なセキュリティ対策水準の底上げと、各分野におけるリスクベースの取組の更なる水準の向上が必要。

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基本的な対策の徹底を図るため、

- サイバーセキュリティ戦略本部にて、政府機関が取り組むべき施策についての**統一基準を新たに作成**（2026年10月施行予定）。
- 政府機関にて、特性や実情を踏まえ、各分野の施策を推進するための**実施計画を策定**（2027年夏を目処）し、
- 施策の実施を通して、各分野の**重要インフラ事業者等におけるセキュリティ対策に反映**。
- サイバーセキュリティ戦略本部による**評価等を通じて実施計画を改善**し、実効性を確保。







P

D

C

A

- 第2部では、政府機関が取り組むべき施策やその実効性の確保（PDCAサイクル、分野・事業者の特定等）について記載。
- 第3部では、各分野の安全基準等（省令・ガイドライン等）において、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として規定されるべき事項を記載。

重要インフラ統一基準

（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

- 統一基準の目的等
- 統一基準の適用範囲
- 統一基準に基づく施策の改善
- 統一基準の構成等
- 統一基準の改定

第2部 政府機関における施策の基準

- 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

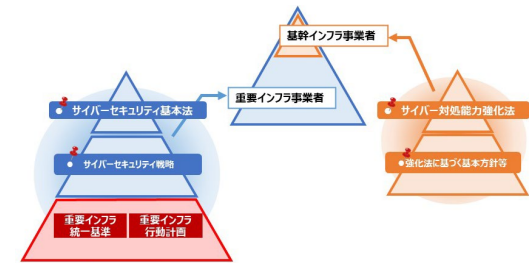
※1 第3部については、所管省庁等が安全基準等の策定に当たって参照するための「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」（今夏策定予定）に詳細事項を記載予定。

※2 「技術・脅威の動向等を踏まえた対策」の具体的な内容は、専ら安全基準等策定ガイドラインに記載予定。

重要インフラ統一基準の適用範囲（重要インフラ防護範囲の見直し）

○ 基幹インフラ事業者を含め関係事業者において基本的な対策を徹底

- 基幹インフラの対象範囲については、原則、重要インフラの防護範囲に含める。これにより、関係事業者におけるより効果的な取組を促し※、重要インフラのサイバーセキュリティを強化。
※ サイバー対処能力強化法等における届出やインシデント報告に当たって前提となる対策を含め、分野・事業者横断的に講ずべき基本的な対策を徹底。
- 実施計画において対象となる事業者等を特定。



重要インフラ統一基準を通じて取り組むべき主な対策（例）

① 「閉域網だから安全」との考え方の刷新

従来、事業者によっては閉域網という理由でサイバー攻撃を想定していなかった基盤・制御システムも、システム更改による環境変化や攻撃手法の変化によって、リスクは高まっている。閉域網だから安全とは限らないとの認識の下、基盤・制御システムのセキュリティ対策を徹底することが重要。

② サプライチェーン・リスクへの対応

デジタル化の進展に伴い、自組織へのサイバー攻撃がサプライチェーン全体に影響を及ぼすリスクや、委託先等へのサイバー攻撃が自組織に影響を及ぼすリスクが高まっている。組織の壁を越えた対策が重要。

③ ランサムウェア攻撃等の被害を低減するためのレジリエンス向上

日々、巧妙化・高度化の進むサイバー攻撃から完全に防御することは困難。誰しもサイバー攻撃を受ける可能性があることを前提に、障害等による影響をいかに低減し、事業継続させるか等、レジリエンスの向上が重要。

④ 技術・脅威の動向等を踏まえた対策

例えば、生成AIを始めAI技術の進展による恩恵の一方で、AIを活用した攻撃の自動化やAIに対する攻撃等、新たなサイバーセキュリティ上のリスクが生じている。こうした技術革新等への適時的確な対応が重要。※2

⑤ 官民双方向でのコミュニケーションの強化

国家を背景とした攻撃キャンペーン等、深刻化するサイバー脅威に対しては、官のみ、民のみの防御では限界がある。サイバー攻撃による被害拡大防止に向けた官民双方向でのコミュニケーションの強化が重要。

- 基幹インフラの対象範囲については、原則、重要インフラの防護範囲に含める。
- これにより、サイバー対処能力強化法等に基づく基幹インフラ事業者の届出やインシデント報告に当たって前提となる対策を含め、関係事業者において分野・事業者横断的に講ずべき基本的な対策を徹底し、重要インフラのサイバーセキュリティを強化。
- 重要インフラのサイバーセキュリティ水準の継続的な向上を図るため、実施計画において対象となる重要インフラ事業者等を特定。

